time2act



www.time2act.info
read2act@proton.me

© 2026 Kimèric · Creative Commons BY-NC-ND 4.0 (Reconocimiento-NoComercial-SinObraDerivada).

¿Quién es Kimèric?

En el silencio de una página que se regala a todo aquel que tenga la inquietud de leerla, la voz de *time2act* es un intento de sacudir la psique del mundo que nos ha tocado vivir.

Puedo estar presente dentro de cada línea y, a la vez, ausente de la portada. Esta reserva no es un juego de misterio, sino la condición misma del proyecto: en un libro que trata de creer las cosas por cómo son y no por quién te las cuenta, el autor elige no demostrar nada de sí mismo. El argumento debe sostenerse solo, como una estructura que resuena independientemente de quién la sostenga.

La confianza que pide este libro no recae en la firma, sino en aquello que se puede verificar. Cada afirmación va acompañada de sus fuentes; cada capítulo invita al lector a comprobar, no a creer. Quien lee está invitado a juzgar el texto con sus propios criterios, como un científico que examina la muestra sin saber quién la ha depositado.

El silencio alrededor del nombre es parte del pacto: no se busca notoriedad, sino un empuje colectivo hacia la verdad compartida. Si lo que está escrito es cierto, lo es diga quien lo diga. Y si no lo fuera, ninguna firma lo salvaría.

Y, por ser didáctico con aquello que os mostraremos en esta obra, el autor se podrá demostrar cuando él lo decida: la edición inicial, con su nombre real, ha sido certificada a perpetuidad en la blockchain en esta transacción.

SHA-512: 4b3d04d648aca3f72568bb68932a30ff6d284a33ab4c712a1c4a97fd5294f0f4 8608eb671c84a0d1ddd6c6f61f6c77d5b6e0a71f85ecf0f7aff6ac1d68aa6e9c

Transacción (Polygon): 9e004bbd87383b30867fdd5d6c9100c859a9da014c43d5d982a6d83d34239108

https://polygonscan.com/tx/0x9e004bbd87383b30867fdd5d6c9100c859a9da014c43d5d982a6d83d34239108

17 de julio de 2026

Si en algún momento el autor quisiera desvelar su identidad, le bastaría con mostrar el contenido del archivo que da exactamente el mismo hash que se ha certificado en la blockchain, para que cualquier persona del mundo —incluidos los peritos informáticos— tenga la certeza de la integridad del dato.

Todos los derechos de esta obra quedan reservados en la misma certificación blockchain, que fija su contenido y su fecha de manera inalterable. Hecha esta reserva, la obra es libre: cualquier tercero puede utilizarla, citarla o difundirla siempre que nombre la fuente, time2act.info. Y si alguien no lo hace y pretende apropiarse de la obra, total o parcialmente, tarde o temprano la blockchain demostrará qué se escribió, y cuándo; y eso bastará para desenmascararlo.

Aprender y aplicar esta sencilla pero poderosa combinación es lo que nos permitirá combatir las mentiras en el entorno digital que condiciona los designios del mundo que nos ha tocado vivir.

Índice

- Prólogo — De 2004 a 2026: el día que tocamos el límite

Parte I — El lenguaje de la confianza

- 1. El protocolo de la confianza: cómo se prueba que algo es cierto

Parte II — La máquina energética, revisitada

- 2. Encender el fuego, revisitado
- 3. El último petróleo fácil… y por qué ya importa menos
- 4. El futuro ya está aquí: renovables, baterías y vehículo eléctrico
- 5. La energía es poder
- 6. Demasiado caliente: el clima en 2026

Parte III — Las consecuencias, hoy

- 7. Dar a la gente lo que quiere: consumo, eficiencia y «menos es más»
- 8. Las grandes energéticas, ansiosas
- 9. La nueva tensión: la IA como salvación y como sed de energía
- 10. La crisis de la verdad: desinformación y deepfakes

Parte IV — Las soluciones: IA y la capa de confianza

- 11. Seguridad energética reinventada: redes inteligentes e IA
- 12. La mano (ya no tan) invisible: blockchain como capa de confianza
- 13. t2p: la prueba de existencia contra las deepfakes
- 14. Hidrógeno, captura y las apuestas que faltan

Parte V — Cinco frentes contra las deepfakes

- 15. Detectar no es suficiente: la prueba de existencia como defensa duradera
- 16. Dinero y confianza: fraude, compliance y finanzas
- 17. La imagen como testimonio: fotoperiodismo y medios
- 18. Vida o muerte de los datos: salud e imagen médica
- 19. Credenciales y autoría: educación e investigación
- 20. La verdad como arma: defensa y derechos humanos

Parte VI — La confianza al servicio del clima: créditos, certificados y movilidad

- 21. Créditos de carbono: el mercado del cumplimiento
- 22. El mercado voluntario del carbono: promesa, fraude y la carrera por la integridad
- 23. CAE: certificar el ahorro sin hacer trampa
- 24. Autoconsumo y comunidades energéticas: la lectura verificable
- 25. Movilidad I: flotas y empresas, evidencia sólida
- 26. Movilidad II: coche compartido y particulares, repartir la confianza
- 27. Retrasos de transporte: probar la hora de llegada

Parte VII — La prueba de existencia en la economía real: activos, bienes, ideas e instituciones

- 28. Seguros: la prueba del siniestro
- 29. Cadena de suministro: el origen verificable contra la falsificación
- 30. Consumo: reseñas falsas, precios inflados y garantías con reloj
- 31. La segunda mano entre particulares: el estado del artículo, con fecha cierta
- 32. El alquiler de cosas: el estado al recoger y al devolver
- 33. El cliente contra la compañía: la baja, la permanencia y el call center
- 34. La factura y la morosidad: el reloj del cobro
- 35. Inmobiliario: el estado de la propiedad y el registro de la tierra
- 36. Alquiler y vivienda: el estado de las cosas, con fecha cierta
- 37. La comunidad de propietarios: actas, derramas y acuerdos con fecha cierta
- 38. Reformas en casa: el anticipo, la obra y la prueba

- 39. Activos del mundo real: tokenizar con pruebas, no a ciegas
- 40. Autoría creativa: probar quién lo hizo primero en la era de la IA
- 41. Patentes y prior art: la publicación defensiva con fecha cierta
- 42. Secretos empresariales: probar sin revelar
- 43. Govtech: contratación pública y registros a prueba de manipulación
- 44. El ciudadano ante la Administración: el reloj del silencio
- 45. El azar verificable: sorteos que nadie puede cargar
- 46. Oposiciones y exámenes: la prueba sellada antes

Parte VIII — Confianza para la sociedad: personas, instituciones, mercados y cultura

- 47. Identidad digital: la prueba de que existes
- 48. Integridad electoral: probar qué pasó en las urnas
- 49. Ayuda humanitaria: probar que la ayuda llega
- 50. La ayuda en especie: la cadena de custodia del socorro
- 51. Fronteras y asilo: la evidencia de quien huye
- 52. Testamentos y herencia: la última voluntad, demostrable
- 53. Derecho de familia: la coparentalidad con fecha cierta
- 54. Trade finance: el mismo cargamento financiado dos veces
- 55. Auditoría: cuentas e informes a prueba de manipulación
- 56. Fraude publicitario: el anuncio que nadie vio
- 57. Ciberseguridad: registros que el atacante no puede reescribir
- 58. Tus datos filtrados: la reclamación del ciudadano
- 59. La caída documentada: SLA, nube y continuidad
- 60. Arte y antigüedades: la procedencia contra la falsificación y el expolio
- 61. Memoria histórica: los archivos contra el negacionismo
- 62. Whistleblowing: probar sin delatarse

Parte IX — Confianza en las nuevas fronteras: ciencia, cuerpo, máquinas y mercados

- 63. Integridad de la investigación: el dato que nadie puede repetir
- 64. Pensiones: probar que aún estás aquí, hoy
- 65. Prueba de vida: secuestros virtuales, desaparecidos y la voz que no era
- 66. Integridad deportiva: la muestra que alguien cambió de noche
- 67. Música y espectáculos: el humano real detrás del play
- 68. Telecomunicaciones y voz: autenticar a quien llama de verdad
- 69. El fraude bancario del pago «autorizado»
- 70. Hardware: el pedigrí de un chip que no podía fallar
- 71. Software: el pedigrí del código que lo hace funcionar todo
- 72. Pesca y minerales: el origen que se hundió con el barco
- 73. Filantropía: adónde va mi euro
- 74. Cajas negras: el dato que el fabricante decía que no existía
- 75. La caja negra personal: evidencia preventiva para víctimas y para inocentes
- 76. Datos genómicos: el consentimiento de uno expone a muchos
- 77. Justicia penal: la prueba que el tribunal tiene que poder creer
- 78. Historiales médicos: quién tocó el registro, y cuándo

Parte X — Cuando todo se puede falsificar: identidad, imagen, voz y dinero

- 79. Modelos de IA: con qué se entrenaron, y qué ejecutamos realmente
- 80. Los agentes de IA: el mandato verificable
- 81. Tu cara, tu voz: derechos de imagen y réplicas digitales
- 82. Sharenting: la imagen de quien no puede consentir
- 83. Imágenes íntimas no consentidas: el daño, la prueba y la retirada
- 84. El odio en las redes: el daño, la prueba y la dignidad
- 85. Personas mayores: la voz clonada y el abuso invisible
- 86. Comunicaciones oficiales: ¿quién certifica que el jefe de Estado ha dicho esto?
- 87. Suplantar al director financiero: ¿quién ha autorizado de verdad este pago?
- 88. La identidad en directo: ¿quién hay de verdad al otro lado de la pantalla?
- 89. Información que mueve mercados: quién lo ha dicho, y cuándo lo dijo
- 90. Titularidad real: quién es la persona de carne y hueso detrás de la empresa
- 91. Identidad laboral: a quién contratamos de verdad en remoto

- 92. Trabajo de plataforma: cuando el jefe es un algoritmo
- 93. La jornada y el conflicto laboral: horas que constan

Parte XI — El mundo físico no miente: infraestructura, producto, trabajo y planeta

- 94. Construcción e infraestructura: quién demuestra cómo se levantó de verdad
- 95. El pedigrí de una pieza: cuando un certificado falso puede matar
- 96. Emisiones: el sensor que mentía antes que el papel
- 97. Ciencia ciudadana ambiental: los sensores de abajo, con fecha cierta
- 98. El pasaporte del producto: quién jura el contenido reciclado, y cuándo
- 99. Residuos: adónde va de verdad el contenedor
- 100. El campo y la PAC: el cuaderno verificable
- 101. Fraude alimentario: cuando la etiqueta miente sobre lo que te has comido
- 102. Quién lo hizo, y en qué condiciones: la diligencia debida en la mano de obra
- 103. Integridad marítima: dónde está de verdad ese barco, y ¿es quien dice ser?
- 104. Observación de la Tierra: el testigo orbital que también puede falsificarse
- 105. Protección civil y emergencias: quién sabía qué, y cuándo

Parte XII — Confianza para la democracia: elecciones, instituciones y participación

- 106. Elecciones verificables: del «dividendo del mentiroso» a la evidencia anclada
- 107. IA pública auditable: el registro que se puede comprobar
- 108. Participación auténtica: una persona, una voz, sin vigilancia
- 109. Manifestaciones: la prueba simétrica en la calle

Parte XIII — Actuar o no actuar

- 110. Clavar los talones: el coste de no hacer nada
- 111. ¿Cómo llegamos? Una hoja de ruta
- 112. El sello y la cadena: quién controla la prueba, y quién queda atrapado
- 113. El asedio a la verdad: el testigo que no se puede silenciar
- 114. La dignidad de quien existe: la «Magnifica Humanitas» y la prueba de existencia

Prólogo — De 2004 a 2026: el día que tocamos el límite

«Pero incluso una mirada superficial revela que, pese a todos sus grandes éxitos, nuestra economía de la energía es fatalmente defectuosa en casi todos los aspectos.»

— Paul Roberts, El fin del petróleo (2004)

Era enero de 2003 y el sol de Arabia Saudí abrasaba la arena del «Cuarto Vacío» como una manta incandescente. Paul Roberts, periodista y analista de energía, se encontraba en lo alto de una duna inmensa, observando un horizonte que solo rompían las torres de perforación, alzadas como púas de acero en medio del desierto. Allá abajo estaba Ghawar, el campo petrolero más grande jamás descubierto, el corazón que durante medio siglo había bombeado la energía del mundo. Fue entonces cuando un ingeniero, con voz baja y resignada, soltó la frase que lo cambiaría todo: «El *water cut* de Ghawar ya llega al 30 %.»

Aquella cifra —la proporción de agua que sube mezclada con el crudo— era, para Roberts, la grieta en un sistema que parecía eterno. Para mantener el petróleo fluyendo, los ingenieros tenían que inyectar cantidades crecientes de agua en los pozos; cuanta más agua salía, más cerca estaba el final. En aquel instante, con el sol quemándole la espalda, Roberts perdió la fe en la economía energética moderna. Lo explicaría después en su libro *The End of Oil* (2004): Ghawar era la metáfora perfecta del límite que la civilización estaba a punto de tocar.

Han pasado más de dos décadas. Estamos en 2026, y el paisaje ha cambiado de maneras que Roberts no podía imaginar. Pero la pregunta que formuló en aquella duna —¿hasta cuándo puede durar un mundo construido sobre un recurso finito?— sigue siendo el núcleo de nuestra incertidumbre. La diferencia es que hoy, al límite físico de los recursos, se le ha sumado otro límite, más insidioso: el de la **verdad**.

Las apuestas: por qué aquella duna todavía importa

Lo que Roberts intuyó como una señal de agotamiento es hoy una encrucijada de múltiples dimensiones. No hemos llegado solo al límite de un yacimiento; hemos llegado al límite de una manera de entender el progreso. Y por primera vez en la historia, la urgencia energética y climática confluye con una crisis de confianza que amenaza nuestra capacidad misma de ponernos de acuerdo sobre los hechos. Este libro trata de esa convergencia, y de las dos herramientas —la inteligencia artificial y la blockchain— que pueden ayudarnos a resolverla antes de que sea demasiado tarde.

De la predicción a la realidad (2004 → 2026)

Roberts temía, sobre todo, el agotamiento de la **oferta**. Basándose en las tendencias de consumo de la época, proyectaba una demanda mundial de **140 millones de barriles por día (Mb/d) para 2035**, una sed insaciable que chocaría contra unos yacimientos cada vez más vacíos. La pesadilla era el «pico de oferta»: el día en que el mundo querría más petróleo del que la Tierra podría dar.

La realidad de 2026 ha invertido el guion. La demanda no se ha disparado hasta los 140 Mb/d, sino que tiende a una **meseta de unos 105 Mb/d para 2030** [1]. El temor ya no es que se nos acabe el petróleo, sino que dejemos de necesitarlo: es el «**pico de demanda**», impulsado por la adopción masiva del vehículo eléctrico y por una eficiencia que supera todas las expectativas del pasado. El recurso finito no se ha agotado; ha empezado a quedar obsoleto.

Hay una segunda sorpresa, aún más esperanzadora. Las energías renovables, que en 2004 se consideraban marginales y caras, son ahora la opción más barata del mercado. El coste normalizado de la electricidad solar (LCOE) ha caído **alrededor de un 90 % entre 2010 y 2024**, hasta unos **0,043 $/kWh**, y el **91 % de la nueva capacidad renovable instalada en 2024 resultó más barata que cualquier planta fósil nueva** [2]. La «promesa» que Roberts miraba con escepticismo se ha cumplido con creces.

Y sin embargo, su advertencia más grave también se ha materializado. **2024 fue el primer año natural que superó los +1,5 °C** respecto al nivel preindustrial, según Copernicus, con unas emisiones globales de gases de efecto invernadero en máximos históricos [3]. Un solo año por encima del umbral no equivale

a incumplir el Acuerdo de París —que se mide como una media de décadas—, pero es una advertencia inequívoca: hemos tocado el techo simbólico.

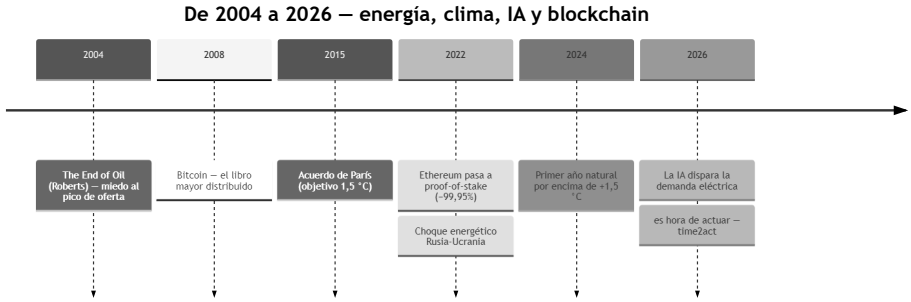


Figura 0.1 — Línea de tiempo 2004 → 2026: los hitos de energía, clima, IA y blockchain que enmarcan este libro.

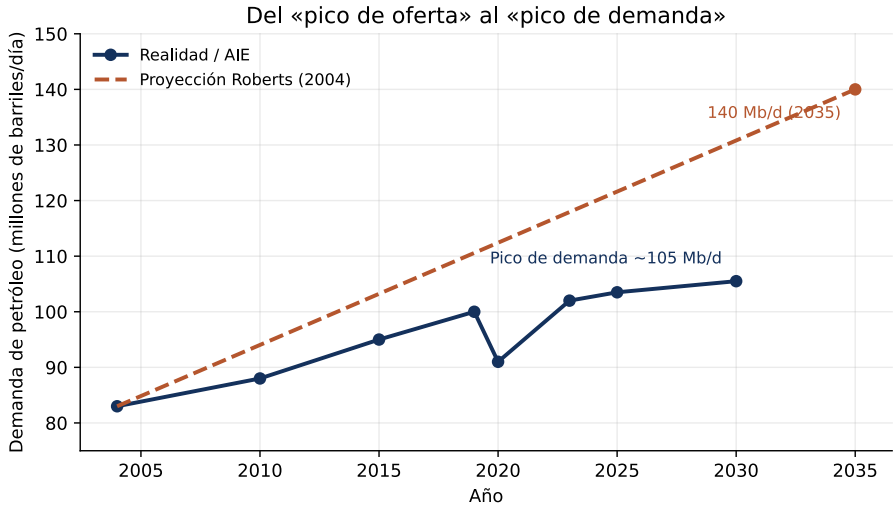


Figura 0.2 — Del «pico de oferta» al «pico de demanda»: la proyección de Roberts (2004) frente a la trayectoria observada.

La crisis que Roberts no podía ver: la verdad

Mientras el mundo se enfrenta a la transición energética, una desconfianza profunda ha emergido como un factor de inestabilidad sistémica. Las **deepfakes**, cada vez más sofisticadas, erosionan la confianza en las instituciones y en los procesos de gobernanza. El fraude ESG, los datos climáticos manipulados y las noticias falsas son hoy una amenaza tangible: de poco sirve descarbonizar si nadie puede fiarse de las cifras que lo demuestran. El estándar de procedencia C2PA ya supera los seis mil miembros, pero certifica el origen de un contenido, no averigua su falsedad [6]. Falta una pieza: una manera fiable de demostrar que un dato existía, intacto, en un momento concreto.

A esta crisis de verdad se añade una **paradoja tecnológica**. La inteligencia artificial, que puede ser la palanca clave de la transición, es también un nuevo y voraz consumidor de energía: los centros de datos del mundo pasarán de unos **485 TWh en 2025 a cerca de 950 TWh en 2030**, casi el doble [4]. La herramienta que debe ayudarnos a ahorrar energía exige, ella misma, cantidades colosales. La solución y el problema comparten enchufe.

Dos palancas que Roberts no tenía: IA y blockchain

El problema de fondo —energía, clima y poder— es el mismo que Roberts describía hace veinte años. Lo que ha cambiado es que ahora disponemos de dos palancas que él no tenía. La primera es la **inteligencia artificial**, capaz de optimizar redes, acelerar el descubrimiento de materiales y modelar el clima con una precisión inédita. La segunda es la **blockchain**, y conviene desactivar enseguida la objeción más repetida: que «malgasta energía». Esto era cierto para Bitcoin, pero el **Merge de Ethereum de 2022 redujo su consumo eléctrico en cerca de un 99,95 %** al adoptar el modelo de *proof-of-stake* [5]. La blockchain

moderna no es un problema energético; es una **capa de confianza**. Y es, precisamente, el fundamento de la **prueba de existencia** —la tecnología de t2p— que puede plantar cara a las deepfakes sellando en un registro inmutable que un dato existía y no se ha alterado. Y antes de entrar en la máquina energética, el capítulo que viene —el pórtico— traduce esta idea a un lenguaje llano que usaremos en cada frente del libro.

La promesa y el peligro

La promesa es extraordinaria y, sobre todo, ya es real: las soluciones existen, son más baratas que nunca y pueden acelerar la transición a la vez que restablecen la confianza. La IA y la blockchain ofrecen una doble función: optimizar los sistemas y garantizar la autenticidad de los datos de los que dependen las decisiones políticas y económicas.

El peligro es igual de nítido. La inacción climática sigue teniendo un coste que se mide en décadas irrecuperables. Pero hay un peligro nuevo: el colapso del consenso sobre la verdad. Sin un marco fiable de autenticidad, los esfuerzos de descarbonización quedan a merced de manipulaciones y fraudes capaces de paralizar cualquier política. La promesa y el peligro, como siempre, viajan juntos.

Es hora de actuar

Roberts hizo el diagnóstico; su mérito fue ver la grieta cuando todos miraban la bonanza. Hoy ya no basta con diagnosticar. Tenemos los hechos, tenemos las herramientas y tenemos, por primera vez, la posibilidad de proteger la verdad sobre la que debemos decidir. Lo que nos falta es actuar. De ahí el título de este libro.

El viaje que propongo arranca con un **pórtico**: un capítulo que traduce a un lenguaje llano qué es la blockchain y qué resuelve la prueba de existencia —la piedra de Rosetta que usaremos en cada página. Después revisitaremos la **máquina energética** de Roberts y la pondremos al día: del petróleo a las renovables, de la geopolítica al clima de 2026. Examinaremos sus **consecuencias** de hoy —y una nueva: la crisis de la verdad. En el **corazón del libro** desplegaremos las soluciones que ofrecen la IA y la capa de confianza, con la prueba de existencia de t2p como pieza insignia contra las deepfakes. Después abriremos **cinco frentes** donde esa defensa ya se juega —dinero, fotoperiodismo, sanidad, educación y derechos humanos— y, finalmente, pondremos sobre la mesa el **coste de no hacer nada** y una hoja de ruta concreta para gobiernos, empresas y ciudadanos. Porque el límite que Roberts vio en Ghawar ya no es una advertencia lejana: es el presente. Y el presente exige acción. Es *time2act*.

---

[1] AIE, *Oil 2025 — Executive summary*. https://www.iea.org/reports/oil-2025/executive-summary ↩

[2] IRENA (vía pv magazine), *Global average solar LCOE $0.043/kWh in 2024*. https://www.pv-magazine.com/2025/07/23/global-average-solar-lcoe-stood-at-0-043-kwh-in-2024-says-irena/ ↩

[3] Copernicus C3S, *2024, first year above 1.5 °C*. https://climate.copernicus.eu/copernicus-2024-first-year-exceed-15degc-above-pre-industrial-level ↩

[4] AIE, *Energy and AI — Executive summary*. https://www.iea.org/reports/energy-and-ai/executive-summary ↩

[5] ethereum.org, *The Merge*. https://ethereum.org/roadmap/merge/ ↩

[6] C2PA (2026), *funcionamiento y límites del estándar de procedencia*. https://truescreen.io/articles/c2pa-standard-history-limitations/ ↩

El protocolo de la confianza: cómo se prueba que algo es cierto

«No puede haber libertad para una comunidad que carece de los medios para detectar las mentiras.»

— Walter Lippmann, Liberty and the News (1920)

Un fin de semana, a primera hora de la mañana, el feed de una red social se llenó de un clip en el que un grupo de adolescentes, con las manos alrededor de una caja negra, anunciaban que habían encontrado «el nuevo recurso energético que cambiará el mundo». El vídeo, de apenas quince segundos, mostraba una explosión de luz verde y una voz emocionada que gritaba: *«¡Esto es el futuro!»* En cuestión de horas, los medios digitales lo compartieron como prueba irrefutable del descubrimiento.

Semanas antes, sin embargo, el mismo fragmento —la misma caja negra, la misma explosión de luz— había circulado como prueba de un manifestante que denunciaba una corrupción policial. En aquel contexto, el clip se usaba para demostrar que una cámara de seguridad había grabado un incidente violento y, por tanto, justificar una denuncia judicial. ¿La diferencia? Solo habían cambiado el título del vídeo y la descripción del pie de foto.

Esta doble vida del mismo archivo digital ilustra a la perfección lo que **Don Tapscott** —consultor y divulgador canadiense, coautor con Alex Tapscott de *Blockchain Revolution* (2016), la obra que situó la cadena de bloques mucho más allá de las criptomonedas— llama el *doble gasto* de los activos digitales: una unidad puede copiarse y «gastarse» dos veces, como un cheque sin fondos [1]. En el ámbito de la verdad, este fenómeno se traduce en un **doble gasto de la confianza**. No hay ninguna señal intrínseca que indique cuál es la versión auténtica del clip ni cuándo existió realmente. La única pista son los metadatos —a menudo borrados o manipulados por quien comparte el contenido— y la fe ciega en el intermediario que lo ha publicado.

Satoshi Nakamoto, con la creación de Bitcoin en 2009, demostró que una red descentralizada podía impedir que un bitcoin se gastara dos veces, gracias a la prueba criptográfica y al registro inmutable [1]. La misma lógica puede aplicarse a cualquier afirmación: si se puede anclar digitalmente el momento y la integridad de un archivo en una cadena pública, se crea un **libro mayor** que nadie puede reescribir sin que se detecte [1]. Así, el clip de las adolescentes podría verificarse como la primera vez que aparece en la red, con una huella única y un sello de tiempo que nadie puede alterar.

Pero hasta ahora, la prueba de existencia ha quedado atrapada dentro de varias tecnologías complejas que la mayoría de los usuarios no entienden.

La necesidad urgente es transformar esta capacidad en un *protocolo de confianza* accesible: un mecanismo que permita a cualquier persona comprobar, con solo su dispositivo, si una versión digital es auténtica y cuándo fue creada.

> *«La blockchain es a la confianza lo que Internet fue a la información.» — Joichi Ito, exdirector del MIT Media Lab* [1]

¿Y si la confianza no hubiera que pedirla a un intermediario, sino que se pudiera comprobar?

Las apuestas

Vivimos una era en la que la confianza se ha convertido en el recurso más escaso y caro de nuestro sistema global. Sin la capacidad de probar que un hecho es real, se desmantelan las bases de la transición energética —que depende de datos ESG fiables y de mediciones de emisiones certificadas—, de los mercados financieros y de la propia democracia.

Las cifras son el grito de alarma: el volumen de deepfakes ha explotado desde **unos 500.000 en 2023** hasta **8 millones en 2025**, con una proyección de que el **90 % del contenido en línea será sintético en 2026** [8]. Este incremento exponencial no es solo una curiosidad tecnológica; ha generado un impacto económico devastador. Las pérdidas por fraude basadas en deepfakes superaron los **mil millones de dólares** en 2025, y las estimaciones de Deloitte prevén **unos 40.000 millones anuales** a partir de 2027 [7].

Los reguladores ya han empezado a responder. El **EU AI Act** impone, a partir de agosto de 2026, la obligación de etiquetar y divulgar todo contenido generado o manipulado por IA [4]. Paralelamente, la implementación de **eIDAS 2.0**, que exigirá una cartera de identidad digital europea antes de diciembre de 2026, pretende crear un marco de autenticación oficial para personas y dispositivos [5]. Pero la etiqueta sola no basta: sin una prueba inmutable que certifique el origen y la fecha de un archivo, las etiquetas pueden falsificarse tan fácilmente como el contenido que pretenden validar.

Aquí es donde entra el concepto de **«hoja de cálculo global»** o **World Wide Ledger**, propuesto por Tapscott ya en 2016 [1]. Este registro distribuido funciona como un libro mayor universal, accesible desde cualquier ordenador, y garantiza que cada transacción o documento quede grabado de manera inmutable. La inmutabilidad es clave: para alterar la cadena habría que **reescribir toda la historia a plena luz del día**, una tarea prácticamente imposible según Tapscott [1].

Esta arquitectura permite fabricar confianza mediante código astuto, lo que Tapscott llama el **«Trust Protocol»** [1]. No se trata de un simple mecanismo técnico; es la base para una nueva economía de la verdad en la que cualquier persona puede verificar la autenticidad y la fecha de una pieza digital solo con su dispositivo. Así, la confianza deja de depositarse en intermediarios centralizados —bancos, notarios o medios— y pasa a ser un recurso verificable por todos.

Por tanto, si no podemos garantizar la certeza de los hechos digitales, el futuro energético, financiero y democrático se ve amenazado. La solución consiste en una infraestructura global de registro inmutable que proporcione la prueba de existencia necesaria para cualquier transacción o información crítica: la piedra angular del **protocolo de confianza** que sustenta todo el libro *time2act*.

Cómo se fabrica la confianza con código

Imaginemos un libro de cuentas sin una única copia guardada en una caja fuerte, sino miles de ejemplares simultáneos distribuidos en cada ordenador conectado a la red. Cada vez que alguien quiere añadir una nueva anotación, todos los ejemplares se actualizan al mismo tiempo, como si fuera un documento colaborativo editado en tiempo real. William Mougayar, inversor y autor de *The Business Blockchain*, describe esta dinámica con una metáfora sencilla: **un archivo que dos usuarios pueden editar simultáneamente**, sin tener que esperar el turno por correo electrónico o por un gestor centralizado [2]. En este escenario, modificar alguna página del libro requiere reescribir **toda** la historia en cada copia a la vez, y hay que hacerlo a plena luz del día. La imposibilidad práctica de este proceso se resume en las palabras de Don Tapscott: «tendrías que reescribir toda la historia a plena luz del día; es prácticamente imposible» [1]. Esta **inmutabilidad** convierte el registro distribuido en un libro mayor que nadie puede manipular, y que cualquiera puede descargar y verificar en su propio equipo.

¿Cómo podemos saber que una entrada concreta no ha sido alterada? La respuesta reside en la idea de una **huella única**, una fotografía digital del contenido que cambia por completo aunque solo se modifique un byte. La huella funciona como una clave de seguridad: si el contenido varía, la huella también lo hace, revelando al instante cualquier intento de manipulación sin necesidad de exponer la información subyacente. Es, en esencia, una prueba criptográfica de que el documento ha quedado intacto y no se ha tocado, manteniendo la privacidad de su contenido.

Un obstáculo histórico para el despliegue masivo de tecnologías basadas en registros distribuidos era el coste energético. Hasta hace poco, la mayoría de las cadenas de bloques operaban con **proof-of-work**, un mecanismo que consumía grandes cantidades de electricidad para validar transacciones. En 2022, Ethereum llevó a cabo el famoso *Merge*, pasando de proof-of-work a **proof-of-stake** y reduciendo su consumo energético aproximadamente un 99,95 % [3]. Esta transformación no solo responde a las críticas ambientales, sino que elimina una de las objeciones más contundentes: la idea de que las soluciones basadas en blockchain son intrínsecamente insostenibles. En este nuevo paradigma, Tapscott destiló **siete principios de diseño** —integridad en red, poder distribuido, valor como incentivo, seguridad, privacidad, derechos preservados e inclusión— que sirven de guía para cualquier implementación responsable [1]. Aseguran que la confianza no se delegue en ninguna entidad central, sino que emerja de las reglas codificadas en el propio protocolo.

Finalmente, el núcleo de esta revolución es el **Trust Protocol**, un conjunto de reglas que permite a cualquier persona «fabricar confianza mediante código astuto» [1]. No hace falta más que seguir el protocolo para crear una capa verificable e inmutable sobre cualquier dato digital. Así, la confianza deja de ser una cuestión de autoridad externa y se convierte en un producto matemático, accesible a todos y

resistente a los ataques. Este es el fundamento del **protocolo de la confianza** que sostendrá las soluciones que exploraremos a lo largo de *time2act*.

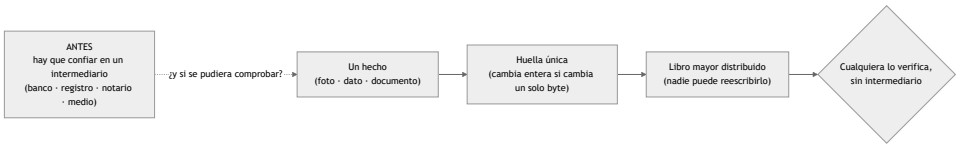


Figura 1.1 — De la confianza centralizada a la distribuida: el viaje de un hecho, de la captura a la verificación que cualquiera puede rehacer.

De la idea al bolsillo: t2p

Imaginemos una reunión de trabajo donde alguien tiene que demostrar que una fotografía tomada hace cinco días muestra el producto exactamente como era en aquel momento. En el modelo tradicional haría falta un notario, un archivo físico o una empresa especializada para almacenar y certificar la imagen. Con **t2p**, todo se reduce a abrir la aplicación del teléfono y pulsar el botón de captura; en segundos el dispositivo genera una huella digital única —una pequeña cadena de bits que resume todo el contenido sin revelarlo— y la fija al instante en una **cadena pública** donde queda registrada para siempre. El resultado es un certificado QR que cualquiera puede escanear, desde un cliente hasta una autoridad reguladora, y verifica, fuera de toda duda, que aquella foto existía, intacta e inalterada, en el momento indicado.

Esta operación se apoya en el **Trust Protocol** que Tapscott describe como un «código astuto» capaz de **fabricar confianza mediante matemáticas**, no a través de una autoridad central [1]. La clave es la inmutabilidad de la cadena pública: modificarla exigiría reescribir toda la historia, una tarea que Tapscott califica de «prácticamente imposible» [1]; por tanto, la comprobación no se le pide a nadie: se hace directamente, con las herramientas de cualquier dispositivo conectado.

El flujo es tan lineal que hasta un usuario sin conocimientos técnicos puede seguirlo: captura → cálculo de la huella → anclaje en la cadena pública → generación del certificado QR. Cada paso se realiza dentro del teléfono, de modo que **el archivo original nunca sale del dispositivo**, preservando la privacidad y evitando fugas de datos [9]. Esta separación entre contenido y prueba resulta clave en un contexto donde regulaciones como el **EU AI Act** obligan a marcar y divulgar el contenido generado por IA, ya que ofrece una capa de autenticidad independiente de cualquier etiqueta o metadato manipulable [4].

Como hemos visto con eIDAS 2.0 (previsto para diciembre de 2026) y los estándares C2PA / Content Credentials adoptados en 2026, las carteras digitales europeas podrán integrar estos certificados, reforzando la confianza en entornos cada vez más virtuales [5][6].

Así, **t2p** convierte el teléfono —la herramienta más omnipresente de nuestro día a día— en un «estudio de pruebas portátil». No hace falta ningún laboratorio costoso ni infraestructura compleja; solo una conexión a la cadena pública y la aplicación que gestiona la huella. El **protocolo de la confianza** se materializa: la confianza no hay que pedirla, sino poder comprobarla en cualquier momento y lugar, con la seguridad que ofrece la criptografía distribuida. Esta puerta abierta es la base sobre la que construiremos las soluciones más avanzadas a lo largo de *time2act*: la prueba de que el futuro de la confianza ya está al alcance de nuestro pulgar.

La promesa y el peligro

Imagina una red donde cualquiera puede demostrar que un documento, una imagen o un acontecimiento existió en un momento determinado, sin recurrir a ningún notario, banco o autoridad central. Esta es la **promesa** del protocolo de confianza: una verificación barata, instantánea y escalable que transforma la confianza de un concepto abstracto en una prueba criptográfica inmutable. Como escribió Joichi Ito, «la blockchain es a la confianza lo que Internet fue a la información» [1]: esta tecnología convierte el simple acto de firmar en una operación tan transparente como consultar un buscador. La capacidad de anclar una huella única en una cadena pública —un libro mayor que nadie puede reescribir y que cualquiera puede verificar— elimina la necesidad de confiar ciegamente en intermediarios tradicionales, tal como propone el **Trust Protocol**: «fabricar confianza mediante código astuto» [1].

Esta nueva forma de confianza tiene un coste operativo casi nulo comparado con las infraestructuras legales y financieras que hemos mantenido durante siglos. No hay que pagar honorarios notariales ni

esperar días para la confirmación de una transacción; el proceso se completa en segundos, y la prueba queda permanentemente disponible en el registro distribuido, una «hoja de cálculo global» que todo el mundo puede descargar y ejecutar en su ordenador [1]. Además, la inmutabilidad de la cadena —alterarla exigiría reescribir toda la historia a plena luz del día— hace prácticamente imposible cualquier manipulación posterior [1].

Sin embargo, esta promesa viene acompañada de unas **amenazas** que hay que entender y mitigar. En primer lugar, el fenómeno de la «basura inmutable» nos recuerda que una cadena no valida la verdad del contenido que se ancla en ella; solo garantiza que ese contenido no cambia una vez registrado [1]. Si se graba una mentira, quedará inmortalizada como certeza criptográfica. La confianza en la tecnología puede, por tanto, convertir falsedades en «hechos verificables».

En segundo lugar, la vinculación de pruebas con metadatos puede erosionar la privacidad y desanonimizar a usuarios vulnerables. Los estudios sobre **C2PA / Content Credentials** muestran que ya en 2026 los teléfonos móviles y las cámaras profesionales firman automáticamente el contenido, pero muchos intermediarios todavía borran los metadatos al recompartirlo [6]. Esta práctica puede exponer a periodistas o activistas a la identificación forense, comprometiendo la seguridad de quien depende del protocolo para proteger su identidad.

Finalmente, el **tecnosolucionismo** —la creencia de que una sola herramienta resuelve todos los problemas de confianza— representa un peligro conceptual. El protocolo de confianza es necesario pero no suficiente; sin marcos reguladores como el EU AI Act, que obliga a marcar y divulgar el contenido generado por IA [4], o eIDAS 2.0, previsto para diciembre de 2026 [5], la tecnología podría ser mal utilizada o quedar limitada en su impacto real. Reconocer estas limitaciones es fundamental para que el lector no las perciba como propaganda, sino como una guía crítica que combina **confianza verificable** con un análisis riguroso de los riesgos inherentes.

El mapa de lo que resuelve

Con esta base de **confianza verificable**, la blockchain se convierte en el libro mayor que nadie puede reescribir y ofrece una nueva manera de leer la realidad: la prueba de existencia. No es solo un truco técnico; es la clave para descifrar las preguntas de confianza que atraviesan todos los ámbitos donde se decide nuestro futuro, porque la **huella anclada en una cadena pública** da una respuesta inequívoca.

En energía y clima, los datos de emisiones son el termómetro de nuestra responsabilidad planetaria. La cuestión es: *¿este dato de emisiones es real y no se ha alterado?* Si se puede demostrar que cada número queda inmutablemente registrado, gobiernos y empresas disponen de una base sólida para políticas climáticas verdaderas y medibles.

En desinformación y deepfakes, el riesgo es evidente: imágenes y vídeos pueden manipularse con facilidad. La prueba de existencia permite preguntar: *¿esta imagen existió así, y cuándo?* Esto contrarresta la proliferación masiva de contenido sintético —como hemos visto, el volumen ha crecido exponencialmente— y responde a las exigencias del EU AI Act, que obliga a marcar el contenido generado por IA a partir de agosto de 2026 [4].

En dinero y compliance, el doble gasto sigue siendo una amenaza para el sistema financiero. La cuestión es: *¿este registro o esta identidad no se han fabricado?* Un certificado inmutable asegura que las transacciones son auténticas, evitando fraudes y reforzando la confianza en los mercados.

El fotoperiodismo depende de la autenticidad visual para narrar la verdad. La pregunta aquí es: *¿esta foto es de donde y de cuándo dice que es?* Con unos metadatos firmados por C2PA, ya incorporados en móviles como el Samsung S25 y el Pixel 10 [6], se puede verificar el origen y la fecha sin depender de terceros.

En sanidad, los resultados clínicos son vitales. La prueba de existencia responde a: *¿esta imagen clínica o este dato de ensayo es íntegro?* Esto protege a pacientes e investigadores contra manipulaciones que podrían comprometer diagnósticos y tratamientos.

En educación, la credibilidad de los títulos y las autoridades académicas se pone a prueba. La pregunta clave es: *¿este título o esta autoría son auténticos y verificables?* Un registro inmutable garantiza que los certificados no sean falsificados, reforzando el valor del conocimiento.

Finalmente, en defensa y derechos humanos, la verdad documental puede ser la última defensa contra la impunidad. La cuestión es: *¿esta orden o esta prueba de una atrocidad es auténtica?* Un registro

inmutable ofrece una prueba firme que no puede borrarse, esencial para tribunales y organizaciones de derechos humanos.

En todos estos dominios, la firma digital C2PA y el anclaje en una cadena pública trabajan conjuntamente para crear un ecosistema donde la confianza no depende de autoridades centralizadas sino de matemáticas verificables [1]. Así, el mapa dibujado aquí conecta cada pregunta de confianza con la solución universal de **t2p**, sentando las bases para el próximo capítulo: volver al origen del problema moderno —la máquina energética— y leerla con una nueva lengua. Es hora de actuar; el futuro se construye con pruebas, no con supuestos.

---

[1] Tapscott, Don y Tapscott, Alex — *Blockchain Revolution* (Portfolio/Penguin, 2016). https://blockchain-revolution.com/ ↩

[2] Mougayar, William — *Explaining the Blockchain via a Google Docs Analogy* (2016). https://medium.com/@wmougayar/explaining-the-blockchain-via-a-google-docs-analogy-56326b1bbe58 ↩

[3] ethereum.org — *The Merge*. https://ethereum.org/roadmap/merge/ ↩

[4] EU AI Act — *Article 50: Transparency Obligations* (Reglamento (UE) 2024/1689). https://artificialintelligenceact.eu/article/50/ ↩

[5] Comisión Europea — *European Digital Identity Wallet (eIDAS 2.0)*. https://www.eudi-wallet.eu/ ↩

[6] C2PA — *Content Credentials*. https://c2pa.org/ ↩

[7] Deloitte — *Generative AI and the fraud risk for financial services* (proyección de fraude por IA). https://www2.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html ↩

[8] Europol — *Facing reality? Law enforcement and the challenge of deepfakes*. https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes ↩

[9] t2p — *Manual de usuario (Solución de Integridad de Datos)*, v1.0, 2026. ↩

Encender el fuego, revisitado

«[El fuego,] que se ha revelado maestro de todas las artes para los mortales, y un gran recurso.»

— Esquilo, Prometeo encadenado (s. V a. C.)

En la penumbra de un apartamento de Barcelona, Marta se gira hacia el interruptor que controla la pequeña luz del pasillo. Un toque de dedo, un clic, y la bombilla se ilumina con una calidez familiar; en ese mismo instante, una cadena invisible de recursos despierta. Desde los pozos profundos de Azerbaiyán hasta los oleoductos sumergidos que serpentean por el fondo del mar Negro, la señal eléctrica viaja a través de transformadores que responden con un zumbido, y cada paso de la luz se convierte en una vibración que recorre cientos de miles de kilómetros de infraestructura: barcos cargados de petróleo que cruzan el océano Atlántico, centrales termoeléctricas que soplan vapor al cielo de Texas, y líneas de transmisión de alta tensión, curvadas como serpientes de plata sobre las montañas suizas.

Marta arranca su coche eléctrico en la puerta del bloque. Un murmullo suave de motores silenciosos acompaña la aceleración; pero dentro del vehículo, la batería se alimenta de una red que todavía depende mayoritariamente del carbono: en 2024, el 86,7 % del consumo mundial de energía provenía de fuentes fósiles, mientras que las renovables, que ya lideran el crecimiento, eran aún solo una fracción del total [1]. Cada kilómetro recorrido por Marta es una pequeña revolución de una máquina planetaria que, aunque se fragmenta cada vez más, sigue girando en torno a estos recursos ocultos.

Al otro lado del mundo, en el desierto de Arabia Saudí, los trabajadores del campo de Ghawar encienden las antorchas para una inspección nocturna. El fuego baila sobre el metal frío y recuerda que la energía que alimenta las luces de Barcelona es la misma que mantiene las economías globales en movimiento: una demanda mundial que se acerca al pico de 105 millones de barriles por día previsto para 2030, y que presiona aún más los yacimientos y las infraestructuras existentes [2].

Mientras la luz de Marta ilumina la cocina, observadores invisibles —desde los gestores de redes hasta los reguladores internacionales— monitorizan el equilibrio precario entre oferta y demanda. Cada clic del interruptor, cada giro de llave, se convierte en un microacontecimiento que alimenta la gran orquesta de la energía global: una danza de corrientes que atraviesan el planeta sin que nadie la vea, pero que determina cómo crecen las ciudades, cómo operan los negocios y cómo se posicionan las naciones en el escenario geopolítico.

Esta invisibilidad es a la vez la fuerza y la vulnerabilidad de nuestra era. La máquina energética sigue siendo abrumadoramente fósil, pero por primera vez el centro de gravedad empieza a desplazarse hacia fuentes más limpias y descentralizadas. Cada acción cotidiana —encender una bombilla, poner en marcha un vehículo— es ahora una oportunidad para observar la gran infraestructura que nos sustenta y, al mismo tiempo, para cuestionarla. Aquí reside el potencial de cambio: reconocer la magnitud del sistema para poder impulsar las tecnologías emergentes que han de transformarlo. Pero antes de querer hacer girar la máquina, hay que entender cómo se construyó y por qué cuesta tanto moverla.

Seis mil años encendiendo fuegos

Desde las primeras brasas que nuestros antepasados domesticaron en los valles del Nilo y del Tigris, la energía ha sido la fuerza invisible que ha impulsado cada paso de nuestra evolución. En aquel momento prehistórico, una simple piedra tallada se convertía en una herramienta para cazar; un tronco encendido era la primera luz que rompía la oscuridad nocturna y la primera fuente de calor rudimentaria de una comunidad nómada. Aquellas llamas, modestas pero decisivas, permitieron a los grupos humanos cocinar alimentos, alargar las horas de trabajo y, más importante aún, crear un espacio social donde se transmitían historias y conocimientos.

Con el paso de los siglos, la fuerza animal fue el primer motor: bueyes y mulos arrastraron carros e hicieron girar molinos, y convirtieron la fuerza de los músculos en trabajo continuado. La leña, recogida de bosques que ahora son recuerdos de un paisaje preindustrial, pasó a ser la fuente primaria para encender hornos y calderas. Este modelo de dependencia directa de los recursos locales duró milenios, pero ya en el siglo XVIII una nueva revolución se alzaba en el horizonte: el carbón.

El descubrimiento y la explotación masiva del carbón lo cambiaron todo. Las minas de Gales, de Pensilvania y de Silesia alimentaron las primeras fábricas de hilado y las locomotoras de vapor que conectaron ciudades y continentes. El carbón se convirtió en la columna vertebral de una economía

industrial emergente y redujo drásticamente el tiempo necesario para transformar materias primas en productos acabados. En este periodo, la máquina energética se hizo cada vez más visible: las altas chimeneas que dominaban los horizontes urbanos eran testigos humeantes de una nueva era.

El siglo XX trajo otra gran transición: el petróleo y el gas natural sustituyeron progresivamente al carbón como fuentes preferidas. La explotación de campos petrolíferos en Texas, en el golfo Pérsico y en la costa de Noruega creó una red global de infraestructuras que alimentaba automóviles, aviones y centrales eléctricas. El gas natural, más limpio y flexible, se integró en sistemas de calefacción y generación distribuida. Este cambio no solo aumentó la eficiencia energética, sino que también consolidó una dependencia global que un siglo después aún no hemos deshecho: la misma que Marta despierta cada noche con un clic.

Esta dominación oscura ha generado una demanda sin precedentes, que ahora se acerca al techo que hemos entrevisto en Ghawar. Pero la historia nos muestra que cada revolución energética ha comportado una reconfiguración del poder y de las oportunidades; y ahora hay otra en marcha. El relato de hoy, como el que Paul Roberts —periodista y analista de energía, autor de *The End of Oil* (2004)— situaba en los orígenes del fuego hace milenios, es una llamada a observar cómo las llamas que encendemos —tanto físicas como digitales— podrían ser la clave para transformar esta máquina invisible en una fuerza transparente y sostenible.

La máquina, hoy

En 2026, la «máquina energética» sigue siendo una estructura masiva y casi inamovible, dominada por una tríada de combustibles fósiles que actúa como el núcleo de una estrella. El petróleo aporta un 33,6 % de la energía total consumida; el gas natural, un 25,2 %; y el carbón —aunque ha perdido peso en las últimas décadas— representa aproximadamente un 28 %. Estas tres fuentes suman aquel 86,7 % del mix energético mundial, una cifra que, según el Global Energy Review de la AIE, se mantiene prácticamente estable pese a las políticas climáticas y las inversiones en renovables [1].

Esta proporción no es solo una cifra: refleja la magnitud y la inercia de un sistema construido durante más de dos siglos. Las infraestructuras asociadas —refinerías, redes de gasoductos, centrales térmicas y minas de carbón— son activos físicos que cuestan décadas de desmantelar o reconvertir, y que consumen recursos financieros y políticos a una escala tal que cualquier intento de sustituirlos ha de afrontar una resistencia estructural comparable a la fricción de un engranaje antiguo en movimiento.

Esta inercia se ve reforzada por la interdependencia global del mercado energético. Un aumento inesperado del precio del petróleo —como el del primer trimestre de 2024, cuando los conflictos geopolíticos impulsaron las cotizaciones a máximos históricos— desencadena una reacción que afecta desde los costes de transporte hasta la producción industrial. De manera similar, una interrupción del suministro de gas natural —como la reducción de exportaciones rusas— puede provocar apagones temporales y aumentar la presión sobre las centrales de carbón, que se convierten en la válvula de seguridad que cubre los huecos.

Aun así, algo se mueve. Las fuentes limpias representan el 38 % del crecimiento total del consumo energético entre 2020 y 2024, e impulsan una diversificación que, aún modesta a escala global, ya está cambiando la configuración de las redes locales y regionales. La descentralización —con microrredes solares e instalaciones eólicas comunitarias— empieza a crear puntos de inflexión donde el centro de gravedad energético se desplaza lentamente hacia una arquitectura más distribuida.

No obstante, la fuerza del cambio todavía choca con la enorme masa de la máquina fósil. La inercia no es solo física; es también institucional y cultural. Las empresas energéticas tradicionales, que controlan una parte determinante de los activos del sector, mantienen una influencia decisiva sobre las políticas reguladoras y los estándares de mercado. Este poder consolidado se traduce en barreras de entrada para los nuevos actores basados en blockchain o IA, que ofrecen soluciones de transparencia y verificación pero todavía luchan por ganarse la confianza de un ecosistema dominado por grandes conglomerados.

El panorama energético de 2026 es, pues, una combinación paradójica: una máquina masiva y predominantemente fósil que se encuentra a las puertas de una transformación lenta pero inevitable. Su inercia colosal implica que cualquier avance hacia fuentes limpias ha de ser no solo tecnológico sino también institucional, y requiere una reconfiguración profunda de los incentivos y de la gobernanza global de la energía. Este es el punto de partida sobre el que se construye la narrativa de «encender el fuego» revisitado: las llamas que ahora se alzan no son solo las del petróleo o del carbón, sino también las de

datos verificados, contratos inteligentes y redes descentralizadas que podrían redefinir el funcionamiento interior de nuestra máquina energética.

El inicio del giro

En la primavera de 2024, un grupo de analistas de Bloomberg Energy observó una señal que hasta entonces había pasado desapercibida entre las cifras masivas del consumo global: **las energías renovables representaban el 38 % del crecimiento total del suministro energético**. No se trataba solo de un incremento marginal; era la fuerza motriz que impulsaba la expansión de nuestra máquina energética, todavía dominada por los combustibles fósiles pero cada vez más dependiente de una nueva fuente de potencia [1]. Esta dinámica ha cambiado el paradigma de la seguridad energética: hasta hace poco, la preocupación central era el agotamiento de las reservas, aquello que Roberts describía como «el último petróleo fácil»; ahora la incertidumbre gira hacia el **pico de demanda**, el techo que las proyecciones sitúan en torno a 2030 [2].

Este desplazamiento de las apuestas tiene repercusiones profundas. En primer lugar, que las renovables impulsen más de un tercio del crecimiento indica que los inversores y las políticas públicas ya están canalizando capital hacia tecnologías como la eólica marina, la fotovoltaica de alta eficiencia y el almacenamiento avanzado. Según el informe de la Agencia Internacional de la Energía (AIE), la capacidad eólica y solar instalada batió récords y activó una cadena de suministro que va desde el hierro para las torres hasta los sistemas de control basados en IA. Este aumento no solo diversifica la cartera energética: también comporta una **reducción de la dependencia** del petróleo y del gas natural, aunque el carbón todavía mantiene una presencia significativa.

En segundo lugar, la llegada del pico de demanda cambia las reglas del juego de la gobernanza global. La presión ya no recae exclusivamente en la necesidad de extraer más recursos; ahora se trata de optimizar el consumo y de garantizar que las infraestructuras puedan soportar una demanda que supera los límites históricos. Las redes inteligentes, alimentadas por contratos inteligentes basados en blockchain, permiten **equilibrar la oferta y la demanda en tiempo real**, con menos pérdidas y más capacidad de respuesta ante imprevistos como las tormentas que interrumpen la producción eólica. Así, el peligro tradicional —el colapso del suministro— se transforma en un nuevo riesgo: **la vulnerabilidad cibernética** de un sistema cada vez más digitalizado.

Esta transición no es solo técnica; es cultural y económica. Las empresas que antes basaban sus modelos de negocio en la extracción de recursos fósiles se ven obligadas a reinventarse: adoptan plataformas descentralizadas para la gestión de activos energéticos, aprovechan la analítica predictiva para anticipar las fluctuaciones del mercado y reorientan una parte creciente de su inversión hacia la eólica marina y la solar.

El **giro estructural** que Roberts no pudo prever se manifiesta, pues, en tres dimensiones clave: un crecimiento impulsado por las renovables que alimenta la máquina energética, una demanda que se acerca a nuevos picos históricos y una infraestructura digital que cambia la manera en que gestionamos la energía. Estas fuerzas convergentes abren una era en la que el fuego que encendemos ya no depende exclusivamente del petróleo ni del carbón. ¿Qué prometen estas llamas nuevas, y qué arriesgamos al encenderlas?

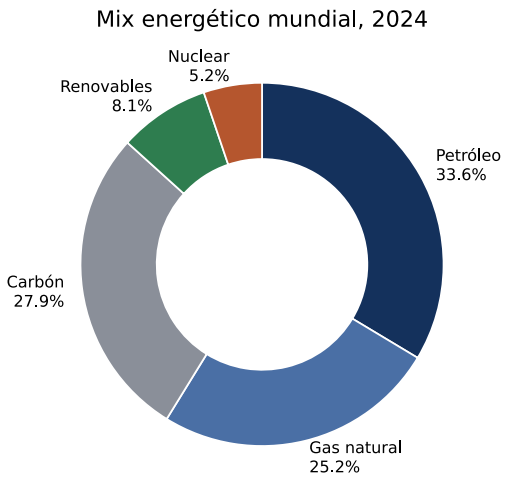


Figura 2.1 — El mundo todavía funciona con combustibles fósiles (~86,7 % del suministro primario en 2024), pero las renovables ya lideran el crecimiento.

La promesa y el peligro

Por primera vez en la historia de la civilización, una alternativa a la energía fósil no solo es tecnológicamente viable sino también económicamente dominante. Las renovables encabezan el crecimiento energético mundial y empiezan a roer la cuota fósil, aquella proporción todavía abrumadora pero ya en declive constante. Esta inversión de tendencia se acompaña de una nueva economía digital: redes de sensores, plataformas blockchain y algoritmos de inteligencia artificial que permiten monitorizar, optimizar y facturar la energía con una precisión antes impensable. Y el coste marginal de generar energía solar o eólica ha caído hasta el punto de que, en muchos mercados, ya resulta más barata que la de cualquier planta fósil nueva. La oferta renovable no solo es más limpia; es más barata que el modelo tradicional.

Esta combinación de costes reducidos y escalabilidad digital crea una promesa clara: la «maquinaria energética» del futuro puede operar con una base de alimentación principalmente limpia, sostenida por datos verificados y contratos inteligentes que eliminan gran parte de las ineficiencias asociadas a las cadenas de suministro fósiles. El impacto potencial es doble. Primero, la reducción del precio de la energía impulsa el crecimiento económico y facilita la transición hacia sectores de alto valor añadido como la manufactura avanzada o los servicios digitales. Segundo, una infraestructura energética más transparente y descentralizada refuerza la confianza de los consumidores y de los inversores, y contrarresta la era de las «deepfakes», que ha erosionado la credibilidad en muchos ámbitos.

Sin embargo, el peligro reside en la inercia del sistema actual. Las instalaciones fósiles —centrales de carbón, refinerías y gasoductos— representan inversiones de billones de euros y una vida útil que se extiende durante décadas. Este capital fósil no desaparecerá de golpe: su amortización, las obligaciones contractuales y los intereses políticos que protegen estas infraestructuras crean una fricción estructural que retrasará cualquier cambio sustancial. Además, la percepción equivocada de que el simple encendido de un nuevo «fuego digital» equivale a una solución completa puede conducir a una complacencia prematura. Los primeros éxitos de las renovables y de la blockchain se celebran a menudo como victorias definitivas, pero en realidad solo marcan el comienzo de una transición compleja y de largo recorrido.

El riesgo mayor, por tanto, es confundir el inicio del giro con el trabajo hecho. Las políticas que prometen eliminar los combustibles fósiles en un horizonte corto, sin abordar las barreras de inversión ni la necesidad de reconvertir el capital existente, pueden crear una falsa sensación de seguridad mientras la realidad sigue dominada por estructuras de poder fósil. Para evitar este escenario, hay que diseñar marcos reguladores que integren los costes de desmantelamiento del patrimonio fósil y que incentiven a la vez las inversiones en tecnologías digitales y renovables. Solo así la promesa de una energía más limpia y asequible se transformará en una nueva base estable para nuestra máquina energética global.

El mapa del viaje

Después de habernos adentrado en las raíces de la máquina energética —aquella que ha alimentado civilizaciones desde el primer fuego hasta la era del petróleo—, es momento de trazar el mapa del próximo viaje. La Parte II de *time2act* se despliega como una ruta con paradas pensadas para revelar cómo la dependencia fósil todavía domina y cómo, a la vez, el centro de gravedad ya empieza a moverse hacia nuevas fuentes y tecnologías.

En el capítulo 3 nos sumergiremos en la oferta de petróleo. No solo revisaremos las reservas que todavía alimentan las economías más poderosas, sino que desglosaremos las cadenas de valor que mantienen viva la infraestructura fósil: refinerías, oleoductos y mercados de futuros que, como una red nerviosa, regulan el flujo de capital y de energía. Pondremos a prueba aquel 33,6 % del consumo mundial que todavía es petróleo, y exploraremos escenarios en los que su reducción se acelere con políticas de desmantelamiento que integren los costes reales de la transición.

El capítulo 4 girará el foco hacia las renovables y el vehículo eléctrico. Las fuentes de energía limpia, con aquel 38 % del crecimiento a la espalda, son el motor emergente que puede reconfigurar nuestra máquina: analizaremos cómo la explosión de la capacidad solar y eólica, junto con las redes inteligentes basadas en blockchain, permite una gestión descentralizada y transparente del flujo energético. Y el vehículo eléctrico —como el de Marta— se presenta no solo como sustituto del motor de combustión interna, sino como nodo móvil que potencia la integración de energía distribuida y crea un ecosistema en el que cada coche es también una batería colectiva.

En el capítulo 5 abordaremos la geopolítica del poder energético. La distribución desigual de los recursos fósiles ha modelado fronteras y alianzas durante décadas; ahora, la emergencia de una matriz más diversificada obliga a redibujarlas. Examinaremos cómo países tradicionalmente dominantes en el petróleo han empezado a invertir masivamente en renovables para mantener su influencia, y cómo nuevas potencias energéticas digitales —con IA que optimiza redes y blockchain que asegura transacciones— se convierten en actores clave del escenario global.

Finalmente, el capítulo 6 nos llevará al clima. Aquel pico de demanda que corre hacia 2030 es también una presión que amplifica los riesgos climáticos y las incertidumbres sociales [2]. Analizaremos cómo la combinación de IA para predecir patrones meteorológicos y blockchain para rastrear emisiones puede transformar la respuesta global a la crisis climática, y convertir la promesa de una energía limpia en una base estable y verificable.

Y sin embargo, el mapa no se cierra cuando se enfría el último motor de combustión. Si estas primeras paradas nos enseñan cómo se mueve la energía, el resto del viaje persigue algo más escurridizo: la confianza misma. Porque en un mundo donde una imagen, una voz o un documento pueden fabricarse en segundos, la energía es apenas el primer sistema que aprendemos a hacer verificable. A partir de aquí, *time2act* deja atrás los oleoductos para seguir el rastro de la prueba —la prueba de existencia— por cada terreno donde hoy se juega la credibilidad. Conviene, pues, ganar altura y mirar el mapa entero desde arriba.

Las Partes III y IV cierran el arco que abrimos con la energía. La III baja a las consecuencias que ya vivimos —el consumo que no cede, las grandes energéticas inquietas y esa nueva tensión en la que la inteligencia artificial es a la vez promesa de eficiencia y sed voraz de electricidad— hasta desembocar en la crisis de la verdad: la desinformación y las deepfakes que corroen aquello en lo que podemos creer. La IV responde con las herramientas: redes inteligentes gobernadas por IA, la blockchain como capa neutral de confianza y t2p, la prueba de existencia que planta cara a la falsificación, sin olvidar las apuestas —hidrógeno, captura de carbono— que aún deben madurar.

En la Parte V, el libro despliega cinco frentes contra las deepfakes: allí donde detectar ya no basta, la prueba de existencia se revela como defensa duradera —en el dinero y el fraude, en el fotoperiodismo, en la imagen médica, en las credenciales académicas y en el terreno más crudo de la defensa y los derechos humanos.

Después se abre el gran atlas de la confianza aplicada. La Parte VI la pone al servicio del clima —créditos de carbono, certificados de ahorro, autoconsumo y movilidad verificable—; la Parte VII la lleva a la economía real, del seguro y la cadena de suministro a la vivienda, las patentes y la contratación pública; la Parte VIII la extiende a la sociedad entera —identidad, elecciones, ayuda humanitaria, herencias, auditoría, memoria histórica—; y la Parte IX se adentra en las nuevas fronteras, donde la ciencia, el cuerpo, las máquinas y los mercados reclaman la misma certeza, desde la prueba de vida hasta el pedigrí del chip y del código que lo sostienen todo.

Las Partes X y XI afrontan el filo del momento. Primero, cuando todo se puede falsificar —tu cara, tu voz, tu dinero, la identidad de quien te llama o de quien trabaja al otro lado de una pantalla—; después, la terca honestidad del mundo físico, donde una obra, una pieza, un sensor o un barco tienen que poder demostrar cómo, dónde y en qué condiciones existieron de verdad.

Y el viaje culmina en lo colectivo. La Parte XII eleva la confianza a la escala de la democracia —elecciones verificables, IA pública auditable, participación auténtica sin vigilancia—, y la Parte XIII nos deja ante la única pregunta que de verdad importa: actuar o no actuar. Allí se mide el coste de la inacción, se traza la hoja de ruta, se pregunta quién controla el sello y quién podría quedar atrapado por él, y se cierra, como debe ser, con la dignidad de quien existe.

Esta travesía no es meramente descriptiva; es una llamada a la acción. La máquina energética está viva, y por fin empieza a mutar. Cada capítulo ofrece principios de diseño y hojas de ruta que permiten a los lectores —ya sean responsables políticos, ejecutivos de empresa o ciudadanos conscientes— participar activamente en este cambio estructural. El futuro no es una utopía distante: es un proyecto concreto que requiere decisiones informadas hoy mismo. Esta noche, cuando Marta vuelva a pulsar el interruptor del pasillo, la cadena invisible despertará otra vez, desde los pozos de Azerbaiyán hasta el clic de la bombilla; la diferencia es que ahora sabemos qué encendemos. Es hora de encender el fuego, revisitado y dirigido hacia un horizonte donde la confianza y la sostenibilidad conviertan nuestra máquina energética en una fuerza para el bien común.

---

[1] AIE, *Global Energy Review 2025 — Key findings*. https://www.iea.org/reports/global-energy-review-2025/key-findings ↩

[2] AIE, *Oil 2025 — Executive summary*. https://www.iea.org/reports/oil-2025/executive-summary ↩

El último petróleo fácil… y por qué ya importa menos

«La Edad de Piedra no terminó por falta de piedra, y la era del petróleo terminará mucho antes de que al mundo se le acabe el petróleo.»

— Ahmed Zaki Yamani, citado en The Economist (2003)

Marzo de 2022. A primera hora de la mañana, Bruselas se llenó de una tensión como hacía años que no se recordaba: el precio del petróleo volvía a sonar como una alarma. En horario de Londres, el Brent había roto la barrera simbólica de los **130 $ por barril**, y el pico corrió por canales de información y redes sociales hasta poner a toda Europa en alerta. El mercado, ya sacudido por el estallido de la invasión rusa de Ucrania solo días antes, se encontraba ante una realidad nueva: el petróleo recuperaba el papel de arma geopolítica que los analistas temían desde hacía décadas.

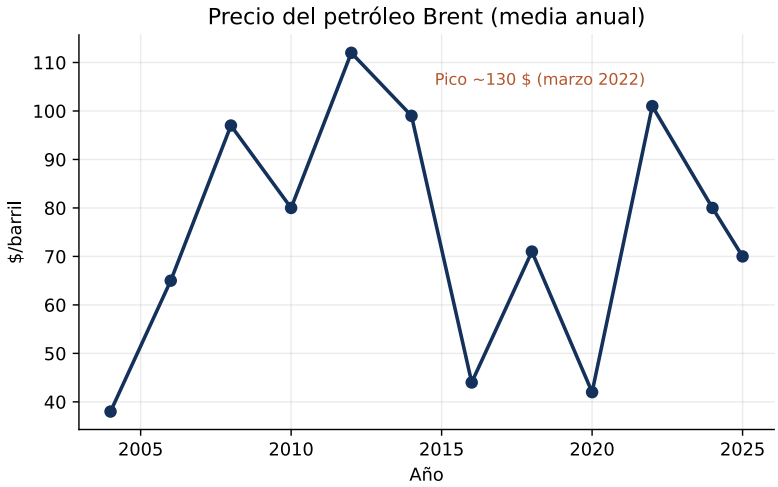


Figura 3.1 — El precio del Brent: del choque de 2022 (~130 $) a la estabilización hacia los ~67 $ en 2025.

Aquel pico, sin embargo, fue el principio de un descenso. Las cifras que vendrían después contaban una historia que nadie esperaba: del máximo de **130 $** a una media de **101 $** en 2022, a **83 $** en 2023, hasta acabar en unos modestos **67 $** en septiembre de 2025 [1]. No eran solo números: eran el reflejo de una dependencia todavía aferrada a las vías tradicionales del suministro, pero también la prueba de que la oferta era mucho más robusta de lo que se temía.

La pregunta que flotaba en el aire era clara: **¿cómo garantizar la seguridad energética sin depender de un mercado tan volátil?** Las respuestas, aunque fragmentadas, apuntaban a una combinación de diversificación de fuentes y aumento de reservas estratégicas.

Los medios de comunicación, con su cobertura constante, transformaron aquel momento en una narración casi apocalíptica: «el petróleo vuelve a ser arma geopolítica», se leía en titulares que llamaban a la acción y al cambio. En las redes, los expertos energéticos compartían gráficos que mostraban la correlación entre el conflicto militar y la escalada del Brent, y recordaban a los lectores que el mercado no era una entidad abstracta, sino un reflejo directo de las decisiones de los estados.

Aquella escena de incertidumbre y presión fijó el telón de fondo de una era nueva, en la que la oferta de petróleo ya no sería el factor limitante. Lo que había cambiado era la **demanda**: todavía creciente, pero cada vez más influida por las tensiones geopolíticas y por la urgencia de encontrar alternativas. La visión que Paul Roberts, autor de *The End of Oil* (2004), había ofrecido sobre el agotamiento del petróleo empezaba a mostrarse incompleta; el verdadero reto ya no era encontrar el último depósito de oro negro, sino gestionar una demanda volátil en un mundo que se reconfiguraba con cada nueva crisis.

El choque de 2022 y la seguridad energética

Aquella mañana de Bruselas no fue un episodio aislado: fue la señal de un choque que resonaría durante toda la década. Pocos días habían pasado desde la invasión de Rusia a Ucrania, en febrero de 2022, y el

Brent tocaba el nivel más alto en más de una década [1]. La subida no solo reflejaba la interrupción inmediata de los flujos de crudo ruso: revelaba una dependencia estructural que muchos países habían ignorado durante décadas.

Los «petroestados» —así se conoce a los países que dependen de las exportaciones de petróleo para su balanza comercial— vieron de golpe cómo su peso geopolítico volvía a primer plano. Arabia Saudí y los demás miembros de la OPEP+ gestionaban la oferta con recortes coordinados de la producción para intentar sostener un mercado que se mostraba cada vez más frágil [1]. Pero a partir de septiembre de 2025 la organización empezó a deshacer aquellos recortes: la presión a la baja sobre los precios ya no justificaba mantener el crudo fuera del mercado. El Brent se situaba entonces en torno a los 67 $ por barril, una caída drástica respecto al pico de tres años antes [1].

Mientras la oferta recuperaba el equilibrio, el choque se trasladaba a otro terreno: la geopolítica. Los países que tradicionalmente habían importado gran parte de su petróleo de Rusia tuvieron que buscar alternativas en un mercado en el que las rutas comerciales se reconfiguraban a ritmo vertiginoso. El crudo ruso encontró nuevos destinos: algunos flujos se redirigieron hacia Asia, a menudo a través de contratos con precios volátiles que alimentaban una incertidumbre propagada por todas las cadenas de suministro.

En paralelo, la producción interior de Estados Unidos alcanzaba récords históricos. El auge no venía de ninguna plataforma marina, sino de tierra adentro: la cuenca del Pérmico, en el suroeste del país, se había convertido en el motor de una oferta global que ya no dependía exclusivamente de los países de la OPEP+ [2]. Esta abundancia reducía la presión sobre las reservas estratégicas y daba a las naciones cierto margen de maniobra para afrontar la volatilidad del mercado. El riesgo ya no era el agotamiento de los depósitos, sino la incapacidad de adaptarse a fluctuaciones bruscas de la demanda.

Y era precisamente la demanda la que marcaba el nuevo horizonte. Las proyecciones apuntaban a una estabilización del consumo mundial en torno a los **105 millones de barriles diarios** para 2030, antes de entrar en declive a medida que avancen la eficiencia energética y el vehículo eléctrico [3]. Era el **pico de demanda**: aunque la producción pudiera aumentar, la necesidad mundial de petróleo dejaría de crecer sin freno. El temor de Roberts —que el mundo se enfrentaría a una crisis de oferta— había evolucionado hacia una angustia diferente: el exceso de dependencia geopolítica y la incertidumbre de una demanda que sube y baja como una ola.

Así, el choque de 2022 no solo demostró que el petróleo todavía es un recurso crítico: reveló las fracturas de un sistema basado en flujos de poder e influencia. La clave de la seguridad energética ya no reside únicamente en asegurar reservas, sino en construir una red resiliente capaz de absorber choques geopolíticos, diversificar fuentes y gestionar una demanda cada vez más volátil.

La abundancia inesperada

Mientras los escenarios de Roberts dibujaban un futuro dominado por el agotamiento de los campos tradicionales —el famoso «último petróleo fácil»—, en 2023 y 2024 Estados Unidos superaba cualquier récord anterior de producción de crudo. El epicentro era aquel motor tierra adentro, la cuenca del Pérmico, donde una oleada de perforaciones y de expansión de infraestructura llevó al país más allá de lo que ningún analista de la época habría podido predecir. El incremento se debía sobre todo a los avances tecnológicos en la fracturación hidráulica y a unos costes de extracción que, aunque elevados, se mantenían viables a aquellos precios [2].

Paralelamente, la OPEP+ ha adoptado una estrategia de gestión activa de la oferta que contradice la narrativa de un declive inexorable: al deshacer progresivamente los recortes de los años anteriores, devolvía crudo a un mercado que había que estabilizar ante la caída del precio del Brent. El largo descenso desde el pico de marzo de 2022 no refleja solo una oferta más abundante, sino también la capacidad de los actores globales de ajustar sus políticas y evitar los huecos de suministro que habían alimentado las expectativas del **pico de oferta** («peak oil»).

Esta nueva realidad pone en cuestión el paradigma central del libro de Roberts: la oferta no es el cuello de botella. La abundancia de la producción norteamericana ha generado un excedente que, aunque costoso de explotar —las reservas del esquisto requieren tecnologías avanzadas e inversión continuada—, ha mantenido los precios en niveles asequibles para la economía mundial. Esto no quiere decir que el petróleo sea una solución permanente; al contrario, su abundancia actual se muestra como un **recurso temporal** que se puede explotar mientras las estructuras energéticas evolucionan hacia alternativas más limpias y descentralizadas.

El desafío, ahora, es gestionar la volatilidad de la demanda. Con el consumo mundial cerca del techo, aquel pico de demanda previsto para 2030, la presión sobre el mercado ya no viene de la falta de oferta, sino de la incertidumbre geopolítica —conflictos regionales, sanciones económicas y tensiones entre grandes productores— que puede alterar bruscamente los flujos comerciales. En este nuevo escenario, la seguridad energética depende más que nunca de la capacidad de adaptarse rápidamente a cambios inesperados, tanto en la oferta como en la demanda.

El «último petróleo fácil», pues, no se ha agotado; ha resurgido en forma de una oferta norteamericana robusta y de una gestión dinámica de la OPEP+. Pero esta abundancia es un arma de doble filo: abre la oportunidad de reducir la dependencia de fuentes inestables y, a la vez, amplifica la necesidad de mecanismos de regulación y diversificación que puedan absorber las futuras sacudidas del mercado. La clave sigue siendo aquella red resiliente: encarar tanto la soberanía de la oferta como la incertidumbre de la demanda.

Roberts tenía razón... y no

Volvamos por un momento a marzo de 2022. Mientras el Brent tocaba su pico [1], el eco de un pico de oferta inminente resonaba en las salas de conferencias y en los foros en línea. La llamada profecía de Roberts —que el mundo se enfrentaría a una escasez inevitable de petróleo que forzaría una crisis energética profunda— parecía grabada en piedra. Pero el mercado, como un río que cambia de curso, encontró caminos inesperados para esquivar aquella catástrofe.

Los caminos ya los hemos recorrido: el giro de la OPEP+, que devolvió crudo al mercado, y los récords de producción del Pérmico, más allá de las proyecciones del sector [1][2]. El resultado fue un precio notablemente inferior a las expectativas de muchos analistas, y un aumento inesperado de oferta que desactivó el alarmismo sobre un agotamiento inminente.

Pero la verdadera transformación no proviene tanto de la cantidad disponible como de **quién la consume**. Aquel techo de consumo previsto para el final de la década —fruto de la eficiencia energética y de la proliferación de los vehículos eléctricos— redefine por completo el paradigma: ya no se trata tanto de «cuánto queda», sino de «cuánto querremos». La presión sobre las infraestructuras tradicionales —refinerías, terminales de almacenamiento y redes de transporte— cambia de naturaleza a medida que la demanda se transforma.

El nuevo paradigma plantea una doble encrucijada. Por un lado, la abundancia de oferta da margen para mitigar los efectos de los conflictos geopolíticos que tradicionalmente han sacudido el mercado del petróleo. Por otro, puede fomentar una **volatilidad de precios** aún más pronunciada: las fluctuaciones de la demanda —impulsadas por políticas climáticas, cambios regulatorios y avances tecnológicos— pueden provocar ciclos de exceso y escasez a corto plazo.

El reto, por tanto, vuelve a ser aquella red resiliente que absorba las sacudidas: diversificar las fuentes —con las renovables y el resto de alternativas limpias— y desarrollar mecanismos de regulación que se ajusten a las variaciones de la demanda. El pico de oferta queda atrás; el pico que cuenta es el de demanda, aquel ante el que la sociedad ha de decidir cómo responder. Y elegir el camino está, ahora, en nuestras manos.

La promesa y el peligro

El exceso de oferta que el esquisto norteamericano —con los nuevos campos del Pérmico— y el ajuste de la OPEP+ han generado a partir de 2023 transforma el panorama energético en una oportunidad sin precedentes. La abundancia de crudo es ahora un amortiguador que puede reducir la presión sobre las balanzas comerciales y, al mismo tiempo, favorecer la flexibilidad de los precios. Cuando el Brent tocó el pico, parecía que el mundo se enfrentaría a una espiral incontrolable; tres años después, el retorno del crudo de la OPEP+ al mercado y la producción récord norteamericana han hecho bajar el precio y mantienen una oferta que supera las expectativas iniciales [1][2].

Esta abundancia crea un margen de actuación para los gobiernos y las empresas: la necesidad urgente de reducir las emisiones se puede abordar sin la amenaza inmediata de una escasez energética. La diversificación de fuentes, incluyendo gas natural y renovables, reduce el «chantaje» que tradicionalmente han ejercido los petroestados sobre las economías emergentes. La presión por mantener una producción

constante se debilita, y abre espacio para que las políticas climáticas avancen sin temer un desbordamiento de precios ni una crisis de abastecimiento.

Sin embargo, el mismo excedente comporta riesgos que hay que gestionar con rigor. La volatilidad de los precios, alimentada por la incertidumbre geopolítica y las fluctuaciones de la demanda, puede desencadenar oleadas de caídas bruscas que erosionen los ingresos de los países exportadores y desestabilicen mercados emergentes que dependen del petróleo. Además, la percepción de un mercado abundante amplifica el atractivo de invertir en proyectos de extracción a largo plazo; pero estos activos corren el peligro de quedar **varados** (stranded assets) si las políticas climáticas se intensifican o si la demanda se frena una vez alcanzado su techo, hacia 2030 [3].

Por abundante que sea, el combustible sigue siendo fósil, y la dependencia mantiene las economías vinculadas a una transición que todavía no se ha completado. Cada inversión en infraestructura petrolera nueva aumenta la inercia del sistema energético y dificulta la migración hacia fuentes limpias. Así, el peligro se manifiesta tanto en el aumento de los costes de adaptación futura como en la posible creación de un excedente que provoque caídas de precios abruptas y genere incertidumbre económica y social.

En un platillo de la balanza, pues, una ventana de oportunidad para políticas climáticas más agresivas y para una diversificación energética que reduzca la influencia de los petroestados. En el otro, una nueva forma de inestabilidad: precios volátiles, inversiones mal alineadas y una dependencia prolongada del petróleo que podría convertir los activos fósiles en cargas económicas. Aprovechar la promesa y mitigar el peligro exige una planificación coordinada, que tome las decisiones de inversión con plena conciencia de los riesgos del mercado y del calendario de la transición.

Cuánto queremos quemar

Si la oferta ya no es el cuello de botella, la pregunta cambia de lugar. El petróleo ha superado las expectativas más optimistas de hace una década; los campos de esquisto y las decisiones coordinadas de la OPEP+ han mantenido la oferta en niveles que, hasta ahora, solo se veían en escenarios de «boom» [1]. Pero este excedente no es ninguna garantía de tranquilidad: el peligro ha mutado hacia la demanda, impulsado por una economía global cada vez más electrificada y por tensiones geopolíticas que hacen fluctuar los precios en cuestión de horas.

El temor de Roberts era que se nos acabara el petróleo. Lo que hemos descubierto es casi lo contrario: tenemos de sobra, y el reto ya no es arrancar la última gota, sino decidir cuánto queremos quemar. La transición hacia las renovables y el vehículo eléctrico avanza, pero la oferta fósil abundante y barata es, a la vez, el amortiguador que nos da tiempo y la tentación que puede frenarla.

Y aquí se abre el terreno del capítulo siguiente. Si el petróleo deja de ser el factor limitante, el centro de gravedad se desplaza hacia las fuentes que han de sustituirlo —las renovables, las baterías, el vehículo eléctrico— y hacia la red que ha de sostenerlas. La seguridad energética del futuro no se medirá solo en barriles, sino en la capacidad de hacer fiables, accesibles y resilientes las alternativas limpias. Esta es la frontera que exploraremos a continuación.

---

[1] EIA/IEA, *precios del Brent y OPEP+ (2022-2025)*. https://www.eia.gov/todayinenergy/detail.php?id=55020 ↩

[2] AIE, *Oil Market Report (sept. 2025) — esquisto EE. UU.*. https://www.iea.org/reports/oil-market-report-september-2025 ↩

[3] AIE, *Oil 2025 — Executive summary (pico de demanda)*. https://www.iea.org/reports/oil-2025/executive-summary ↩

El futuro ya está aquí: renovables, baterías y vehículo eléctrico

«El futuro ya está aquí — solo que no está repartido de manera uniforme.»

— William Gibson (documentado desde 1992)

Con la primera luz del día, el horizonte del desierto de Mojave se transforma en una llanura de oro líquido. Unos cientos de paneles fotovoltaicos se alzan como filigranas de plata que capturan el sol naciente y lo convierten de inmediato en electricidad. Unos kilómetros más abajo, la pantalla de un panel de control muestra números verdes que caen: 0,043 $/kWh. El precio es tan bajo que bate cualquier oferta de una central de gas natural o de carbón, y la subasta de energía solar termina con una ronda de aplausos contenidos pero contundentes. Los inversores, habitualmente reservados ante las nuevas tecnologías, echan un vistazo a las cifras y sonríen: el sol acaba de ganar la partida del precio al gas y al carbón [1].

Mientras el sol calienta las placas de silicio, en la ciudad cercana se despliega una escena que hace unas décadas solo existía en el optimismo futurista. Un aparcamiento subterráneo, iluminado por luces LED azules, está lleno de vehículos eléctricos que se cargan en fila ordenada durante la noche. El sonido suave de los ventiladores de refrigeración y los pings periódicos de los sistemas de gestión de energía son el único eco que rompe el silencio del desierto. Cada coche, con una batería de química LFP cada año más barata, recibe su dosis de electricidad fresca sin ningún rastro de combustión [2].

A estos vehículos no los alimenta solo la energía más limpia: detrás hay una infraestructura que ha crecido como una red nerviosa, con microrredes locales que equilibran la producción solar con el consumo instantáneo, sistemas avanzados de gestión de almacenamiento y plataformas digitales que optimizan cada kilovatio-hora. En la pantalla central del parque, un gráfico muestra en tiempo real cómo las baterías comunitarias absorben el exceso de generación de las horas de máximo sol y lo liberan cuando el sol se retira.

Por el lugar pasan ingenieros, conductores e inversores. Una joven ingeniera del departamento de energía dice: «Hace cinco años, la idea de conducir un coche cargado por completo con energía solar era casi un sueño; hoy, más del 20 % de los coches nuevos son eléctricos y ya se vendieron más de 17 millones en un solo año a escala global» [2]. Un agricultor local, que usa la electricidad del propio campo para el riego, añade: «Los costes de la energía solar nos han permitido reducir los gastos operativos e invertir en más cultivos».

Esta escena no es una proyección futurista; es el presente palpable de un mundo donde las renovables ya son la opción económica dominante y el vehículo eléctrico, un producto de masas. Pero, como advierte la historia que Paul Roberts narró en *The End of Oil* (2004), este avance comporta cuellos de botella que todavía hay que resolver: redes que han de escalar sin perder estabilidad, almacenamiento masivo que necesita minerales críticos y una logística global para las baterías. El futuro ha llegado; que se consolide dependerá de cómo afrontemos estos retos.

La promesa cumplida

Hace una década, este panorama parecía un sueño de ciencia ficción: paneles fotovoltaicos extendidos como campos de oro sobre los desiertos, turbinas eólicas balanceándose al ritmo del viento —y todo ello todavía más caro que una central de carbón. Hoy el relato se ha invertido. El coste normalizado de la electricidad (LCOE) de los sistemas solares ha caído un 90 % entre 2010 y 2024, hasta los 0,043 $ por kWh que lucían en verde en la pantalla del Mojave [1]: una cifra que hace la luz del sol más barata que la electricidad fósil en casi cualquier mercado desarrollado. Este descenso vertiginoso no es solo una tendencia estadística; es el resultado combinado de tecnologías mejoradas, economías de escala y políticas públicas que han impulsado el despliegue masivo de la fotovoltaica en todo el mundo.

2024 marcó, además, un punto de inflexión histórico: el 91 % de la nueva capacidad renovable añadida aquel año fue más económica que cualquier planta fósil nueva. Esta mayoría no refleja solo la caída del coste de producción: también pesan la eficiencia operativa creciente y la inversión en redes inteligentes que maximizan el aprovechamiento de recursos intermitentes como el sol y el viento. Las empresas energéticas han adoptado modelos de financiación basados en bonos verdes, que reducen los costes de capital y aceleran la construcción de infraestructuras renovables.

A escala global, la convergencia de estos factores ha reconfigurado el mercado: las centrales de gas natural, hasta hace poco consideradas el puente transitorio hacia un futuro limpio, se ven ahora superadas en competitividad económica por las instalaciones solares y eólicas. La caída del LCOE solar ha desatado una «fiebre del oro» entre los desarrolladores, que corren a aprovechar la diferencia de costes antes de que cambien las regulaciones o se ajusten los precios de las materias primas.

Esta transformación, sin embargo, no es una simple cuestión de números; es una revolución en la manera en que la sociedad produce y consume energía. Las comunidades rurales de África y América Latina, que antes dependían de una infraestructura eléctrica limitada o inexistente, ahora pueden acceder a electricidad fiable gracias a microrredes solares de coste ultrabajo. En Europa, las políticas de «tarifas netas» incentivan a los consumidores a instalar paneles en el tejado de sus hogares, y convierten cada vivienda en un pequeño productor de energía.

La misma ola ha llegado al transporte. Con la electricidad más barata y abundante, el coste operativo de los vehículos eléctricos ha caído drásticamente, y la adopción masiva se ha convertido en una cuestión de rentabilidad tanto como de conciencia ambiental. La reducción del LCOE solar se traduce directamente en electricidad de carga más barata, y esto refuerza el círculo virtuoso entre energía limpia y movilidad sostenible.

La promesa que Roberts solo podía imaginar con una dosis de escepticismo se ha materializado: las renovables son ahora la opción más barata y tecnológicamente madura, y abren la puerta a un futuro con una dependencia de los combustibles fósiles sustancialmente menor. La base económica es sólida; el sistema que ha de sostenerla —infraestructura, almacenamiento, gestión de los recursos críticos— todavía no lo es.

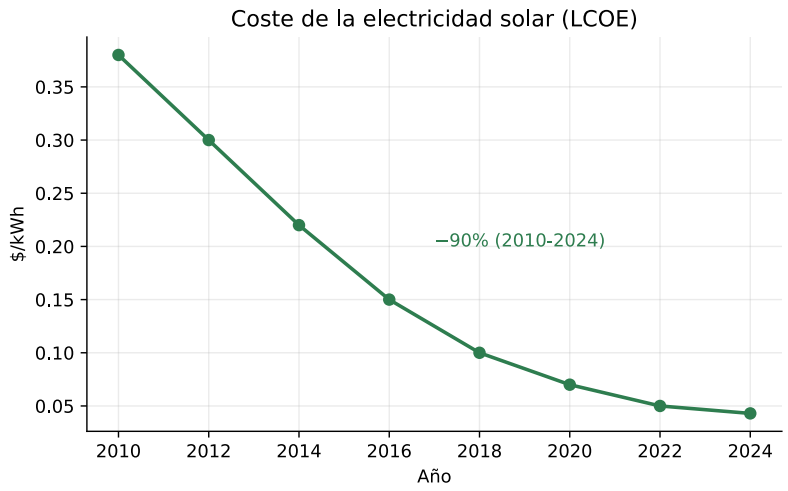


Figura 4.1 — El coste de la electricidad solar cayó cerca de un 90 % entre 2010 y 2024: la transformación de precio más rápida de la historia de la energía.

Baterías y vehículo eléctrico

Después de una década de promesas y dudas, el vehículo eléctrico (VE) ha dejado de ser una curiosidad de laboratorio para convertirse en la corriente principal del mercado. En 2024 se vendieron más de **17 millones** en todo el mundo, **más del 20 % de los coches nuevos** que llegaron a los concesionarios aquel año [2]. La cifra no solo supera cualquier proyección realista hecha hace una década; confirma, sobre todo, que la movilidad limpia ya no es cosa de una minoría entusiasta. Y la tendencia se acelera: para 2025 se proyectan alrededor de 22 millones [2].

Detrás de este salto hay una revolución silenciosa pero fundamental: las baterías. El coste del kilovatio-hora (kWh) de las celdas de iones de litio ha caído a **115 $ por kWh en 2024**, con una proyección de **108 $ por kWh en 2025**: la misma curva descendente que hundió el coste del solar durante los últimos quince años [2]. La tendencia no es ningún accidente, sino la suma de economías de escala en las fábricas de celdas, mejoras en la cadena de suministro de materiales y la adopción creciente de una química más asequible —el fosfato de hierro y litio (LFP)— que ha ganado terreno tanto en vehículos de gama media como en modelos premium.

El auge del LFP es especialmente revelador. A diferencia de las baterías de níquel-cobalto-manganeso, el LFP no depende del cobalto, un mineral con problemas éticos y logísticos que ha encallado la cadena de suministro en varias regiones de África y Asia. Que los packs de baterías fabricados en China hayan bajado hasta los **84 $ por kWh** en líneas de producción masiva ha reducido la presión sobre los precios de los materiales críticos y ha facilitado una expansión más rápida del parque de vehículos. Además, el LFP ofrece una vida útil larga y más seguridad térmica, dos argumentos que han convencido a cada vez más fabricantes de incorporarlo en modelos de alta demanda [2].

Ahora bien, la caída del coste no elimina del todo los cuellos de botella. La producción global de baterías todavía depende en gran medida del litio y del manganeso, dos recursos concentrados geográficamente y que exigen una gestión ambiental rigurosa. Con las ventas de VE al ritmo actual, la demanda de estos minerales presiona unas minas y unos procesos de extracción que todavía no se han optimizado del todo [2].

La infraestructura de recarga, además, se encuentra en plena transición. Aunque las redes de carga rápida se han expandido con fuerza, el reparto sigue siendo desigual: las zonas rurales y algunas regiones de la Europa oriental todavía sufren escasez de estaciones de alta potencia. Este desequilibrio limita la confianza de los consumidores e impide aprovechar todo el potencial de las baterías baratas.

El vehículo eléctrico está, pues, a las puertas de una era en la que la energía para el transporte es tan asequible como la que genera el sol. Las baterías, al reducir drásticamente los costes, han impulsado una adopción masiva y han abierto la puerta a un modelo de movilidad más limpio y sostenible. Pero el camino hacia la consolidación completa todavía choca con obstáculos estructurales: la necesidad de una cadena de suministro de materiales críticos más resiliente y de una red de recarga que llegue a todos los rincones del territorio. Superarlos será el último paso para que la promesa de las renovables y el VE se traduzca en una realidad universal.

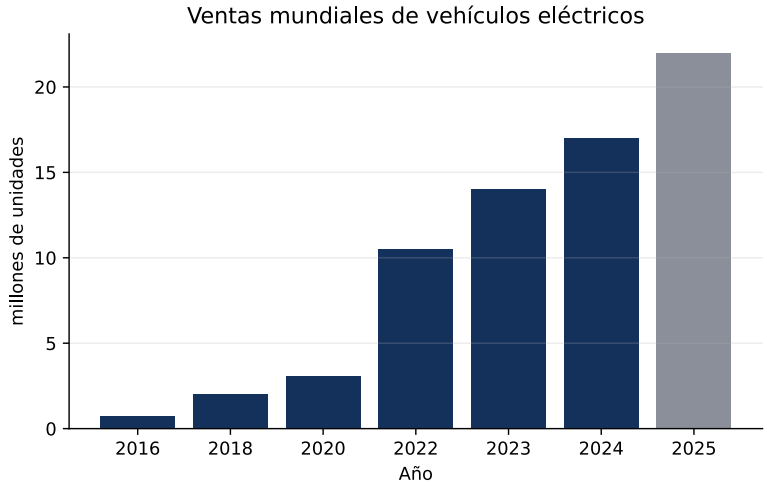


Figura 4.2 — Las ventas de vehículos eléctricos superan los 17 millones en 2024 y ya son más de uno de cada cinco coches nuevos.

Lo que todavía falta

La generación barata, pues, ya la tenemos. Pero la apariencia de abundancia esconde una realidad mucho más compleja: la electricidad económica no se traduce automáticamente en un sistema completo y fiable. Entre el panel que produce a precio de récord y el enchufe que no falla nunca hay tres cuellos de botella.

El primero son las redes eléctricas. Las infraestructuras de transmisión y distribución se diseñaron para flujos constantes y previsibles, los característicos de las centrales de energía convencional. Ahora, con la proliferación de una generación descentralizada y altamente intermitente —el sol brilla solo durante el día y el viento sopla en momentos imprevisibles—, las redes han de poder ajustar la potencia en tiempo real. Esto requiere inversiones masivas en sistemas de gestión inteligente, sensores IoT y algoritmos avanzados basados en IA que equilibren oferta y demanda sin interrupciones. Sin esta modernización, las zonas con alta concentración de renovables pueden sufrir sobrecargas o cortes de suministro que minan la confianza de consumidores y empresas.

El almacenamiento a gran escala es el segundo. Las baterías son la herramienta clave para suavizar la intermitencia, y sus precios caen, como acabamos de ver; pero la necesidad de instalar cientos de gigavatios-hora de capacidad de almacenamiento en el mundo supera con creces las inversiones actuales [2]. Sin suficiente almacenamiento, el exceso de producción solar o eólica se pierde, y la red sigue dependiendo de fuentes convencionales para garantizar la continuidad del suministro.

El tercer reto es la dependencia de los minerales críticos. Las baterías, los inversores fotovoltaicos y muchos componentes electrónicos requieren cobalto, litio, níquel y tierras raras, y la demanda de estos materiales se ha disparado con el aumento de los VE y la construcción de infraestructuras de almacenamiento [2]. Las cadenas de suministro son vulnerables a tensiones geopolíticas y a prácticas mineras que a menudo no cumplen estándares ambientales ni sociales. Sin una estrategia clara para diversificar fuentes, reciclar materiales y desarrollar alternativas menos dependientes, el crecimiento sostenible queda ligado a la disponibilidad de estos recursos.

Tres frentes, pues: redes inteligentes y resilientes, almacenamiento masivo y asequible, y una cadena de suministro de minerales críticos que sea sostenible. Superarlos requerirá coordinación entre gobiernos, empresas y comunidad científica, e inversiones dirigidas a tecnologías emergentes capaces de transformar estas limitaciones en oportunidades para consolidar el futuro energético limpio.

La promesa y el peligro

2024 se cerró, pues, con un hito que solo unos pocos analistas habían podido prever: por primera vez desde la Revolución Industrial, la energía limpia es más barata que la sucia. No es ningún fenómeno marginal, sino una transformación estructural, y la combinación de una energía cada vez más asequible con un parque automovilístico que se electrifica ha desencadenado una espiral positiva: la demanda de generación limpia aumenta, el precio de las tecnologías asociadas cae y la aceptación social se consolida.

La nueva dinámica sacude las viejas estructuras basadas en los combustibles fósiles. Los grandes consumidores —desde la industria pesada hasta las ciudades inteligentes— pueden planificar el futuro energético sin la presión constante del precio del petróleo o del gas natural. Las empresas de energía, que hace una década dependían de contratos a largo plazo con proveedores de combustibles, compiten ahora en eficiencia y en capacidad de integrar fuentes intermitentes como el sol y el viento. La promesa, pues, no es solo económica; es una redefinición del poder geopolítico, porque las naciones que tradicionalmente controlaban los recursos fósiles ven erosionada su influencia.

Esta época de optimismo, sin embargo, vive a la sombra de los tres cuellos de botella que ya conocemos, y que amenazan con frenar su avance. Primero, las redes eléctricas —construidas hace décadas para transportar energía centralizada y constante— no están preparadas para gestionar flujos masivos y variables de origen distribuido. Las limitaciones en la capacidad de transmisión y en los sistemas de control inteligente generan congestiones que, en el peor de los casos, obligan a curtailments (reducciones forzosas de suministro) aunque la producción renovable sea abundante.

Segundo, el almacenamiento todavía no llega a la escala ni al coste necesarios para equilibrar del todo las fuentes intermitentes. Pese a la caída de precios que hemos visto, el coste sigue siendo un factor limitante para aplicaciones a gran escala como los sistemas de almacenamiento estacionario o las flotas de vehículos comerciales electrificados. La necesidad de tecnologías complementarias —como el flujo de potencia en redes híbridas y las baterías LFP de ciclos de vida más largos— es urgente, pero su adopción requiere inversiones masivas y una cadena de suministro robusta.

Finalmente, la dependencia creciente de los minerales críticos —litio, cobalto, níquel y otros elementos esenciales para las baterías avanzadas— concentra el riesgo geopolítico en pocas regiones productoras. Sin una diversificación real de las fuentes y un marco regulador que garantice prácticas sostenibles, la cadena de suministro se convierte en una vulnerabilidad estructural que pueden explotar actores con intereses contrarios a la transición limpia.

La promesa, pues, ya se ha materializado, y el crecimiento renovable avanza inexorablemente; pero si las barreras de redes, almacenamiento y minerales no se superan, esta época de optimismo puede transformarse en una nueva era de dependencia concentrada. Desactivar estos riesgos —hacer que la transición no solo sea posible, sino también resiliente y equitativa— es el trabajo que queda.

El poder detrás de los paneles

La tecnología ya no es el problema; el poder, sí. Los datos de este capítulo son irrefutables y apuntan todos en la misma dirección: el sol más barato que cualquier fósil, más de uno de cada cinco coches nuevos ya eléctrico, baterías que pierden precio año tras año. La economía ha dado el paso decisivo hacia la energía limpia.

Pero detrás de estas victorias tecnológicas se esconde una red de relaciones de poder que nadie ha desafiado todavía. Las cadenas de suministro de minerales críticos —cobalto, litio y níquel— se concentran en un número reducido de países y empresas multinacionales. China domina buena parte de esta cadena: controla alrededor del 75 % de la fabricación mundial de baterías y cerca del 91 % del refinado de tierras raras. Esta concentración convierte los recursos esenciales en palancas de negociación, y permite a unos pocos actores dictar precios y condiciones de entrega.

Además, la infraestructura de redes eléctricas todavía se basa en modelos centralizados que dependen de inversores tradicionales y de operadores de gran escala. La falta de estandarización en las tecnologías de almacenamiento impide una integración fluida de los recursos distribuidos y deja las regiones más expuestas a interrupciones y a la manipulación del flujo energético. En este escenario, el control de las redes no es solo un tema técnico; es una cuestión de autonomía nacional y de soberanía económica.

La geopolítica que se despliega en torno al nuevo paradigma energético sigue la misma lógica que la del petróleo hace medio siglo: quien controla la fuente controla las economías y, por extensión, los sistemas políticos. Pero, a diferencia del pasado, ahora tenemos herramientas digitales —blockchain, IA avanzada y contratos inteligentes— que pueden deshacer esta concentración de poder. La clave será crear plataformas abiertas y transparentes que permitan el seguimiento en tiempo real de los flujos de minerales, la certificación de origen y la gestión descentralizada de las redes.

En el próximo capítulo analizaremos cómo desplegar estas soluciones a escala global, qué actores han de emerger como guardianes del nuevo ecosistema energético y cómo evitar que una nueva élite energética se consolide sobre la base de una infraestructura tecnológica ya probada. La transición no depende solo de la reducción de los costes o de la adopción masiva de los VE; depende, en última instancia, de quién decide qué parte del valor generado por las renovables se ha de redistribuir y cómo se regula ese flujo. En la pantalla del Mojave, los números verdes seguirán cayendo. El futuro ya está aquí; su beneficio, todavía, ha de equilibrarse entre todos los protagonistas.

---

[1] IRENA / Wood Mackenzie, *LCOE renovable 2024-2025.* https://www.pv-magazine.com/2025/07/23/global-average-solar-lcoe-stood-at-0-043-kwh-in-2024-says-irena/ ↩

[2] BloombergNEF / AIE, *Global EV Outlook 2025 y precios de baterías.* https://www.iea.org/reports/global-ev-outlook-2025/electric-vehicle-batteries ↩

La energía es poder

«El comunismo es el poder soviético más la electrificación de todo el país.»

— V. I. Lenin, discurso en Moscú (1920)

Octubre de 2025. En una sala de reuniones de un complejo de alta tecnología de Pekín, el sol de invierno se filtra por el cristal polarizado y dibuja líneas de luz sobre una mesa ovalada cubierta de mapas digitales, gráficos de flujo y muestras de polvo metálico. En el panel central, un gran monitor sigue en tiempo real la cadencia de los envíos de neodimio y de otras tierras raras.

Ante la pantalla, un grupo de representantes occidentales —directivos de la automoción europea, inversores norteamericanos en baterías, un delegado del Ministerio español de Energía— observa con una mezcla de incredulidad e inquietud. Al otro lado, con la cara seria y los ojos fijos en los datos que se despliegan, el portavoz del Ministerio de Comercio chino suelta la frase que lo cambia todo: «A partir de hoy, el Gobierno chino impone restricciones estrictas a la exportación de todo componente relacionado con las cadenas de suministro limpias: paneles fotovoltaicos, turbinas eólicas, baterías de iones de litio y, por encima de todo, las tierras raras que son la columna vertebral de cada vehículo eléctrico, de cada instalación de almacenamiento de energía y del hardware que hace funcionar la inteligencia artificial.»

Un silbido anuncia una alerta nueva en el sistema de seguimiento global. Los gráficos lo dicen sin retórica: la cuota china en la producción mundial de paneles solares ya supera el 80 %; la de los aerogeneradores, el 60 %; la de los vehículos eléctricos (VE), el 70 %. Las baterías que alimentan estas máquinas se fabrican en China casi en su totalidad —un 75 %—, y el refinado de las tierras raras, el cuello de botella de todo ello, se concentra allí en un 91 % [1]. Y ahora este dominio se extiende, por decreto, a todos los componentes intermedios que convierten la materia prima en producto acabado.

Los representantes se miran entre ellos. No es un embargo de petróleo como los que sacudieron las economías el siglo pasado; es otra clase de asedio económico, una «guerra fría» del acceso: a la materia prima y al conocimiento tecnológico limpio. Un arma de negociación capaz de desestabilizar las cadenas de suministro de Europa, de América del Norte e incluso de países emergentes como la India. Mientras el monitor muestra la caída instantánea de los envíos hacia las empresas europeas —en 2024, casi la mitad de las exportaciones limpias chinas, un 47 %, había ido al Sur Global, y ahora cada destino depende de una decisión tomada en esta sala [2]—, el portavoz concluye: «El mundo cambiará la manera en que produce energía. Quien no se adapte a una nueva arquitectura basada en recursos limpios controlados por nosotros quedará fuera del juego.»

Los occidentales recogen los papeles en un silencio espeso. La energía sigue siendo poder, pero el mapa del poder se ha redibujado de arriba abajo. Este capítulo explica cómo ha ocurrido, y qué hay en juego.

Del petróleo a los minerales

En el relato que el periodista Paul Roberts tejió en *The End of Oil* (2004), el petróleo era el hilo conductor de una jerarquía mundial: las naciones con grandes reservas definían rutas comerciales, dictaban precios y modelaban el orden geopolítico. En poco más de dos décadas, aquel orden ha sufrido una metamorfosis profunda. Hoy el poder ya no se mide por la cantidad de crudo que duerme bajo tierra, sino por quién controla las cadenas de suministro limpias: paneles fotovoltaicos, baterías de alta capacidad y minerales críticos.

El epicentro de esta arquitectura nueva es China, y su dominio no es solo cuantitativo. Concentrar la fabricación —las cuotas que acabamos de ver en el monitor de Pekín— le da también el control de las especificaciones técnicas y de los estándares de calidad: la mayor parte de los proyectos solares de Europa, de América del Norte y de África dependen de elementos fabricados en el continente asiático, y cada VE, cada instalación de almacenamiento y cada dispositivo móvil lleva dentro baterías salidas de fábricas chinas. Esto convierte al país en el proveedor indispensable del sector energético limpio.

Pero el monopolio más profundo no es el de las fábricas: es el del **procesamiento**. Refinar cerca del 91 % de las tierras raras del mundo —los elementos esenciales para imanes potentes, catalizadores, sensores y electrónica avanzada— significa que cualquier interrupción de las exportaciones puede paralizar la cadena global de equipos de alta tecnología [1]. No hace falta controlar la extracción si controlas el paso que la convierte en material útil. La decisión de octubre de 2025 de ampliar los controles de exportación

encendió las alarmas en Washington y en Bruselas precisamente por esto, y ambas capitales buscan ahora alternativas para reducir su vulnerabilidad.

La inversión de la dinámica de poder es completa, y plantea un doble escenario. Por un lado, la proliferación de tecnologías limpias ofrece una oportunidad única para recortar las emisiones globales y deshacer los lazos con el petróleo. Por otro, la concentración de estas tecnologías en manos de un solo actor crea vulnerabilidades nuevas: un bloqueo o una restricción comercial puede provocar escasez de componentes críticos y afectarlo todo, desde la movilidad urbana hasta las redes eléctricas interconectadas. Las naciones que antes negociaban con petroestados ahora negocian con una potencia que no les vende la energía, sino las máquinas que la convierten —y que hace, a la vez, de guardiana de los materiales imprescindibles para el futuro. La pregunta ya no es solo quién tiene petróleo, sino quién controla los flujos de energía y de materiales que alimentan la transición hacia un mundo limpio.

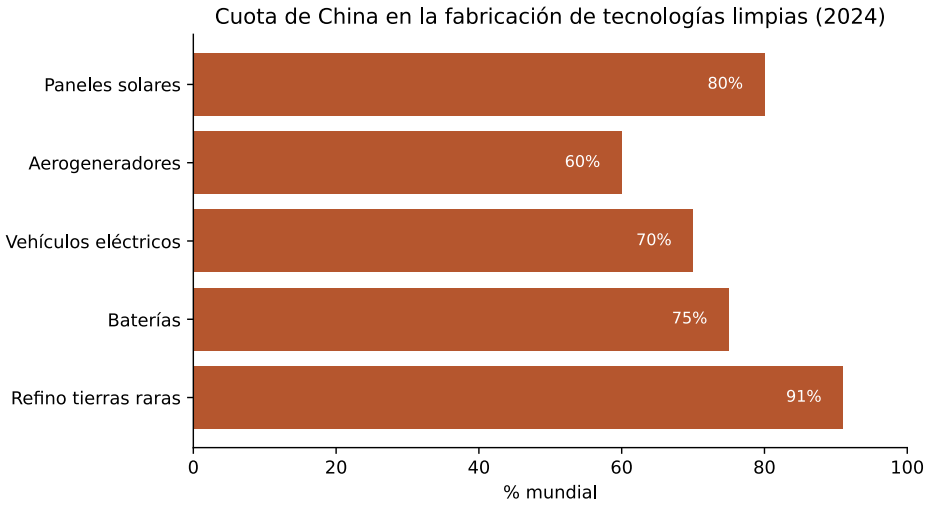


Figura 5.1 — China domina la fabricación de la transición: del 60 % de los aerogeneradores al ~91 % del refinado de tierras raras.

La nueva dependencia

Cuando los petroestados de Oriente Medio dominaban la geopolítica del siglo pasado, una sola región podía dictar las condiciones del mercado energético mundial con la fuerza de un tapón en la fuente. Aquel poder se ha trasladado al noreste asiático, y el grifo ya no es el crudo: son los componentes. En 2024, el 47 % de las exportaciones chinas de VE, baterías, paneles solares y aerogeneradores fue al Sur Global —América Latina, el África subsahariana y el sur de Asia— [2]. No es una cifra cualquiera: es una reconfiguración profunda de las relaciones internacionales, donde la dependencia energética se mezcla con la necesidad crítica de minerales y de componentes electrónicos.

Este dominio no ha caído del cielo: es el fruto de una política industrial agresiva y de inversiones masivas en infraestructura de producción. Y para los países sin alternativas propias se traduce en una vulnerabilidad estructural. La ampliación de los controles de exportación de octubre de 2025 —justificada oficialmente como una medida de seguridad nacional y de protección de los recursos— lo ha dejado claro: la capacidad de imponer límites a la exportación es hoy un arma diplomática tan poderosa como lo fue, hace unas décadas, la presión sobre los flujos petroleros.

Los efectos ya son palpables. Países del Sur Global que habían apostado por la transición verde han visto cómo se encarecían las baterías y se alargaban los plazos de entrega, con retrasos en infraestructuras críticas como las redes de recarga pública y las instalaciones de generación distribuida. Y estos atascos alimentan tensiones políticas: gobiernos que antes dependían del petróleo ahora se ven obligados a renegociar acuerdos comerciales, a buscar alternativas locales o a aliarse con quien impulsa programas de producción propia, como la Unión Europea. El poder de China sobre las cadenas limpias se traduce, pues, en influencia directa sobre las políticas energéticas e industriales de medio mundo.

La nueva dependencia no es una cuestión de cantidad, sino de control. Y la pregunta que se deriva de ello —¿cómo se gestiona esta vulnerabilidad sin sacrificar la transición verde?— exige una respuesta colectiva: diversificar las fuentes, desarrollar capacidades locales y construir marcos reguladores internacionales que

garanticen el acceso equitativo a las tecnologías limpias. La confianza en un futuro sostenible depende de nuestra capacidad de equilibrar dependencia y soberanía energética.

La promesa y el peligro

La promesa es clara: la generación eléctrica renovable puede ser del todo autóctona. Un panel solar en el desierto de Atacama o un aerogenerador en las costas del mar Báltico producen energía que no depende de ninguna ruta marítima ni de ningún canal petrolero. Esto recorta de raíz el «chantaje energético» —la coacción ejercida a través de la dependencia del suministro—, porque cada país puede cubrir gran parte de su consumo con recursos propios. Y la descentralización de la generación —microrredes comunitarias, almacenamiento a escala local, redes inteligentes que gestionan los flujos— ofrece una visibilidad y un control del consumo sin precedentes.

El peligro es la otra cara exacta de la misma moneda. El sol y el viento son inagotables y universales, pero la infraestructura que los convierte en energía utilizable sale, de manera abrumadora, de una sola región del mundo. Esta concentración genera un **punto único de fallo**: una política de exportación restrictiva como la de octubre de 2025, un problema logístico o una crisis de seguridad en las instalaciones pueden paralizar el acceso mundial a tecnologías críticas. Y quien más perdería es quien más confía en ello: el Sur Global, receptor de casi la mitad de las exportaciones limpias chinas [2], podría quedarse sin alternativas viables para su descarbonización mientras las tensiones geopolíticas se disparan.

La salida no es renunciar a la promesa, sino desconcentrarla: invertir en fábricas locales de paneles y baterías, desarrollar capacidad de refinado de tierras raras fuera de China y establecer marcos reguladores internacionales que aseguren el acceso equitativo. Solo así la soberanía energética podrá traducirse en una independencia auténtica.

La lección de Pekín

El poder energético se reconfigura, pero el motor que lo impulsa todo —el clima— no espera. Las cuotas que han ido saliendo a lo largo del capítulo no son estadísticas de mercado: son la infraestructura crítica que determina qué parte del mundo puede acceder a la electricidad limpia, a la descarbonización y, al fin y al cabo, a su propio futuro climático. Para las economías emergentes que quieren sustituir el petróleo que ha alimentado durante décadas su industrialización, la relación con China recuerda las viejas rutas del crudo con un núcleo diferente: minerales críticos y componentes electrónicos [2]. Y para cualquier país que quiera construir capacidad renovable propia, aquel 91 % del refinado de tierras raras concentrado dentro de unas solas fronteras es el recordatorio de que ninguna soberanía energética es completa si depende de una única fuente de suministro [1].

El peligro mayor es la inacción. Cada año que pasa sin diversificar las cadenas aumenta la probabilidad de tensiones geopolíticas, de precios manipulados y, en el peor de los escenarios, de restricciones de acceso a la energía limpia para los países más vulnerables —con una presión reguladora china que puede estrechar aún más el flujo de materiales esenciales [1]. El paso siguiente, en cambio, es conocido: una estrategia coordinada de gobiernos y empresas que combine inversión en infraestructura propia con apertura internacional —centros de investigación conjuntos, acuerdos de cooperación para el desarrollo sostenible de los minerales críticos y una normativa global que proteja los intereses colectivos ante las maniobras unilaterales. Solo así el poder energético podrá estar realmente distribuido, y el clima —el motor invisible pero inexorable de nuestro tiempo— no quedará a la espera de una decisión tardía.

El capítulo siguiente hace balance de esa otra presión, la que no negocia: la emergencia climática de 2026, con fenómenos meteorológicos cada vez más intensos que exigen que las soluciones avancen tan deprisa como cambia el planeta. Los occidentales de aquella sala de Pekín salieron habiendo aprendido la lección del siglo: quien controla la máquina de la transición controla el tiempo de todos. Y el tiempo es, precisamente, lo que se nos acaba. El momento es ahora: **time2act**.

---

[1] AIE / CFR, *dominio chino en minerales y tecnologías limpias (2024-2025).* https://www.iea.org/commentaries/with-new-export-controls-on-critical-minerals-supply-concentration-risks-become-reality ↩

[2] Sightline / análisis, *exportaciones limpias chinas al Sur Global (2024).* https://www.sightlineclimate.com/research/a-tour-of-chinas-electrostate ↩

Demasiado caliente: el clima en 2026

«El "control de la naturaleza" es una frase concebida con arrogancia, nacida de la edad de Neandertal de la biología y la filosofía, cuando se suponía que la naturaleza existe para conveniencia del hombre.»

— Rachel Carson, Primavera silenciosa (1962)

Enero de 2025. La sala de operaciones del Centro Europeo de Predicción Meteorológica a Medio Plazo está inmersa en la luz azulada de los paneles de control. En una pantalla gigante, un gráfico de líneas se eleva como la ladera de una montaña que se va quedando sin nieve. El último punto es 2024, con una temperatura media global en torno a +1,6 °C por encima de los niveles preindustriales: por primera vez en la historia humana, un año supera el umbral simbólico de París. «Es el primer año natural que supera los 1,5 °C», anuncia con voz firme la directora del centro. El grupo de expertos y periodistas se queda en silencio: aquella cifra no es solo un dato climático, sino la advertencia de unas consecuencias que ya se despliegan por todo el planeta.

Los monitores parpadean con datos del programa Copernicus: la temperatura global sigue subiendo y los extremos de calor son cada vez más frecuentes. En el oeste de Europa, ciudades costeras como Barcelona y Lisboa luchan contra olas de calor que baten récords. En África, los campos de cultivo sufren sequías prolongadas que erosionan las cosechas. En Asia, las inundaciones monzónicas, impulsadas por corrientes atmosféricas más intensas, han desplazado a multitudes de personas en el sur de la India y en Bangladés.

Mientras los científicos se mueven entre mesas llenas de informes, una imagen de la Tierra vista desde satélite llena una de las pantallas: nubes blancas como espuma sobre un azul cada vez más oscuro. En aquel instante, el optimismo que a menudo acompaña a las nuevas tecnologías queda ahogado por la realidad de una crisis climática que avanza a pasos agigantados.

A la misma hora, en el Parlamento Europeo, los grupos políticos discuten el paquete legislativo sobre transición energética. Unos piden acelerar los objetivos de reducción de emisiones; otros se resisten a imponer restricciones adicionales al sector fósil. La presión de las naciones petroleras se hace sentir en cada voto. Es lo que muchos llaman «la trinchera entre la ciencia y la voluntad política»: la brecha que ha retrasado las medidas necesarias para frenar el calentamiento.

En este contexto, la figura de Paul Roberts —el periodista que en *The End of Oil* (2004) ya anticipaba las consecuencias climáticas de la dependencia fósil— aún resuena como un eco del pasado: su advertencia sobre un planeta que cruzaría el umbral de 1,5 °C se ha materializado. Los datos y las imágenes convierten la abstracción en una llamada urgente a la acción. La ciencia ha demostrado que el planeta ya roza el límite, y el futuro del clima depende de la capacidad colectiva de transformar esta prueba en una solución concreta e inmediata. La pregunta que queda abierta es si la política puede responder con la misma rapidez. [1]

La advertencia cumplida

En 2026 el termómetro global sigue marcando los valores que Roberts y muchos otros habían señalado como límites críticos. Los datos de Copernicus que la directora presentaba aquel enero lo certifican: 2024 fue el primer año natural en que la temperatura media de la superficie terrestre superó los +1,5 °C respecto al periodo preindustrial, una cifra que hasta hace poco parecía reservada a los escenarios de modelado [1]. Roberts ya lo advertía: «el proceso ya no se puede detener, solo frenar».

Las emisiones de gases de efecto invernadero (GEI), lejos de moderarse, han marcado un máximo histórico [1]. La tendencia contradice claramente las trayectorias de reducción propuestas por el IPCC y recuerda que, pese al abaratamiento de las alternativas limpias, el consumo de combustibles fósiles todavía no ha tocado techo a escala global.

Un matiz, antes de continuar: un año con una temperatura media superior a +1,5 °C no equivale automáticamente al incumplimiento del Acuerdo de París, que se basa en la media de temperaturas a largo plazo (aproximadamente 20 años). Pero superar el umbral puntualmente es una señal inequívoca de la dirección en la que nos movemos, y cada año adicional cerca de esa temperatura incrementa los riesgos de fenómenos extremos: olas de calor más intensas y frecuentes, incendios forestales devastadores y un aumento del nivel del mar que amenaza zonas costeras densamente pobladas.

Las recomendaciones del IPCC en su sexto informe de evaluación (AR6) son contundentes: para limitar el calentamiento a 1,5 °C hay que reducir las emisiones globales un 43 % antes de 2030 y un 60 % antes de 2035 respecto a los niveles de 2019 [2]. La diplomacia, en cambio, vacila: la COP28 de 2023 hizo un llamamiento a acelerar la transición hacia las energías renovables [3], pero las cumbres siguientes —COP29 y COP30— ni siquiera mencionaron los combustibles fósiles en el texto principal, bajo la presión creciente de los petroestados, los gobiernos que viven de los ingresos fósiles y que trabajan por diluir los compromisos más ambiciosos.

Esta disonancia entre la urgencia científica y la reticencia política es el corazón de lo que Don Tapscott, en *Blockchain Revolution*, describe como «la promesa y el peligro». La tecnología está preparada: soluciones basadas en inteligencia artificial para optimizar las redes eléctricas, plataformas blockchain para garantizar la trazabilidad de las certificaciones de energía verde y mecanismos de prueba de existencia (t2p) que combaten las deepfakes y refuerzan la confianza pública. Pero sin una voluntad política decidida a romper el poder de los grupos de presión de los combustibles fósiles, estas herramientas se quedarán en el papel: una promesa no materializada.

El reto para el lector es claro: exigir que las autoridades traduzcan los datos y las advertencias en políticas concretas, financiación urgente y marcos reguladores robustos. Solo así podremos transformar la advertencia cumplida de Roberts en una acción real que frene —y posiblemente revierta— la trayectoria actual hacia un futuro insostenible.

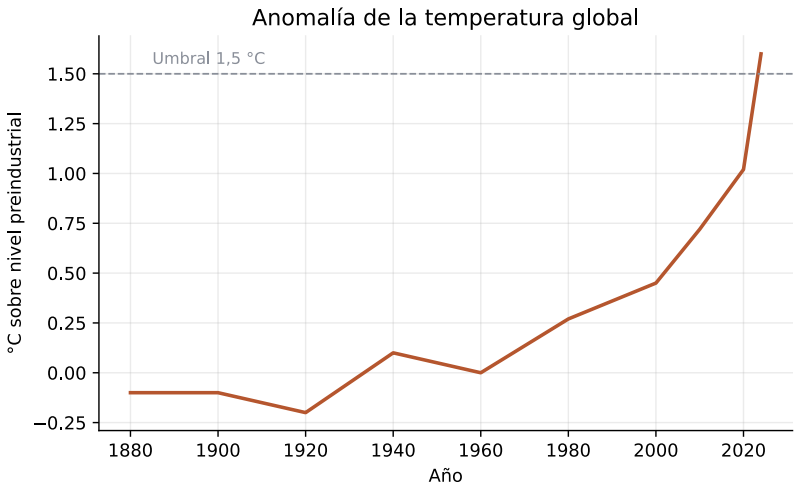


Figura 6.1 — El calentamiento global ha superado por primera vez los +1,5 °C en un año natural (2024).

El presupuesto de carbono

Aquel 43 % antes de 2030 y aquel 60 % antes de 2035 no son aspiraciones idealistas: son el resultado de una modelización rigurosa que integra miles de variables, desde los flujos energéticos hasta las dinámicas socioeconómicas. Son, literalmente, el presupuesto de carbono que nos queda para mantener la temperatura media mundial dentro del límite de 1,5 °C. Y el primer año natural por encima de este límite no es solo un dato estadístico: es el punto de inflexión donde la inacción empieza a pagarse muy cara.

La distancia entre este presupuesto y la realidad actual es alarmante. Con las emisiones instaladas en aquel máximo histórico, cada año que pasa sin una reducción sustancial ensancha la brecha entre las metas del IPCC y el camino que seguimos realmente. Y cada fracción de grado adicional no solo eleva el riesgo de eventos climáticos extremos, sino que también incrementa los costes sociales y económicos asociados: inundaciones costeras, sequías prolongadas y desplazamientos masivos de población.

La solución, según la ciencia, es clara; la voluntad política, en cambio, muestra fisuras. La falta de urgencia se traduce en financiación insuficiente para proyectos de energía verde y en marcos reguladores débiles, que no imponen penalizaciones efectivas a los agentes que siguen dependiendo de los fósiles y dejan sin respuesta el núcleo del problema.

Cerrar el bucle entre la ciencia y la acción exige un conjunto de medidas coordinadas: (1) establecer metas vinculantes de reducción de emisiones a escala nacional, con revisiones periódicas; (2) canalizar fondos internacionales hacia proyectos de energía renovable en los países emergentes, donde el crecimiento

económico todavía depende del petróleo; (3) crear un precio del carbono que refleje realmente los costes ambientales y sociales; (4) impulsar la innovación en captura y almacenamiento de carbono (CCS) y garantizar a la vez una transición justa para las comunidades afectadas. Solo con esta combinación de ambición científica y compromiso político se evitará que la advertencia de Roberts se convierta en la crónica de un error irreversible.

Las COP: palabras y hechos

El desierto de Dubái vibró en diciembre de 2023 cuando los delegados de la 28.ª Conferencia de las Partes (COP28) alcanzaron, por primera vez, un acuerdo explícito para «transitar alejándose de los combustibles fósiles». La resolución establecía como objetivo triplicar la capacidad instalada de energía renovable mundial y duplicar el ritmo de mejora de la eficiencia energética antes de 2030 [3]. Aquel paso formal, celebrado como el «principio del fin» de la era de los combustibles fósiles, abrió la puerta a acelerar las inversiones en tecnologías eólicas y fotovoltaicas, en la modernización de redes inteligentes y en el desarrollo de almacenes de energía.

El ritmo diplomático, sin embargo, se ralentizó enseguida: la COP29, celebrada en Bakú en noviembre de 2024, y la COP30, en Belém en noviembre de 2025, cerraron las sesiones sin mencionar los combustibles fósiles en el texto principal de las resoluciones. La COP29 se centró en un nuevo objetivo de financiación climática; la COP30 aprobó una hoja de ruta voluntaria de transición con el apoyo de una coalición de más de 80 países; pero en ninguno de los dos casos se incluyó una mención directa a la extracción o al consumo de petróleo, gas natural y carbón. Según varios observadores, esta omisión fue el resultado de una presión coordinada de los petroestados para evitar una condena internacional directa.

Estos bandazos diplomáticos crean un vacío entre las promesas políticas y las medidas reales. Pese a la declaración de la COP28, las inversiones en proyectos fósiles siguieron creciendo durante los años posteriores, una contradicción que alimenta la duda sobre la voluntad política real de alcanzar los recortes que pide el IPCC para 2030 y 2035 [2].

Y este silencio tiene consecuencias más que simbólicas. Sin una mención clara, los países con grandes reservas de hidrocarburos no se ven obligados a presentar planes de desmantelamiento ni a establecer mecanismos de justicia climática para las comunidades afectadas. Esto dificulta la creación de un marco regulador robusto que pueda canalizar financiación internacional hacia la captura y almacenamiento de carbono o hacia programas de reconversión laboral para los trabajadores del sector fósil.

La COP28 encendió una chispa de esperanza con un acuerdo claro y una meta renovable ambiciosa; las dos conferencias siguientes han diluido este impulso con una retórica que evita nombrar los combustibles fósiles. Se habla de transición, pero no se definen las condiciones para abandonar realmente el petróleo y el gas. Para que las palabras se conviertan en hechos hacen falta compromisos vinculantes y transparentes, con un seguimiento verificable y consecuencias para quien se desvíe del camino. Sin esto, la política climática seguirá hablando mientras el termómetro sube.

La promesa y el peligro

La promesa es real: por primera vez, en palabras, el mundo se orienta hacia abandonar los combustibles fósiles, y las herramientas para hacerlo son cada vez más baratas. Lo que hace solo unos años parecía una utopía es hoy tecnológicamente viable gracias a dos revoluciones convergentes.

La primera: la energía solar y la eólica han llegado a un coste de producción inferior al del carbón en la mayoría de los mercados. Según IRENA, el coste normalizado de la electricidad (LCOE) de la solar fotovoltaica a gran escala fue de 0,043 $/kWh en 2024, una reducción de aproximadamente el 90 % respecto a 2010 [4]. Esta caída de costes ha permitido que empresas y gobiernos desplieguen grandes proyectos sin necesidad de ayudas masivas. La segunda: la blockchain se utiliza ya para crear sistemas de certificación descentralizados que verifican en tiempo real el origen limpio de cada unidad de electricidad, una capa de autenticidad que reduce la necesidad de auditorías costosas y permite verificar de manera transparente el cumplimiento de las cuotas.

Pese a este escenario prometedor, el peligro persiste con una intensidad creciente. Las emisiones, como hemos visto, todavía aumentan [1], impulsadas en buena parte por economías que dependen del petróleo y el gas natural para el crecimiento industrial. Además, la voluntad política ha empezado a vacilar: tras la COP30, varios gobiernos han retrasado la publicación de sus planes de energía limpia, alegando

incertidumbres económicas y la presión del sector fósil. Este retroceso no es solo una cuestión de calendario; el coste del retraso se traduce en décadas irrecuperables de calentamiento global, y cada año adicional de inacción aumenta la probabilidad de superar umbrales cada vez más peligrosos, con consecuencias graves para la agricultura, la salud y la migración humana [1][3].

Las herramientas, pues —energía renovable asequible y certificación blockchain transparente—, ya son accesibles; el verdadero reto reside en traducir estas capacidades técnicas en acciones políticas firmes. La diferencia entre una promesa escrita y un compromiso ejecutable se mide en la capacidad de las instituciones de imponer consecuencias efectivas a quien rompe sus propias normas. Sin este marco de responsabilidad, el riesgo es que las emisiones sigan subiendo, que se consuman décadas de avances climáticos y que nos acerquemos irreversiblemente al punto de no retorno. El futuro del planeta depende, ahora más que nunca, de la capacidad de los líderes de transformar una promesa en una acción verificable e irreversible.

El termómetro y la verdad

El termómetro ha dictado sentencia: aquel primer año natural por encima de los +1,5 °C ya no es la hipótesis lejana que Roberts advertía, sino nuestra realidad cotidiana. Las olas de calor extremas se extienden desde la Europa meridional hasta el sur de Estados Unidos; los incendios forestales, alimentados por vientos más intensos y vegetación más seca, consumen áreas que hace una década todavía eran bosques exuberantes. Cada hora de producción detenida se traduce en pérdidas cuantiosas, y los desplazamientos masivos de poblaciones cuestan vidas y recursos a sociedades ya frágiles.

Pero lo más alarmante no es solo la temperatura: también está en peligro la confianza que cimienta nuestras instituciones. En un mundo donde las imágenes y los audios pueden generarse con una precisión indistinguible de la realidad, la capacidad de identificar falsedades se convierte en una necesidad vital. Actores estatales y no estatales ya han empezado a usar deepfakes para desacreditar informes climáticos, manipular elecciones y minar la credibilidad de los científicos que piden medidas urgentes. La crisis de la verdad se convierte así en una extensión directa del cambio climático: si el público no puede confiar en los datos que demuestran el impacto real, la presión política para actuar disminuye drásticamente.

Las promesas políticas están ahí —la transición proclamada en Dubái, las metas renovables para 2030—, pero todavía no se han traducido en acciones verificables: la presión de los petroestados condicionó las dos COP siguientes, y el marco científico del IPCC AR6 sigue sin una respuesta política a la altura. La disparidad entre lo que la ciencia pide y lo que la política ofrece revela una zona de incertidumbre donde las decisiones erróneas pueden ser fatales.

En este contexto, la verdad se convierte en un recurso tan estratégico como la energía. Las tecnologías de registro inmutable basadas en blockchain ofrecen una pista de auditoría transparente para los datos climáticos: cada medición de emisión, cada inversión en renovables y cada certificación de eficiencia puede verificarse de manera independiente, lo que evita la manipulación y refuerza la confianza pública. La inteligencia artificial, a su vez, puede analizar grandes volúmenes de datos para detectar anomalías y predecir tendencias, pero solo si se mantiene una base de datos fiable.

La llamada a la acción, pues, no es solo reducir las emisiones; es construir un ecosistema de información veraz que dé soporte a las políticas climáticas. Hemos revisado la máquina, la oferta, las alternativas, el poder y el clima. Ahora toca mirar las consecuencias de hoy —y una nueva que Roberts no podía imaginar: la crisis de la verdad. Es la Parte III.

---

[1] Copernicus C3S, *2024, primer año por encima de 1,5 °C*. https://climate.copernicus.eu/copernicus-2024-first-year-exceed-15degc-above-pre-industrial-level ↩

[2] IPCC AR6 (vía COP28 Global Stocktake), *recortes de emisiones 2030/2035*. https://www.iea.org/topics/cop28-tracking-the-energy-outcomes ↩

[3] UNFCCC / Comisión Europea, *resultados de COP28-COP30*. https://climate.ec.europa.eu/news-other-reads/news/what-did-cop30-achieve-2025-12-01_en ↩

[4] IRENA (vía pv-magazine), *LCOE solar global = 0,043 $/kWh en 2024*. https://www.pv-magazine.com/2025/07/23/global-average-solar-lcoe-stood-at-0-043-kwh-in-2024-says-irena/ ↩

Dar a la gente lo que quiere: consumo, eficiencia y «menos es más»

«Un hombre es rico en proporción al número de cosas que puede permitirse dejar en paz.»

— Henry David Thoreau, Walden (1854)

En la cocina de una familia típica de Barcelona, el horizonte está dominado por una constelación de aparatos electrónicos que brillan como estrellas en una noche clara. Un televisor OLED de grandes dimensiones emite una luz suave mientras el padre sigue el partido de fútbol en directo; al lado, la madre controla un asistente de voz que regula la temperatura del termostato inteligente y activa el difusor de la rutina nocturna. En la mesa, tres portátiles, dos tabletas y un teléfono plegable se mueven al ritmo de mensajes instantáneos y videollamadas que viajan por una red 5G que nunca duerme.

En el piso superior, una habitación de estudio alberga un conjunto de dispositivos IoT: luces LED regulables por aplicación, sensores de presencia que encienden la calefacción solo cuando alguien entra, y una pequeña instalación solar que alimenta el cargador del teléfono. Pese a este baluarte de energía renovable, la demanda sigue creciendo como un río sin control: el aire acondicionado se pone a máxima potencia para contrarrestar un calor insistente; la lavadora se activa en horas valle para aprovechar las tarifas más bajas, y el congelador de la cocina funciona todo el día para mantener los alimentos frescos.

El ambiente está impregnado de una sensación de satisfacción inmediata: cada clic, cada orden, cada «encendido» es una respuesta instantánea al deseo que la gente ha expresado durante décadas: tenerlo todo a mano, sin esperar. Pero esta escena, tan cotidiana y aparentemente inofensiva, esconde un desequilibrio profundo. La demanda insaciable no solo consume energía; crea una presión constante sobre unas redes eléctricas que ya muestran signos de saturación.

Paul Roberts, en *The End of Oil* (2004), se preguntaba: si la gente quiere todo lo que desea, ¿cómo podemos cambiar la curva? La respuesta no es simplemente ofrecer más energía limpia; la verdadera clave es reducir la cantidad que se necesita. La paradoja de Jevons nos recuerda que cada ganancia de eficiencia tiende a ser devorada por un aumento del consumo, lo que llamamos el efecto rebote [2]. Así, mientras las luces LED y los electrodomésticos inteligentes prometen reducir la factura energética, el hecho de tener más dispositivos y una vida más conectada puede contrarrestar estas ventajas.

En esta casa llena de innovación, el enigma se convierte en un reflejo del mundo: ¿cómo podemos transformar una cultura que celebra la abundancia inmediata en una que abraza la suficiencia? La respuesta ha de surgir de una combinación de eficiencia tecnológica, políticas que incentiven el consumo responsable y una nueva narrativa que valore «menos es más». Solo así podremos empezar a cortar la curva del deseo infinito y avanzar hacia un futuro donde la energía limpia sea, de hecho, la que no gastamos.

La energía que no gastamos

En 2024, la mejora del rendimiento energético global dibujó una curva casi plana. ¿La cifra clave? Un incremento de solo **un por ciento** respecto al año anterior, la mitad del ritmo observado entre 2010 y 2019 [1]. Esta lentitud no es ningún accidente; refleja una realidad estructural: **el vatio más barato y limpio es aquel que nunca se genera**.

Esta constatación, tan simple como profunda, convierte la eficiencia en el «primer combustible» de la transición energética. No solo se trata de mejorar las tecnologías —las bombillas LED, los motores de altas prestaciones o los algoritmos de optimización basados en IA— sino de reconocer que cada unidad de energía ahorrada es una unidad que no ha de ser producida, transportada y distribuida. En este sentido, la eficiencia se convierte en una forma directa de reducir las emisiones sin necesidad de invertir en nuevas fuentes de generación, ni por tanto en infraestructura costosa o en la explotación de recursos naturales.

Pero el camino hacia este escenario no es lineal. La **paradoja de Jevons** —el fenómeno por el que los avances en eficiencia conducen, paradójicamente, a un aumento del consumo total— sigue planeando como una sombra sobre las expectativas optimistas. Cuando la tecnología hace que la electricidad sea más barata, el coste marginal disminuye y aparecen nuevos usos: dispositivos conectados incesantes, aplicaciones de inteligencia artificial que requieren potencia computacional masiva, o incluso una cultura

de «compra y tira» que aprovecha la percepción de recursos abundantes. Este efecto rebote absorbe parte de la ganancia obtenida por las mejoras técnicas, y se convierte en un obstáculo invisible pero potente [2].

La solución no reside solo en el aumento de los porcentajes de eficiencia; hace falta una **sinergia entre tecnología, política y comportamiento**. La COP28 estableció como objetivo duplicar el ritmo anual de mejora de la eficiencia hasta 2030, un reto que requiere más que el simple avance científico [1]. Hacen falta políticas que penalicen el exceso e incentiven la suficiencia: tarifas escalonadas que aumentan con el consumo, créditos fiscales para edificios de bajo consumo y regulaciones que limiten las prácticas de «obsolescencia programada». Además, hace falta una narrativa que valore el «menos es más», y que transforme la percepción del bienestar desde una acumulación material hacia la optimización de los recursos.

En este contexto, cada porcentaje de ahorro se convierte en un activo estratégico. Un aumento del 1 % puede parecer modesto, pero si se aplica de manera global y se complementa con políticas que impiden el rebote, los efectos acumulativos son significativos: menos necesidades de generación nueva, reducción de inversiones en infraestructura fósil y una disminución directa de las emisiones de CO_2. Por tanto, la eficiencia no es solo una mejora técnica; es la base sobre la que se construye una economía energéticamente sostenible.

El futuro energético más limpio depende de una regla sencilla pero poderosa: **no gastaremos energía que no necesitemos**. Esto implica impulsar la eficiencia a una velocidad superior al ritmo actual y crear marcos reguladores y culturales que impidan que esta ganancia se disipe en nuevos consumos. Solo así podremos avanzar hacia un modelo donde el «primer combustible» sea realmente la no producción de energía, convirtiendo el ahorro en nuestra principal fuente de sostenibilidad.

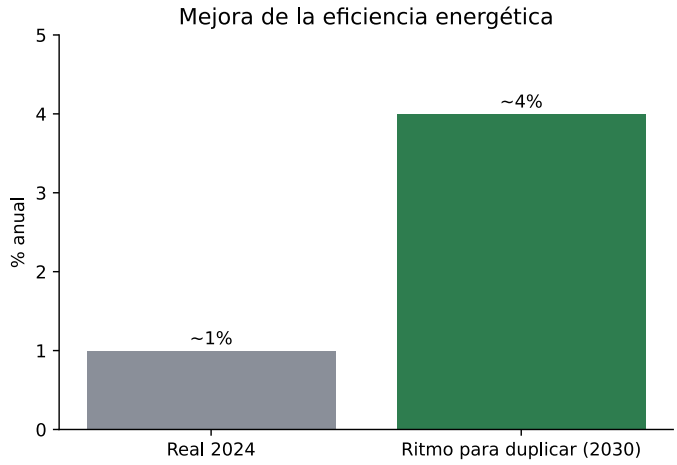


Figura 7.1 — La mejora de la eficiencia (~1 % en 2024) va muy por debajo del ritmo necesario para duplicarla hacia 2030.

El freno de Jevons

Imaginad un centro de datos que reduce el consumo medio por metro cuadrado gracias a una nueva arquitectura de refrigeración más inteligente. La noticia se difunde como una prueba contundente de que la tecnología puede romper el lazo entre crecimiento económico y consumo energético, pero solo unos meses después la facturación muestra un aumento del volumen total de energía consumida por los mismos centros, impulsado por una expansión simultánea de servicios en la nube y por precios de la electricidad más bajos, derivados precisamente de la mejora de eficiencia. Esta es la paradoja que William Stanley Jevons describió en el siglo XIX: cuando un recurso se abarata mediante mejoras tecnológicas, su uso tiende a aumentar en lugar de disminuir.

La evidencia contemporánea lo confirma: la mejora de la eficiencia se queda en aquel escaso 1 % anual [1]. La disminución del coste por unidad de energía hace que tanto las empresas como los consumidores perciban la electricidad como un bien más asequible, y esto favorece nuevos patrones de demanda. En el sector residencial, la proliferación de aparatos inteligentes y la adopción masiva de sistemas de calefacción y refrigeración de alta eficiencia han generado una «casa conectada» que consume más energía en total, aunque cada dispositivo sea individualmente menos intensivo.

Esta dinámica se ve reforzada por la falta de señales de precio adecuadas. Cuando el coste marginal de la electricidad se mantiene artificialmente bajo —por ejemplo gracias a subvenciones o tarifas reguladas— los consumidores no perciben el verdadero coste ambiental de su uso. La combinación de eficiencia y precios bajos crea un incentivo perverso: la reducción de costes operativos anima a las empresas a expandir su capacidad productiva, mientras que los hogares aumentan la cantidad de aparatos conectados sin una concienciación clara de su impacto energético.

Para romper este círculo vicioso hay que introducir un «freno de Jevons» mediante políticas que alineen el precio de la energía con su coste real y ambiental. Primero, establecer tarifas dinámicas basadas en la demanda horaria, de modo que los consumidores sean penalizados económicamente por usar energía durante los picos de congestión; segundo, implementar mecanismos de «suficiencia» que limiten el crecimiento indiscriminado del consumo: regulaciones que establezcan límites máximos de energía por equipo o por vivienda e incentivos fiscales para la reducción voluntaria del consumo total.

Además, la transparencia es clave. Las etiquetas energéticas han de mostrar no solo el ahorro por unidad, sino también el potencial incremento de demanda que puede derivarse de una tecnología más eficiente. Esto ayudaría a los consumidores a valorar realmente sus decisiones y a evitar la tentación de «comprar más porque cuesta menos». En conjunto, una combinación de instrumentos de precio, límites reguladores y educación sobre el coste total del consumo puede actuar como un freno efectivo contra el efecto rebote, y convertir la mejora de eficiencia en una verdadera reducción neta de energía utilizada.

Solo así podremos avanzar hacia un modelo donde «menos es más» deje de ser una mera aspiración y se convierta en la base de una transición energética sostenible.

¿Menos es más?

En la plaza de un mercado, un grupo de emprendedores locales ha instalado pequeñas placas solares que alimentan solo los quioscos donde venden frutas y verduras. La clave no es añadir más energía sino reducir el consumo en el origen: diseños modulares que se adaptan al flujo real de clientes, sin sobrecargas ni espacios vacíos. Esta escena encarna la visión de Roberts sobre una demanda modelada por la suficiencia y no por el crecimiento indefinido.

Aquel escaso 1 % de mejora anual [1] es la pista de que el simple perfeccionamiento técnico no basta: cada ganancia de eficiencia tiende a ser absorbida por un aumento del uso, como describe la paradoja de Jevons —cuando el coste marginal de un recurso cae, el consumo total a menudo sube y anula parte del beneficio ambiental [2]. Para romper este círculo hace falta una nueva arquitectura de demanda que combine tres pilares.

Primero, la **suficiencia**. No se trata solo de reducir las facturas, sino de replantear qué necesidades son esenciales. Las ciudades inteligentes pueden ofrecer servicios compartidos —bicicletas eléctricas de uso puntual, sistemas de refrigeración comunitaria y calefacción de distrito basada en energía renovable— que disminuyen la necesidad de inversiones individuales y, por tanto, el consumo global. Estos modelos reparten entre muchos usuarios unos recursos que antes cada uno duplicaba por su cuenta.

Segundo, el **diseño inteligente**. Los productos y las infraestructuras han de incorporar la mentalidad «menos es más» desde el primer trazo. Una arquitectura descentralizada, basada en microrredes y almacenamiento local, puede minimizar las pérdidas de transmisión y permitir un uso optimizado según las horas punta, sin necesidad de incrementar la capacidad total del sistema. Este enfoque reduce directamente la energía requerida para mover información y energía a través de redes extensas.

Tercero, la **electrificación inteligente**, que combina sensores IoT con algoritmos de aprendizaje automático para ajustar el suministro en tiempo real. Un sistema de gestión energética basado en IA puede reducir el consumo de iluminación y climatización de un edificio sin ningún sacrificio por parte de los usuarios, y evita la generación excesiva y el desaprovechamiento.

Finalmente, el **cambio de comportamiento**. Las campañas de educación energética han demostrado que cuando las personas entienden el coste total de su consumo —no solo el precio de la factura sino el impacto ambiental y social— adoptan prácticas más moderadas. Los programas de retroalimentación en tiempo real sobre el uso de agua y electricidad suelen provocar una reducción medible del consumo en los hogares participantes en pocos meses.

Así, la cara de la demanda que Roberts intuía se materializa cuando la tecnología se combina con políticas que limitan los incentivos al consumo excesivo y promueven diseños que maximizan el valor por unidad

de energía. Solo así «menos es más» dejará de ser una aspiración utópica y se convertirá en el fundamento de una transición energética verdaderamente sostenible.

La promesa y el peligro

En este marco, la eficiencia energética es la palanca más barata y ágil que tenemos a nuestro alcance: cada punto porcentual de reducción del consumo suprime la necesidad de inversiones en infraestructura, minimiza las emisiones y libera capital para otros proyectos de transición. Por eso la COP28 fijó el objetivo de duplicar el ritmo de mejora antes de 2030 —el doble de aquel escaso 1 %—, un salto que exige tanto innovación tecnológica como marcos reguladores robustos y coherentes [1].

Esta promesa de reducir el consumo a través de mejoras técnicas viene empaquetada con un peligro persistente: la paradoja de Jevons. Cuando la energía se abarata o se hace más accesible, la tendencia natural del comportamiento humano es aumentar su uso, una dinámica que se manifiesta en el **efecto rebote** [2]. Esto no solo contrarresta las ganancias de eficiencia, sino que puede generar un incremento neto de demanda superior al esperado. Un ejemplo claro son los dispositivos inteligentes en los hogares: cada vez más aparatos conectados consumen energía constantemente, y el consumo total se mantiene o incluso aumenta pese a las mejoras de eficiencia de cada unidad.

A este escenario se suma una **inercia cultural del consumo** que dificulta la transición hacia un modelo basado en la suficiencia. Las campañas publicitarias, los hábitos de compra y la obsolescencia programada crean una demanda incesante de innovación productiva, incluso cuando las necesidades reales son limitadas. Sin una respuesta política que regule estas dinámicas —por ejemplo, impuestos sobre la obsolescencia, etiquetas energéticas obligatorias o incentivos para el «derecho a reparar»— las ganancias técnicas se diluyen en un ciclo de crecimiento de demanda que desestabiliza cualquier avance neto. La solución, por tanto, no puede limitarse a la sola mejora del rendimiento de los equipos; hace falta una **estrategia integral** que combine eficiencia, suficiencia y política.

1. **Políticas de incentivo estructuradas**, como tarifas escalonadas basadas en el uso anual de energía o subvenciones para la renovación de productos de alta eficiencia.
2. **Regulaciones contra la obsolescencia programada**, que obliguen a los fabricantes a garantizar una vida útil mínima y a facilitar el reciclaje y la reparación.
3. **Campañas de educación y cambio cultural** que promuevan la idea de que «menos es más» y destaquen casos reales de consumo responsable y ahorro económico.

Solo cuando estas tres dimensiones converjan podremos transformar la eficiencia en una fuerza neta, capaz de reducir realmente el consumo energético sin ser engullida por el rebote. En este equilibrio entre promesa y peligro se encuentra la clave para un futuro donde la energía más limpia sea, efectivamente, la que no gastamos.

De la demanda a la oferta

Si la demanda es parte del problema, la oferta institucional también lo es. Los grandes grupos energéticos han construido una infraestructura que, de por sí, refuerza el consumo: centrales de gran escala, redes de transmisión costosas y modelos de negocio basados en la venta constante de electricidad. Estas empresas, hasta ahora, defendían que aumentar la capacidad productiva resuelve cualquier escasez percibida, pero su papel no se limita a suministrar energía; también modelan las expectativas de los consumidores e influyen en las políticas públicas.

A menudo la expansión de la red se justifica para garantizar seguridad y fiabilidad cuando una región se inclina hacia fuentes renovables intermitentes. No obstante, sin reducir simultáneamente el consumo, estas inversiones corren el riesgo de aumentar el volumen total de electricidad consumida, a causa del efecto rebote que a menudo acompaña a la mejora de la eficiencia [2].

Esta dinámica se refleja también en las políticas reguladoras. Algunas normativas sobre mercados eléctricos establecen mecanismos de incentivo para las grandes compañías, como tarifas garantizadas y certificados verdes, que premian la producción adicional más que la optimización del consumo. El resultado puede ser una «gran retirada verde» que solo abandona parcialmente las fuentes fósiles sin reducir el total de electricidad demandada, y que contraviene el llamamiento de la COP28 a duplicar el ritmo anual de mejora de la eficiencia [1].

Para romper este círculo vicioso hace falta que las grandes energéticas adopten una nueva mentalidad: no solo ofrecer energía más limpia, sino también reducir el volumen total de energía necesaria. Esto implica invertir en tecnologías de gestión de la demanda y en plataformas que permitan a consumidores y empresas intercambiar capacidad de manera descentralizada y transparente, alineando los incentivos económicos con objetivos de suficiencia; también requiere políticas públicas que penalicen el crecimiento descontrolado del consumo y premien las prácticas de economía circular y de autoproducción distribuida.

En definitiva, la solución no es solo mejorar la eficiencia un punto porcentual al año, sino reconfigurar todo el ecosistema energético para que la oferta institucional se convierta en un motor de reducción del consumo y no en un impulsor del mismo. Solo cuando eficiencia, suficiencia y política converjan podremos transformar la promesa de una energía más limpia en una realidad tangible: que la energía más limpia sea realmente la que no gastamos.

---

[1] AIE, *Energy Efficiency 2024 — Executive summary*. https://www.iea.org/reports/energy-efficiency-2024/executive-summary ↩

[2] *Jevons paradox / rebound effect* (revisión). https://en.wikipedia.org/wiki/Jevons_paradox ↩

Las grandes energéticas, ansiosas

«No hay nada más difícil de llevar a cabo, ni de más dudoso éxito, ni más peligroso de gestionar, que iniciar un nuevo orden de cosas.»

— Nicolás Maquiavelo, El Príncipe, VI (1513)

Era una tarde de verano y la sala donde se celebraba la junta de accionistas estaba llena de una energía que recordaba las campañas de la época del boom petrolero de los años 2000. Entonces, los fotógrafos de las revistas financieras capturaban a ejecutivos con sonrisas perfectamente alineadas; ahora, el mismo escenario se convertía en un teatro de ansiedad y de decisión estratégica.

En el centro del escenario, la pantalla gigante mostraba el logotipo de una de las mayores petroleras mundiales —un símbolo que había dominado los mercados energéticos durante décadas—. El anuncio era claro: «Reequilibramos nuestra estrategia». Aquel término, tan neutro y casi poético, esconde una realidad más cruda. En lugar de una transición hacia las energías renovables, el mensaje se traduce en un giro firme hacia el petróleo y sus derivados.

Cuando el CEO —un hombre de mirada fría pero con la voz cargada de optimismo— pronunció sus palabras, la audiencia se quedó inmóvil durante unos segundos, como si esperara una revelación inesperada. «Tras un breve periodo de experimentación verde», dijo, «hemos decidido reforzar nuestra apuesta por los activos fósiles para garantizar el retorno de nuestros accionistas». El murmullo que siguió se transformó rápidamente en aplausos sincronizados, una ovación que parecía más un acuerdo colectivo de confianza financiera que un reconocimiento de innovación.

Los inversores —principalmente fondos de pensiones y gestores de activos institucionales— levantaron las manos, algunos con folletos que mostraban gráficos ascendentes del precio del petróleo y otros con teléfonos móviles que anotaban de inmediato los nuevos objetivos de rentabilidad. En su entusiasmo, se podía leer la presión incesante de los accionistas que exigen recortes en los gastos de proyectos verdes y una aceleración en la producción de crudo.

Al mismo tiempo, el silencio era palpable en la mesa donde se encontraban los representantes de las organizaciones climáticas. Los portavoces de ONG internacionales, que habían sido invitados como testigos para «mostrar compromiso», se quedaron con la mirada fija en el suelo, sin palabras para contrarrestar el anuncio. Su desconcierto contrastaba brutalmente con los gritos de aprobación del público financiero.

Los resultados financieros recientes reforzaban esta decisión: las empresas energéticas estatales del G20 habían invertido aproximadamente 360.000 millones de dólares en CAPEX en 2024, con un 81 % destinado a proyectos fósiles [1]. En paralelo, BP había recortado 5.000 millones de dólares de su plan bajo en carbono y Shell había frenado sus inversiones en renovables por presión de accionistas [2]. La proporción de dinero público destinado a fósiles era cinco veces superior a la invertida en renovables, aumentando el riesgo de activos varados [3].

Esta escena, llena de aplausos y silencio simultáneos, encapsula la ansiedad que se ha apoderado de las grandes energéticas: una apuesta por volver al petróleo como respuesta a la presión accionarial, sabiendo que el mercado global se mueve hacia una economía baja en carbono. La pregunta que queda suspendida en el aire —y que resonará durante los próximos años— es si este «reequilibrio» será solo un retroceso temporal o el preludio de una nueva era de desafío para la confianza del sector energético.

El giro verde que duró poco

La duda no es nueva. A principios de 2020, las grandes majors energéticas presentaron un compromiso firme con la transición hacia fuentes limpias, reducciones sustanciales de emisiones y una apuesta clara por proyectos renovables. Los informes anuales de BP, Shell y Eni mostraban mapas estratégicos con inversiones multimillonarias en eólica, solar e hidrógeno verde, y los consejos de administración se comprometieron públicamente a alinearse con los objetivos del Pacto de París. Las expectativas de los analistas eran altísimas; el mercado valoraba estas declaraciones como una señal clara de que las empresas dejaban atrás la dependencia del petróleo.

No obstante, entre 2024 y 2025 este relato se deshizo con la fuerza de una tormenta inesperada. La presión de los accionistas —impulsada por resultados a corto plazo y una demanda creciente de

dividendos más elevados— hizo que las directrices de transición quedaran en suspenso. BP, por ejemplo, materializó aquel recorte de 5.000 millones del plan bajo en carbono y aumentó el gasto en fósiles [2]; al mismo tiempo, Shell congeló buena parte de sus programas renovables y puso en pausa iniciativas anunciadas como pilares de su nueva estrategia empresarial. No eran simples ajustes operativos: era el retroceso de un compromiso que se había promocionado como fundamento del futuro energético.

La «gran retirada verde» se ha convertido en una frase clave para describir este giro inesperado. Como hemos visto, las empresas energéticas estatales del G20 destinaron aproximadamente 360.000 millones de dólares a CAPEX en 2024, con un 81 % de estos fondos dirigidos hacia proyectos fósiles [1]; en el caso concreto de Eni, la inversión en petróleo y gas llegó a 6.900 millones de euros, mientras que la destinada a energía limpia se quedó en solo 764 millones de euros, una proporción que revela la magnitud del desequilibrio [1].

Esta reorientación no solo pone en peligro los objetivos climáticos globales, sino que crea un riesgo financiero significativo: el aumento de la exposición a activos fósiles en un mercado que avanza hacia una economía baja en carbono eleva la probabilidad de activos varados. El dinero público ya se destina cinco veces más a los fósiles que a las renovables, reforzando el desequilibrio entre apoyo estatal y desarrollo sostenible [3]. El reto, por tanto, no es solo volver a las promesas verdes; hay que abordar la tensión estructural entre los intereses accionariales y la necesidad urgente de descarbonizar. Si las grandes majors siguen priorizando beneficios inmediatos sobre la sostenibilidad a largo plazo, el mercado energético podría verse sacudido por una nueva ola de crisis de confianza —un escenario que combina promesa y peligro en igual medida.

Los números no mienten

Como hemos visto, un año después de los discursos verdes y las promesas de energía limpia, las cifras financieras del sector muestran una realidad mucho más sobria. En 2024, las empresas estatales del G20 dedicadas a la energía destinaron aproximadamente **360.000 millones de dólares** al capital (capex), y un sorprendente **81 %** de este presupuesto se canalizó hacia los proyectos fósiles —pozos de perforación, refinado e infraestructuras para el transporte del petróleo y el gas natural— [1]. Esta proporción supera con gran diferencia las expectativas de transición verde planteadas hace cinco años y contradice los compromisos adoptados en la Conferencia de las Partes (COP) y en las declaraciones de objetivos Net-Zero.

Un ejemplo emblemático es **Eni**. En el ejercicio 2024, invirtió **6.900 millones de euros** en proyectos relacionados con el petróleo y el gas, mientras que la partida destinada a sus actividades limpias —energía eólica y solar— se quedó en solo **764 millones de euros** [1]. Esta disparidad de casi nueve a uno revela una apuesta clara por mantener y expandir el ecosistema de los combustibles fósiles, pese a la presión creciente de inversores institucionales que piden una reorientación hacia fuentes más sostenibles.

La tendencia no es exclusiva del sector privado; los fondos públicos siguen el mismo camino. Los datos de financiación gubernamental muestran que las inversiones públicas en energía fósil son **cinco veces superiores** a las destinadas a proyectos renovables [3]. Por cada euro invertido en solar o eólica, cinco euros se destinan a nuevas plataformas petroleras o a la expansión de redes de gas. Este desequilibrio perpetúa la dependencia de combustibles contaminantes e incrementa el riesgo de activos varados, ya que las tecnologías fósiles se enfrentan a regulaciones más estrictas y a una demanda de mercado que gira hacia alternativas limpias.

La presión de los accionistas ha jugado un papel crucial en este giro. Lo demuestran los recientes recortes de inversión de BP —**5.000 millones de dólares** retirados del plan bajo en carbono— y el frenazo de las iniciativas renovables por parte de Shell, impulsados por accionistas que temen una disminución de los dividendos a corto plazo [2]. Estas decisiones reflejan un dilema clave: equilibrar los intereses financieros inmediatos con la necesidad de una transición sostenible.

En conclusión, el panorama de 2024 deja claro que **el capital sigue prefiriendo los activos fósiles**. Tanto las empresas estatales como las corporaciones privadas, e incluso los fondos públicos, siguen apostando por una infraestructura basada en petróleo y gas, incrementando el riesgo de activos varados y poniendo en duda la capacidad del sector para cumplir con los objetivos climáticos a largo plazo. La pregunta que emerge ahora es cómo revertir este desequilibrio antes de que las consecuencias económicas y ambientales sean irreversibles.

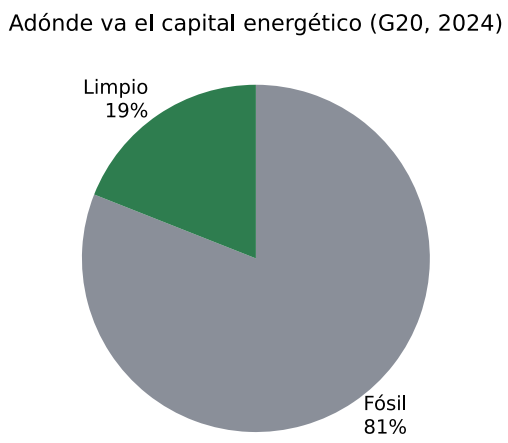


Figura 8.1 — Pese a la retórica verde, el 81 % de la inversión de las energéticas estatales del G20 todavía va a combustibles fósiles (2024).

La trampa de los activos varados

En este escenario, las grandes petroleras siguen destinando una parte cada vez mayor de su capital a proyectos de perforación y refinado; lo que parecía una respuesta inmediata a la presión de accionistas se revela como una paradoja estructural.

Como hemos visto, en 2024 las empresas energéticas del G20 canalizaron la mayoría de su CAPEX hacia proyectos fósiles, y esto crea una exposición significativa a activos varados [1].

Esta dinámica se alimenta de la presión directa de los accionistas, que temen perder rendimientos a corto plazo y han obligado a compañías como BP a recortar miles de millones del plan de reducción de emisiones y a Shell a frenar sus proyectos renovables [2]; el ejemplo de Eni ilustra claramente la desproporción entre las inversiones en activos fósiles y las destinadas a energía limpia.

El dinero público refuerza el desequilibrio, ya que las inversiones estatales en proyectos fósiles son cinco veces superiores a las destinadas a renovables [3]; este flujo de capital dirige la competencia hacia tecnologías al límite de su vida útil económica y genera un efecto dominó de activos potencialmente obsoletos.

En resumen, lo que hoy se percibe como una maniobra prudente —doblar la apuesta por los fósiles para satisfacer las expectativas de los accionistas— es, en realidad, una bomba de relojería que amenaza la salud financiera del sector. La clave es cambiar la narrativa: de «preservar el valor actual» a «transitar hacia un modelo sostenible que garantice rentabilidad a largo plazo».

La promesa y el peligro

...perdidos, poniendo en riesgo tanto los retornos de los inversores como la viabilidad de una transición climática urgente. La clave para evitar esta trampa reside en cambiar la narrativa: de «preservar el valor actual» a «transitar hacia un modelo sostenible que garantice rentabilidad a largo plazo».

Las grandes energéticas disponen de un arsenal de recursos que ninguna startup o gobierno regional podría igualar: miles de millones en capital disponible, redes de ingeniería refinada durante décadas y una infraestructura global de transporte de hidrocarburos. Esta base masiva les confiere un potencial transformador único; si decidieran redirigir sus inversiones hacia tecnologías limpias, podrían acelerar la descarbonización en una escala que las políticas públicas solo sueñan. Como hemos visto, el grupo de compañías estatales del G20 destinó un CAPEX de unos 360.000 millones de dólares en 2024, con un 81 % todavía dedicado a proyectos fósiles [1].

No obstante, la misma magnitud que ofrece esta promesa se convierte también en un peligro estructural. Los accionistas —mayoritariamente instituciones financieras y fondos de pensiones— siguen priorizando el retorno a corto plazo, ya que los activos fósiles todavía generan rendimientos superiores al coste del capital. La presión es palpable: BP ha recortado 5.000 millones de dólares de su plan bajo en carbono, mientras Shell ha frenado sus inversiones renovables para satisfacer las expectativas de sus accionistas [2].

Este comportamiento no solo perpetúa la dependencia de combustibles fósiles, sino que también atrapa capital público y privado en proyectos cada vez más arriesgados de acabar como activos varados. Los datos muestran que el dinero público invertido en sectores fósiles es cinco veces superior al destinado a renovables [3]; este desequilibrio alimenta una espiral de riesgo financiero y ambiental.

Para romper este círculo vicioso hay que reconfigurar los mecanismos de incentivo. Las políticas públicas deberían alinearse con los objetivos corporativos, introduciendo tasas de carbono que penalicen el exceso de fósiles y ofreciendo créditos fiscales robustos para proyectos renovables; a la vez, fondos de pensiones e instituciones financieras han de reevaluar su criterio de evaluación del riesgo, incorporando la probabilidad de activos varados como factor clave. Solo cuando este marco de rendición de cuentas se consolide las grandes energéticas podrán canalizar capital e ingeniería hacia una transición verdadera, convirtiendo su poder estructural en motor de cambio más que en freno para el futuro sostenible.

Una voz inesperada en la sala de juntas

Tal como se ha señalado anteriormente, la inteligencia artificial se convierte en una voz inesperada que resuena entre las salas de juntas donde los consejos directivos revisan balances y presiones accionariales. No es una mera herramienta de optimización operativa; es un catalizador que puede girar el eje de las decisiones estratégicas hacia una nueva orientación energética.

En primer lugar, los algoritmos predictivos ya pueden ayudar a las grandes petroleras a mapear con precisión la probabilidad de activos varados. Mediante modelos que integran datos climáticos, reguladores y de mercado, se puede cuantificar el riesgo de quedar atrapadas en infraestructuras fosilizadas que perderán valor tan pronto como la transición se acelere. Esto ofrece una respuesta directa al problema expuesto en la sección anterior: incorporar el factor de activos varados en los criterios de evaluación del riesgo.

En segundo lugar, la IA puede acelerar la transición hacia las renovables no solo identificando oportunidades de inversión, sino también optimizando la gestión de recursos distribuidos y redes inteligentes. El aprendizaje automático permite equilibrar la producción solar y eólica con la demanda en tiempo real, reduciendo costes operativos y pérdidas en la red. Este tipo de aplicación demuestra cómo la tecnología puede transformar una empresa tradicional en un proveedor de energía más ágil y resiliente.

No obstante, la promesa de la IA viene acompañada de un peligro igual de sustancial. La misma capacidad analítica que permite predecir activos varados también puede ser explotada por manipuladores de mercado o por actores estatales que busquen maximizar beneficios cortos en detrimento de la seguridad energética global. Así, el riesgo de «caja negra» se convierte en una nueva forma de opacidad: decisiones clave delegadas a sistemas opacos que pueden ocultar conflictos de interés o errores sistémicos.

Además, la concentración de datos y poder computacional en manos de pocas corporaciones —en gran medida las mismas grandes energéticas— puede reforzar su control sobre el ecosistema energético, perpetuando la dinámica de «freno». La presión de accionistas que ya ha conducido a una retirada de fondos hacia los fósiles [2] podría encontrar un nuevo impulso si la IA se convierte en un arma para maximizar rendimientos a corto plazo, ignorando externalidades sociales y ambientales.

La solución, como siempre, reside en el equilibrio entre oportunidad y vigilancia. Las empresas han de establecer marcos de gobernanza robustos que garanticen transparencia algorítmica, auditoría independiente y una alineación clara con objetivos climáticos verificables. La IA debería ser un motor que impulse la transición verdadera, no una nueva capa de opacidad que oculte sus propias limitaciones.

En resumen, la inteligencia artificial ofrece una doble cara: puede convertir el riesgo de activos varados en una brújula para decisiones más responsables y, a la vez, crear nuevas formas de vulnerabilidad si se deja sin control. La pregunta que queda por responder es cuál de las dos fuerzas predominará. La respuesta no depende solo de la tecnología, sino del marco de rendición de cuentas que las grandes energéticas estén dispuestas a adoptar. Si este marco se fortalece, la IA puede ser el motor de una transición verdadera; si se mantiene en la sombra, se convertirá en un nuevo freno para el futuro sostenible.

---

[1] Reclaim Finance, *Assessment of oil & gas companies' climate strategy (2024).* https://reclaimfinance.org/site/en/assessment-of-oil-and-gas-companies-climate-strategy/ ↩

[2] The Bureau of Investigative Journalism, *BP rowing back on renewables (2025).* https://www.thebureauinvestigates.com/stories/2025-03-06/bp-renewables-net-zero-banks ↩

[3] IISD, *Public money: 5x more to fossil fuels than renewables*. https://www.iisd.org/articles/press-release/governments-five-times-more-public-money-fossil-fuels-than-renewables ↩

La nueva tensión: la IA como salvación y como sed de energía

«El mundo del futuro será una lucha cada vez más exigente contra las limitaciones de nuestra inteligencia, no una cómoda hamaca donde tumbarnos a esperar que nos sirvan nuestros esclavos robots.»

— Norbert Wiener, God & Golem, Inc. (1964)

En el corazón de un gran campus tecnológico, una enorme sala de servidores se alza como un bosque mecánico de cables, luces LED y ventiladores que zumban incesantemente. Las paredes son de metal gris, recubiertas por paneles de aluminio que reflejan la luz fría del día y el azul tenue de las pantallas de monitorización. Cada rack es una torre donde los LED parpadean en secuencias rítmicas, indicando la temperatura interna, el consumo instantáneo y el estado de cada nodo de cálculo, y crea una sinfonía industrial que parece no tener pausa.

En el mismo edificio, pero en un laboratorio adyacente, una pantalla táctil muestra un gráfico dinámico: la potencia consumida por los servidores baja y sube como las olas de un mar digital. Encima, un sistema de inteligencia artificial analiza en tiempo real miles de variables —temperatura ambiente, flujo de aire, carga computacional, precios del mercado energético y predicciones meteorológicas—. Cada segundo, el sistema ajusta los parámetros de los ventiladores, redirige las tareas más intensivas hacia nodos que operan en condiciones óptimas e incluso activa o desactiva grupos de servidores para equilibrar la demanda.

El momento clave llega cuando salta una alerta: un pico inesperado de actividad a causa de una consulta masiva de IA generativa. En lugar de aumentar indiscriminadamente el consumo, el sistema reconfigura al instante la topología de refrigeración, reduce la velocidad de los ventiladores en los racks menos sobrecargados e incrementa la eficiencia del flujo de aire hacia los puntos críticos. En pocos segundos, el gráfico muestra una caída de la potencia consumida, manteniendo las temperaturas dentro del rango de seguridad.

Esta escena es un microcosmos de la paradoja que define 2026: la misma máquina que necesita energía para aprender y procesar datos se convierte también en el arquitecto de una gestión más limpia y racionalizada. El ruido de los ventiladores, que antes era solo una señal del coste energético, ahora se transforma en el sonido de la optimización —una melodía que indica que la IA no solo consume energía, sino que aprende a minimizarla. Es una imagen potente: un cerebro artificial que, con cada ajuste, corta sus propias cadenas de alimentación para vivir en un ecosistema más sostenible.

Mientras los servidores siguen zumbando día y noche, la pantalla muestra una nueva línea en el gráfico: «energía limpia prevista». Es un recordatorio visual de que el futuro no depende solo del volumen de cálculo, sino de cómo ese cálculo se integra con las fuentes de energía renovable. La paradoja se convierte en oportunidad —un punto de bifurcación donde la IA puede ser tanto la causa del consumo descontrolado como el motor de una transición energética limpia. Esta dualidad, capturada en una sola sala de servidores, marca el inicio de un debate crucial: ¿cómo asegurar que la inteligencia artificial sea realmente una salvación y no una sed insaciable de energía?

El acelerador

En este contexto de doble cara, DeepMind ha conseguido reducir un 40 % la energía dedicada a la refrigeración de los centros de datos de Google, una mejora equivalente a una caída del 15 % en el PUE (Power Usage Effectiveness), y ahora asume directamente el control de la refrigeración con algoritmos de aprendizaje automático. Este éxito no es solo una victoria operativa; es la prueba viva de que la inteligencia artificial puede actuar como palanca para reducir el consumo energético de las infraestructuras más intensivas del mundo.

La sinergia entre Google, PJM y Tapestry ha llevado esta misma lógica a escala nacional. Mediante modelos de IA que analizan la demanda y la oferta de electricidad en Estados Unidos, se está modernizando la gestión de la red eléctrica, equilibrando fuentes variables como la eólica y la solar con una precisión antes impensable. Conectar nuevos generadores, anticipar la congestión y asignar la carga de forma más inteligente permite integrar mejor la generación renovable y aprovechar mejor la red existente, y ha reducido la necesidad de centrales de reserva costosas y contaminantes.

Más allá de la optimización operativa, la IA se está convirtiendo en una herramienta de descubrimiento científico. Los modelos de aprendizaje automático aceleran la búsqueda de nuevos materiales para baterías de alta densidad energética, y han reducido el tiempo de investigación que antes se contaba en años. Este avance no solo promete vehículos eléctricos más eficientes; también ofrece soluciones de almacenamiento para las redes renovables que, sin una batería fiable, se ven limitadas por su carácter intermitente.

A la vez, los modelos climáticos basados en IA han llegado a un nuevo nivel de resolución. Combinando datos de satélite con aprendizaje profundo, los equipos de investigación pueden simular escenarios con un detalle que antes era inalcanzable. Este grado de precisión permite a los planificadores urbanos y a los gestores de recursos hídricos tomar decisiones informadas sobre infraestructuras resilientes, y ha reducido los costes sociales y evitado desastres ambientales.

La conjunción de estas aplicaciones demuestra que la IA no es solo un consumidor voraz de energía; es una fuerza multiplicadora de la eficiencia energética. Cada grado centígrado que se reduce en los centros de datos, cada punto ganado en la integración renovable y cada mejora en el almacenamiento en baterías representa un paso hacia un futuro donde el coste ambiental de la computación se vuelve marginal. No obstante, este potencial solo se materializará si las políticas energéticas reconocen estas sinergias y las apoyan, con inversión en infraestructuras inteligentes y en investigación de energía limpia que alimente los cerebros digitales del mañana.

La sed de energía

Los centros de datos son los monstruos invisibles que alimentan la revolución de la inteligencia artificial. Su consumo eléctrico, ya impresionante, está a punto de explotar en una escala que supera las fronteras nacionales. Según las proyecciones más recientes, la energía total que absorben estos hubs digitales pasará de aproximadamente **485 TWh** en 2025 a **~950 TWh** en 2030 —casi la misma cantidad que consume todo Japón— y se extenderá hasta unos **~1.200 TWh** en 2035 [2]. Esta escalada no es un simple incremento de demanda; representa una nueva forma de presión sobre las redes eléctricas globales, una tensión que podría desestabilizar los esfuerzos de descarbonización si no se gestiona con cuidado.

En este contexto, la herramienta que debería actuar como motor de ahorro energético —la propia IA— se convierte en una paradoja. Para entrenar modelos cada vez más sofisticados y ofrecer servicios en tiempo real, las infraestructuras digitales necesitan energía colosal, a menudo procedente de fuentes todavía no completamente limpias. Cada iteración de un gran modelo de lenguaje exige una enorme cantidad de energía solo para su entrenamiento inicial; el coste energético de los procesos de inferencia continuada y de la actualización constante de pesos puede equivaler al de una pequeña ciudad industrial.

DeepMind ha conseguido reducir un 40 % la energía necesaria para la refrigeración de sus centros de datos, una mejora que se traduce en una caída del 15 % del **PUE** (Power Usage Effectiveness) y ahora controla directamente [1]; como ya se ha señalado, esta reducción es solo una gota dentro de un océano que se amplía a ritmos exponenciales. La modernización de las redes eléctricas con IA —como la colaboración entre Google, PJM y Tapestry para optimizar la distribución y la asignación de carga— es un paso imprescindible, pero solo puede ser efectiva si se combina con una fuente de energía limpia y abundante.

La cuestión clave, pues, no es solo reducir el consumo por unidad de cálculo, sino asegurar que la suma total de energía requerida provenga de fuentes renovables. Esto implica una inversión masiva en infraestructura inteligente: baterías avanzadas, microrredes y sistemas de gestión dinámica que puedan responder a las fluctuaciones de demanda de forma instantánea. Sin este marco, la IA podría convertirse en la nueva «sed de energía» del planeta, un consumidor voraz que absorbe recursos escasos y pone en peligro los objetivos climáticos establecidos para 2030.

Por tanto, la decisión que ha de tomar la comunidad global —gobiernos, empresas tecnológicas e inversores— es clara: canalizar las políticas energéticas hacia una sinergia entre IA y energía limpia, como hemos visto. Esto no solo garantizará que los avances en inteligencia artificial sean sostenibles, sino que convertirá la IA en un aliado para la transición verde, más que en un obstáculo energético. En este equilibrio delicado se encuentra una de las decisiones más cruciales de la década.

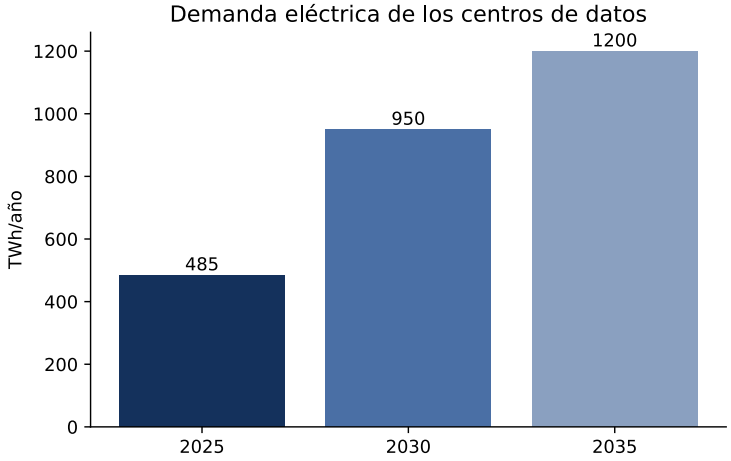


Figura 9.1 — El consumo eléctrico de los centros de datos se duplica hacia 2030 (~950 TWh), impulsado por la IA.

Resolver la paradoja

Así, la solución no consiste en detener el desarrollo de la inteligencia artificial, sino en alimentarla con energía limpia y transparente. En un mundo donde los centros de datos son cada vez más grandes e intensivos, la estrategia clave pasa por situar estas instalaciones cerca de orígenes renovables —parques eólicos, campos fotovoltaicos o centrales hidroeléctricas— y aprovechar la flexibilidad intrínseca de los procesos de entrenamiento e inferencia para equilibrar la demanda con la oferta variable de la red. Esta sinergia se traduce en tres pilares operativos.

Primero, la **localización inteligente**. Las empresas tecnológicas ya están desplegando centros de datos en zonas donde el coste marginal de la electricidad renovable es mínimo. Situar la computación cerca de grandes parques solares o de eólica offshore conectada directamente a instalaciones de alta densidad reduce las pérdidas de transmisión y permite aprovechar la energía limpia en el mismo punto donde se genera, en lugar de transportarla a largas distancias.

Segundo, la **demanda flexible**. La IA puede programarse para realizar tareas intensivas durante periodos de superávit renovable —las horas de más sol o de viento más fuerte— y reducir el consumo en momentos de déficit. DeepMind ha demostrado que este enfoque no solo minimiza el impacto ambiental, sino que también optimiza los costes operativos: la compañía consiguió una reducción del 40 % en energía dedicada a la refrigeración de sus centros de datos, y esto se tradujo en una caída del 15 % del PUE (Power Usage Effectiveness) [1]. Esta capacidad de «cargar» la IA con energía limpia se convierte, por tanto, en un pago indirecto: el algoritmo contribuye a la transición verde reduciendo la necesidad de fuentes fósiles y, al mismo tiempo, beneficia su propio coste de ejecución.

Tercero, la **transparencia del consumo**. Exigir que las empresas publiquen informes detallados sobre la procedencia y la eficiencia energética de sus centros de datos es una demanda cada vez más fuerte por parte de los reguladores y los inversores. El establecimiento de estándares comunes que permitan comparar y validar las prácticas sostenibles a escala mundial crea un mercado de confianza donde la IA se convierte en una garantía de credibilidad ambiental, no solo en un consumidor voraz.

Como hemos visto, el consumo de los centros de datos va camino de duplicarse en cinco años, y de seguir creciendo después [2]. Sin una respuesta coordinada, la IA amenazaría con convertirse en un emisor neto de carbono que contrarresta las ganancias climáticas logradas por las energías renovables; pero si se convierte en un motor que impulse la propia transición —optimizando redes, prediciendo fallos y maximizando el uso de energía limpia— la IA pagaría con creces su factura energética y convertiría el riesgo en una oportunidad. Ahora hacen falta políticas coherentes, inversión en infraestructura renovable y un compromiso firme de transparencia que permitan a la inteligencia artificial ser tanto la salvación como el motor de una economía limpia y resiliente.

La promesa y el peligro

Imagina una sala de control donde miles de servidores fluyen como un río de electricidad líquida y, en el centro, una mente artificial que recalcula la ruta óptima para cada bit. Esta es la promesa de la IA:

optimizar el funcionamiento de una red global aumentando su eficiencia energética gracias a algoritmos de aprendizaje automático que priorizan fuentes renovables y minimizan las pérdidas. En la fabricación, los modelos generativos ajustan la composición de los materiales con una precisión que antes requeriría años de pruebas; en la agricultura, la IA predice microclimas locales y regula el riego en tiempo real, evitando el despilfarro de agua y reduciendo las emisiones a escala regional. Estas mejoras se traducen en una disminución directa de la demanda energética global: cada gigavatio-hora ahorrado es un paso más hacia el cumplimiento de los objetivos del Acuerdo de París.

No obstante, si se alimenta de una infraestructura sucia y poco transparente, esta potencia se convierte en el nuevo motor de un consumo energético descontrolado. Los grandes modelos de lenguaje requieren centros de datos con el hambre eléctrica que ya hemos cuantificado [2]. Sin un marco regulador que imponga límites de emisiones y exija certificaciones de carbono para cada operación de entrenamiento, la IA podría actuar como una coartada para empresas que, en lugar de invertir en renovables, simplemente aumentan su consumo para mantener la competitividad. Esto intensifica la presión sobre las redes eléctricas y crea un incentivo perverso: más IA, más necesidad de energía, y una justificación para retrasar políticas climáticas críticas.

Esta dualidad se manifiesta también en la gestión de datos. Una IA que optimiza la distribución de carga a través de redes inteligentes puede reducir el PUE (Power Usage Effectiveness) de un centro de datos, como ha demostrado DeepMind con una mejora del 40 % en la energía de refrigeración, equivalente a una caída del 15 % del PUE [1]. Pero, si esta optimización se mantiene dentro de una «caja negra», las empresas pueden ocultar el crecimiento exponencial del consumo energético bajo la capa de eficiencia aparente, dificultando la supervisión pública e impidiendo que los reguladores apliquen medidas correctivas en tiempo real.

La clave para transformar esta tensión reside en tres pilares interdependientes: transparencia, responsabilidad y alineación con fuentes limpias. Primero, las organizaciones han de abrir sus herramientas de optimización energética, permitiendo auditorías independientes que verifiquen el impacto real frente a las declaraciones de mejora. Segundo, hay que establecer marcos legales que obliguen a reportar el consumo total de energía por cada modelo entrenado y operado, con penalizaciones por exceder los límites preestablecidos. Finalmente, las inversiones en infraestructura renovable —desde baterías avanzadas hasta microrredes solares y eólicas— han de estar vinculadas directamente al crecimiento computacional: cada nuevo incremento de capacidad de cálculo ha de ir acompañado de una capacidad equivalente de energía limpia.

En resumen, la IA puede ser el motor que impulse una transición energética más rápida y eficiente; pero solo si se gobierna con rigor y se conecta intrínsecamente a fuentes limpias. Sin estas garantías, la propia inteligencia artificial podría convertirse en el último gran consumidor de energía, retrasando las decisiones climáticas que en 2026 ya no se pueden permitir posponer.

La otra sed

En el silencio frío de un centro de datos, una voz sintética explicó con la misma convicción que un juez experimentado por qué el cambio climático era solo una leyenda urbana. Aquel fragmento, generado en menos de una hora por un modelo de lenguaje entrenado sobre miles de millones de textos, se difundió en las redes sociales y, en cuestión de minutos, fue citado como prueba definitiva de un escándalo medioambiental fabricado. Este es el reflejo más súbito de la tercera dimensión de la inteligencia artificial: no solo consume energía, sino que también puede consumirnos la capacidad de discernir la realidad.

La crisis de la verdad se presenta como una amenaza transversal que atraviesa sectores, desde la energía hasta la salud y la seguridad nacional. Cuando un algoritmo engendra imágenes, audios y textos indistinguibles de las creaciones humanas, el coste de verificar cada afirmación aumenta exponencialmente. La demanda de herramientas de rastreo de fuentes y de verificación de contenidos ha crecido con fuerza, impulsada por start-ups especializadas en aprendizaje automático y en el anclaje de pruebas. Este aumento no es solo una oportunidad de negocio; es una señal de alarma que indica cómo el consumo energético de las redes de verificación se convierte en otro nudo del problema.

Al mismo tiempo, las grandes corporaciones de la nube, conscientes de su papel clave, han empezado a integrar mecanismos para registrar y validar la procedencia de cada contenido. Google, con la ayuda de DeepMind, ha reducido la energía de refrigeración de sus centros de datos un 40 % —una caída del 15 % en el PUE— y ahora intenta aplicar esta misma eficiencia a las cadenas de verificación de contenido; pero todavía se enfrenta a un desafío: ¿cómo garantizar que la infraestructura energética que sustenta estos

procesos sea limpia? Si el coste energético de una verdad certificada supera la producción neta de energía renovable disponible, nos enfrentaremos a una paradoja donde la solución tecnológica se convierte en el origen del problema.

La respuesta no puede ser solo técnica; ha de ser institucional y cultural. Primero, las políticas públicas han de establecer estándares mínimos de eficiencia energética para sistemas de IA que generen contenido público. Segundo, las empresas han de adoptar una arquitectura donde cada modelo se diseñe teniendo como primer requisito la compatibilidad con fuentes renovables y el balance energético neto. Finalmente, los ciudadanos han de estar equipados con herramientas de alfabetización digital que les permitan reconocer deepfakes y desinformación generada por IA, una inversión en capital humano tan crucial como cualquier instalación solar.

En resumen, la crisis de la verdad es el nuevo frente donde se disputa el futuro energético. Si no conseguimos alinear la potencia computacional de la IA con una infraestructura limpia y transparente, corremos el riesgo de que las mentiras generadas por máquinas eclipsen las soluciones reales a la crisis climática. El momento de actuar es ahora: establecer reglas claras, impulsar innovaciones sostenibles y educar a la sociedad para que la verdad no se convierta en un recurso escaso sino en el fundamento sobre el que construir una transición energética verdadera.

---

[1] Google DeepMind, *AI reduces data centre cooling energy by 40%*. https://deepmind.google/blog/deepmind-ai-reduces-google-data-centre-cooling-bill-by-40/ ↩

[2] AIE, *Energy and AI — Executive summary*. https://www.iea.org/reports/energy-and-ai/executive-summary ↩

La crisis de la verdad: desinformación y deepfakes

«El Partido te decía que rechazaras la evidencia de tus ojos y tus oídos. Era su orden final, la más esencial.»

— George Orwell, 1984 (1949)

En una sala austera de un tribunal francés, en 2025, los magistrados pronunciaron una sentencia que parecía una chispa de luz en medio de una guerra desigual por la verdad. Ante un público reducido —abogados, periodistas y un grupo escaso de activistas climáticos— se leyó el veredicto contra TotalEnergies, la gigante petrolera que durante años había construido una narrativa de «carbono neutral» en torno a sus proyectos de energía renovable.

El tribunal declaró que el mensaje publicitario era engañoso y constituía una forma de greenwashing que vulneraba la confianza del consumidor y distorsionaba las políticas públicas de transición energética. Cuando una empresa proclama neutralidad de carbono sin pruebas verificables y sin compensar las emisiones reales, se convierte en un actor que alimenta la desinformación fósil.

La audiencia sintió cómo una pequeña pero significativa victoria resonaba entre las paredes de la sala. Un grupo de activistas se levantó y aplaudió en silencio. Los abogados de TotalEnergies, visiblemente sorprendidos, intentaron argumentar que la compañía había invertido en proyectos de energía eólica y solar, pero el tribunal rechazó esta defensa como una compensación simbólicamente insuficiente.

Esta sentencia no solo marcaba un precedente legal en Europa; era una señal clara de que la sociedad ya no toleraría las promesas vacías. La decisión se basó en el análisis de informes independientes que demostraban que el término «neutral» no se correspondía con las emisiones reales de la empresa.

Esta pequeña victoria, tan singular y limitada como una gota de agua en un océano de mentiras, se convierte en el primer paso de una lucha que se extiende más allá del sector energético. Enfrentarse al greenwashing es esencial para restaurar la confianza colectiva y permitir que las políticas climáticas se guíen por datos reales y no por narrativas fabricadas. La decisión de 2025, pese a ser un acontecimiento puntual, simboliza el potencial de un sistema judicial que puede frenar la erosión de la verdad compartida —una erosión que, si se deja sin respuesta, paralizaría la gobernanza necesaria para la transición energética.

Décadas de ingeniería de la duda

A finales de la década de los setenta, mientras las primeras alertas científicas sobre el cambio climático emergían en revistas especializadas, otra conversación se estaba tejiendo en las salas de conferencia de las grandes compañías petroleras. No era solo un ensayo de información; era un proyecto deliberado para sembrar incertidumbre y diluir la responsabilidad. El American Petroleum Institute (API) formalizó esta estrategia en un memorándum interno de 1998 que declaraba con una claridad fría: «la victoria se alcanza cuando el ciudadano medio reconoce incertidumbres en la ciencia climática» [1]. Aquel documento no solo reflejaba una percepción de la opinión pública como obstáculo, sino que la convertía en un objetivo estratégico.

Esta «ingeniería de la duda» se desplegó con las mismas técnicas que una campaña publicitaria: selección interesada de estudios científicos, promoción de voces escépticas y financiación de grupos de presión que ponían en duda la existencia o la gravedad del fenómeno. Los resultados fueron inmediatos y profundos. Durante los años noventa y la década de 2000, el debate público se transformó de una discusión basada en evidencias a una arena donde las opiniones se alineaban con intereses económicos. Las redes sociales todavía no existían; la difusión se hacía por medios tradicionales, pero el impacto era igual de devastador: un segmento creciente del público empezaba a percibir el cambio climático como una cuestión incierta y politizada.

A medida que las generaciones posteriores crecieron con esta narrativa fragmentada, la confianza colectiva en la ciencia se erosionó. El resultado es una opinión pública fracturada, donde los consensos científicos son vistos como puntos de partida para disputas ideológicas más que como hitos incuestionables. Esta fractura no solo ha retrasado las políticas climáticas; ha creado un ambiente en el

que cualquier propuesta de acción se encuentra con una resistencia preexistente, alimentada por la memoria colectiva de la «duda» sembrada hace más de tres décadas.

La herencia de estas prácticas se manifiesta hoy en formas nuevas pero reconocibles: las campañas de greenwashing que presentan productos y servicios como sostenibles sin fundamento real, y los deepfakes que manipulan la información visual y auditiva con una precisión que supera lo que jamás se había imaginado. Pero el hilo conductor es el mismo: una estrategia para desestabilizar la verdad compartida y crear espacios donde las narrativas de poder puedan prosperar sin ser cuestionadas.

En este contexto, la ausencia de una materia prima sólida no solo impide que las políticas climáticas sean adoptadas; amenaza el tejido mismo de la gobernanza democrática. Sin una verdad consensuada, los procesos de decisión se convierten en juegos de información, donde el ganador es quien controla la percepción, no quien ofrece las soluciones más eficientes. La desinformación, entonces, deja de ser un simple subproducto del debate y se convierte en un arma estructural que paraliza la aceleración necesaria hacia una transición energética justa y sostenible.

Esta herencia de ingeniería de la duda es el punto de partida para comprender cómo la crisis de la verdad ha llegado a su pico actual, y para explorar las herramientas —como la prueba de existencia que se desarrollará en la Parte IV— que podrían restaurar la confianza y permitir una gobernanza basada en hechos reales.

El greenwashing, a juicio

2025 marcó un punto de inflexión en la lucha contra el lavado verde: por primera vez las sanciones económicas se convirtieron en testigos públicos de que el engaño ambiental ya no podía quedar impune. Shein, la icónica marca de moda rápida, recibió una multa de **1,15 millones de euros** por haber promocionado sus colecciones como «eco-friendly» mientras su modelo de negocio seguía dependiendo de tejidos sintéticos de gran impacto climático. Al mismo tiempo, un **tribunal francés** condenó a **TotalEnergies** por presentar como engañoso su mensaje de «carbono neutral», una decisión que ha encendido un debate sobre la responsabilidad legal de las grandes empresas energéticas en la era de la transparencia digital.

Quizá más impactante fue el caso del gestor de activos **DWS**, multado con **25 millones de euros** por exagerar sus credenciales ESG y vender productos financieros como «verdes» cuando, en realidad, no respondían a esas promesas. Este escándalo no solo sacudió los mercados de capital, sino que también puso de relieve la fragilidad del marco regulador existente: las declaraciones ESG, a menudo basadas en auditorías internas y certificaciones de terceros, se revelaron vulnerables a manipulaciones sofisticadas.

En respuesta, la **relatora especial de las Naciones Unidas** ha reclamado una medida que ha generado un clamor internacional: criminalizar la desinformación y el greenwashing de la industria fósil. Su posición sostiene que el engaño medioambiental no es solo una infracción administrativa, sino una amenaza directa a la confianza pública y a la voluntad política necesarias para la acción climática [2].

Esta respuesta jurídica, sin embargo, todavía corre por detrás del ritmo al que se generan las nuevas formas de manipulación. Las empresas, ahora más conscientes de los riesgos legales, recurren a la inteligencia artificial para crear narrativas «verdes» que parecen creíbles y, a la vez, son difíciles de desmontar sin una prueba robusta. Los algoritmos pueden generar informes ESG engañosos en cuestión de minutos, y las plataformas sociales amplifican estos mensajes con la ayuda de cuentas automatizadas que imitan voces auténticas.

Así, mientras el derecho empieza a reaccionar con sanciones y propuestas legislativas, el fenómeno del greenwashing evoluciona hacia formas más sofisticadas y difusas. La necesidad de mecanismos verificables —como la prueba de existencia que se desarrollará en la Parte IV— se vuelve urgente: solo una capa de confianza basada en datos inalterables puede contrarrestar la ola de desinformación ambiental que, como el humo de las centrales de carbón, esconde la verdad y paraliza la gobernanza necesaria para una transición energética justa.

En este escenario, la lucha contra el lavado verde no es solo un asunto de multas; es una batalla por preservar la credibilidad del discurso climático y garantizar que las políticas públicas se fundamenten en hechos verificables, no en promesas engañosas. La respuesta jurídica ha de ir acompañada de herramientas tecnológicas que aseguren la trazabilidad y la veracidad de cada afirmación ambiental,

porque solo así podremos restaurar la confianza colectiva y avanzar hacia una sociedad basada en la verdad compartida.

Las deepfakes industrializan la mentira

En los últimos dos años, la IA generativa ha transformado lo que antes era una curiosidad académica en un instrumento de producción masiva de engaño. El número de deepfakes creados a nivel mundial ha estallado de **~500.000** en 2023 a **8 millones** en 2025, una tasa de crecimiento que supera cualquier evolución tecnológica reciente en la historia digital [3]. Esta explosión no es un simple incremento numérico; es la manifestación de una nueva economía de la falsedad donde las imágenes y los audios pueden fabricarse a pequeña escala con recursos mínimos, pero también a gran escala por parte de entidades organizadas.

Europol ha alertado de que, si esta tendencia continúa, **hasta el 90 % del contenido en línea podría ser sintético en 2026** [3]. Esta proyección no solo representa una cifra alarmante; es un indicio claro de que la confianza por defecto —el supuesto de que lo que vemos en internet refleja la realidad— está llegando a su punto de ruptura. Cuando cualquier fotografía, vídeo o declaración puede ser generada artificialmente con una calidad casi indistinguible del material auténtico, el hilo conductor que sostiene las relaciones sociales y políticas se desintegra.

Las consecuencias de este fenómeno son múltiples e interdependientes. En primer lugar, la **credibilidad de las instituciones** queda en juego. Una declaración oficial manipulada puede difundirse como prueba irrefutable de un error o una mala intención, alimentando el cinismo ciudadano y menguando la autoridad de los gobiernos. En segundo lugar, los mercados financieros se ven vulnerables a **campañas de desinformación** que pueden manipular precios de acciones con vídeos falsos de ejecutivos o informes falsificados sobre resultados empresariales. Finalmente, la **seguridad nacional** queda expuesta: las deepfakes pueden usarse para crear falsas declaraciones de Estado, provocar crisis diplomáticas o incitar al odio y al conflicto.

Esta nueva era de mentira industrial no es una mera extensión del greenwashing tradicional. Mientras que el primero se basa en la manipulación de datos ambientales para mejorar la imagen corporativa —como demuestran los escándalos de Shein, TotalEnergies y DWS— las deepfakes operan a un nivel más visceral: alteran la percepción directa de lo que es real. Esto crea una **barrera cognitiva** que impide a los ciudadanos distinguir entre información fiable y engaño, aumentando la polarización y reduciendo el espacio para el diálogo constructivo.

Para combatir esta amenaza hay que adoptar una doble estrategia: **tecnológica y normativa**. Desde un punto de vista tecnológico, las soluciones que anclan el origen y la integridad de los contenidos digitales —como el marco «t2p» que desarrollaremos en la Parte IV— ofrecen una pista para verificar la procedencia de lo que vemos. Desde el punto de vista normativo, hay que establecer marcos legales que penalicen la creación y difusión malintencionada de deepfakes, tal como ya se ha empezado a hacer con el greenwashing sancionado en 2025 [2].

En síntesis, la industrialización de las mentiras a través de las deepfakes representa un **punto crítico** para la confianza colectiva. Si no se toman medidas decisivas ahora, la sociedad podría entrar en una era donde la verdad compartida deja de existir y las decisiones políticas se basan únicamente en percepciones manipuladas. El reto es grande, pero la combinación de tecnología verificable y regulación rigurosa ofrece un camino viable para restaurar la fe en lo que vemos y escuchamos.

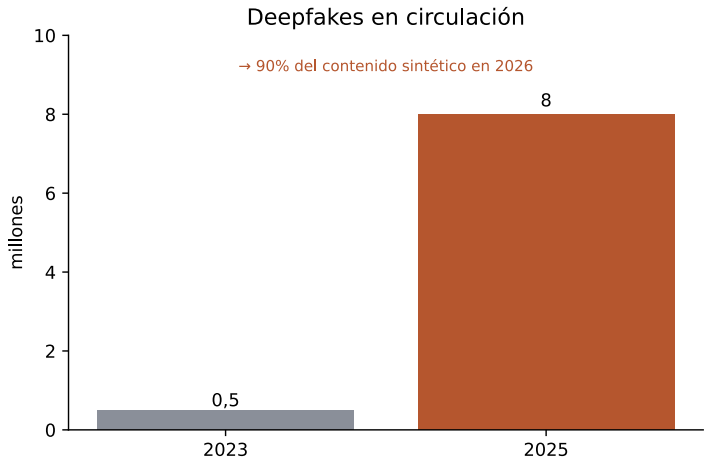


Figura 10.1 — Las deepfakes se multiplican: de ~500.000 (2023) a 8 millones (2025), camino del 90 % del contenido en línea en 2026.

Por qué esto mata la transición

En una era donde las políticas climáticas se miden en décimas de grado y en toneladas de emisiones evitadas, la confianza en los datos es el combustible invisible que impulsa la descarbonización. Sin fuentes fiables, cualquier objetivo se convierte en un espejismo: los inversores no pueden validar si una planta solar produce realmente la energía anunciada; los reguladores desconocen si las declaraciones de emisiones de una empresa petroquímica son auténticas o manipuladas; y la ciudadanía, que ha de soportar las decisiones públicas, se encuentra ante un laberinto de información incierta.

El problema se intensifica cuando el falsificador no solo altera datos numéricos, sino que fabrica narrativas visuales enteras. Un vídeo de una instalación eólica con turbinas girando majestuosamente sobre la costa puede salir de una IA sin ninguna conexión con una infraestructura real. Cuando las imágenes y los sonidos son tan fáciles de fabricar como hemos cuantificado, el criterio tradicional «ver es creer» se desvanece.

Esta erosión de confianza tiene repercusiones inmediatas en el mercado de los capitales verdes. El greenwashing ha llegado a un punto de inflexión: solo en 2025, empresas como Shein (multada con 1,15 millones de euros) y TotalEnergies (condenada por un tribunal francés por su mensaje de «carbono neutral») fueron sancionadas, y DWS pagó 25 millones de euros por exagerar sus credenciales ESG [2]. La relatora de la ONU ha pedido que estas conductas se criminalicen, reconociendo que el fraude ambiental no solo engaña a los inversores, sino que distorsiona las políticas climáticas globales.

Además, la crisis de verdad afecta directamente a las metas establecidas en acuerdos internacionales. Un memorándum del American Petroleum Institute de 1998 ya advertía que «la victoria se alcanza cuando el ciudadano medio reconoce incertidumbres en la ciencia climática» [1]; hoy esa incertidumbre es artificial. Si las emisiones declaradas son manipuladas, los informes de avance hacia la neutralidad de carbono se convierten en simples documentos de marketing, y los reguladores, sin herramientas para verificar la autenticidad, se ven obligados a basarse en declaraciones tan falsas como un vídeo generado por IA.

En resumen, la incapacidad de identificar datos fiables paraliza cualquier esfuerzo de descarbonización creíble. La transición depende de una cadena de confianza: desde el laboratorio donde se mide el CO_2 hasta el consejo de administración que aprueba un proyecto de energía renovable. Cuando esta cadena se rompe por la desinformación y los deepfakes, las decisiones políticas se basan en percepciones manipuladas y la sociedad corre el riesgo de quedar atrapada en una espiral de duda e inacción. La solución no es solo técnica; requiere un marco regulador riguroso y tecnologías verificables que restauren la fe en lo que vemos y escuchamos.

La promesa y el peligro

En este momento histórico somos testigos de una doble explosión de incertidumbres: la crisis climática que ya se mide en grados y millones de muertes evitables, y una erosión acelerada de la verdad compartida que transforma cada dato en un posible engaño. La **promesa** es clara y sin precedentes: por primera vez

disponemos de herramientas capaces de detectar, desenmascarar y validar la información a escala global, abriendo el camino para que la sociedad pueda recuperar la confianza en sus propias percepciones.

Las tecnologías emergentes —algoritmos de detección de manipulaciones, sistemas de certificación del origen del contenido y plataformas de auditoría abierta que integran pruebas criptográficas— empiezan a ofrecer vías para rastrear cada pieza de información hasta su fuente original, creando una capa de transparencia que antes era impensable. Estas soluciones se convierten en los pilares del futuro **t2p**, el marco que la Parte IV desarrollará para contrarrestar la ola de desinformación.

No obstante, el **peligro** que se esconde detrás de esta oportunidad es tan real como las incertidumbres climáticas que intentamos mitigar. Si no actuamos con urgencia y rigor regulador, la crisis de la verdad alimentará una retroalimentación negativa con la crisis climática: una población cada vez más desconfiada rehusará aceptar datos científicos, retrasando políticas esenciales como la descarbonización del sector energético. Las cifras que hemos visto —ocho millones de deepfakes y un internet camino de ser mayoritariamente sintético— dibujan una saturación de falsedades donde las decisiones políticas se toman sobre bases manipuladas, y dejan a la sociedad atrapada en una espiral de duda e inacción.

Además, el fenómeno del **greenwashing** se ha convertido en un verdadero riesgo reputacional y legal: empresas como Shein han pagado **1,15 millones de euros** por sanciones relacionadas con declaraciones engañosas sobre sostenibilidad [2]; TotalEnergies ha sido condenada por un tribunal francés por su mensaje de «carbono neutral», y DWS ha sido multada con **25 millones de euros** por exagerar sus credenciales ESG. La relatora especial de las Naciones Unidas ya ha pedido la criminalización de estas prácticas, subrayando el riesgo de una regulación ineficaz si no se reconoce la dimensión tecnológica del problema.

En resumen, la **promesa** reside en la capacidad de las nuevas herramientas para restaurar la confianza y establecer un nuevo contrato social basado en pruebas verificables; el **peligro**, si dejamos que la desinformación siga proliferando sin una respuesta coordinada, es que la crisis climática se vea aún más obstaculizada, conduciendo a una parálisis global donde ni las políticas ni las acciones individuales podrán avanzar. La decisión clave está ante nosotros: invertir ahora en infraestructuras de verificación y en un marco legal robusto, o ver cómo ambas crisis se refuerzan mutuamente hasta el punto de un bloqueo irreversible.

Además de alejarnos de las falsedades visibles, hemos de enfrentar lo que Beth Noveck llama el «dividendo del mentiroso»: la capacidad de las deepfakes no solo crea engaños, sino que ofrece una defensa fácil a quien quiere borrar datos incómodos: descartarlos como simples «montajes de IA» [4]. Este escenario transforma lo falso en un instrumento de negación estructural; cualquier informe científico que advierta sobre el calentamiento global podría ser reducido a una invención digital y quedar sin peso ante el público. Para romper este círculo hace falta un ancla neutral —un registro criptográfico inmutable que demuestre que un hecho real existió antes de ser manipulado—, más allá de los sistemas de detección o de las marcas de agua como C2PA. La prueba de existencia basada en blockchain, independiente del creador y sin depender de terceros, ofrece exactamente ese punto de llegada: no pretende detectar lo falso: certifica la autenticidad del original, e impide que la verdad se pueda descartar como una simple ilusión. El robocall clonado de Joe Biden de enero de 2024, sancionado por la FCC con una alerta contra las llamadas automáticas, ejemplifica cómo una prueba de existencia neutral habría permitido contrastar su origen y frenar su difusión incontrolada [5].

El doble diagnóstico

Hemos diagnosticado el doble problema: energía y verdad. La crisis climática ya no es solo una cuestión de fuentes de energía o de políticas de descarbonización; ahora se encuentra paralelamente con un colapso de la verdad compartida, alimentado por la desinformación fósil, el greenwashing y los deepfakes. Esta erosión de la confianza pública paraliza la gobernanza que la transición energética necesita para avanzar. Sin una base común de información fiable, las decisiones colectivas se convierten en un juego de azar donde las narrativas manipuladas ganan protagonismo sobre los datos reales.

Los indicios son innegables: el memorándum del American Petroleum Institute de 1998 ya advertía que «la victoria se alcanza cuando el ciudadano medio reconoce incertidumbres en la ciencia climática» [1]. Hoy, esas incertidumbres se convierten en una inundación deliberada de información falsa. El greenwashing ha pasado de ser un simple recurso de marketing a una amenaza legal: en 2025, Shein fue multada con 1,15 millones de euros por prácticas engañosas; TotalEnergies fue condenada por un tribunal francés; y DWS pagó 25 millones de euros por exagerar sus credenciales ESG [2]. La relatora de la ONU ya

pide que se criminalice este comportamiento, reconociendo su impacto devastador sobre la confianza del mercado y la voluntad política.

Paralelamente, la fábrica de deepfakes se ha disparado hasta los volúmenes que abrían este capítulo [3]. Esta realidad no solo desorienta a la opinión pública: compromete la seguridad nacional, los procesos judiciales y las negociaciones internacionales.

La respuesta ha de ser tan doble como el problema: hemos de invertir ahora en infraestructuras de verificación robustas y establecer marcos legales que penalicen la manipulación deliberada. Es aquí donde la Parte IV del libro ofrece una vía de salida concreta. La inteligencia artificial, combinada con la blockchain, puede crear un registro inmutable de origen y autenticidad, una prueba de existencia (t2p) que permitirá validar información en tiempo real y hacer frente a los deepfakes con evidencias verificables.

En este contexto, nuestra llamada a la acción es clara: **actuar ahora**. Las empresas, los gobiernos y la sociedad civil han de adoptar sistemas de certificación transparentes y auditables; han de promover legislaciones que definan sanciones severas para el greenwashing y la difusión deliberada de falsedades; y han de invertir en educación mediática avanzada para capacitar a los ciudadanos a reconocer y rechazar el contenido manipulado.

Como hemos visto, no podemos permitir que las dos crisis se refuercen mutuamente hasta el punto de un bloqueo irreversible. La verdad es el combustible de la confianza, y la confianza es el engranaje que hará girar la rueda de la transición energética. Con las herramientas adecuadas —IA, blockchain y una regulación decidida— podemos restaurar esta base esencial y transformar la crisis en una oportunidad para un futuro más resiliente y transparente. El momento de actuar es ahora; el futuro depende de nuestra capacidad de reconstruir la verdad compartida.

---

[1] Union of Concerned Scientists, *Fossil fuel industry's decades of deceit.* https://www.ucs.org/about/news/new-ucs-report-details-fossil-fuel-industry-decades-deceit ↩

[2] Naciones Unidas, *Greenwashing*. https://www.un.org/en/climatechange/science/climate-issues/greenwashing ↩

[3] (deepfakes) Blockchain Council / Europol — véase research 00 §6. https://www.blockchain-council.org/blockchain/preventing-deepfake-fraud-with-blockchain-content-provenance-verification-workflows/ ↩

[4] Beth Simone Noveck — *Reboot: AI and the Race to Save Democracy* (Yale UP, 2026), cap. 3. ↩

[5] FCC (2024). https://www.fcc.gov/document/fcc-makes-ai-generated-voice-robocalls-illegal ↩

Seguridad energética reinventada: redes inteligentes e IA

«En el petróleo, la seguridad y la certeza residen en la variedad, y solo en la variedad.»

— Winston Churchill, Cámara de los Comunes (1913)

Era una tarde fría de octubre de 2028 cuando el núcleo de la central nuclear de Three Mile Island, que durante décadas había simbolizado el peor accidente nuclear de la historia norteamericana, volvió a vibrar. Los monitores de control mostraban un flujo constante de electrones limpios: 837 MW de electricidad emergían de la Unidad 1 rehabilitada por Microsoft y Constellation, alimentando una constelación de centros de datos que procesaban modelos de inteligencia artificial para la gestión global de la red eléctrica.

Los trabajadores del proyecto, reunidos ante las grandes puertas de acero, observaban cómo los gráficos de potencia se alzaban en una curva suave pero implacable. «Esto no es solo un retorno a la actividad», decía el sentimiento compartido en la sala de control, «es la prueba de que la seguridad energética del futuro se mide en electrones fiables, no en barriles».

Mientras las turbinas se ponían en marcha, una pantalla mostraba el logotipo de Microsoft junto al de Helion, recordando al mundo que la fusión nuclear —todavía en fase experimental— era el objetivo de su acuerdo de suministro para 2028 [2]. Otra pantalla recordaba el reactor modular de 500 MW que Google había encargado a Kairos Power, con la primera unidad programada para entrar en funcionamiento en 2030 [2]. La misma pantalla anunciaba que DeepMind había reducido un 40 % el consumo energético de refrigeración de los centros de datos de Google, una eficiencia que se traduce directamente en menos demanda sobre la infraestructura física y, por tanto, en más margen para fuentes renovables [1].

En el exterior, los campos verdes donde antes se extendían las estructuras de almacenamiento de combustibles fósiles ahora estaban recubiertos de paneles solares y turbinas eólicas que, sincronizadas con algoritmos predictivos desarrollados por Google, PJM y Tapestry, equilibraban la carga en tiempo real, evitando los picos que tradicionalmente provocaban fallos de suministro [1].

El ruido habitual de una central nuclear —el zumbido constante de los sistemas de seguridad, las alarmas de presión— había sido reemplazado por una melodía casi musical: el susurro de los servidores que optimizaban la distribución de energía y el suave zumbido de las turbinas modernizadas. La atmósfera era de confianza renovada; cada electrón que atravesaba las líneas se contaba como testigo de una nueva era donde la inteligencia artificial no solo predecía la demanda, sino que también aseguraba su entrega sin interrupciones ni vulnerabilidades.

Aquel momento marcó un punto de inflexión en la narrativa de la seguridad energética: ya no se trataba de controlar el petróleo, sino de crear una red resiliente e inteligente capaz de autosostenerse y adaptarse a las necesidades del mundo digital. La reactivación de Three Mile Island no era solo un retorno al pasado industrial; era la confirmación de que la confianza en la energía se puede reconstruir sobre cimientos digitales, donde cada dato, cada modelo de IA y cada registro criptográfico contribuyen a garantizar que el futuro sea alimentado por electrones limpios y fiables.

De la seguridad del petróleo a la seguridad eléctrica

Cuando Paul Roberts, periodista y analista de energía, abordaba la seguridad energética en *The End of Oil* (2004), el término «seguridad» se envolvía en una imagen clara: controlar los flujos de petróleo, protegiendo las rutas marítimas y las infraestructuras de refinería. Hoy, en 2026, la trama ha cambiado radicalmente; la clave ya no es la reserva de crudo, sino la capacidad de mantener una red eléctrica limpia, abundante y resiliente ante una demanda creciente impulsada por la inteligencia artificial.

Esta nueva vulnerabilidad se manifiesta en varias dimensiones interrelacionadas. Primero, la dependencia creciente de fuentes renovables —solar y eólica— añade una variabilidad natural que hace que la red sea más sensible a las fluctuaciones climáticas y, por tanto, requiera una gestión dinámica en tiempo real. Segundo, la proliferación de centros de datos y equipos de IA pone presión directa sobre las infraestructuras de transmisión: ya representaban alrededor del 2 % de la electricidad mundial en 2022, cifra que podría duplicarse hacia 2026 [2]. Tercero, la aparición de capas digitales para la certificación de

la energía introduce una dimensión criptográfica que, si bien refuerza la trazabilidad, también crea nuevos vectores de ataque cibernético.

Las soluciones emergentes son tan innovadoras como controvertidas. DeepMind ha demostrado que la optimización basada en IA puede reducir el consumo energético de los centros de datos de manera significativa gracias a una mejor regulación de la refrigeración, y este modelo se está extendiendo a las redes de distribución pública [1]. Además, proyectos colaborativos como Google-PJM-Tapestry modernizan la infraestructura norteamericana con algoritmos predictivos que anticipan los picos de demanda y redistribuyen flujos en fracciones de segundo, minimizando cortes inesperados [1].

Paralelamente, el renacer de lo nuclear —ahora en forma de reactores modulares pequeños (SMR) y de fusión experimental— ofrece una fuente de electricidad estable y de alto rendimiento. Google y Kairos Power están construyendo un SMR de 500 MW con la primera unidad prevista para 2030, como hemos visto; Microsoft y Constellation han puesto en marcha la reactivación de la Unidad 1 de Three Mile Island, con una capacidad de 837 MW también citada anteriormente [2]. Además, la colaboración entre Microsoft y Helion apunta a la fusión nuclear como objetivo para 2028, prometiendo una energía limpia y casi inagotable que podría alimentar directamente las grandes redes de IA sin aumentar las emisiones [2].

Esta convergencia —IA para la optimización de la red y nuclear avanzado como fuente constante— crea un ecosistema donde la seguridad eléctrica se mide tanto en disponibilidad como en la capacidad de detectar y neutralizar amenazas cibernéticas en tiempo real. Cada registro que certifica el origen de un kilovatio es a la vez una prueba criptográfica contra manipulaciones y fraudes, mientras los modelos predictivos anticipan fallos potenciales antes de que se produzcan.

El reto de 2026 no consiste en proteger un recurso finito como el petróleo, sino en garantizar una infraestructura digital-energética tan adaptable como la IA que la consume. La vulnerabilidad ya no es el combustible en sí mismo, sino la red que lo transporta y lo procesa; solo a través de una sinergia entre inteligencia artificial y tecnologías nucleares avanzadas podemos construir una seguridad energética realmente resiliente para el futuro.

Redes inteligentes e IA

En un laboratorio de Google en Mountain View, una sala fría que antes servía para mantener en marcha miles de servidores ahora vibra con el murmullo de las redes neuronales de DeepMind. El equipo redujo la necesidad de refrigeración un 40 % optimizando los flujos de energía de sus centros mediante algoritmos predictivos que anticipan los picos de carga y redistribuyen la potencia hacia zonas menos congestionadas [1]; como hemos visto, este éxito no es una curiosidad académica sino la prueba viva de que la inteligencia artificial puede actuar como el sistema nervioso de una red energética, detectando, procesando y reaccionando a señales en tiempo real con una precisión que ninguna infraestructura tradicional ha podido ofrecer.

Esta nueva arquitectura se consolida en Estados Unidos, donde Google, PJM (el operador independiente del mercado eléctrico que coordina la región del Medio Atlántico) y Tapestry han lanzado un proyecto colectivo para modernizar la red nacional. El objetivo es integrar una proporción creciente de energía renovable —eólica offshore, solar fotovoltaica de gran escala— sin sacrificar la fiabilidad. La IA gestiona la demanda flexible: aprende de los patrones de consumo residencial e industrial, ajusta las tarifas en tiempo real y activa o desactiva cargas no críticas según la disponibilidad de energía limpia; así, una fábrica que produce componentes para vehículos eléctricos puede reducir temporalmente su producción cuando los vientos son débiles, mientras un parque de baterías comunitarias almacena el exceso de energía eólica y lo descarga durante las horas punta.

El modelo de control distribuido se fundamenta en una red de sensores IoT que recogen datos sobre temperatura, flujos de corriente, condiciones meteorológicas y estado de los equipos. Cada nodo procesa localmente la información con microalgoritmos de aprendizaje para tomar decisiones inmediatas, mientras un núcleo central de IA optimiza la estrategia global. Este enfoque híbrido ofrece una respuesta casi instantánea ante incidentes inesperados: si una subestación se ve afectada por una tormenta, la IA recalcula las rutas de flujo y redirige la electricidad a través de líneas alternativas en cuestión de segundos, evitando apagones masivos.

Como hemos visto, la reducción del consumo por refrigeración disminuye directamente las emisiones de CO_2 y, aplicada a la gestión de la red, multiplica este ahorro a escala de todo el sistema eléctrico [1]. Además, la capacidad de coordinar generación intermitente y almacenamiento en tiempo real reduce la

dependencia de los combustibles fósiles y refuerza la seguridad energética: las redes se vuelven menos vulnerables a interrupciones externas, ya que su funcionamiento depende de procesos autónomos y adaptativos más que de infraestructuras rígidas.

Así, la IA no solo monitoriza; actúa como un cerebro distribuido que aprende constantemente del comportamiento del sistema y se ajusta para maximizar la eficiencia y la resiliencia. La combinación de datos masivos, algoritmos avanzados e infraestructura digital convergentes redefine la seguridad energética: ya no se trata solo de garantizar el suministro de un recurso escaso, sino de orquestar una red inteligente capaz de autosostenerse ante los retos del futuro. La visión de Roberts sobre la energía como vulnerabilidad ha evolucionado; ahora la clave es construir esa sinergia entre IA y energía limpia para asegurar un mundo donde la confianza en el suministro sea tan robusta como las propias redes que la sustentan [1].

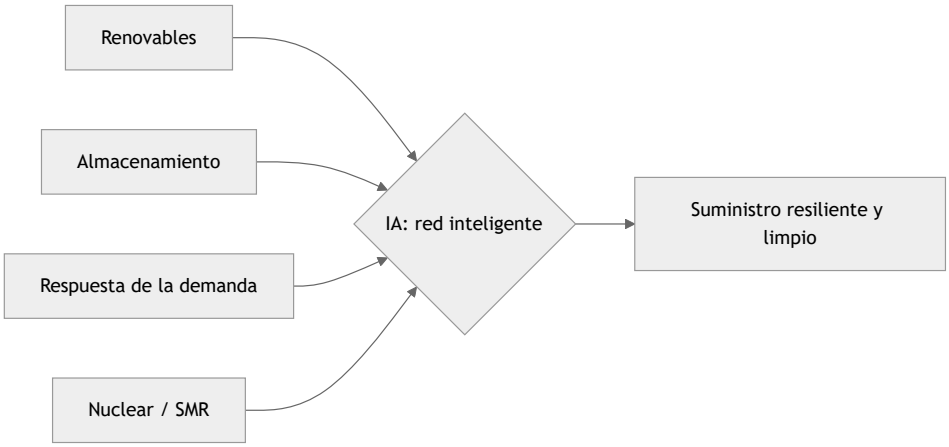


Figura 11.1 — La IA orquesta renovables, almacenamiento, respuesta de la demanda y nuevo nuclear en una red resiliente.

El retorno (controvertido) de lo nuclear

En octubre de 2024 Google encargó a Kairos Power una flota de reactores modulares pequeños por 500 MW, con la primera unidad prevista para operar antes de 2030; es la prueba de que la IA no solo consume energía, sino que la dirige hacia fuentes limpias y constantes [2].

Microsoft y Constellation reactivarán la Unidad 1 de Three Mile Island, que originalmente aportaba 837 MW, con tecnología de control avanzado para volver a generar electricidad en 2028, mostrando que la estabilidad de las redes inteligentes depende de una fuente ininterrumpida y exenta de carbono [2].

En Ontario, OPG obtuvo la aprobación en abril de 2025 para construir un reactor GE Hitachi BWRX-300, con entrada en operación prevista para 2029 —una de las primeras aprobaciones de este tipo en Occidente [2]. Paralelamente, Microsoft y Helion firmaron un acuerdo para que, hacia 2028, un reactor de fusión empiece a aportar energía a la red y alimente centros de datos dedicados al entrenamiento de grandes modelos de IA, ofreciendo un ciclo energético totalmente limpio y casi ilimitado [2].

Estas iniciativas, pese a ser controvertidas, revelan una lógica clara. La IA, con la capacidad de predecir y equilibrar las demandas energéticas en fracciones de segundo, necesita una infraestructura que pueda garantizar una producción constante y sin emisiones. Los SMR ofrecen modularidad, seguridad intrínseca y un tiempo de instalación reducido respecto a los reactores tradicionales; la fusión promete una fuente casi inagotable con residuos mínimos. En este contexto, las redes inteligentes se convierten en el alma de la nueva arquitectura energética: algoritmos que anticipan picos de demanda, redistribuyen cargas y optimizan el rendimiento de los reactores para minimizar pérdidas y maximizar la eficiencia operativa.

No obstante, la apuesta no está exenta de riesgos. La concentración de infraestructura crítica en manos de un número limitado de empresas tecnológicas puede crear nuevos puntos vulnerables a ciberamenazas o presiones políticas. Además, la aceptación pública de lo nuclear sigue siendo un obstáculo cultural y regulador que requiere una comunicación transparente y basada en datos verificados. La promesa de «energía firme y sin carbono a cualquier precio» ha de ir acompañada de una gestión responsable de los residuos nucleares, de protocolos de seguridad rigurosos y de un marco normativo que garantice la confianza global.

En definitiva, el retorno de lo nuclear se presenta como una respuesta pragmática a las necesidades energéticas de la IA. Es una apuesta que combina el espíritu visionario de Don Tapscott, coautor de *Blockchain Revolution* —una solución anclada en datos y casos reales— con la conciencia de los peligros inherentes, abriendo un camino hacia redes eléctricas más resilientes, inteligentes y limpias [2].

La promesa y el peligro

Imagina una red eléctrica que aprende en tiempo real de cada pico de demanda, optimiza la distribución de energía como un médico regula la dosis de un medicamento y, a la vez, reduce drásticamente las emisiones de carbono. Esta es la promesa de las redes inteligentes alimentadas por IA: una seguridad energética basada no en el control de las rutas petroleras, sino en la capacidad de predicción y adaptación de sistemas autónomos. DeepMind ha demostrado que la optimización algorítmica puede reducir hasta el 40 % el consumo energético de los centros de datos gracias a una refrigeración más eficiente, una mejora que se traslada directamente al sector eléctrico cuando se aplican los mismos principios a la gestión de la red nacional [1]; proyectos como Google-PJM-Tapestry modernizan las infraestructuras norteamericanas con plataformas basadas en IA que anticipan fallos, redistribuyen cargas y minimizan pérdidas, incrementando la resiliencia ante desastres naturales o ataques cibernéticos [1].

Paralelamente, el auge de las centrales nucleares modulares pequeñas (SMR) ofrece una fuente de electricidad constante y limpia que puede alimentar estas redes inteligentes sin depender del petróleo. Google y Kairos Power ya han anunciado un SMR de 500 MW con la primera unidad prevista para 2030, mientras Microsoft y Constellation reactivan la Unidad 1 de Three Mile Island, con una capacidad de 837 MW, para 2028; Microsoft colabora también con Helion en un acuerdo de fusión que apunta al mismo año [2]. Como hemos visto, las reducciones de energía llegan hasta el 40 % y los proyectos SMR prevén instalaciones de 500 MW para 2030 y 837 MW para 2028. La combinación de una generación nuclear fiable y de una gestión basada en IA crea un ecosistema donde la seguridad energética se convierte en una función automática, transparente y medible.

No obstante, el peligro que se esconde detrás de esta visión es igual de real. Cuando las decisiones críticas sobre flujos de electricidad pasan a ser determinadas por modelos algorítmicos, la integridad de los datos y la verificabilidad del código se convierten en puntos únicos de fallo; un ataque que manipule los sensores o corrompa el entrenamiento del modelo podría desencadenar una sobrecarga artificial, un corte de electricidad a gran escala o incluso la desviación intencionada de la producción nuclear hacia escenarios inseguros. Por eso, cada capa de la infraestructura ha de estar protegida por mecanismos de confianza descentralizados —como los registros inmutables que registran los valores de los sensores y las decisiones algorítmicas—, garantizando que cualquier alteración sea detectada de inmediato y rechazada.

Esta doble cara, promesa y peligro, exige una arquitectura de confianza integrada: IA para la optimización y blockchain para la verificación. Solo así se puede asegurar que la red inteligente no se convierta en un nuevo vector de ataque, sino en el pilar más robusto de la seguridad energética del futuro. La clave es desarrollar marcos reguladores y estándares abiertos que obliguen a la transparencia de los modelos, al control independiente de sus salidas y a la auditoría continua por parte de entidades independientes. En este equilibrio entre innovación y vigilancia, la seguridad energética reinventada puede dejar atrás el petróleo y avanzar hacia una era donde la confianza es tan segura como la propia energía que alimenta nuestras sociedades.

¿Quién vigila los electrones?

Una red inteligente no solo mueve electrones de una subestación a otra; es una corriente de datos que registra cada operación, cada transacción comercial y cada derecho contractual en tiempo real. Esta doble circulación crea oportunidades inmensas pero también expone vulnerabilidades: si la información que guía los algoritmos no es fiable, la optimización de la generación y el consumo puede convertirse en una fuente de inestabilidad, con consecuencias que van desde el desequilibrio de frecuencia hasta apagones masivos. La pregunta central se convierte, pues, en quién garantiza que estos flujos son verídicos.

La respuesta emerge como una capa de confianza distribuida: la blockchain. En su núcleo, esta tecnología registra cada acción —desde el despacho de un contrato de energía renovable hasta el pago de una tarifa de consumo de un usuario final— en bloques inalterables y verificables por cualquier participante autorizado. Esto impide manipulaciones malintencionadas y permite auditorías independientes continuadas. Cuando una IA decide desviar la energía hacia un centro de datos donde se entrena el

próximo modelo de aprendizaje profundo, la transacción queda grabada y puede ser revisada por entidades reguladoras o auditores externos, asegurando que no hay desviaciones ocultas ni beneficios indebidos.

Las experiencias recientes demuestran cómo esta sinergia puede funcionar a gran escala. DeepMind ha conseguido reducir el consumo energético de refrigeración en los centros de datos de Google —como hemos visto— y, si se integra este ahorro en una cadena de bloques que registre cada kilovatio-hora, se garantizará la transparencia del beneficio ambiental [1]. De manera paralela, el consorcio Google-PJM-Tapestry moderniza la red eléctrica de Estados Unidos con plataformas de IA que equilibran la generación distribuida; codificar los datos de flujo y los acuerdos de compraventa en una blockchain pública ayudaría a evitar conflictos de interés y a asegurar la trazabilidad del comercio energético [1].

A escala nuclear, proyectos como el SMR de 500 MW desarrollado por Google y Kairos Power (previsto para 2030) podrían incorporar registros blockchain para la gestión de permisos, mantenimiento y rendimientos operativos, creando una pista de auditoría consultable en tiempo real por reguladores independientes [2]. De manera similar, la reactivación de la Unidad 1 de Three Mile Island por parte de Microsoft y Constellation —837 MW, prevista para 2028— se podría documentar con un registro distribuido que recoja cada fase del proceso de seguridad y cada intervención humana o automática. Este enfoque se reforzaría con la colaboración de Helion y Microsoft en fusión nuclear, con el objetivo puesto en 2028, donde los datos de producción de energía y los costes operativos se podrían certificar con una cadena de bloques, evitando cualquier manipulación que pudiera comprometer la confianza del mercado [2].

Estos ejemplos muestran cómo la blockchain puede actuar como columna vertebral de la confianza en un ecosistema energético cada vez más inteligente y autónomo. No se trata solo de una solución técnica, sino de un marco institucional que combina transparencia, responsabilidad y auditoría continua; el control del petróleo queda atrás y la seguridad energética depende de garantizar que cada electrón, cada dato y cada derecho se mueven en un entorno verdaderamente fiable. La tarea para las empresas, los reguladores y la sociedad es clara: adoptar plataformas blockchain abiertas, establecer estándares de auditoría independientes e integrar estas capas de confianza con las soluciones de IA que ya transforman la gestión de redes, asegurando así una seguridad energética resiliente, inteligente y limpia.

---

[1] Google DeepMind / Data Center Frontier, *IA para la red.* https://www.datacenterfrontier.com/energy/article/55282719/googles-ai-powered-grid-revolution-how-data-centers-are-reshaping-the-us-power-landscape ↩

[2] IAEA / NucNet, *nuclear avanzado y SMR para la demanda de IA (2024-2025).* https://www.iaea.org/bulletin/data-centres-artificial-intelligence-and-cryptocurrencies-eye-advanced-nuclear-to-meet-growing-power-needs ↩

La mano (ya no tan) invisible: blockchain como capa de confianza

«Lo que se necesita es un sistema de pago electrónico basado en la prueba criptográfica en lugar de la confianza, que permita a dos partes dispuestas transaccionar directamente entre ellas sin necesidad de un tercero de confianza.»

— Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008)

Al atardecer, el barrio de Sant Antoni del Parc se transforma en una pequeña bolsa de energía. Las luces de las fachadas resplandecen con la calidez suave de los paneles solares instalados sobre las terrazas y los tejados de los edificios de vivienda social. Cada hogar, equipado con un inversor inteligente, mide en tiempo real cuánta energía genera y cuánta consume. Cuando el sol se pone y la producción supera la demanda interior, una notificación aparece en la aplicación de Powerledger en el teléfono de Marta, que vive en el piso del tercero; ella puede ver, con solo un toque, cuántos kilovatios-hora (kWh) tiene disponibles para vender.

Sin ningún intermediario, sin facturas ocultas ni tarifas adicionales, Marta decide enviar el excedente a su vecino, Joan, que trabaja de noche y necesita energía para su taller de herramientas electrónicas. Joan recibe una alerta: «Energía disponible, ¿aceptas?». Acepta con un clic, y al instante el contrato se codifica como transacción en la cadena de bloques de Powerledger, donde cada unidad de energía está representada por un certificado renovable tokenizado (REC) —un REC equivale a 1 MWh— [1]. En cuestión de segundos, el acuerdo queda registrado de forma inmutable: el sensor del panel solar de Marta envía los datos de producción al nodo de la blockchain; los sensores de consumo de Joan verifican que la energía ha sido recibida y consumida; todo el proceso queda grabado de forma transparente pero segura.

En la plaza central, un pequeño monitor muestra en tiempo real las transacciones del barrio: cuántos RECs han circulado, qué porcentaje de energía se ha intercambiado entre vecinos y qué impacto ha tenido sobre las emisiones de carbono locales. Los residentes observan cómo el gráfico sube, orgullosos de ver que su comunidad está reduciendo la dependencia de las grandes compañías energéticas y, a la vez, fomentando una economía circular basada en la energía verde.

Esta escena ilustra a la perfección la «mano invisible» del mercado —esta vez no es un misterioso balance de intereses que opera desde detrás de las puertas de una sala de conferencias— sino una red visible y auditable, codificada en código abierto. La blockchain actúa como testigo digital, asegurando que cada transacción sea verificable por cualquier participante, sin necesidad de confianza ciega en un tercero. Esto contrasta con el modelo tradicional donde las compañías distribuidoras registran los datos en sistemas propietarios y opacos, a menudo inaccesibles para los consumidores.

Sin embargo, este experimento todavía se encuentra en la fase de prueba de concepto. La mayoría de los 39 proyectos analizados muestran que el potencial es real, pero se enfrentan a obstáculos como registros fragmentados, datos MRV (monitorización, reporte y verificación) inconsistentes y una falta de reconocimiento legal para los RECs tokenizados [2]. Aun así, la eficiencia energética de la capa subyacente ha mejorado drásticamente: el Merge de Ethereum ya es sostenible —una prueba de que la blockchain ya no es una fuente de despilfarro sino una herramienta sostenible para la energía verde [3].

En este barrio, la mano invisible se ha hecho visible. Cada clic, cada token y cada registro en el libro digital convierten la confianza en un activo medible, abriendo las puertas a un nuevo paradigma energético basado en el P2P, los certificados renovables tokenizados y el MRV casi en tiempo real. La pregunta que queda por responder es: cuando esta capa de confianza se estandarice y se reconozca legalmente, ¿cuántos otros barrios podrán replicar este modelo y transformar por completo la manera en que comprendemos y consumimos energía?

Los mercados que Roberts imaginaba

Cuando Paul Roberts, en *The End of Oil* (2004), describía los mercados de la energía como una gran bolsa de valores: precios determinados por el juego invisible de oferta y demanda y oportunidades distribuidas entre inversores y consumidores. Su relato no era solo de entusiasmo; también mostraba las sombras que se extendían detrás del telón, con el ejemplo emblemático de Enron —una trampa de contabilidad y manipulación de precios— que ilustraba la vulnerabilidad de un sistema donde la información era privilegio de unos pocos y la transparencia un lujo.

Roberts llamaba a esta «opacidad» el verdadero enemigo del mercado libre. Las transacciones se hacían a través de contratos ocultos, los datos de producción y consumo eran manipulados por intereses corporativos y los reguladores, a menudo sobrepasados, no podían garantizar la veracidad de los informes. Hoy, más de una década después, la blockchain ofrece una respuesta tecnológica a esa llamada: su arquitectura distribuida crea un registro inmutable donde cada transacción de energía —desde el momento en que el sol genera un kilovatio-hora hasta el punto en que este se consume en el hogar— queda grabada de manera permanente y verificable por cualquier participante, sin intermediarios que puedan editar o suprimir datos.

Esta nueva capa de confianza ya se está poniendo a prueba en el terreno. Powerledger ha desarrollado una plataforma donde vecinos de un barrio pueden comprar energía directamente entre ellos, sin pasar por la compañía eléctrica tradicional. Cada kWh transaccionado se vincula a un certificado renovable tokenizado; un REC representa exactamente un megavatio-hora y se registra en la blockchain, garantizando que el comprador recibe una certificación verificable del carácter renovable de la energía adquirida [1]. Sensores avanzados instalados en las instalaciones fotovoltaicas y eólicas transmiten datos de producción a la cadena, permitiendo un MRV (monitorización, reporte y verificación) casi instantáneo, y cualquier desajuste entre la producción declarada y la real se detecta de inmediato, reduciendo el margen de fraude.

Como indica la encuesta reciente que recoge 39 proyectos, la mayoría de estos esfuerzos todavía son pruebas de concepto [2]; los obstáculos son diversos: registros fragmentados entre distintas plataformas, datos MRV inconsistentes y una falta de reconocimiento legal que impide que los tokens sean aceptados como instrumentos financieros regulados. Hay que establecer estándares comunes para que las transacciones puedan interconectarse a escala global.

En este momento histórico, la blockchain se beneficia de una evolución energética crucial: el Merge de Ethereum ya es sostenible, convirtiendo una tecnología que antes se criticaba por su ineficiencia en una infraestructura casi neutra desde el punto de vista energético [3] —un mercado donde la confianza ya no depende de una mano invisible, sino de un registro visible para todos.

La capa de confianza

Más allá de la escena del barrio, vale la pena desgranar cómo la blockchain actúa de capa de confianza en tres aplicaciones concretas. La primera es el mercado P2P de energía: protocolos como Powerledger permiten el comercio directo de electricidad entre vecinos, con cada transacción inmutable y verificable [1]. La clave es que la cadena elimina los intermediarios tradicionales: la confianza ya no recae en una «mano invisible» de operadores centralizados, sino en un registro transparente al que todos los participantes tienen acceso simultáneo.

Una segunda aplicación que refuerza este nuevo paradigma son los certificados de origen renovable (REC) tokenizados. Cada certificado representa exactamente 1 MWh de energía limpia producida y se codifica como token único en la blockchain, asegurando que no pueda ser duplicado ni falsificado [1]. Esta trazabilidad llena de transparencia permite a consumidores y empresas comprobar con un simple escaneo el origen de su energía, convirtiendo el «greenwashing» en una práctica inviable. Además, la tokenización simplifica la liquidación de los certificados: las transacciones se procesan en segundos, sin burocracia ni costes asociados a los sistemas tradicionales de registro.

Finalmente, la monitorización, reporte y verificación (MRV) del carbono se ha transformado con sensores IoT que escriben datos directamente en la cadena. Este flujo de información casi en tiempo real elimina las lagunas entre la generación física y el registro digital, reduciendo significativamente el error humano y la manipulación de datos [1]. Con cada lectura de sensor codificada como transacción inmutable, los proyectos de compensación de carbono pueden demostrar con evidencia verificable su contribución real a la descarbonización.

El mito energético que sostenía que las tecnologías blockchain eran una carga para el consumo global ha quedado obsoleto. Tras el Merge de Ethereum, el consumo energético de la red se desplomó respecto al anterior modelo de prueba de trabajo [3]; como hemos visto, esto convierte la blockchain en una infraestructura sostenible para el nuevo ecosistema energético.

Pese a estas promesas, el panorama actual todavía es de una fase experimental. Una encuesta reciente sobre 39 proyectos basados en blockchain revela que la mayoría se encuentran en etapa de prueba de concepto, con obstáculos como registros fragmentados, datos MRV inconsistentes y falta de

reconocimiento legal [2]. Para que esta capa de confianza pueda desplegarse a gran escala, hay que establecer estándares comunes y marcos reguladores que garanticen la interoperabilidad y la validez jurídica. Solo así la blockchain podrá consolidarse como el fundamento fiable de un mercado energético descentralizado, transparente y verdaderamente sostenible.

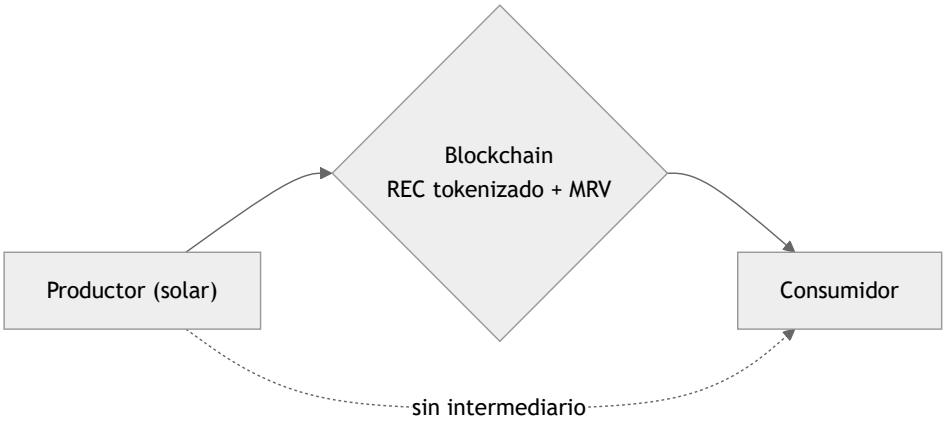


Figura 12.1 — Productor y consumidor intercambian energía y certificados directamente; la blockchain aporta confianza sin intermediario.

El realismo: todavía es pronto

Una encuesta reciente que recoge el progreso de treinta y nueve iniciativas blockchain dedicadas a la energía constata que la mayoría se encuentran todavía en fase de prueba de concepto. Estos datos revelan un panorama donde la innovación avanza con paso decidido pero sin haber superado las barreras fundamentales que impiden una adopción masiva. Los obstáculos identificados son tres: registros fragmentados que dificultan la interoperabilidad entre plataformas; datos de monitorización, reporte y verificación (MRV) inconsistentes que comprometen la fiabilidad del sistema; y, finalmente, la ausencia de un marco legal reconocido que legitime las transacciones basadas en blockchain [2].

Esta situación no ha de ser interpretada como un fracaso tecnológico, sino como una etapa inevitable dentro del ciclo de adopción de una infraestructura tan disruptiva. La promesa que la blockchain ofrece al sector energético es clara: crear una capa de confianza inmutable que garantice que cada certificado renovable (REC) tokenizado representa realmente un megavatio-hora producido, y que los intercambios P2P de energía —como los facilitados por Powerledger— se puedan registrar de forma transparente y verificable en tiempo casi real [1]. Además, la integración de sensores IoT con contratos inteligentes permite un MRV casi instantáneo, reduciendo las latencias que tradicionalmente han debilitado los sistemas de certificación de carbono.

Sin embargo, la falta de estándares comunes convierte esta promesa en una ilusión parcial. Cada proyecto desarrolla su propio esquema de tokenización y su propia arquitectura de datos, generando un ecosistema de «islas blockchain» que no pueden comunicarse entre sí sin costosos procesos de interfaz. Sin una normativa clara que establezca criterios mínimos para la calidad de los datos MRV y la validez jurídica de los tokens, las transacciones se mantienen vulnerables a disputas y a manipulaciones potenciales.

El Merge de Ethereum —la actualización que hizo sostenible la red— demuestra que la tecnología blockchain puede evolucionar hacia una eficiencia sostenible [3]. No obstante, esta mejora estructural no soluciona los problemas de interoperabilidad y de reconocimiento legal que todavía persisten. La comunidad ha de traducir este avance energético en un marco regulador que establezca: (1) estándares de formato para certificados tokenizados, garantizando que 1 REC equivale realmente a 1 MWh independientemente del proveedor; (2) protocolos de intercambio de datos MRV uniformes, con auditorías independientes y certificaciones de calidad; y (3) reconocimiento legal de los contratos inteligentes como instrumentos vinculantes en jurisdicciones clave.

En este contexto, la necesidad de una colaboración estrecha entre reguladores, empresas tecnológicas y actores del sector energético se vuelve imperativa. Las autoridades pueden impulsar el establecimiento de esquemas de certificación abiertos, similares a los estándares que ordenan otras industrias, mientras las empresas como Powerledger han de participar activamente en la definición de APIs comunes que

permitan la interoperabilidad entre redes blockchain diversas. Solo con esta sinergia se podrá transformar la promesa de confianza inmutable en una realidad operativa y escalable.

En resumen, el panorama actual es un equilibrio delicado: la tecnología ha demostrado su capacidad para crear una capa de confianza robusta, pero todavía le falta madurez. Los estándares y marcos reguladores son los pilares que hay que construir ahora, para que la blockchain pueda consolidarse como el fundamento fiable de un mercado energético descentralizado, transparente y verdaderamente sostenible. La decisión de poner en marcha estos mecanismos no es solo una cuestión técnica, sino un compromiso colectivo para garantizar que la nueva «mano invisible» sea realmente visible y confiable para todos los actores del sistema.

La promesa y el peligro

Imagina un mercado de energía donde cada kWh negociado lleva impresa una pequeña huella de verdad: quién lo ha producido, qué fuente lo genera, qué impacto de carbono tiene y en qué momento exacto se ha entregado. Esta es la promesa que la blockchain ofrece como capa de confianza para los mercados de energía y de créditos de carbono. En lugar de una confianza ciega en intermediarios o certificaciones centralizadas, las transacciones se registran en un libro inmutable donde cualquier actor —generador solar comunitario, distribuidor local, consumidor industrial o regulador— puede auditar la cadena completa con unos clics, eliminando la opacidad que ha alimentado fraudes de certificados renovables falsos y de incumplimientos en los informes de reducción de emisiones.

Powerledger ya permite el comercio P2P de energía entre vecinos, anotando cada transacción en el registro distribuido y vinculándola a sensores que miden la producción real casi en tiempo real [1]. Además, los certificados renovables (REC) se están tokenizando: un REC equivale a 1 MWh de energía limpia y se puede transferir como cualquier otro activo digital, garantizando la trazabilidad del origen y evitando duplicidades [1]; los sensores IoT alimentan directamente la cadena, creando un sistema MRV casi instantáneo que reduce errores humanos y aumenta la confianza en los datos reportados. Como hemos visto, una encuesta reciente sobre 39 proyectos blockchain relacionados con energía indica que la mayoría operan todavía como pilotos, con registros fragmentados, datos MRV inconsistentes y falta de marcos reguladores que impiden la interoperabilidad y generan confusión más que claridad [2].

Además, la confianza que ofrece una cadena de bloques depende de los datos que se le introducen. La expresión «garbage in, garbage on-chain» resume el peligro de alimentar la blockchain con información no verificada o manipulada; si los sensores son vulnerables a ciberataques o si los certificados se crean sin una auditoría rigurosa, la cadena inmutabilizará errores y fraudes difíciles de corregir. Por eso, establecer estándares de calidad para las fuentes de datos y protocolos de autenticación robustos es imprescindible antes de desplegar soluciones a gran escala [2].

El Merge de Ethereum ha mitigado la preocupación energética que tradicionalmente rodea a las tecnologías blockchain, haciendo el protocolo sostenible y convirtiendo la infraestructura en una opción viable para aplicaciones de gran volumen como los mercados de energía [3]. Esto elimina el obstáculo aparente de los «costes ocultos» y permite centrarse en la cuestión clave: garantizar que los datos sean fiables, verificables y compatibles entre todas las partes del ecosistema.

En resumen, la blockchain puede ser la capa de confianza que transforma los mercados de energía y carbono en sistemas transparentes y resistentes al fraude, siempre que se desarrollen estándares comunes y se proteja el origen de los datos. Sin estos fundamentos, el potencial revolucionario podría quedar atrapado en una red de silos incompatibles, dejando la «mano invisible» tan intocable como antes.

El contrato social de la energía

En un ecosistema donde cada kilovatio-hora puede ser comprado, vendido o intercambiado entre vecinos, la confianza ha de ser verificable e inmutable. Aquí entra el concepto central de nuestro libro, **t2p**, la prueba de existencia basada en blockchain que cierra el círculo de la confianza: un mecanismo criptográfico que garantiza que la energía o el crédito de carbono certificado no puede ser alterado sin dejar una huella ineludible.

Imaginad una comunidad de autoconsumidores en Barcelona que genera energía solar y la vende en un mercado P2P. Cada generador emite un **REC tokenizado** (1 REC = 1 MWh) que representa el derecho a vender aquella energía verificada [1]. Al registrarlo en la blockchain se incluye una prueba de origen: los

datos del contador inteligente, la fecha y hora exactas y la certificación del proveedor de energía renovable. La blockchain graba esta información en un libro distribuido donde cualquier actor puede consultarla sin dudar de su autenticidad.

Esta capa de prueba de existencia se convierte en el fundamento para **MRV (monitoring, reporting, verification)** casi en tiempo real. Sensores instalados a lo largo de la red recogen datos de producción y consumo; estos datos son resumidos criptográficamente y añadidos a bloques en una infraestructura que, tras el **Merge de Ethereum**, mantiene un consumo energético mínimo [3]. Cada transacción es transparente y sostenible.

Aun así, el camino hacia una adopción masiva todavía está lleno de obstáculos. Una encuesta reciente sobre 39 proyectos indica que la mayoría se encuentran todavía en fase de prueba de concepto, limitados por **registros fragmentados** y datos MRV inconsistentes [2]. Sin un marco normativo común, las autoridades reguladoras no reconocen legalmente estos tokens y los actores del mercado se muestran reticentes a confiar en una infraestructura que todavía no está totalmente estandarizada, generando silos de confianza donde cada plataforma opera con su propio protocolo.

La solución pasa por establecer **estándares abiertos** que definan cómo se ha de emitir, firmar y validar una prueba de existencia. Organizaciones de normalización pueden liderar este proceso, asegurando que las pruebas sean reconocidas legalmente en todas las jurisdicciones; una vez estos estándares estén en vigor, la blockchain dejará de ser una tecnología experimental y se convertirá en la capa invisible pero palpable de confianza que habilita mercados P2P, certificados renovables tokenizados y MRV transparente.

En resumen, **t2p** no es solo una herramienta técnica; es el contrato social del futuro energético. Asegura que lo que entra en la cadena es auténtico, crea un registro inmutable de confianza y ofrece una base sólida para las políticas climáticas y económicas que dependen de una verificación fiable. El próximo paso está claro: adoptar estándares globales, integrar pruebas de existencia en todos los sistemas y permitir que la blockchain se convierta en el verdadero núcleo de confianza del nuevo sistema energético.

---

[1] RWA.io / Powerledger, *RECs tokenizados y MRV en blockchain*. https://www.rwa.io/post/renewable-energy-credits-on-blockchain-a-tokenized-approach ↩

[2] Frontiers in Blockchain (2025), *estado de los mercados de carbono en blockchain*. https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2025.1603695/full ↩

[3] ethereum.org, *The Merge*. https://ethereum.org/roadmap/merge/ ↩

t2p: la prueba de existencia contra las deepfakes

«La lucha del hombre contra el poder es la lucha de la memoria contra el olvido.»

— Milan Kundera, El libro de la risa y el olvido (1979)

Marzo de 2026, una tarde soleada en el área de Barcelona-Sabadell, el consejero delegado de una de las mayores compañías eléctricas españolas aparece en un vídeo difundido por Twitter. En solo 38 segundos, la imagen —una oficina elegante con vistas panorámicas al Parque Tecnológico del Vallès— muestra al ejecutivo, con la mirada seria y una carpeta llena de gráficos de emisiones, declarando que «hemos decidido ajustar los datos de emisión para reflejar mejor la realidad operativa». La frase, pronunciada con un tono aparentemente transparente, se convierte de inmediato en el escenario de una crisis inesperada.

En menos de una hora, el precio de las acciones de la compañía cae un 12 % en la bolsa ibérica. Las noticias se multiplican: analistas financieros advierten de que los inversores dudan de cualquier certificación ESG y temen una posible sanción del regulador de mercados. Los medios, desde La Vanguardia hasta Bloomberg, publican titulares alarmantes —«La verdad borrada: el gran engaño de la transición energética». En este momento, las redes sociales se llenan de expertos en ciberseguridad que recuerdan los últimos informes de Europol: las deepfakes han pasado de unas 500.000 en 2023 a 8 millones en 2025 [2].

Siete horas más tarde, una empresa de verificación forense digital publica un informe detallado: el vídeo es una deepfake. Mediante análisis de algoritmos de detección avanzados y comparativas con metadatos originales, demuestran que la cara del consejero ha sido generada por una red neuronal entrenada en imágenes públicas y que el audio ha sido sintetizado a partir de muestras de voz disponibles en archivos corporativos. La duda, sin embargo, ya no desaparece. Los inversores, los reguladores y el público se encuentran atrapados entre la certeza de una declaración oficial y la incertidumbre de un engaño tecnológico.

Este escenario ilustra una realidad cada vez más palpable: la transición hacia una economía descarbonizada depende de datos fiables. Los informes ESG, los métodos MRV (Measurement, Reporting and Verification) de carbono y las certificaciones de energía limpia son el fundamento sobre el que se construyen inversiones multimillonarias y políticas climáticas globales. Cuando la verdad visual puede ser alterada en cuestión de minutos, estas capas de información pierden credibilidad y, con ellas, la confianza necesaria para impulsar proyectos de energía renovable a gran escala.

En este contexto, la necesidad de una capa de confianza inmutable se hace evidente. La blockchain moderna ofrece exactamente esto: un registro descentralizado donde cada dato —desde certificados de emisión hasta contratos inteligentes que garantizan el cumplimiento de límites de energía— puede ser verificado sin depender de un único punto de fallo. La prueba de existencia, denominada t2p, nace como la respuesta insignia: un mecanismo criptográfico que registra la hora y el contenido de un documento o medio en una cadena de bloques, creando una huella indeleble que cualquiera puede auditar.

Esta escena, tan sobria como cinematográfica, no solo captura la urgencia del momento, sino que pone de relieve la paradoja central del capítulo: sin un sistema robusto para garantizar la autenticidad de los datos, la transición energética se queda atrapada en una nebulosa de incertidumbre. La solución está en las manos —y en el código— de la prueba de existencia, que promete restaurar la confianza perdida y permitir que los proyectos verdaderos avancen sin que la sombra de las deepfakes los ahogue.

Las apuestas

Como hemos visto, el número de deepfakes ha pasado de unas 500.000 en 2023 a 8 millones anuales, y Europol prevé que en 2026 hasta el 90 % del material audiovisual en línea podría ser generado artificialmente, una realidad que transforma el panorama de la información y, por extensión, el de los datos energéticos [2].

Esta ola de falsificaciones digitales se enfrenta a un marco regulador todavía incipiente pero cada vez más firme. El **EU AI Act**, adoptado en 2024, obliga a las plataformas a marcar claramente los contenidos sintéticos y a proporcionar una **marca de agua** que indique su procedencia [3]. En Estados Unidos, el **Take It Down Act** establece sanciones para quien aloje o difunda deepfakes sin etiquetarlos

adecuadamente. Y desde enero de 2025, la **CISA** (Cybersecurity and Infrastructure Security Agency) ha publicado un aviso que insta a las empresas de infraestructura crítica —incluidas las de generación y distribución de electricidad— a reforzar la verificación de la integridad de los datos antes de utilizarlos en informes ESG [3].

Sin una capa fiable de confianza, la transición hacia una economía descarbonizada se vuelve vulnerable a manipulaciones. Los reguladores necesitan datos limpios para validar el cumplimiento de los objetivos climáticos; los inversores buscan certificados de **MRV (monitoring, reporting and verification)** que garanticen que las reducciones de emisiones anunciadas son reales y no simples narrativas de marketing. El público, cada vez más consciente, exige transparencia: si una foto de una nueva planta solar puede ser un deepfake, la credibilidad del proyecto se desintegra en cuestión de segundos.

En este contexto, la **prueba de existencia** emerge como respuesta tecnológica imprescindible. En su forma más conocida —el protocolo **OpenTimestamps**—, esta capa criptográfica registra la hora exacta e inmutable de un documento o de unos datos, asegurando que cualquier intento de modificación posterior queda en evidencia [1]. La integridad del registro se consolida en la cadena de bloques, donde cada hash —incluyendo versiones perceptualmente similares desarrolladas en investigación avanzada de **hash perceptual**— se verifica y se enlaza con el bloque anterior, creando una cadena ininterrumpida de autenticidad [5].

Además, la evolución del **Merge de Ethereum**, que redujo su huella energética en un **99,95 %**, demuestra cómo las infraestructuras de blockchain pueden ser sostenibles y a la vez robustas para este propósito [6]. Así, una prueba de existencia insertada en una cadena de bloques verde no solo garantiza la veracidad del contenido, sino que lo hace sin comprometer los objetivos climáticos.

Las apuestas son claras: **si no podemos confiar en los datos**, ninguna política ni inversión para la descarbonización puede avanzar con legitimidad. La combinación de una regulación exigente y una capa de confianza basada en blockchain ofrece el marco necesario para que la verdad se convierta en el ancla de la transición energética. Es necesario que las empresas, los gobiernos y la sociedad civil adopten de inmediato esta arquitectura de prueba de existencia; solo así podremos impedir que los deepfakes se conviertan en el obstáculo insuperable para un futuro limpio y fiable.

Qué es la prueba de existencia

Imagina que tienes delante un informe de descarbonización con miles de datos de sensores, certificados ESG y cálculos de MRV (monitorización, reporte y verificación) del carbono. Quieres demostrar que aquel documento existió en una fecha concreta y que su contenido no ha sido alterado desde entonces. La respuesta se encuentra en la prueba de existencia, un mecanismo de tres pasos que convierte cualquier archivo —desde hojas de cálculo hasta vídeos de inspección de turbinas— en una huella inmutable registrada en la blockchain pública.

Paso 1 — Hash SHA-256 del archivo. El primer paso consiste en aplicar el algoritmo criptográfico SHA-256 al contenido del archivo. Este algoritmo produce una cadena de 64 caracteres —una huella digital única y unidireccional— que representa el documento completo. La propiedad clave es su irreversibilidad: cualquier cambio, aunque sea un solo byte, genera una nueva huella totalmente diferente. Esto garantiza que el archivo nunca tiene que salir del dispositivo para ser procesado; la privacidad se mantiene intacta porque solo la pequeña cadena hash, y no el contenido original, se transmite.

Paso 2 — Árbol de Merkle. Una vez disponemos de un conjunto de hashes (puede ser un solo archivo o miles de archivos relacionados), estos se organizan en una estructura jerárquica conocida como árbol de Merkle. Cada par de hashes se combina y se vuelve a hashear, creando nodos intermedios hasta llegar a la raíz —el «Merkle root». Esta raíz consolida todo el conjunto de datos en una única huella que representa la integridad completa del bloque de información. La ventaja es doble: permite verificar cualquier elemento individual comparando solo su ruta hacia la raíz, y reduce drásticamente la cantidad de datos que hay que transmitir para la verificación.

Paso 3 — Anclaje en una blockchain pública. El último paso consiste en grabar el Merkle root en una cadena de bloques inmutable, como Bitcoin, mediante servicios de estampado temporal como OpenTimestamps [1]. El proceso envía la raíz a la red Bitcoin, que la incluye dentro de un bloque minado y le asigna un sello de tiempo verificable. Una vez el bloque es confirmado, se genera una prueba .ots que contiene la ruta criptográfica desde el Merkle root hasta el hash del bloque donde se ha inscrito. Esta prueba puede descargarse y almacenarse localmente sin depender de terceros.

La verificación es totalmente autónoma: cualquier lector recomputa el SHA-256 del archivo original, reconstruye el árbol de Merkle correspondiente y compara su raíz con la que aparece en la prueba .ots. Si aunque sea un solo byte ha sido modificado, la comparación falla de inmediato y demuestra la manipulación. No hay que confiar en ninguna autoridad central; la seguridad se basa únicamente en las propiedades matemáticas del algoritmo hash y la inmutabilidad de la blockchain.

Este procedimiento convierte la prueba de existencia en una capa de confianza que puede integrarse en cualquier flujo de trabajo ESG o MRV. Las empresas energéticas pueden registrar sus certificados de reducción de emisiones, las autoridades reguladoras pueden verificar la autenticidad de los informes sin necesidad de auditorías presenciales y la sociedad civil dispone de una herramienta para validar la veracidad de los datos que sustentan la transición hacia un futuro limpio. En un mundo donde los deepfakes amenazan la credibilidad de cualquier declaración visual o documental, la prueba de existencia ofrece una respuesta tecnológica clara y verificable —un escudo digital contra la desinformación que protege el núcleo mismo de la transición energética.

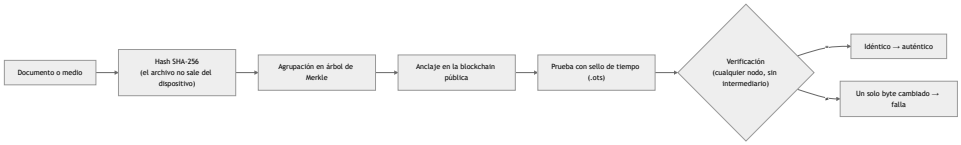


Figura 13.1 — Del hash a la verificación descentralizada: nadie tiene que confiar en nadie; solo en las matemáticas.

Por qué la blockchain, y por qué ahora

La primera vez que el público oyó hablar del coste energético de las cadenas de bloques, la imagen que quedaba grabada era la de una granja de mineros alimentando una red de Bitcoin con cientos de megavatios, un monstruo verde que devoraba electricidad como si fuera combustible. Aquel escenario convirtió el término «blockchain» en sinónimo de despilfarro e ineficiencia, y la crítica se extendió hasta las mesas ejecutivas que consideraban la tecnología un gasto inaceptable para proyectos de energía limpia.

La realidad ha cambiado radicalmente. El paso del modelo proof-of-work (PoW) al de proof-of-stake (PoS) no solo es una evolución técnica, sino una revolución en el balance entre seguridad y consumo. La operación conocida como «Merge» de Ethereum, completada a finales de 2022, sustituyó su arquitectura PoW por un mecanismo PoS que ha reducido el consumo energético del protocolo en un **99,95 %** [6] —como hemos visto—; una red que antes requería energía comparable al consumo anual de un país pequeño ahora funciona con el equivalente de la potencia de una ciudad mediana. El coste marginal de añadir una transacción pasa a ser casi nulo, mientras que la seguridad se mantiene gracias al estímulo económico del staking.

Las cadenas PoS modernas, aprovechando este modelo, son ahora capaces de proporcionar una **capa de confianza** con un coste energético mínimo y una escalabilidad que las hace aptas para aplicaciones masivas. Un solo anclaje de existencia, registrado en una transacción que contiene la cabecera Merkle de una colección de documentos, puede validar miles —incluso millones— de archivos con un único hash. Esta eficacia se traduce en una reducción drástica del consumo de recursos informáticos y, por tanto, en una pequeña huella de carbono asociada al proceso de certificación.

Además, el modelo PoS ofrece beneficios adicionales que van más allá del consumo. La **descentralización** se mantiene robusta porque la participación no depende de una infraestructura costosa de hardware especializado, sino de tokens que cualquier actor puede adquirir y «apostar». Esto democratiza el acceso a la infraestructura de verificación, permitiendo a entidades pequeñas —como cooperativas locales de energía renovable u ONG de monitorización ambiental— integrarse en una red global sin tener que invertir en grandes centros de datos.

En este contexto, la prueba de existencia (t2p) se convierte en una solución práctica y fiable para la crisis de verdad que amenaza la transición energética. La confianza que aporta una capa blockchain no es un «coste oculto», sino una inversión mínima comparada con el valor económico y social de un sistema de información verificable, transparente y resistente a manipulaciones. Los datos ESG, los informes MRV de carbono y cualquier otro registro crítico para la credibilidad de la descarbonización pueden ser anclados a esta infraestructura sin temer que el acto de certificación se convierta en una fuente de contaminación.

En resumen, el mito del despilfarro energético de la blockchain pertenece al pasado PoW. Las cadenas PoS de hoy ofrecen **confianza a coste mínimo**, escalabilidad y accesibilidad, convirtiéndose en una capa de

confianza viable para las infraestructuras que sustentan la transición hacia un futuro limpio. El momento de adoptarlas es ahora: solo así podremos garantizar que los datos que impulsan el cambio climático sean tan fiables como es debido.

C2PA y la prueba de existencia, complementarias

En el marco de las **Content Credentials** impulsadas por la iniciativa **C2PA**, el primer paso hacia la veracidad es registrar el origen del contenido en el momento exacto de su creación. Cada archivo recibe una huella criptográfica SHA-256 que, junto con un árbol Merkle y una firma X.509 de un proveedor acreditado, forma una cadena de confianza que se puede verificar sin depender de terceros intermediarios [4]. Esta arquitectura ha demostrado su utilidad en sectores como el periodismo digital y la producción audiovisual, donde las plataformas pueden certificar que un vídeo o una imagen procede de una fuente legítima y no ha sido alterado posteriormente.

Sin embargo, este modelo tiene una limitación estructural: **la confianza depende de la cooperación del creador**. Si el proveedor decide retirar la credencial —por motivos comerciales, legales o simplemente por olvido— la ausencia de esta prueba no ofrece ninguna información útil sobre si el contenido ha sido manipulado o no. En otras palabras, **la eliminación de la credencial equivale a una nula evidencia**, y el sistema queda incapaz de demostrar que alguna vez existió una certificación [4]. Esto crea una vulnerabilidad crítica en un entorno donde las deepfakes se están propagando a ritmos alarmantes: según datos de **Europol**, el número de deepfakes en circulación ha pasado de unas 500.000 en 2023 a 8 millones en 2025, con una proyección de Europol que sitúa hasta el **90 % del contenido en línea como sintético en 2026** [2].

La **prueba de existencia** (t2p) ofrece una respuesta a este vacío. Basada en el mismo principio que **OpenTimestamps**, esta solución registra el hash del contenido directamente en una cadena de bloques PoS, creando un ancla **independiente e inmutable** que persiste aunque los metadatos originales desaparezcan o sean borrados [1]. La característica clave es que la prueba no requiere ninguna autorización previamente acordada: cualquier usuario puede generar el hash y publicarlo en la red, asegurando que el momento de creación queda inmortalizado. Esto elimina por completo el riesgo de un «borrado silencioso» y proporciona una capa adicional de confianza que sobrepasa las limitaciones del modelo C2PA.

No se trata de una solución rival sino de una **sinergia**. La combinación de la certificación de origen de C2PA con el anclaje inmutable de t2p forma un ecosistema de defensa en cuatro frentes: (1) procedencia verificable, (2) ancla temporal irreversible, (3) detección automática basada en hashes perceptuales —una línea de investigación que en 2025-26 ha vinculado con éxito a medios digitales almacenados en blockchain [5]— y (4) alfabetización mediática para usuarios finales.

Esta alianza es especialmente relevante para las infraestructuras críticas de la transición energética. Los informes ESG y los mecanismos MRV de carbono dependen de una **trazabilidad fiable** de los datos de producción, transporte y consumo de energía. Sin una capa de confianza robusta, cualquier intento de descarbonización se ve minado por dudas sobre la veracidad de las declaraciones. Implementar simultáneamente C2PA y t2p significa garantizar que los certificados de emisiones, los informes de reducción y las auditorías sean **no solo auditables, sino también imposibles de alterar**.

En conclusión, la convergencia entre C2PA y la prueba de existencia cierra una breve laguna técnica y crea un **marco de confianza integral** capaz de respaldar las políticas climáticas más exigentes y contrarrestar la ola de desinformación digital. La llamada a la acción es clara: empresas, reguladores y desarrolladores han de adoptar simultáneamente ambas tecnologías, estableciendo protocolos abiertos que integren credenciales de contenido y anclaje de blockchain en sus plataformas. Solo así podremos garantizar una transición energética basada en datos verdaderos y resistentes al bombardeo de deepfakes.

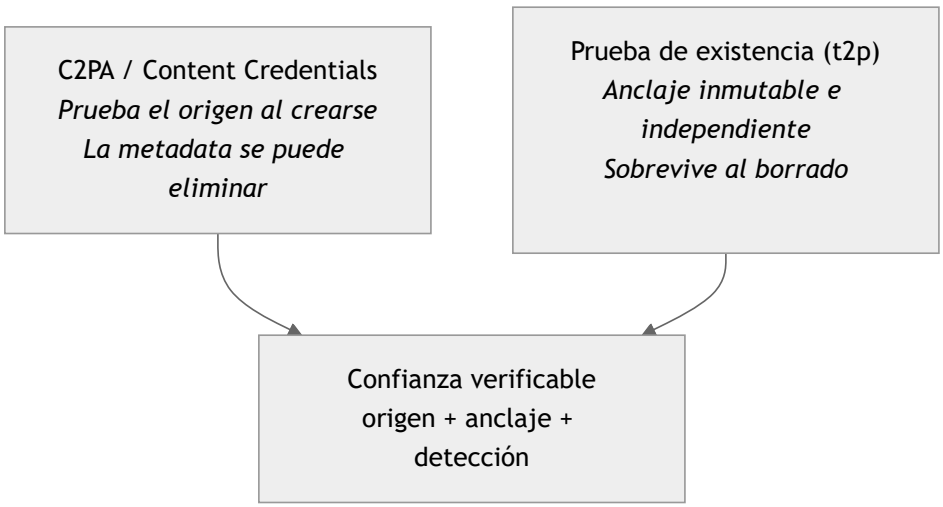


Figura 13.2 — C2PA demuestra «quién y cuándo» en origen; el anclaje en blockchain demuestra «esto existía y no se ha alterado».

t2p, la solución insignia

Aquí es donde la teoría se hace bolsillo. t2p convierte un teléfono en un estudio de pruebas portátil: cada foto, vídeo, audio, documento escaneado, página web o grabación de pantalla recibe, en el instante de crearse, una huella criptográfica única —un hash **SHA-512**— que queda registrada en una **blockchain pública** — hoy, la de **Polygon**; la aplicación puede implementar cualquier otra L2 de Ethereum, porque la prueba no depende de ninguna cadena concreta, sino del hecho de que el ancla sea pública y verificable por todos. El resultado es una prueba a prueba de manipulaciones de que algo existió y cuándo, verificable por cualquiera y para siempre. Y un principio de diseño lo gobierna todo: el archivo original **nunca sale del dispositivo**; solo viaja su huella. t2p no puede ver lo que capturas.

El flujo es la prueba de existencia descrita —como hemos visto— pero aplicada con rigor forense. Al capturar, la app calcula el hash a partir de los bytes exactos del archivo y lo ancla a la blockchain pública con una marca de tiempo. Añade, además, un sello de tiempo de confianza **RFC 3161** (estándar eIDAS) independiente de la cadena y, si el usuario lo permite, unas coordenadas **GPS de grado forense**: solo se sellan si la señal es genuina —precisión de unos 50 metros y una antigüedad máxima de 30 segundos—; una ubicación simulada bloquea la certificación para proteger el valor probatorio. Cada certificación genera un **certificado PDF** profesional con el hash, el identificador de la transacción, el sello RFC 3161, la ubicación y un **código QR** para comprobarlo en el explorador de la cadena.

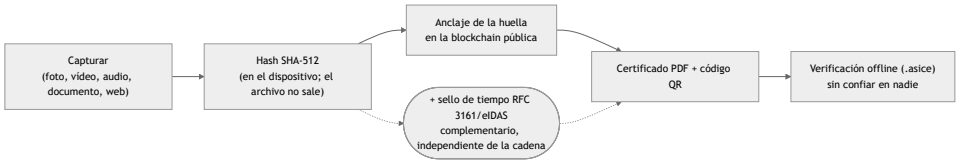


Figura 13.3 — El flujo de t2p: capturar, sellar la huella en la blockchain pública y poder verificarlo incluso sin conexión ni intermediarios.

La pieza más sólida para uso legal es el **paquete de evidencia** `.asice`: un contenedor estándar ASiC-E (ETSI EN 319 162) que incluye una copia byte a byte del archivo, el certificado, el sello de tiempo y su cadena de confianza, e incluso un archivo de texto con los comandos `openssl` para comprobarlo. Cualquiera puede verificar la prueba **completamente sin conexión, sin la app y sin tener que confiar en t2p**; es, en esencia, la diferencia entre «confía en nosotros» y «compruébalo tú mismo».

Sobre esta base, los casos de uso se despliegan solos.

- **Periodismo y medios.** Un reportero certifica una foto o un vídeo en el momento exacto de la captura; el lector verifica su origen escaneando el QR del certificado.
- **Pruebas legales y cadena de custodia.** El GPS forense, el sello RFC 3161 y el paquete `.asice` hacen que una prueba resista el escrutinio de un tribunal. Y la **firma con vídeo-selfie** —con pruebas de vida y verificación biométrica— vincula un documento a una persona real y presente.

- **Propiedad intelectual y autoría.** Sellar una obra demuestra que existía en una fecha cierta, sin registros ni intermediarios.
- **Integridad de datos climáticos y ESG**, el puente con la tesis de este libro. Una empresa puede certificar la lectura de un sensor de emisiones, un informe MRV o la fotografía de una instalación de manera que nadie —ni ella misma— pueda alterarlos después. La transición necesita exactamente esta clase de datos incontrovertibles.

t2p encarna una idea tan sencilla como poderosa: la confianza no hay que pedirla, hay que poder comprobarla. En una época en la que cualquier imagen puede ser falsa, volver verificable la verdad —y hacerlo desde el bolsillo— es quizá la infraestructura más discreta y, a la vez, más decisiva de toda la transición.

La promesa y el peligro

La prueba de existencia (t2p) ofrece una **confianza verificable** que se puede demostrar con un coste marginal: cada hash de datos se registra en la blockchain pública, donde la inmutabilidad y la transparencia están garantizadas por la red descentralizada. Esto transforma una declaración —por ejemplo «este informe ESG refleja las emisiones reales de una planta»— en una evidencia criptográficamente probada que cualquier actor puede consultar sin necesidad de confiar en un intermediario. El coste marginal de añadir una prueba es mínimo: una sola transacción de anclaje puede validar miles de hashes a la vez mediante el árbol de Merkle. Esta reducción drástica, fruto de una fusión de tecnologías (Merge de Ethereum −99,95 % en consumo energético) y de soluciones de capa 2, hace que la prueba de existencia sea **escalable a millones de inserciones diarias** sin crear barreras económicas para ONG o pequeñas empresas [6].

A escala de la operación, el beneficio es claro: las autoridades reguladoras pueden validar en tiempo real los informes de MRV (monitoring, reporting and verification) de carbono; los inversores pueden auditar la trayectoria de un proyecto sin depender de certificaciones centralizadas que a menudo son objeto de presiones políticas. La **capa de confianza** aportada por la blockchain se convierte así en el fundamento sobre el que se asienta la credibilidad de toda la transición energética. Sin este apoyo, las deepfakes —que según Europol podrían llegar al 90 % del contenido en línea en 2026— erosionan la fe pública y hacen que cualquier dato ESG sea visto con escepticismo [2].

No obstante, esta promesa viene acompañada de un peligro inherente. La **desanonimización** es una consecuencia inevitable cuando las pruebas de existencia se enlazan con metadatos identificables. El consorcio C2PA ha señalado que la divulgación de firmas digitales puede revelar el origen del contenido, exponiendo a periodistas y activistas a represalias en regímenes autoritarios [4]. Esto requiere un diseño cuidadoso de privacidad: las pruebas han de estar separadas de cualquier información personal y, si es necesario, utilizar **hash perceptual** para proteger el contenido sin comprometer la verificabilidad [5].

Además, la prueba de existencia **no detecta falsos por sí sola**; un atacante puede crear un documento fraudulento, registrar su hash y presentarlo como verdadero. La seguridad del sistema depende de procesos complementarios —como auditorías independientes, certificaciones de fuentes fiables y mecanismos de revocación— que han de estar integrados en el ecosistema. Un exceso de confianza en la tecnología podría conducir a una **laxitud reguladora**, donde las instituciones delegan todo el control en la cadena y obvian la necesidad de supervisión humana.

En conclusión, la prueba de existencia es una **tecnología necesaria pero no suficiente** para garantizar la verdad en la era de las deepfakes. Su éxito depende de la creación de un ecosistema que combine transparencia blockchain con marcos reguladores robustos (EU AI Act, Take It Down Act, CISA) y principios de privacidad diseñados para proteger a los más vulnerables [3]; solo así podremos convertir la promesa de confianza verificable en una realidad sostenible para la transición energética.

Además, Beth Noveck confirma que las tecnologías descentralizadas —y entre ellas la blockchain— son una de las vías propuestas para garantizar la autenticidad del contenido digital y aumentar su transparencia [7]. Sin embargo, ella defiende con claridad que las marcas de agua y los estándares de procedencia, por sí solos, no resuelven el problema porque dependen de la cooperación del creador y de las plataformas que las implementan [8]. Es aquí donde el anclaje neutral de **t2p** muestra todo su potencial: registrar el hash en una cadena pública sin ningún intermediario ni autoridad central asegura que la prueba de existencia se mantiene independiente del creador y de los terceros de confianza, cerrando el vacío señalado por Noveck y reforzando la promesa de una confianza verificable y universal.

Es hora de actuar

Verás que la verdad ya no es una condición natural del debate público; es un recurso que hay que comprar y proteger. Por eso cada grupo social tiene una misión concreta en el ecosistema de **t2p**.

1. Ciudadanía: el primer filtro

Antes de enviar o compartir cualquier vídeo, audio o imagen, pide la prueba de existencia. Las herramientas basadas en OpenTimestamps permiten verificar que un archivo se creó antes de un momento determinado y que no ha sido alterado desde entonces [1]. Este simple paso —un clic en una extensión del navegador o una app móvil— puede evitar la propagación masiva de deepfakes, una ola que Europol documenta al alza [2]. Cada usuario que se convierte en vigilante es una capa adicional de seguridad: la confianza no se construye solo a nivel institucional, sino también a través de una cultura de duda constructiva.

2. Medios de comunicación: el compromiso de publicar con prueba

Los portales informativos han de hacer del **timestamp** un requisito para todo contenido visual que pueda influir en la opinión pública o en decisiones políticas. Esto implica integrar una API de verificación blockchain en el flujo editorial y añadir, como metadatos visibles, el hash perceptual certificado en la cadena (véanse los estudios que demuestran la resistencia de estos hashes ante manipulaciones sutiles [5]). Cuando un medio indica «verificado con t2p», ofrece una garantía tangible que supera las declaraciones de buena fe. La falta de estas prácticas ya ha traído sanciones por parte del EU AI Act, que prevé multas de hasta el 7 % de la facturación anual global en las infracciones más graves [3].

3. Empresas: anclar los datos ESG y MRV

Las corporaciones que reportan emisiones de carbono o certificados ESG han de almacenar sus informes en una cadena pública inmutable. La migración hacia la red Ethereum, que ha reducido el consumo energético casi por completo con el último merge proof-of-stake [6], ofrece un entorno sostenible para este propósito. Cada registro de datos se firma con una clave privada y se asocia a un hash perceptual que garantiza la integridad del documento original. Además, la interoperabilidad entre estándares como el C2PA (que actualmente muestra limitaciones en la autenticación de origen) y las soluciones de timestamping permite crear una capa de confianza híbrida: la blockchain aporta inmutabilidad, mientras los protocolos de metadatos añaden contexto y rastro de propiedad [4].

4. Reguladores: definir estándares y fomentar la interoperabilidad

Las autoridades han de establecer marcos normativos que obliguen al uso de pruebas de existencia para cualquier información con impacto social o ambiental. Esto implica:

- **Requisitos de interoperabilidad** entre soluciones de timestamping, C2PA y las iniciativas del Take It Down Act, para asegurar que los certificados sean reconocidos transversalmente en la UE y en Estados Unidos.
- **Auditorías independientes** para validar la implementación de los protocolos a gran escala, con informes públicos trimestrales que incluyan el estado de cumplimiento de las empresas y los medios.
- **Incentivos fiscales** para las organizaciones que adopten soluciones basadas en blockchain de baja energía, como el Merge de Ethereum.

5. Un futuro sin verdad verificable no es un futuro sostenible

Sin una capa de confianza verificable, la transición energética se queda sin credibilidad: inversores, ciudadanos y gobiernos no podrán confiar en los datos que sustentan los proyectos de descarbonización. La prueba de existencia **t2p** ofrece el mecanismo para convertir promesas climáticas en hechos contrastados.

Por tanto, la llamada es clara: **actúa ahora**, verifica antes de compartir, publica solo con prueba y ancla tus datos en la blockchain. Solo así podremos avanzar hacia una transición energética creíble y duradera. Es *time2act*.

---

[1] OpenTimestamps — *a timestamping proof standard*. https://opentimestamps.org/ ↩

[2] Blockchain Council — *Preventing deepfake fraud with blockchain*. https://www.blockchain-council.org/blockchain/preventing-deepfake-fraud-with-blockchain-content-provenance-verification-workflows/ ↩

[3] London Blockchain — *Can blockchain save truth? (2025)*. https://londonblockchain.net/blog/blockchain-in-action/can-blockchain-save-truth-tackling-deepfakes-and-disinformation-in-2025/ ↩

[4] C2PA — *Content Credentials Explainer (especificación oficial)*. https://spec.c2pa.org/specifications/specifications/2.4/explainer/Explainer.html ↩

[5] arXiv — *Provenance Verification via a Perceptual Hash Registry Anchored on Blockchain*. https://arxiv.org/html/2602.02412v1 ↩

[6] ethereum.org — *The Merge*. https://ethereum.org/roadmap/merge/ ↩

[7] Beth Simone Noveck — *Reboot* (Yale UP, 2026), cap. 3. ↩

[8] Beth Simone Noveck — *Reboot* (Yale UP, 2026), cap. 3. ↩

Hidrógeno, captura y las apuestas que faltan

«Creo que un día el agua será empleada como combustible, que el hidrógeno y el oxígeno que la constituyen, usados solos o juntos, proporcionarán una fuente inagotable de calor y de luz.»

— Julio Verne, La isla misteriosa (1874-75)

Era una tarde de octubre de 2025 en Immingham, al norte del Reino Unido, donde el frío marino se infiltra entre las estructuras metálicas de uno de los complejos industriales más esperados del continente. Las torres de acero se alzaban como gigantes que prometían transformar la energía en hidrógeno verde, una llama invisible de futuro sostenible. Sobre el papel, el proyecto debía producir hidrógeno a partir de electrólisis alimentada por energía renovable y convertirse en una de las piezas de la descarbonización industrial europea.

Pero aquella mañana, el sonido que rompió la rutina no era el zumbido tranquilo de los compresores, sino un anuncio repentino: **Air Products había decidido cancelar el proyecto de H_2 verde de Immingham**, una iniciativa valorada en unos 2.000 millones de libras y considerada una de las mayores apuestas globales por la descarbonización industrial. El mensaje, corto pero contundente —«Proyecto suspendido indefinidamente»— se difundió al instante por los medios y por las redes donde ingenieros y analistas de la industria empezaron a comentar con una mezcla de incredulidad y resignación.

La noticia no era solo un revés financiero; era el reflejo de un fenómeno que se estaba consolidando a lo largo de los últimos años: **un sueño sobredimensionado sobre el hidrógeno verde**. Desde la promesa inicial, el sector había invertido recursos inmensos en prometer una energía limpia capaz de sustituir los combustibles fósiles en todos los sectores, desde el transporte marítimo hasta las ciudades. No obstante, 2025 marcó un **reset brutal** para el mercado. Según informes consolidados, aproximadamente **60 grandes proyectos de hidrógeno verde fueron cancelados aquel año**, suprimiendo una capacidad prevista de **−4,9 millones de toneladas por año** y reduciendo la proyección del pipeline global para 2030 de unos **49 a solo 37 millones de toneladas** [1].

En el corazón del complejo, las torres que se habían erigido como símbolos de una nueva era quedaron silenciadas. Los ingenieros que habían dedicado años a optimizar los procesos de electrólisis se encontraron mirando sus equipos con una mirada que oscilaba entre la frustración y la aceptación: el coste del hidrógeno verde había subido un **25-40 % desde 2022**, situándose ahora entre **4 y 7 euros por kilogramo** —casi tres veces más caro que su predecesor gris, que todavía rondaba los **1,5-2,5 euros/kg**, y claramente por encima del azul con captura de carbono (CCS), que se mantenía en un rango de **2-3,5 euros/kg** [2].

La conclusión que resonaba en Immingham viajó mucho más allá de las paredes del complejo; se convirtió en un eco que recorría la cadena de suministro global, recordando a todos los actores del sector que el optimismo sin datos puede ser tan peligroso como la inacción. El hidrógeno verde, tal como se había imaginado —energía para todo—, no era viable a gran escala en aquel momento. El despertar de este sueño sobredimensionado marcaba el principio de una nueva etapa: una llamada a la honestidad y a la revalorización de las apuestas, centrándose en aplicaciones concretas —acero, fertilizantes y química— donde el hidrógeno verde puede aportar realmente un cambio sustancial.

El sueño del hidrógeno

Cuando Paul Roberts, en *The End of Oil* (2004), dedicaba al hidrógeno un capítulo titulado irónicamente *And Now for Something Completely Different*, este gas se presentaba como la pieza clave de una economía limpia: un combustible que, al quemarse, solo dejaría huella de agua y, por tanto, podría sustituir al petróleo sin dejar huella de carbono. La visión, tan seductora, movilizó a inversores, gobiernos y grandes conglomerados energéticos; las previsiones apasionadas anunciaban una transición rápida hacia una red global de estaciones de hidrógeno, turbinas alimentadas por este gas limpio y un «ciclo de vida» completamente sostenible.

Esta esperanza se alimentó con números espectaculares y con una avalancha de proyectos de escala industrial, como las megainversiones de Air Products en Immingham o el proyecto de BP en Duqm, Omán. La idea era clara: si se podían producir millones de toneladas anuales, el mercado se ajustaría y el hidrógeno se convertiría en la nueva base energética.

Pero la realidad de 2025 rompió este cuento de optimismo con una llamada a la honestidad. Aproximadamente sesenta grandes proyectos de hidrógeno verde fueron cancelados aquel año y, como hemos visto, la producción prevista se redujo drásticamente mientras los precios aumentaban entre un 25 % y un 40 %, situándose en una franja de 4-7 €/kg [1].

Además, la infraestructura necesaria para distribuir hidrógeno a escala global —depósitos, conductos y estaciones de servicio— todavía presenta barreras técnicas y reguladoras. Las pérdidas en el transporte y las dificultades para almacenarlo de manera segura hacen que la propuesta de «hidrógeno universal» sea menos atractiva que alternativas como la electricidad directa. Paralelamente, la captura y almacenamiento de carbono (CCS) avanza a un ritmo lento y es cara, dejando el azul con CCS en una posición incierta [2].

Así, la promesa original —un combustible limpio que solo deja agua— se ha visto diluida por las limitaciones económicas y tecnológicas. El hidrógeno verde todavía tiene un papel crucial, pero ya no como solución universal, sino como complemento especializado en sectores donde el carbono es intrínsecamente difícil de eliminar: la producción de acero, los fertilizantes y las reacciones químicas de base. En estos nichos el impacto puede ser medible y justifica inversión dirigida, pero hay que abandonar la narrativa de «energía para todo» y adoptar una perspectiva basada en datos concretos y riesgos bien cuantificados.

El reset de 2025

2025 marcó un punto de inflexión que ha sacudido las expectativas más optimistas sobre el hidrógeno verde. En un año iniciado con promesas de inversiones masivas y una avalancha de proyectos anunciados como pilares de la transición energética, el mercado se enfrentó a datos duros: aproximadamente 60 de los grandes proyectos de H_2 verde fueron cancelados. Este retroceso supone una pérdida estimada de 4,9 millones de toneladas por año de producción potencial y ha reducido las proyecciones globales de H_2 verde en casi una cuarta parte respecto al plan original para 2030. Ahora la expectativa es de 37 millones de toneladas anuales —una caída drástica comparada con los 49 millones previstos hace dos años—, y se ha concretado en casos emblemáticos como el proyecto de Air Products en Immingham (Reino Unido), la iniciativa de BP en Duqm (Omán) y el esfuerzo de ArcelorMittal por descarbonizar sus plantas siderúrgicas en Alemania [1].

Esta ola de cancelaciones no es aleatoria, sino el reflejo de un modelo económico demasiado frágil ante la realidad del mercado. Muchos proyectos habían sido dimensionados para aprovechar subvenciones e incentivos gubernamentales sin un análisis riguroso de la demanda real a corto plazo. La debilidad de los pedidos industriales —especialmente en sectores que todavía dependen fuertemente del carbono fósil— ha dejado estas instalaciones con infraestructura costosa y sin clientes suficientes para justificar la amortización de los gastos iniciales.

Además, el coste de producir hidrógeno verde se ha disparado entre un 25 % y un 40 % desde 2022; actualmente oscila entre 4 y 7 euros por kilogramo, muy por encima del precio del hidrógeno gris y del azul con captura de carbono —como hemos visto—. Esta diferencia hace que el hidrógeno verde sea competitivo solo en aplicaciones donde la reducción de emisiones aporta un valor añadido crítico, como la producción de acero, los fertilizantes y algunos procesos químicos, pero resulta poco viable como sustituto universal de los combustibles fósiles en sectores como el transporte pesado o la electricidad de base.

El impacto combinado de una demanda insuficiente y de un aumento de costes ha generado una espiral negativa: los inversores, atemorizados por el retorno incierto, han reducido sus aportaciones, provocando que más proyectos se queden sin financiación y reforzando la percepción de que el hidrógeno verde todavía es una apuesta arriesgada. Este escenario obliga a replantear el papel del hidrógeno dentro del mix energético: no como solución universal, sino como componente estratégico para nichos donde la reducción de emisiones se traduce directamente en ventajas competitivas y reguladoras.

En resumen, 2025 ha funcionado como un «reset» brutal que ha obligado a la industria a abandonar las narraciones de futuro universalista y a adoptar una visión basada en datos concretos, costes transparentes y un análisis riguroso del mercado real. La lección más clara es que la viabilidad del hidrógeno verde depende menos de una política de incentivos masiva y más de una integración inteligente con las cadenas de valor donde el carbono es intrínsecamente difícil de eliminar, una perspectiva limitada en alcance pero capaz de generar impactos medibles y sostenibles. [1][2]

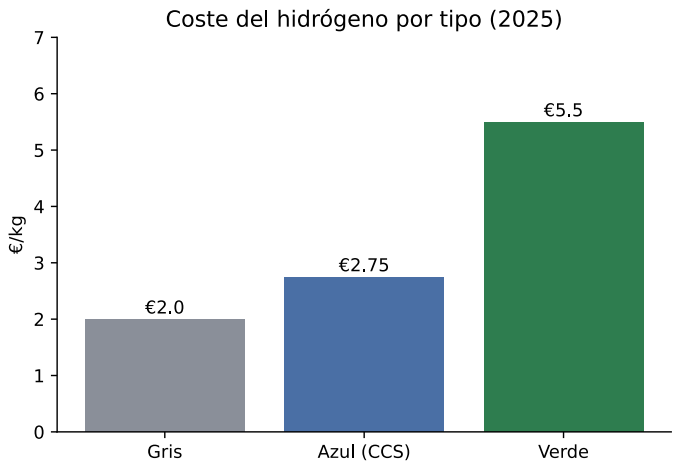


Figura 14.1 — El hidrógeno verde (4-7 €/kg) todavía es mucho más caro que el gris o el azul: el reto no es técnico, sino de coste y demanda.

Dónde sí tiene sentido

A la orilla del puerto de Immingham, donde las torres de Air Products se perfilan contra el cielo gris británico, es fácil imaginar a un grupo de ingenieros revisando los diagramas de flujo del hidrógeno verde que alimentaría una planta de acero de altas prestaciones. El objetivo no es celebrar una revolución energética universal, sino validar una apuesta concreta: sustituir el gas natural y el carbón en procesos donde la electrificación directa todavía es inviable o prohibitivamente cara. En esta zona, el hidrógeno verde se convierte en una herramienta de precisión, no en una bala de plata que prometa una transición masiva sin fundamentos.

En el sector siderúrgico, la reducción del hierro mediante hidrógeno (Direct Reduced Iron, DRI) ofrece una ruta clara para descarbonizar un proceso que tradicionalmente depende del carbón. Las iniciativas de ArcelorMittal para llevar el hidrógeno verde a sus plantas en Alemania apuntan en esta dirección, aunque el coste adicional —que ha subido un 25-40 % desde 2022, situándose entre 4 y 7 € por kilogramo— sigue siendo una barrera real [2]. Cuando se integra directamente en el flujo productivo, este sobrecoste se puede compensar con el ahorro en derechos de emisión y evita la necesidad de una infraestructura eléctrica a gran escala para alimentar una planta totalmente eléctrica.

En el ámbito de los fertilizantes, el amoníaco sigue siendo uno de los pilares del sistema alimentario mundial. La producción convencional depende casi exclusivamente del gas natural como fuente de hidrógeno gris; sustituirlo por hidrógeno verde permitiría reducir drásticamente sus emisiones de CO_2. Como ya se ha señalado, el coste superior (entre 4 y 7 € por kilogramo) puede ser compensado en plantas integradas por la mejora de la eficiencia del proceso y los incentivos a la reducción de emisiones, haciendo viable la producción a escala regional. Esta aplicación se convierte en una de las «zonas sin alternativa», donde la electrificación directa no puede sustituir la naturaleza intensiva del proceso químico.

En la química fina y petroquímica, el hidrógeno verde ya se utiliza como reactivo clave en procesos de hidrogenación que requieren condiciones de presión y temperatura difíciles de reproducir con electricidad. La integración de reactores alimentados por hidrógeno verde permite reducir las emisiones indirectas asociadas al transporte del gas y favorece una cadena de suministro más limpia. Disponer de hidrógeno verde producido localmente reduce los riesgos logísticos y mejora la trazabilidad del producto final.

Finalmente, en el sector de los transportes pesados —camiones de largo recorrido y buques de carga— el hidrógeno verde y sus derivados sintéticos ofrecen una alternativa posible donde las baterías de alta capacidad todavía no son prácticas. Es, justamente, uno de los usos que el recorte del pipeline ha aplazado: proyectos como el de BP en Duqm, cancelado en diciembre, han quedado en suspenso [1].

En resumen, el hidrógeno verde no morirá; simplemente encontrará su lugar en las áreas donde la sustitución por alternativas eléctricas es tecnológicamente imposible o económicamente inaceptable. La clave es tratarlo como una herramienta de precisión —una pieza que encaja perfectamente dentro de procesos industriales específicos— y no como una solución universal para todas las formas de energía.

Esta visión, basada en datos reales y casos concretos, ofrece un camino claro hacia una descarbonización medible y sostenible.

La captura de carbono y las apuestas que faltan

En los albores de 2026, la tecnología de captura y almacenamiento de carbono (CCS) sigue siendo una promesa incompleta. Avanza poco y sigue siendo cara: el coste por tonelada de CO_2 capturado todavía supera con gran diferencia las expectativas económicas de la mayoría de industrias. Este desequilibrio ha convertido la CCS en un refugio sospechoso para actores que buscan prolongar la vida útil de los activos fósiles sin afrontar el verdadero desafío de reducir la demanda de energía basada en hidrocarburos.

La captura de carbono todavía representa una fracción mínima de las emisiones globales de CO_2. La realidad es que la tecnología funciona bien en escenarios controlados —por ejemplo, en refinerías o en grandes fuentes puntuales de emisión— pero choca con barreras técnicas y reguladoras cuando se intenta aplicar a fuentes dispersas como el sector del cemento o el acero. Además, las estructuras de financiación actuales penalizan los proyectos de largo plazo: los inversores prefieren retornos rápidos, mientras que la vida útil de un depósito subterráneo seguro se extiende durante décadas.

Esta situación ha alimentado una narrativa peligrosa: presentar la CCS como «bala de plata» para las emisiones difíciles y, a la vez, utilizarla como justificación para retrasar políticas más contundentes de abandono del petróleo. La verdad es que la captura puede ser útil en nichos específicos —como el tratamiento de las emisiones de procesos siderúrgicos o la producción de hidrógeno azul con CCS—, pero solo si se combina con una reducción real de la energía basada en combustibles fósiles y con una política clara que limite las nuevas instalaciones de carbono. No es casual que BP, el mismo año que cancelaba Duqm, también pusiera en pausa su proyecto de hidrógeno azul con CCS en Whiting.

Mientras la CCS avanza a paso lento, otras apuestas emergentes ganan protagonismo. El almacenamiento de energía de larga duración se presenta como una solución clave para equilibrar las fuentes renovables intermitentes, con proyectos que exploran la conservación de energía en cavernas salinas y otras formaciones geológicas. La geotermia avanzada, impulsada por nuevas técnicas de perforación y recirculación de agua, empieza a abrirse camino. Y las redes eléctricas continuas —basadas en convertidores HVDC de nueva generación— ayudan a reducir las pérdidas de transmisión y facilitan la integración de energía renovable desde zonas remotas hacia los centros de demanda. Ninguna de estas opciones es, por sí sola, una «bala de plata».

En este contexto, el enfoque ha de ser holístico: la CCS se convierte en una herramienta complementaria para emisiones difíciles de reducir, pero no en el núcleo de una estrategia de descarbonización. Las inversiones han de priorizar tecnologías que ofrezcan flexibilidad y escalabilidad, como el almacenamiento de energía de larga duración y la geotermia avanzada, a la vez que se refuerzan las políticas reguladoras para evitar que la CCS se utilice como pretexto para mantener vivas las infraestructuras fósiles. Solo así podremos garantizar una transición verdadera hacia un futuro energético sostenible y resistente.

La promesa y el peligro

En los escenarios industriales donde la descarbonización es una obligación reglamentaria y no solo un objetivo de reputación, el hidrógeno verde se ha convertido en una pieza clave de un rompecabezas energético. En las siderúrgicas europeas, por ejemplo, la reducción directa del hierro requiere una fuente de calor y un agente reductor que no se pueden sustituir fácilmente por electricidad sin una inversión masiva. Aquí, un flujo constante de H_2 verde —producido a partir de energía eólica o solar— permite mantener la producción sin aumentar las emisiones de CO_2. De manera similar, en la fabricación de fertilizantes, donde el amoníaco concentra una parte muy importante del consumo de hidrógeno, la transición hacia H_2 verde reduce las emisiones asociadas al proceso, tal como apuntan varios proyectos piloto del sector.

Esta promesa se ve reforzada, en algunos casos, por la captura y almacenamiento de carbono (CCS). Aunque el despliegue global de la CCS ha avanzado poco, las instalaciones integradas con procesos de hidrógeno azul —donde el gas natural es reformado y el CO_2 resultante es capturado antes de ser liberado — pueden ofrecer una transición pragmática hacia un sector más limpio. La combinación de H_2 verde para las aplicaciones donde la electrificación directa todavía no es viable, con H_2 azul alimentado por CCS para usos intermedios, dibuja una arquitectura energética que puede reducir emisiones allí donde hoy no hay alternativa limpia.

No obstante, la tentación de presentar este conjunto como una solución universal amenaza con alejarnos del camino más económico y eficiente. La mayoría de los estudios comparativos muestran que electrificar directamente procesos como el transporte de mercancías por carretera o la calefacción residencial suele ser bastante más barato que sustituirlos por H_2 verde, teniendo en cuenta los costes actuales del combustible (entre 4 y 7 €/kg) y la infraestructura asociada [2]. Además, la proliferación de ofertas «verdes» sin una certificación rigurosa ha alimentado un mercado de créditos de hidrógeno que se comporta como las primeras bolsas de carbono: el riesgo de greenwashing aumenta a medida que las empresas buscan cumplir objetivos ESG con soluciones aparentemente sencillas pero poco sustanciales.

El peligro, por tanto, no es solo económico sino también estructural. Promover el hidrógeno verde y la CCS como respuesta única puede retrasar inversiones cruciales en infraestructura eléctrica de gran escala —como las redes de recarga ultrarrápida o los almacenes de energía con baterías— que son necesarias para aprovechar al máximo el exceso renovable. Cada año que se destina capital a instalar una planta de electrólisis de gran capacidad, en lugar de reforzar la red eléctrica o desarrollar sistemas de gestión de la demanda, se pierde una oportunidad de reducir las emisiones globales con un coste marginal inferior.

El hidrógeno verde y la CCS son componentes imprescindibles del rompecabezas industrial: ofrecen soluciones viables para sectores donde la electrificación directa todavía no es factible. Pero su valor real solo se mantiene si se utilizan de manera focalizada, sin pretensiones de universalidad que podrían desviar recursos y retrasar la transición hacia una electrificación más amplia y económicamente eficiente. La clave es equilibrar las apuestas: priorizar la electricidad donde es más rentable y reservar el hidrógeno verde y la CCS para los nichos que realmente lo necesitan.

El precio del tiempo perdido

Imaginemos una mañana en Immingham, al norte de Inglaterra: las torres de la planta de Air Products, que hace unos años prometía ser el faro del hidrógeno verde, quedan ahora silenciadas detrás de una pared de avisos de cancelación. El proyecto, junto con una sesentena de iniciativas similares, fue retirado del programa global en 2025, reduciendo la producción prevista en casi cinco millones de toneladas anuales (−4,9 Mt/año) [1]. Esta caída no es un simple retroceso numérico; es una señal de alerta que demuestra cómo el exceso de esperanza puede convertirse en una carga para la transición energética.

El colapso se explica por el desajuste entre las expectativas de mercado y las realidades técnicas y económicas. El coste del hidrógeno verde ha aumentado entre un 25 % y un 40 % respecto al precio de 2022, situándose ahora entre 4 y 7 €/kg [2], superando ampliamente el del hidrógeno gris (1,5-2,5 €/kg) e incluso el del azul con captura de carbono (2-3,5 €/kg) [2]. En un contexto donde las inversiones son cada vez más exigentes y la financiación se dirige hacia soluciones con retornos más rápidos, el hidrógeno verde sigue siendo una zona gris: prometedor, pero demasiado caro para ser adoptado a gran escala sin subsidios masivos. Esta realidad ha afectado también a los grandes proyectos de pipeline previstos para 2030, que han caído de 49 a 37 Mt —como hemos visto anteriormente—, fragmentando la cadena de suministro y limitando las oportunidades en sectores clave como el acero, los fertilizantes o la química.

Pero el verdadero peligro reside en el tiempo perdido. Cada año que se retrasa la adopción de una infraestructura de hidrógeno verde y CCS donde tiene sentido implica más emisiones de carbono, costes de descarbonización más altos y una dependencia creciente del gas natural y de los combustibles fósiles. La falta de acción amplifica la necesidad de soluciones alternativas, como la electrificación directa en procesos industriales, que se muestra cada vez más competitiva tanto a escala técnica como económica.

En este escenario, decidir dónde y cómo invertir es crucial. No podemos permitir que el «hype» nos desvíe hacia proyectos con retornos largos e inciertos; hemos de orientar los recursos hacia nichos donde el hidrógeno verde ofrece una ventaja clara: la descarbonización de procesos que no se pueden electrificar fácilmente, como la reducción del hierro o la síntesis de amoníaco. Simultáneamente, hay que impulsar la investigación y el desarrollo de tecnologías CCS más eficientes y menos costosas, para alcanzar una transición realista y equilibrada.

En resumen, si no desplegamos estas soluciones con la urgencia que exigen, el coste de la inacción se traducirá en un aumento de los precios energéticos, una inseguridad climática mayor y una oportunidad perdida para posicionar a las economías europeas como líderes en tecnologías limpias. Con esto se cierra el repaso de las soluciones energéticas. La Parte V traslada esta misma urgencia al terreno de la confianza: por qué detectar las falsificaciones no basta, y cómo la prueba de existencia empieza a desplegarse en los primeros frentes —finanzas, fotoperiodismo, sanidad, educación y derechos humanos.

[1] IEA, *Global Hydrogen Review 2025* / CleanTechnica. https://www.iea.org/reports/global-hydrogen-review-2025/executive-summary ↩

[2] IEA / The Extractor, *coste del H₂ verde 2022-2025*. https://cleantechnica.com/2025/07/07/hydrogens-brutal-month-billions-lost-as-mega-projects-collapse/ ↩

Detectar no es suficiente: la prueba de existencia como defensa duradera

«Para que una tecnología tenga éxito, la realidad debe prevalecer sobre las relaciones públicas, porque a la naturaleza no se la puede engañar.»

— Richard Feynman, informe Rogers sobre el Challenger, apéndice F (1986)

Era una tarde fría de enero de 2026 cuando la editorial **LlumVerda** recibió, a través de su canal seguro de transferencia de archivos, un vídeo que prometía cambiar el curso de las elecciones locales en Barcelona. El clip mostraba al candidato principal, Marc Soler, pronunciando una frase incendiaria: *«Los impuestos para la cultura aumentarán un 30 % este año»*. La voz era clara, la expresión facial parecía genuina y el fondo de una sala de reuniones municipal se reconocía al instante. El equipo editorial, consciente del crecimiento exponencial de los deepfakes —de 500.000 en 2023 a casi **8 millones** en 2025 según Sumsub [9]—, sometió el archivo al *DeepSight Pro*, el detector de manipulaciones más avanzado disponible en aquel momento. El programa, alimentado por una red neuronal entrenada con las últimas bases de datos de falsificación, emitía un informe escueto: **«Probablemente auténtico»**, con un porcentaje de confianza del 78 %.

Sin perder tiempo, la redactora jefe, Laura Martínez, programó la publicación en el portal digital, añadiendo una breve nota que recordaba a los lectores que la verdad visual todavía era fiable. El tráfico se disparó: miles de comentarios y compartidos aparecieron en las redes sociales en cuestión de horas, y el debate político ya se vislumbraba encendido.

Tres días después, una alerta interna del departamento de seguridad informática reveló la verdad. El vídeo había sido generado con un modelo de síntesis más reciente que cualquier actualización del detector DeepSight Pro: la tecnología para crear el falso se había adelantado a la capacidad de detección. Ningún sello de procedencia acompañaba el archivo, y el detector —entrenado con falsificaciones de una generación anterior— había sido engañado. En otras palabras, la defensa reactiva siempre iba un paso por detrás del atacante.

Este escenario no es una ficción aislada; los datos de *DeepFake-Eval-2024* muestran que los detectores fallaban entre un **45 % y un 50 %** de los casos en entornos reales [1]. Cada vez que dependemos únicamente de la detección, nos encontramos atrapados en una carrera armamentística donde el generador avanza más rápido que el análisis. La pregunta que emerge es inevitable: **¿y si, en lugar de perseguir la mentira, pudiéramos demostrar la verdad desde su origen?**

La respuesta a esta cuestión define el núcleo de la defensa duradera propuesta a lo largo de este capítulo. No se trata solo de detectar una manipulación, sino de **certificar la procedencia y la integridad del contenido en el momento mismo en que se crea**, tal como recomiendan las autoridades norteamericanas (NSA/FBI/CISA) a partir de 2023 [4]. Esta visión, que combina pruebas criptográficas con anclaje en blockchain —la huella del archivo anclada en una cadena pública, con el sello de tiempo RFC 3161 como complemento, tal como la aplica la iniciativa *t2p* [7]—, ofrece una respuesta al peligro de confiar únicamente en detectores cada vez más obsoletos.

En las próximas secciones exploraremos cómo esta prueba de existencia se traduce en cinco frentes sectoriales —compliance, fotoperiodismo, sanidad, educación y defensa— y qué pasos concretos podemos tomar hoy para transformar la teoría en práctica. El futuro de la verdad digital depende, no solo de ver bien, sino de **saber de dónde viene** y poder demostrarlo sin duda.

La carrera que perdemos

En el momento en que la mayoría de organizaciones confían solo en una línea de defensa —la detección de deepfakes— se encuentran inmersas en una carrera armamentística asimétrica que, hasta ahora, han perdido. El banco de pruebas DeepFake-Eval-2024, que recoge muestras reales de algoritmos generadores en circulación en el mercado en 2024, revela unas caídas dramáticas: los mejores detectores open-source registran una precisión del **45-50 %** respecto a los entornos de laboratorio, con un rendimiento de **0,75** en vídeo, **0,86** en audio y **0,63** en imagen —todo por debajo del **~90 %** que consigue un analista humano entrenado [1]. Incluso los comerciales más avanzados llegan solo al **78 %** de exactitud, una diferencia significativa cuando se trata de preservar la confianza en entornos críticos.

Esta brecha no es casual. El fenómeno del *domain shift* —donde los modelos entrenados con datos limpios y controlados fallan en escenarios reales donde audio y vídeo son comprimidos, codificados o manipulados por plataformas sociales— crea una vulnerabilidad estructural que el simple reentrenamiento no puede cerrar de manera sostenible. Cada vez que se introduce un nuevo filtro de compresión o se modifica el algoritmo de grabación, los modelos de detección pierden precisión y han de ser recalibrados; mientras tanto, los generadores de deepfakes avanzan a una velocidad exponencial, mejorando la calidad y la eficiencia de sus resultados. En este juego de intercambio, el atacante decide *cuándo* y *cómo* atacar, dejando las defensas reactivas en constante desventaja.

El volumen de contenido falso no hace sino aumentar. Según datos de Sumsub, el número de deepfakes circulantes pasó de **~500.000** en 2023 a **~8 millones** en 2025 —un incremento de más de quince veces en solo dos años [9]— y esta explosión amplifica la probabilidad de que un contenido malicioso llegue a una audiencia amplia antes de que cualquier detector pueda identificarlo. Además, la proliferación de herramientas de generación accesibles democratiza el poder de crear falsificaciones convincentes, reduciendo las barreras de entrada para actores maliciosos y aumentando la diversidad de los escenarios de ataque.

En resumen, depender exclusivamente de la detección es como intentar cerrar una puerta con una cadena mientras el ladrón tiene una sierra. Las limitaciones técnicas —el *domain shift*, la falta de generalización sostenible— y la escalada del volumen y sofisticación de los deepfakes convierten esta estrategia en una carrera que, hasta ahora, hemos perdido. Para invertir el balance, hay que avanzar hacia soluciones que no solo identifiquen lo falso, sino que **certifiquen el origen y la integridad del contenido** desde el momento de su creación; esta es la premisa fundamental sobre la que se apoyan los cinco frentes sectoriales que exploraremos a continuación.

De la detección a la procedencia

En un aula de la Universidad de Stanford, el profesor Hany Farid muestra a un grupo de alumnos una imagen aparentemente auténtica de un discurso político y, con unos cuantos clics, revela que el vídeo contiene una capa de manipulación invisible para los ojos entrenados pero no para la tecnología actual de detección. «La detección reactiva es como intentar apagar un incendio después de que el edificio ya se ha derrumbado», afirma Farid, y subraya que **la clave es conocer el origen del medio**, tal como una etiqueta nutricional indica los ingredientes de un producto [2]. Esta metáfora ilustra la limitación de los detectores —que caen entre el 45 % y el 50 % en pruebas reales, según el estudio DeepFake-Eval-2024 [1] — y, como hemos visto, ofrece una ruta clara: registrar la procedencia desde el primer instante.

El experto en seguridad digital Sam Gregory, fundador de WITNESS, ha defendido durante más de una década el programa **«Prepare, Don't Panic»**, una llamada a construir una infraestructura de autenticidad que vaya más allá de la simple detección [3]. En sus presentaciones, Gregory describe cómo una cadena de confianza —captura firmada, metadatos verificables y certificación de origen— puede integrarse directamente en los flujos de producción multimedia. Esta infraestructura permite que cada archivo lleve consigo una prueba inmutable del momento y del contexto en que se creó, evitando que un deepfake pueda ocultar su verdadera historia.

Incluso las agencias gubernamentales más conservadoras reconocen la necesidad de este cambio de paradigma. La guía conjunta de la NSA, el FBI y la oficina CISA —como ya se señaló en 2023— establece como prioridad igual tanto la detección de contenidos manipulados como el establecimiento de su procedencia [4]. El documento subraya que, si los generadores de IA avanzan más rápidamente que las herramientas de detección, confiar únicamente en identificar lo falso es una apuesta perdida; **verificar de dónde viene y si ha sido alterado desde el origen** ofrece una defensa matemáticamente verificable y escalable.

Esta transición no es solo técnica sino cultural. Pasar de preguntar «¿Es falso?» a preguntar «¿De dónde viene y cómo ha evolucionado?» implica reconfigurar las prácticas editorial, legal y empresarial. Los creadores han de adoptar estándares como el **C2PA/Content Credentials**, pese a la vulnerabilidad de los metadatos eliminables [5]; y organizaciones como OpenTimestamps ya están sellando millones de archivos —alrededor de 750 millones del Internet Archive— con transacciones blockchain, ofreciendo una capa de anclaje irreversible [6].

En resumen, la **procedencia** se convierte en el núcleo de una defensa duradera contra las deepfakes. No es solo un complemento a la detección; es la alternativa que transforma la lucha por la verdad en un proceso verificable y auditable desde el primer instante de creación del contenido. Esta visión, respaldada

por expertos académicos, empresariales y gubernamentales, marca el punto de inflexión hacia una era donde la confianza se basa en pruebas concretas y no en suposiciones.

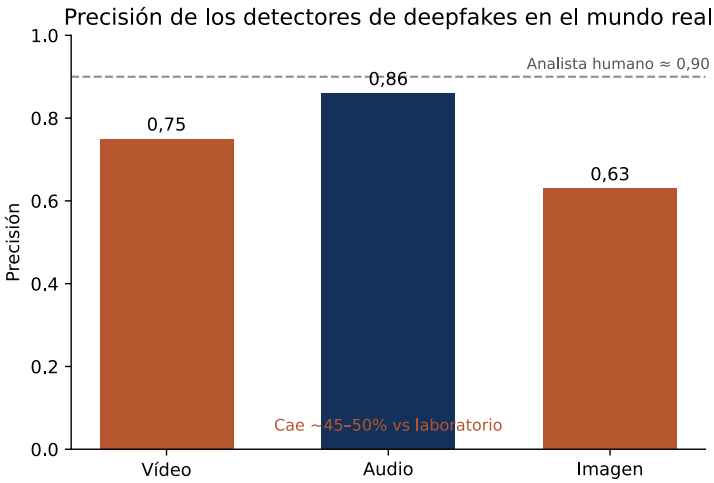


Figura 15.1 — La precisión de los detectores cae en el mundo real a medida que mejoran los generadores; un ancla de procedencia no se degrada con el tiempo.

Dos piezas complementarias

En el panorama actual donde las deepfakes proliferan a ritmos exponenciales —de 500.000 casos estimados en 2023 a cerca de 8 millones solo en 2025 según Sumsub [9]— la detección por sí sola se convierte en una carrera armamentística insostenible. Los detectores más avanzados caen entre un 45 % y un 50 % en pruebas reales (DeepFake-Eval-2024) [1], como hemos visto, mientras que los generadores de contenido falso siguen superando las mejoras tecnológicas a una velocidad superior. La respuesta sostenible ha de ir más allá del «ver y bloquear»; ha de establecer una cadena de confianza inalterable desde el momento de la creación y que persista aunque los metadatos sean borrados o manipulados.

C2PA / Content Credentials: el registro criptográfico del origen

El consorcio C2PA (Coalition for Content Provenance and Authenticity) ha desarrollado los *Content Credentials*, un manifiesto firmado con certificados X.509 que captura, en forma de estructura JSON, la información clave del proceso creativo: quién generó el archivo, qué herramientas se han utilizado y en qué momento se aplicaron las distintas ediciones. Esta infraestructura ofrece una prueba criptográfica del «quién/cuándo» en el origen, permitiendo a editores, plataformas y consumidores verificar la procedencia de una imagen o vídeo sin depender de un tercero de confianza [5]. En su diseño, C2PA se basa en firmas digitales que, si se conservan íntegras, son imposibles de falsificar.

No obstante, el modelo presenta una vulnerabilidad fundamental: las credenciales pueden ser eliminadas. Las redes sociales, los procesos de recodificación e incluso la simple exportación de un archivo a menudo suprimen o sobrescriben este manifiesto. Cuando la credencial desaparece, no queda ninguna huella verificable de su contenido original; su ausencia, por tanto, no demuestra nada [5]. Esta limitación ha llevado a expertos como Hany Farid a afirmar que «la procedencia es la mejor defensa», pero solo si esta se mantiene accesible e intacta a lo largo del ciclo de vida del contenido [2].

Prueba de existencia: el ancla inmutable

La solución a este vacío se encuentra en el mecanismo de *proof of existence* descrito en el capítulo 13. La idea es simple pero poderosa: calcular una huella criptográfica del archivo —un hash— y anclarla en una transacción de una blockchain pública. Esta operación crea una prueba inmutable que demuestra que el archivo existía en aquel momento, sin necesidad de incluir ningún metadato adicional; de forma complementaria, un sello de tiempo conforme al estándar RFC 3161, independiente de la cadena, añade la certificación de una autoridad cualificada. Proyectos como OpenTimestamps ya han aplicado este enfoque a millones de archivos del Internet Archive con una sola transacción, como hemos visto (Peter Todd) [6].

A diferencia del C2PA, que depende de la conservación del manifiesto, el anclaje del hash es independiente de cualquier capa intermedia. Incluso si los metadatos son suprimidos o el archivo se reprocesa, la huella

anclada en la blockchain conserva un ancla verificable que confirma la existencia inalterada del contenido original en la fecha registrada [7].

Sinergia entre procedencia y prueba de existencia

Las dos tecnologías no son rivales; son complementarias. C2PA aporta la información «quién/cuándo» en el momento de la creación, mientras que la huella anclada en la blockchain pública garantiza «esto existía, inalterado, antes de esta fecha». Al combinarlas se obtiene una defensa robusta que supera las limitaciones de cada método por separado. La procedencia puede perderse, pero la prueba de existencia persiste; a la vez, la prueba de existencia no revela quién creó el contenido, pero la credencial C2PA lo hace siempre que se mantenga.

Esta doble capa de verificación transforma la lucha contra las deepfakes de una detección reactiva a una arquitectura preventiva y auditable. Como recomiendan las autoridades gubernamentales —NSA, FBI y CISA— en sus directrices de 2023, establecer la procedencia es clave para garantizar la integridad de la información [4]. Sin el ancla inmutable de la prueba de existencia, esta garantía se queda a medias. La combinación de ambas piezas forma una defensa duradera y verificable desde el primer instante de creación hasta el momento en que el contenido llega a las manos del público. Esta es la base sobre la que los cinco frentes sectoriales —compliance, fotoperiodismo, sanidad, educación y defensa— podrán construir políticas y sistemas resilientes ante la era de las deepfakes.

El «cuándo» inalterable: OpenTimestamps y RFC 3161

En primavera, mientras los equipos de verificación de imágenes se veían superados por la explosión de las deepfakes —como hemos visto [9]— una solución sencilla pero poderosa empezaba a ganar tracción: la prueba de tiempo verificable. OpenTimestamps, el estándar abierto ideado por Peter Todd, transforma cualquier archivo en una huella digital inmutable agrupando miles de hashes en un árbol de Merkle y anclando su raíz a la cadena de bloques de Bitcoin con una única transacción. Este procedimiento produce una prueba compacta que cualquiera puede validar sin depender de una entidad centralizada, tal como describe su diseño: «la prueba es verificable por cualquiera, sin confiar en ninguna empresa» [6].

Hasta el momento, OpenTimestamps ha sellado una gran cantidad de archivos del Internet Archive con una sola transacción en Bitcoin y convierte este vasto catálogo histórico en un registro inmutable de su momento de existencia [6]. Cada raíz de árbol Merkle funciona como testigo criptográfico: si el contenido se modifica, el hash resultante ya no coincide con la raíz anclada y la prueba queda rota. Así, el mecanismo ofrece una respuesta directa al problema central de las deepfakes: **cuándo** apareció por primera vez un archivo y que no se ha alterado desde entonces.

Sin embargo, como advierte Hany Farid, «la procedencia es la mejor defensa» [2]; el sello de tiempo, pese a ser una garantía robusta del *cuándo*, no comprueba la autoría ni la veracidad intrínseca del contenido. Un vídeo puede estar perfectamente anclado a una fecha concreta y, a la vez, contener información engañosa o manipulada. Por eso el modelo t2p ancla la huella SHA-512, calculada en el propio dispositivo de origen, directamente en una transacción de una blockchain pública —ese anclaje es la prueba— y añade, como refuerzo independiente de la cadena, un sello de tiempo RFC 3161 (el estándar eIDAS de sellado de confianza). Este «cinturón y tirantes» asegura que, aunque las claves privadas de la autoridad de sellado caduquen o sean comprometidas, la prueba pública sigue siendo verificable gracias a la huella inmutable almacenada en la cadena [7].

Esta arquitectura también permite una integración fluida con infraestructuras de autenticidad emergentes como WITNESS, que promueven «Prepare, Don't Panic» y ofrecen capas adicionales de verificación basada en metadatos firmados [3]. En la práctica, un creador de contenido puede generar la huella del archivo en el momento de la captura y anclarla en una blockchain pública —directamente, o agregada en un árbol de Merkle mediante servicios como OpenTimestamps—, y añadir, si necesita la certificación de una autoridad, un sello RFC 3161 complementario. El resultado es una cadena verificable que indica: *este archivo existía en esta fecha, sin alteraciones posteriores*, y que puede ser contrastada con los metadatos de procedencia registrados por WITNESS u otras entidades reguladoras.

Esta combinación de elementos —huella local, anclaje en blockchain pública y sello RFC 3161 complementario— constituye la base tecnológica de la defensa duradera contra las deepfakes. No se trata solo de detectar una manipulación, sino de demostrar inequívocamente el momento original de creación y mantenerlo intacto a lo largo del ciclo de vida digital. En un entorno donde los generadores de IA evolucionan a ritmos acelerados, esta prueba de tiempo se convierte en la piedra angular para las políticas

sectoriales que abordarán la crisis de confianza: desde el compliance corporativo hasta el fotoperiodismo, pasando por sanidad, educación y defensa. Sin ella, cualquier detección sería una carrera armamentística; con ella, disponemos de un marco verificable que transforma la **procedencia** en un activo tangible e inmutable.

El marco legal llega

La entrada en vigor del **EU AI Act**, artículo 50, el 2 de agosto de 2026 marca un punto de inflexión claro: cualquier contenido generado por inteligencia artificial ha de llevar una etiqueta legible por máquina que indique su procedencia y, específicamente, las deepfakes han de estar marcadas como «synthetic» [8]. En la práctica, las empresas que ya usan soluciones **t2p** —la huella anclada en la blockchain pública, con el sello RFC 3161 como complemento, tal como hemos descrito en el capítulo 13 [7]— se encuentran un paso por delante: su infraestructura puede generar automáticamente la marca de procedencia requerida por la normativa, convirtiendo la prueba de existencia en una respuesta directa a la obligación legal.

En Estados Unidos, la **TAKE IT DOWN Act**, firmada en mayo de 2025, eleva la cuestión a un nivel penal. La ley criminaliza explícitamente la distribución no consentida de imágenes íntimas —incluidas las «digital forgeries» o deepfakes— e impone a las plataformas una obligación de retirada en **48 horas** desde el momento de la denuncia [8]. El requerimiento legal es inequívoco: las plataformas han de poder demostrar, con evidencia criptográfica, que el contenido ha sido verificado o eliminado para cumplir la orden. Esto convierte la **procedencia** en una exigencia operativa y no solo en una buena práctica.

El último eslabón del rompecabezas legislativo es la **DEFIANCE Act**, aprobada por el Senado en enero de 2026 y todavía pendiente de votación en la Cámara de Representantes [8]. Esta ley añade una vía civil para las víctimas de manipulación digital, permitiendo que presenten reclamaciones basadas en la falta de evidencia verificable de origen e integridad del contenido. En otras palabras, una **prueba de existencia** —tal como la proporciona OpenTimestamps, que ha sellado millones de archivos del Internet Archive [6]— se convierte en un activo decisivo para sostener cualquier reclamación.

El hilo conductor de estas tres iniciativas es claro: la ley ya no pide solo «si el contenido es falso», sino **«de dónde viene y cómo se puede demostrar que era íntegro en una fecha concreta»**. Las empresas que todavía dependen únicamente de detectores —que, según DeepFake-Eval-2024, fallan entre un 45 % y un 50 % en entornos reales [1]— se encontrarán en una posición de incumplimiento inevitable. En cambio, las que ya han integrado la prueba de existencia en sus cadenas de suministro digital podrán responder de inmediato con unos metadatos verificables y sellos criptográficos, evitando sanciones y ganando confianza del mercado.

Así pues, el marco legal no solo impulsa el **marcado** de contenido; establece una **exigencia de demostración** que convierte la prueba de existencia en un activo indispensable. Las organizaciones que anticipen esta necesidad —como las que adoptan los estándares C2PA, pese a las limitaciones de metadatos eliminables [5]— podrán transitar hacia una arquitectura de confianza resiliente, evitando el riesgo de quedar «a remolque» ante una regulación que avanza a paso firme. La respuesta no es solo detectar; la respuesta es **documentar**, **sellar** y **probar** —el fundamento sobre el que se construirá la nueva era de credibilidad digital.

Cinco frentes

La crisis de confianza que hemos expuesto no es una catástrofe abstracta; se traduce en pérdidas económicas, daños a la reputación, riesgos para la salud y vidas truncadas. Cada sector comparte una lógica común: **detectar** una deepfake solo es el primer paso, a menudo demasiado tarde; la defensa real consiste en **documentar**, **sellar** y **probar** la procedencia del contenido desde el momento de su creación.

1. **Compliance y finanzas** — El caso más emblemático reciente es la videollamada que engañó a Arup, provocando un fraude de 25,6 millones de dólares. Sin una prueba inequívoca del origen del vídeo, los equipos de control quedaron atrapados en una carrera armamentística con los generadores de deepfake, y la detección posterior no impidió el pago indebido. Aquí la **prueba de existencia** habría permitido validar qué material audiovisual era auténtico antes de cualquier transacción, bloqueando la estafa en su fase incipiente.

2. **Fotoperiodismo y medios** — La imagen sigue siendo el testigo más potente del momento. Cuando una fotografía manipulada circula como prueba de un acontecimiento, el daño reputacional para el diario o para el periodista es irreversible. Las herramientas de sellado como OpenTimestamps ya han **sellado alrededor de 750 millones de archivos** del Internet Archive, ofreciendo una cadena de confianza que puede ser consultada para verificar la procedencia de una foto antes de que llegue al público [6].

3. **Sanidad** — Las imágenes médicas manipuladas amenazan diagnósticos y tratamientos. Un escáner alterado podría conducir a una cirugía innecesaria o, peor aún, a la omisión de un tumor. En este contexto, la procedencia certificada es la mejor defensa, como recuerda Hany Farid: «la procedencia es la mejor defensa» [2]. Un registro inmutable de cada imagen —la huella anclada en la blockchain pública, con sello de tiempo complementario— garantizaría que los profesionales sanitarios trabajen siempre con datos originales y verificables [7].

4. **Educación** — Las credenciales académicas y la autoría de obras digitales son objetivos constantes de falsificación. Un diploma digital alterado puede abrir puertas a empleados no cualificados, mientras que un artículo plagiado o manipulado puede desvirtuar el conocimiento científico. La prueba de existencia permitiría registrar cada entrega académica con una marca de tiempo segura, haciendo imposible la revisión retroactiva del contenido sin dejar rastro.

5. **Defensa y derechos humanos** — En conflictos armados, las deepfakes se convierten en armas de desinformación que pueden manipular la opinión pública y falsificar pruebas de crímenes. La capacidad de atribuir con certeza la fecha y el origen de un vídeo o audio es fundamental para tribunales internacionales y para organizaciones de derechos humanos. Sin esta capa, el riesgo de «falsas narrativas» se convierte en una amenaza directa a la justicia.

En todos estos frentes, la **lógica** es idéntica: detectar arranca tarde y demostrarlo desde el origen, llegando a tiempo. En los capítulos que siguen exploraremos cómo la prueba de existencia se integra en cada sector, revelando tanto la amenaza real como las soluciones concretas para protegernos contra una era donde lo falso puede parecer indistinguible de lo verdadero.

La promesa y el peligro

Imaginemos una red global de autenticidad donde cada vídeo, audio o documento digital lleva con orgullo un sello inmutable que certifica su fecha de creación y el origen del nodo que lo ha generado. Esta capa de confianza verificable es tan barata como cualquier transacción blockchain de baja tarifa y se puede escalar a millones de usuarios sin necesidad de intermediarios centralizados. El modelo propuesto por **t2p** combina la procedencia —la información sobre quién, dónde y cuándo ha producido el contenido— con el anclaje criptográfico de la huella en una cadena de bloques pública, reforzado con un sello de tiempo RFC 3161 independiente de la cadena [7]. Cuando un medio se ve atacado por deepfakes, el receptor puede consultar al instante la prueba de existencia y verificar que aquel archivo ya existía, intacto, en una fecha anterior al supuesto engaño. En la práctica, esta solución ha sido adoptada por proyectos como OpenTimestamps, que ya ha sellado alrededor de **750 millones** de archivos del Internet Archive con una sola transacción [6], demostrando que el coste marginal es casi nulo y que la infraestructura puede soportar cargas masivas.

Esta promesa no es meramente teórica; organizaciones como WITNESS, liderada por Sam Gregory, ya han desplegado una infraestructura de autenticidad que permite a periodistas y organizaciones de derechos humanos «prepararse, no entrar en pánico» ante la manipulación digital [3]. La normativa europea, con el AI Act (Art. 50) aplicado desde el 2 de agosto de 2026, exige explícitamente que el contenido generado por IA lleve una marca de procedencia legible por máquina para reducir los riesgos de difusión de deepfakes [8]. Esto crea un marco legal que impulsa la adopción masiva de estas tecnologías y ofrece una base segura para que las autoridades puedan actuar con evidencia verificable.

No obstante, el peligro reside en la **desanonimización** potencial de los creadores vulnerables. Hany Farid recuerda que «la procedencia es la mejor defensa», pero también advierte que, si se revela demasiada información sobre el origen, periodistas de investigación, disidentes o víctimas de violencia pueden ser localizados y perseguidos [2]. Un sistema mal diseñado podría convertir la procedencia en un arma contra aquellos que dependen de su anonimato para la seguridad personal; por eso los metadatos de procedencia, como las credenciales C2PA, han de poder gestionarse con cuidado [5].

Además, la confianza ciega en el sello puede generar un **excesivo sentimiento de veracidad**: «si lleva sello, es verdad» se convierte en una falacia que descuida las otras líneas de defensa. La prueba de existencia no detecta por sí sola los falsos; solo demuestra que el contenido existía en un momento determinado. Sin una detección activa —y sin alfabetización mediática que enseñe a cuestionar y contrastar— la sociedad podría caer en una falsa seguridad, creyendo que el problema de las deepfakes se ha resuelto por completo.

Por tanto, ninguna tecnología puede ser considerada una bala de plata. La solución robusta se encuentra en la **combinación** de una procedencia fiable, el anclaje criptográfico, sistemas avanzados de detección y una educación continua a la población sobre los límites y las vulnerabilidades de estas herramientas. Solo así podremos aprovechar la promesa de una confianza verificable sin caer en el peligro de un control descontrolado o de una confianza excesiva que, al fin y al cabo, podría ser tan perjudicial como las deepfakes que pretende combatir.

Beth Noveck, en su libro *Reboot*, subraya una realidad que a menudo se pasa por alto: los sistemas de detección de deepfakes son esencialmente una carrera armamentística en la que el atacante puede desactivarlos con recortes mínimos o compresiones de unos pocos kilobytes, y el resultado final es siempre probabilístico, no cierto [10]. Esta vulnerabilidad hace que la confianza exclusiva en detectores sea una ilusión de seguridad; tan pronto como aparece un nuevo algoritmo generador, los modelos de detección se abren a nuevas formas de engaño. La solución, por tanto, no es mejorar indefinidamente la precisión de los detectores, sino cambiar el paradigma: pasar de «detecta si es falso» a «prueba que este contenido existió con un ancla neutral». El anclaje criptográfico en una blockchain —independiente del creador y sin depender de entidades centralizadas— ofrece la prueba inmutable que Noveck considera imprescindible, cerrando el bucle donde los detectores solo pueden jugar al juego del engaño.

Es hora de actuar

Las plataformas digitales son la primera línea de defensa: han de incorporar sistemas que preserven y muestren la procedencia verificada de cada archivo multimedia. Esto significa integrar credenciales de contenido basadas en el modelo C2PA, pero ir más allá de los metadatos que se pueden suprimir; hay que anclar la huella de cada archivo a una cadena de bloques pública o a un registro de tiempo fiable como OpenTimestamps, que ya ha sellado alrededor de **750 millones** de archivos del Internet Archive [6]. Cada vez que un vídeo o una imagen se sube, la plataforma ha de emitir un «certificado de origen» y hacerlo accesible al público, permitiendo a cualquier usuario rastrear el camino completo desde el momento de creación hasta la última modificación.

Los creadores y medios han de adoptar una cultura de publicación con prueba de origen. No es suficiente publicar una noticia; hay que adjuntar la cadena de confianza que demuestre dónde se obtuvo el material, cuándo se creó y qué entidad lo ha firmado digitalmente. Este enfoque sigue la recomendación del NSA/FBI/CISA (2023) de establecer la procedencia como elemento clave para combatir las manipulaciones [4]. Además, utilizando el marco de **t2p** —el anclaje de la huella en la blockchain pública, con el sello RFC 3161 como complemento—, los medios pueden garantizar una prueba inmutable y verificable sin depender exclusivamente de metadatos vulnerables [7].

Las empresas e instituciones han de anclar la huella de sus datos críticos antes de compartirlos. Cualquier informe financiero, estudio clínico o registro educativo ha de estar firmado y sellado en una red descentralizada que ofrezca timestamps fiables. Esto no solo protege contra la sustitución malintencionada de documentos, sino que también cumple con las nuevas obligaciones reguladoras: el EU AI Act (Art. 50) entra en vigor el 2 de agosto de 2026 y exige mecanismos de trazabilidad para el contenido generado por IA [8].

Los reguladores, por su parte, han de definir estándares interoperables que garanticen que todas las partes interesadas puedan verificar la procedencia sin barreras técnicas. Esto implica la adopción de especificaciones comunes como el C2PA, pero también el establecimiento de protocolos de auditoría y certificación para proveedores de servicios de timestamping y blockchain pública. La cooperación internacional será clave para evitar una «barrera de confianza» que frene la innovación y a la vez proteja a los ciudadanos.

Finalmente, la ciudadanía ha de convertirse en el primer filtro: antes de creer o compartir un contenido, hay que verificar su origen a través de herramientas accesibles (extensiones de navegador, apps móviles) que consulten las credenciales emitidas por las plataformas y los medios. Esta práctica, aunque sencilla,

puede reducir drásticamente la propagación de deepfakes, que han pasado de 500.000 casos en 2023 a cerca de 8 millones en 2025 según Sumsub [9].

Ante la mentira industrializada, demostrar la verdad es la acción más poderosa; ahora podemos transformar la prueba de existencia en una defensa duradera. **Time2act** no es solo un lema, sino una llamada a todos los actores del ecosistema digital para que, con procedencia y timestamping, podamos recuperar la confianza y hacer frente a las deepfakes antes de que ellas nos superen.

---

[1] arXiv — *DeepFake-Eval-2024: A Multi-Modal In-the-Wild Benchmark of Deepfakes*. https://arxiv.org/html/2503.02857v4 ↩

[2] ManageEngine Insights — *Content provenance is our best chance in the fight against deepfakes* (Hany Farid). https://insights.manageengine.com/artificial-intelligence/content-provenance-is-our-best-chance-in-the-fight-against-deepfakes/ ↩

[3] WITNESS — *Prepare, Don't Panic: Synthetic Media and Deepfakes* (Sam Gregory). https://www.witness.org/portfolio_page/sam-gregory/ ↩

[4] CISA / NSA / FBI — *Contextualizing Deepfake Threats to Organizations* (2023). https://www.cisa.gov/news-events/alerts/2023/09/12/nsa-fbi-and-cisa-release-cybersecurity-information-sheet-deepfake-threats ↩

[5] C2PA — *Content Credentials Explainer*. https://spec.c2pa.org/specifications/specifications/2.2/explainer/_attachments/Explainer.pdf ↩

[6] Peter Todd — *Carbon Dating the Internet Archive with OpenTimestamps*. https://petertodd.org/2017/carbon-dating-the-internet-archive-with-opentimestamps ↩

[7] ProofStamper — *File timestamp tools compared (RFC 3161 + blockchain anchoring)*. https://proofstamper.com/en/compare/file-timestamp-tools-2026/ ↩

[8] EU AI Act, artículo 50 (transparencia del contenido generado por IA). https://artificialintelligenceact.eu/article/50/ ↩

[9] Sumsub — *Global deepfake incidents surge tenfold*. https://sumsub.com/newsroom/sumsub-research-global-deepfake-incidents-surge-tenfold-from-2022-to-2023/ ↩

[10] Beth Simone Noveck — *Reboot* (Yale UP, 2026), cap. 3. ↩

Dinero y confianza: fraude, compliance y finanzas

«Se dice que la luz del sol es el mejor de los desinfectantes; la luz eléctrica, el policía más eficiente.»

— Louis D. Brandeis, Other People's Money (1914)

A principios de 2020, el gerente de una sucursal en Hong Kong de una empresa japonesa recibió una llamada con una voz que conocía bien: la de un directivo de la casa matriz. El directivo le explicó que la empresa estaba a punto de cerrar una adquisición y que había que autorizar transferencias por valor de **35 millones de dólares**. En la bandeja de entrada había correos del directivo y de un abogado llamado Martin Zelner que confirmaban la operación, y el gerente empezó a hacer las transferencias. Todo era falso: la voz era un clon generado con tecnología de «deep voice». La investigación de los Emiratos Árabes Unidos, revelada por un documento judicial, identificó al menos **17 implicados**, con los fondos repartidos por cuentas de todo el mundo, y rastreó **400.000 dólares** hasta cuentas norteamericanas del Centennial Bank; los EAU acabaron pidiendo ayuda a los investigadores de EE. UU. [8].

Cuatro años más tarde, la estafa había aprendido a hacer videollamadas. En enero de 2024, un empleado financiero de la oficina de Hong Kong de la ingeniería británica **Arup** recibió la instrucción de transferir unos **25,6 millones de dólares**; sospechaba de un correo de *phishing*, pero una videoconferencia con el «director financiero» y varios «colegas» —todos con la cara y la voz exactas— lo tranquilizó, y ejecutó **15 transferencias** a cinco cuentas. Todos los participantes de la llamada, salvo él, eran deepfakes [1]. El capítulo 87 disecciona este caso a fondo; aquí nos ocupa el paisaje entero: el fraude, el cumplimiento normativo y la identidad financiera.

Como concluyó el CIO de Arup tras el incidente: «*Copiar una voz, una imagen o un vídeo está al alcance de cualquiera con poca habilidad técnica.*» Si ver y oír ya no basta para confiar, las finanzas necesitan otra clase de prueba.

Cuando ver ya no es creer

La era digital ha transformado la confianza en una cuestión de verificación constante, y el fenómeno de las deepfakes está acelerando este cambio a una velocidad que supera cualquier predicción anterior. Las cifras aportan una realidad incómoda: Deloitte estima que el fraude generado por inteligencia artificial en Estados Unidos pasaría de 12,3 mil millones de dólares en 2023 a cerca de **40 mil millones** en 2027 [2]. Esta escalada no es solo una proyección económica; es la síntesis de un ecosistema donde las voces y las imágenes de los directivos se vuelven fácilmente manipulables.

En los últimos meses, las empresas han denunciado **voces clonadas de CFO**, **vídeos sintéticos que simulan reuniones del consejo** e **instrucciones «urgentes» enviadas fuera de los canales oficiales**. Cada una de estas estafas se fundamenta en la confianza humana: el reconocimiento facial, la autenticidad vocal y la familiaridad con los gestos corporales eran considerados indiscutiblemente fiables hasta hace poco. Ahora solo hace falta un algoritmo de generación de imagen o una aplicación de síntesis de voz para crear un engaño indistinguible del real.

El impacto más corrosivo no reside en las pérdidas monetarias directas, sino en la **duda sistémica** que se extiende a todo el entorno financiero. Cuando una llamada aparentemente legítima puede ser un deepfake, las organizaciones han de incrementar drásticamente los procesos de verificación, generando más tiempo de espera para confirmar pagos, mayor gasto en tecnologías de autenticación y una carga administrativa que diluye la eficiencia operativa. Esta fricción no solo eleva costes directos; también merma la velocidad de negociación, retrasando inversiones y desincentivando colaboraciones internacionales.

Además, el coste de una verificación errónea se hace evidente en casos como el incidente de Arup en Hong Kong en 2024, donde en una videollamada todos los asistentes —incluido el CFO— eran deepfakes, provocando la transferencia de **25,6 millones de dólares** sin ningún rastro fiable [1]; **como hemos visto**, una sola vulnerabilidad puede desencadenar pérdidas masivas y erosionar la confianza en todo el sistema bancario.

Las autoridades ya han empezado a responder. El **EU AI Act**, con el artículo 50 que obliga al etiquetado de deepfakes a partir del **2 de agosto de 2026** [5], y las directrices del **NIST SP 800-63-4**, que hacen

obligatoria la detección de ataques de inyección en niveles altos para procesos biométricos [4], son pasos esenciales hacia una defensa normativa. No obstante, estas medidas solo mitigan el problema si las instituciones adoptan una arquitectura de confianza que vaya más allá del simple reconocimiento visual o auditivo.

En síntesis, la proliferación de deepfakes transforma cada interacción financiera en un escenario de incertidumbre. El coste oculto —el tiempo y los recursos dedicados a validar la veracidad de cada comunicación— se convierte en una carga estructural que amenaza la fluidez del mercado global. Para preservar la estabilidad del sistema financiero, hace falta una respuesta que restablezca la confianza no solo en las apariencias, sino en el origen verificable e inmutable de cada transacción.

El frente del KYC: ataques de inyección

En una oficina de registro bancario en Nueva York, un operador recibió la solicitud de un nuevo cliente que, a primera vista, parecía completamente legítima: un documento de identidad escaneado y un selfie recientes. El flujo de verificación se interrumpió cuando una capa invisible de software —una cámara virtual inyectada en tiempo real— sustituyó la imagen del dispositivo por una versión generada por IA, produciendo un «selfie» perfectamente alineado con el documento pero que era, en realidad, una deepfake avanzada capaz de superar los algoritmos biométricos más sofisticados.

iProov registra un aumento drástico de ataques de inyección y bypass biométrico contra procesos KYC. Un informe describe cómo una deepfake abrió decenas de cuentas fraudulentas en un banco, explotando la vulnerabilidad del modelo «documento + selfie» [4]. El ataque no solo engaña al reconocimiento facial; manipula toda la cadena de entrada de datos, haciendo que cada paso —captura de la imagen, compresión, transmisión y análisis— se realice sobre una base falsificada. La respuesta técnica emergente parte de una premisa fundamental: la integridad ha de quedar ligada al momento y al punto de captura, no solo al archivo final. La norma NIST SP 800-63-4 ya impone, desde el nivel más alto de aseguramiento, la detección obligatoria de ataques de inyección [4]; por eso los sistemas han de establecer una «captura firmada», un registro criptográfico insertado en el momento en que el sensor físico captura la imagen, de modo que cualquier manipulación posterior —incluida la adición de una capa virtual— se vuelva evidente porque el hash de la captura original ya ha sido archivado en una cadena inmutable.

Esta lógica sustenta la infraestructura de prueba de existencia (t2p) de *time2act*. En lugar de atenerse únicamente al contenido del documento, el sistema genera una huella temporal y verificable que se guarda en un registro distribuido; cada selfie, escaneo o señal biométrica se convierte en una transacción inmutable, de modo que cualquier intento de inyección tendría que reescribir la cadena de bloques y sería detectado de inmediato.

El impacto no se limita a reducir el fraude: responde también a las alertas regulatorias recientes, como el aviso de FinCEN del 13-nov-2024 sobre la necesidad de reforzar los controles CDD ante deepfakes [3] y la obligación del EU AI Act art. 50 de etiquetar este tipo de contenido a partir del 2-ago-2026 [5]. Con una captura segura y un registro verificable, las instituciones financieras pueden cumplir estas exigencias sin tener que añadir ninguna capa operativa onerosa.

En síntesis, la verificación de identidad ha pasado del papel y la pantalla al momento en que se genera la señal. La combinación de detección de inyección obligatoria (NIST) y de pruebas de existencia inmutables (t2p) crea una barrera que, hasta ahora, los defraudadores no han podido superar; el reto es desplegar esta arquitectura a escala global, con la confianza radicada en el origen verificable, no en apariencias engañosas generadas por la IA.

El regulador se mueve

Como hemos visto, el 13 de noviembre de 2024 FinCEN lanzó una alerta que resonaba como un relámpago en las salas de consejos de administración y en los departamentos de compliance de todo el mundo: las deepfakes y la IA generativa se estaban convirtiendo en herramientas preferidas para burlar la verificación de identidad y los controles de diligencia debida (CDD) [3]. El aviso no solo describía una nueva amenaza, sino que exigía un cambio inmediato en la manera en que las instituciones registran e informan las sospechas. FinCEN pidió que los informes de sospecha relacionados incorporaran el término clave «FIN-2024-DEEPFAKEFRAUD», creando así un marcador uniforme para el análisis posterior y la cooperación transfronteriza. Esta petición, aunque aparentemente sencilla, obliga a las entidades financieras a revisar

sus sistemas de detección, a integrar tecnologías de autenticación avanzada y a establecer procesos de auditoría capaces de rastrear el origen real de una imagen o audio.

Como ya se ha indicado, el artículo 50 del EU AI Act estableció que a partir del 2-ago-2026 todas las producciones de contenido generado por IA —incluidas las deepfakes— deberán estar claramente etiquetadas como tal [5]. El etiquetado no es solo una advertencia visual; implica la inserción de metadatos verificables que pueden ser leídos por sistemas automatizados de compliance, y facilita la detección precoz y la elección de acciones correctivas. Esta obligación crea un marco legal que convierte la transparencia en una exigencia normativa, no en una opción empresarial.

Además, el nuevo eIDAS 2.0 ha introducido dos componentes clave: los Qualified Electronic Ledgers (QEL) y el Qualified Electronic Archiving (QEA). Estos registros electrónicos certificados ofrecen una traza de auditoría inmutable que se puede validar a escala reguladora [6]; cada transacción, documento de KYC o informe de sospecha queda registrado en un ledger cualificado y su archivo se mantiene en un entorno de archivo electrónico que garantiza la integridad y la inalterabilidad a lo largo del tiempo. Esta infraestructura permite a las autoridades verificar no solo que una información se ha presentado, sino también que proviene de una fuente auténtica y no ha sido manipulada posteriormente.

El mensaje que emerge es claro: el compliance ya no se puede limitar a «guardar PDF». La mera conservación de documentos escaneados o en formato digital tradicional no ofrece ninguna garantía contra las sofisticadas simulaciones creadas por la IA. El objetivo pasa, como hemos visto en el NIST SP 800-63-4, a demostrar —de manera verificable y auditable— la integridad y el origen de una información desde el momento de su creación, mediante detección de inyección obligatoria, pruebas de existencia inmutables como t2p y los QEL/QEA regulados por eIDAS 2.0, formando una barrera casi infranqueable para los defraudadores.

Esta evolución normativa no solo eleva el nivel de seguridad, sino que crea un ecosistema donde la confianza se basa en el origen verificable y no en apariencias engañosas generadas por algoritmos. Las empresas que adopten estas prácticas avanzadas podrán transformar su modelo de compliance de una tarea administrativa a una defensa proactiva contra las amenazas emergentes, convirtiéndose así en pioneras de un nuevo paradigma de confianza digital.

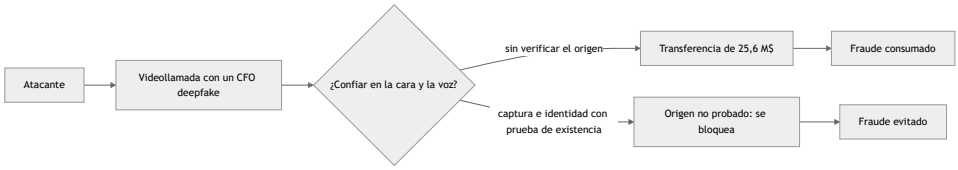


Figura 16.1 — En el fraude por deepfake, la confianza se rompe en la identidad y la instrucción; una prueba de existencia anclada al origen pone un punto de verificación independiente.

Pruebas que se pueden fabricar

En el mundo judicial contemporáneo, la cadena de custodia es el pilar sobre el que se apoyan las pruebas digitales: metadatos que registran cada manipulación, testigos que certifican el origen y documentos que garantizan la integridad. Este modelo, nacido en la era del papel y del formato electrónico, está ahora sometido a una erosión profunda provocada por las deepfakes; cuando un vídeo o una grabación de audio se genera íntegramente con IA, el simple hecho de presentar metadatos ya no es suficiente y la confianza en la autenticidad se desmorona ante un ataque capaz de reproducir con precisión cualquier voz o cara conocida.

En Hong Kong, como hemos visto, una operación fraudulenta de 2024 sustituyó a un «CFO» y varios ejecutivos por avatares generados por IA en una videollamada que autorizó la transferencia de una suma importante hacia cuentas externas. La transacción se validó porque los participantes creían estar ante identidades reales, mientras que todos eran deepfakes [1]. Este caso ilustra cómo la falsificación no solo afecta a las finanzas sino también al proceso judicial: si una prueba audiovisual puede ser engañosa, cualquier juicio basado en ella se vuelve vulnerable.

En Estados Unidos, la respuesta legislativa avanza hacia un marco más riguroso. Las **Federal Rules of Evidence 707 (FRE 707)** —de nueva incorporación— introducen criterios específicos para las pruebas generadas por máquina, exigiendo que se demuestre su fiabilidad y la imposibilidad de manipulaciones posteriores [7]. Paralelamente, la propuesta de regla **901(c)** busca establecer un estándar para las

evidencias electrónicas potencialmente fabricadas o alteradas, obligando a los abogados a presentar una prueba de origen verificable antes de que el juez pueda aceptarlas como válidas [7].

Estas nuevas disposiciones convierten la prueba de existencia —un hash criptográfico anclado con sello de tiempo— en un requisito esencial para cualquier documento o imagen que se pretenda presentar ante el tribunal. Un hash, generado en el momento de la creación y registrado en una cadena de bloques pública, ofrece una huella digital inmutable: ninguna alteración posterior puede modificarlo sin ser detectada. Así, la auditoría de e-discovery pasa a depender no solo de la recopilación de archivos, sino también de la certificación de que esos archivos existieron en un instante determinado y de que su contenido no ha variado desde entonces.

El impacto se ve reforzado por las regulaciones emergentes; el EU AI Act obliga a etiquetar cualquier contenido generado por IA como «deepfake» a partir del 2 de agosto de 2026 [5], y el marco eIDAS 2.0 introduce los Qualified Electronic Ledgers y el Archivo cualificado, que garantizan una auditoría a prueba de manipulación para documentos electrónicos críticos [6].

Como hemos visto, la combinación de una normativa más estricta (FRE 707, regla 901(c)) y del estándar técnico NIST SP 800-63-4, que exige detección de ataques de inyección en niveles altos [4], junto con soluciones basadas en blockchain para la prueba de existencia, crea una nueva infraestructura de compliance. Esta no solo protege las finanzas sino también la integridad del sistema judicial, convirtiendo el proceso de verificación de una tarea reactiva en una defensa proactiva contra la fabricación de pruebas; la clave es que cada documento, imagen o audio pueda ser rastreado hasta su origen y corroborado con un sello de tiempo inalterable.

La prueba de existencia como infraestructura de compliance

Cuando una organización decide que la confianza ha de empezar **en el origen**, el primer paso es capturar cada dato de identidad con una firma digital inmutable y verificable en tiempo real. En el proceso de incorporación, el KYC se captura desde el dispositivo del usuario mediante un certificado de clave pública que genera un hash del documento presentado (pasaporte, carné o selfie biométrico). Este hash, llamado *proof of capture*, se firma al instante con una clave privada custodiada en el Secure Enclave y queda ligado a un sello de tiempo conforme a la normativa RFC 3161; el resultado se publica en una cadena de bloques pública que garantiza **resistencia al ataque de inyección** descrito por iProov y exigido por el NIST SP 800-63-4 [4]. Así, cualquier intento de sustituir la imagen biométrica con una cámara virtual queda detectado: el hash almacenado en la cadena no coincide con ninguna otra versión del archivo.

Una vez registrada la captura, se genera una **traza de auditoría inmutable** que combina el hash original, el sello de tiempo y el anclaje en blockchain. Este registro es accesible para auditores y reguladores sin exponer el contenido sensible, ya que solo se comparten las pruebas criptográficas (hash y firmas). Cuando una entidad ha de demostrar la veracidad de un documento ante un tribunal, puede presentar este conjunto de metadatos como **evidencia de procedencia**. Los tribunales norteamericanos, por ejemplo, ya disponen de reglas como la FRE 901/902 que exigen una cadena de custodia fiable; el *proof of existence* ofrece exactamente eso: un enlace verificable entre el documento original y el registro inmutable, rechazando el argumento «es una deepfake» que ha alimentado casos como el fraude de **25,6 millones** de dólares en Hong Kong, donde todos los asistentes eran avatares generados por IA [1].

Además, la prueba de existencia garantiza **integridad y fecha cierta** para documentos reguladores y contratos. Cada versión del documento se registra con su hash y sello de tiempo; cualquier modificación posterior genera un nuevo registro que deja constancia clara del cambio. Esto se alinea perfectamente con los requisitos de los Qualified Electronic Ledgers y del Qualified Electronic Archiving introducidos por eIDAS 2.0, que exigen una auditoría a prueba de manipulación para transacciones electrónicas de gran valor [6]. La solución, por tanto, no solo cumple la normativa europea, sino que la **potencia**, ya que ofrece una capa de verificación descentralizada que las autoridades nacionales pueden consultar sin depender de un único proveedor.

Hay que subrayar que este mecanismo **no sustituye** los controles tradicionales como el «cuatro ojos» o las comunicaciones fuera de banda; en cambio, actúa como **capa complementaria** que refuerza cada paso del proceso. El archivo nunca abandona el dispositivo: la información sensible queda localizada y protegida por el cifrado del sistema operativo, mientras que solo las pruebas criptográficas se transmiten a la red. De este modo, se mantiene la **privacidad** del individuo sin sacrificar la verificabilidad.

Según Deloitte, como hemos visto, estas cifras son alarmantes [2]; la prueba de existencia convierte la confianza en una infraestructura tangible: captura firmada y sellada en el origen, trazas inmutables que soportan litigios y auditorías, integridad certificada por eIDAS 2.0 y una arquitectura de privacidad-first. La decisión es clara: integrar *t2p* ahora mismo, o afrontar un futuro donde la confianza se disuelve en cada nueva manipulación digital.

La promesa y el peligro

Imagina una sala de reuniones en Hong Kong donde, con la misma fluidez de una videollamada normal, se firman transferencias que totalizan 25,6 millones de dólares. El «CFO» que presenta los documentos es un deepfake tan convincente que nadie sospecha de su origen digital. La operación, descrita por Arup, muestra cómo la confianza en una identidad visual puede ser explotada y transformarse en fraude ejecutivo a escala global [1].

Esta escena muestra la promesa central de *t2p*: una capa de integridad que vincula cada instrucción financiera a su origen verificable, independientemente del formato visual o sonoro. Con pruebas de existencia registradas en ledgers cualificados —conforme a eIDAS 2.0— se puede demostrar con una sola consulta criptográfica que el documento no ha sido alterado desde el momento de su creación y que el emisor es quien afirma ser [6]. El resultado es un onboarding más fiable, donde las entidades pueden validar KYC en minutos en lugar de horas o días, reduciendo drásticamente los costes operativos y eliminando el margen de error humano. Las auditorías se convierten en procesos de verificación instantánea: una cadena de custodia inmutable que puede ser presentada ante los tribunales como prueba admisible, superando las limitaciones de la regla tradicional FRE 707 y la propuesta 901(c) [7].

No obstante, el peligro reside en la ilusión de que una capa tecnológica pueda sustituir por completo los controles internos y el juicio humano. El NIST SP 800-63-4 aboga por la detección obligatoria de ataques de inyección en niveles altos, reconociendo que las cámaras virtuales pueden engañar a sistemas biométricos si no se protegen adecuadamente [4]. Los atacantes ya experimentan con «inyecciones» de datos falsos y bypass biométrico para eludir los procesos de verificación del KYC, como demuestra el informe de iProov sobre vulnerabilidades emergentes [4]. Como hemos visto, el aumento exponencial del fraude generado por IA —según Deloitte, pasando de 12,3 mil millones en 2023 a cerca de 40 mil millones en 2027— no se resuelve solo con una prueba de existencia; la tecnología crea nuevos vectores de ataque que requieren supervisión constante y políticas de gobernanza robustas [2].

Además, una implementación mal diseñada puede comprometer la privacidad de los clientes. El almacenamiento de metadatos detallados en ledgers cualificados implica una exposición potencial si las claves de cifrado son gestionadas inadecuadamente o si se comparte información sensible sin los mecanismos de consentimiento exigidos por el EU AI Act; como hemos visto, esta norma obliga a etiquetar e informar sobre deepfakes en contextos comerciales [5]. Por tanto, la solución no es solo tecnológica, sino también legal y ética: hay que establecer protocolos claros para el tratamiento de datos personales y garantizar que las pruebas de existencia sean «zero-knowledge» cuando sea necesario.

La prueba de existencia representa una capa esencial dentro de una arquitectura más amplia de confianza. No es una bala de plata que elimine todos los riesgos, sino un mecanismo que reduce drásticamente el fraude y restaura la credibilidad del comercio financiero. Su efectividad depende de cómo se combina con controles internos rigurosos, supervisión reguladora y prácticas de privacidad responsables; solo así podremos equilibrar la promesa de un ecosistema financiero más seguro con el peligro de una confianza excesiva en una sola solución tecnológica.

Es hora de actuar

Los bancos y las fintech son el primer escudo ante la tormenta de deepfakes que ya ha demostrado su potencial destructivo; el caso Arup, donde unos **25,6 millones de dólares** fueron transferidos a través de una videollamada poblada exclusivamente por avatares generados por IA, es una advertencia clara de que la confianza en las identidades y las instrucciones ya no se puede asumir como segura [1] —como hemos visto—. Para cortar esta vulnerabilidad hace falta **anclar el KYC** y todas sus trazas de auditoría dentro de un marco verificable fuera de banda, especialmente para órdenes de pago superiores a unos pocos miles de dólares. Esto implica integrar soluciones basadas en **Qualified Electronic Ledgers** y **Qualified Electronic Archiving**, tal como prevé eIDAS 2.0, que garantizan una cadena inmutable donde cada paso del proceso de conocimiento del cliente queda registrado con sellos criptográficos

verificables [6]; así, incluso si un actor malicioso intenta engañar al sistema con una imagen biométrica falsificada, el registro descentralizado revelará la incongruencia entre el origen declarado y los datos almacenados.

Las empresas que manejan contratos y documentos sensibles han de **sellar digitalmente estos activos antes de compartirlos**, utilizando pruebas de existencia (t2p) basadas en blockchain. Un sello criptográfico no solo certifica el estado del documento en el momento de la firma, sino que también proporciona una prueba verificable e inmutable que puede ser consultada por cualquier parte interesada sin necesidad de confiar ciegamente en el emisor original. Esta práctica se vuelve especialmente crucial a medida que los tribunales empiezan a abordar las pruebas potencialmente fabricadas a través de la regla 901(c) y el FRE 707, donde la cadena de custodia tradicional ya está cuestionada [7].

Los auditores y abogados han de convertirse en **defensores de las pruebas de existencia** en su práctica profesional. No basta con comprobar que un documento exista; hay que exigir que su integridad esté vinculada a una prueba verificable independiente, almacenada en un registro electrónico cualificado. Esto implica auditar tanto el contenido como los metadatos de creación y las firmas digitales, asegurándose de que cualquier intento de inyección o bypass biométrico —tal como describe NIST SP 800-63-4— sea detectado en tiempo real [4].

Los reguladores han de liderar la definición de **estándares interoperables y reconocimiento legal del sello criptográfico**, estableciendo marcos que obliguen a las instituciones financieras a adoptar soluciones basadas en blockchain como parte integral de su programa de compliance. La aplicación del EU AI Act (art. 50) el 2 de agosto, **como hemos visto**, es un paso crucial hacia la regulación de estos riesgos emergentes [5]; pero hay que ir más allá, reconociendo legalmente las pruebas de existencia como evidencia admisible y estableciendo requisitos de **verificación fuera de banda** para transacciones de gran magnitud.

En resumen, la confianza es el activo fundamental del sistema financiero; demostrarla no es un lujo sino una necesidad urgente. Cada banco, fintech, empresa, auditor, abogado y regulador tiene un papel concreto y complementario en este ecosistema: capturar, sellar, verificar y reconocer las pruebas de existencia como piedra angular de la credibilidad. **Demostrar la confianza es time2act** — el momento de poner en práctica estas medidas es ahora, antes de que los deepfakes de nueva generación se conviertan en la norma y no en la excepción.

---

[1] CNN Business — *Finance worker pays out $25 million after video call with deepfake 'CFO'* (caso Arup). https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk · World Economic Forum. https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/ ↩

[2] Deloitte — *Generative AI is expected to magnify the risk of deepfakes and other fraud in banking* (≈40 mil M$ en 2027). https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html ↩

[3] FinCEN — *Alert on Fraud Schemes Involving Deepfake Media* (13-nov-2024). https://www.fincen.gov/system/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf ↩

[4] iProov / Biometric Update — *Biometric injection attack surge* (KYC, NIST SP 800-63-4). https://www.biometricupdate.com/202604/biometric-injection-attack-surge-spreads-to-ios-iproov-report ↩

[5] EU AI Act, artículo 50 (etiquetado de deepfakes; aplica 2-ago-2026). https://artificialintelligenceact.eu/article/50/ ↩

[6] Signaturit — *eIDAS 2.0: Qualified Electronic Ledgers and Archiving*. https://www.signaturit.com/blog/eidas-2-regulation/ ↩

[7] Thomson Reuters Institute — *Deepfakes on trial: evidence authentication (FRE 707, 901(c))*. https://www.thomsonreuters.com/en-us/posts/ai-in-courts/deepfakes-evidence-authentication/ ↩

[8] Forbes (Thomas Brewster) — *Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find* (14-10-2021; documentos judiciales de los EAU: al menos 17 implicados, 400.000 $ rastreados hasta cuentas del Centennial Bank en EE. UU.). https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/ ↩

La imagen como testimonio: fotoperiodismo y medios

«Una fotografía pasa por prueba incontrovertible de que algo determinado sucedió.»

— Susan Sontag, Sobre la fotografía (1977)

Era la mañana del 22 de mayo de 2023 cuando un silbido digital atravesó las redes sociales como una explosión invisible. Una cuenta marcada como «verificada», que se hacía pasar por un conocido medio de noticias, compartía una fotografía: una columna de fuego y humo se alzaba violentamente a la sombra del Pentágono. La imagen se difundió en cuestión de segundos; los algoritmos la impulsaron hacia los timelines de miles de usuarios y, durante unos minutos, llegó a mover brevemente los mercados financieros norteamericanos antes de que nadie pudiera confirmar nada.

Los comentarios se multiplicaban como fuegos artificiales: «¡Bombardeo en el Pentágono!», «¡Atentado terrorista!» y, entre las críticas, la pregunta clave que aún resuena hoy: **¿de dónde procede esta imagen?** La respuesta, en aquel instante, era un vacío. Nadie podía rastrear el origen del archivo. La cuenta «verificada» se suprimió poco después de la primera oleada de alertas, dejando solo la imagen viral y una serie de rumores que corrían más rápido que la verdad.

En medio del caos, Hany Farid, pionero en análisis forense digital, examinó la fotografía y concluyó que, con toda probabilidad, había sido generada por inteligencia artificial. La imagen mostraba las inconsistencias propias de los modelos generativos y, sobre todo, no había podido asociarse a ninguna fuente ni a ninguna cámara conocida [1].

Mientras los analistas financieros recalculaban y los reguladores de mercado valoraban el impacto de la desinformación visual, el mundo periodístico se encontraba ante un escenario que había parecido imposible hacía solo dos décadas: una sola imagen, sin ningún rastro verificable, podía desencadenar movimientos de bolsa y cambiar la percepción pública en cuestión de minutos. La incertidumbre sobre el origen de aquella fotografía no era solo un problema técnico; era una amenaza directa a la credibilidad del periodismo y al debate democrático.

Así, aquella breve explosión digital se convirtió en el primer testimonio de una nueva era: una donde la **verificabilidad** —el poder de demostrar de dónde procede cada imagen— se convierte en el único escudo capaz de proteger a la sociedad del caos que puede engendrar un simple píxel. La necesidad de firmar el contenido en el origen, y de anclarlo en una prueba de existencia inmutable, ya no era solo una propuesta técnica; era una urgencia para la supervivencia del discurso público.

La imagen ya no es prueba

Durante más de un siglo, la fotografía ha gozado de un aura de verdad incontestable: el blanco y negro del frente de una guerra, la sonrisa de una familia que se convierte en icono histórico o el fuego de una explosión que captura el instante decisivo de un conflicto. Aquel «momento congelado» era considerado un testimonio fiable porque la tecnología de la época exigía una cadena física y visible —película, laboratorio, impresión— que hacía casi imposible manipularla sin dejar huella. La confianza en la imagen se construía sobre la presunción de que su origen era evidente e inmutable.

Hoy esta premisa se ha deshecho. Las redes neuronales generativas, alimentadas por modelos entrenados con miles de millones de imágenes, son capaces de crear fotogramas indistinguibles de los originales en cuestión de segundos. Como hemos visto en mayo de 2023, la falsa imagen de la «explosión del Pentágono», una composición generada por IA y difundida por una cuenta que se autoproclamaba medio de noticias, provocó una breve pero significativa oscilación de los mercados financieros. El análisis de Hany Farid demostró cómo la manipulación digital puede engañar incluso a los observadores más experimentados [1].

Sin embargo, el peligro no reside únicamente en las deepfakes «puras». En las elecciones de 2024, los medios observaron que las «cheap fakes» —vídeos o fotos reales sacados de su contexto original o retocados con herramientas básicas— superaron a las deepfakes de IA en una proporción aproximada de siete a uno [2]. Estas manipulaciones, aunque no son totalmente sintéticas, eran igualmente devastadoras porque su credibilidad dependía del conocimiento de su origen y del momento de captura. Un clip de un

discurso político reeditado para añadir una frase comprometedora o una fotografía de una manifestación desplazada temporalmente puede generar el mismo impacto que un avatar digital perfectamente recreado.

Esto revela la verdad fundamental: el problema central no es tanto crear imágenes falsas, sino la **procedencia** y el **contexto**. Quién tomó una foto, en qué momento exacto, con qué configuración técnica y si ha sido alterada posteriormente constituyen el único criterio para evaluar su veracidad; sin esta información, cualquier píxel se convierte en un dato potencialmente engañoso.

Las soluciones del campo de la verificabilidad —las credenciales de contenido (C2PA) y las pruebas de existencia inmutables— apuntan precisamente a este vacío. La firma digital en el momento de captura, ya implementada en cámaras como la Leica M11-P o el prototipo Nikon que validó la certificación C2PA en febrero de 2025 [6][4], garantiza una cadena de autenticidad desde el primer instante. No obstante, los metadatos asociados a estas credenciales pueden ser eliminados o alterados por plataformas sociales y procesos de recodificación, dejando la imagen sin rastro verificable [7].

El anclaje en una prueba de existencia basada en blockchain ofrece una capa adicional de seguridad: un hash inmutable registrado en la cadena asegura que, aunque los metadatos desaparezcan, el testimonio digital persista y pueda ser verificado por cualquier actor. Esta doble defensa —firma en el origen y anclaje inmutable— constituye el único escudo viable contra una era donde el píxel se convierte en instrumento de confusión tanto como de información.

Credenciales de contenido: firmar en el origen

En un momento en que la veracidad visual se ha convertido en un bien escaso, la respuesta de la industria ha sido construir una infraestructura que restablezca la confianza desde el primer clic del obturador. El proyecto C2PA (Coalition for Content Provenance and Authenticity) y su iniciativa Content Credentials ofrecen un marco criptográfico para registrar el origen y todo el historial de ediciones de una imagen, de modo que cada paso —desde la captura inicial hasta las modificaciones posteriores— queda documentado en un manifiesto firmado. Esta propuesta no solo aporta transparencia; crea una pista de auditoría verificable para cualquier actor, desde el periodista hasta el lector final.

Como hemos visto, la Content Authenticity Initiative (CAI) ha superado los 5.000 miembros en 2025, entre grandes plataformas digitales, agencias de noticias y fabricantes de hardware [3]. Esta masa crítica refleja una conciencia compartida: la prueba de autenticidad ya no puede ser un lujo reservado a las organizaciones mejor dotadas, sino una infraestructura básica para todo el flujo informativo.

El salto cualitativo hacia el hardware ha sido decisivo. La **Leica M11-P** se lanzó como la primera cámara que incorpora Content Credentials directamente en un chip seguro, capaz de firmar cada fotografía en el momento exacto de la captura. Esta firma criptográfica queda incrustada en los metadatos del archivo, asegurando que cualquier intento posterior de manipulación se detecte. La innovación no se ha quedado solo en la gama premium; Nikon, Canon, Sony, Samsung e incluso Google Pixel han seguido el paso, integrando chips similares en sus líneas más recientes [6]. El resultado es un ecosistema donde la confianza visual se convierte en una característica de producto tanto como la resolución o la velocidad de obturación.

A escala editorial, el impacto ha sido notable. La AFP y Nikon validaron en febrero de 2025 un prototipo de cámara que **firma las fotos con C2PA en el momento de disparar**, garantizando una cadena de autenticidad desde su origen [4]. Como hemos visto, France Télévisions adoptó la firma C2PA para sus informativos diarios a finales de 2025, y el IBC Accelerator «Stamping Your Content» —que reúne a BBC, EBU y Associated Press— ha creado herramientas abiertas para que las redacciones puedan firmar y verificar credenciales de contenido sin fricción técnica [5].

Esta convergencia entre hardware, protocolos abiertos y flujos editoriales constituye la respuesta integral que la industria necesita para contrarrestar la era de las «cheap fakes». No es solo una capa adicional de seguridad; transforma el ciclo de vida de la imagen, con prueba de autenticidad en cada paso desde la captura hasta la difusión. Sin embargo, como subraya el marco de C2PA, los metadatos pueden ser eliminados o alterados durante procesos de recompresión y compartición en redes sociales; por eso el anclaje de esta información en una blockchain pública se vuelve imprescindible para garantizar que la prueba de existencia sobreviva a cualquier intento de supresión [7].

En síntesis, la combinación de credenciales C2PA con pruebas de existencia inmutables representa el camino hacia una nueva confianza visual. La industria ha demostrado que es posible crear un ecosistema

donde la veracidad no sea una opción, sino una garantía incorporada al producto y al flujo editorial, clave para preservar un debate público fundamentado en hechos verificables y para hacer frente a las amenazas emergentes de la IA generativa.

El agujero: los metadatos se borran

Cuando una fotografía sale de su entorno original —la cámara, el laboratorio de redacción o la aplicación que la captura— entra en un ecosistema digital dominado por redes sociales y servicios de almacenamiento. En este viaje, los metadatos que llevan la firma C2PA se encuentran a menudo con una barrera invisible: el proceso de subida y recodificación. Las plataformas como Instagram, TikTok o WhatsApp reprocesan cada imagen para optimizar su tamaño y el ancho de banda; este reprocesamiento elimina las capas de información que no son esenciales para la visualización, incluidas las credenciales de autenticidad.

Esta práctica es más que un inconveniente técnico; es una vulnerabilidad estructural. Una imagen que ha sido compartida en una conversación de grupo o publicada en un hilo de una red social puede perder por completo su «Content Credential» sin ningún aviso al creador ni al espectador. La desaparición de la firma no implica, por fuerza, que la foto sea falsa —una fotografía sin credencial puede ser totalmente genuina— pero también impide que cualquier verificación posterior pueda confirmar su quién y su cuándo original. En otras palabras, la ausencia de un metadato deja un vacío interpretativo: el lector se encuentra ante un testimonio visual desprovisto de su cadena de custodia.

Las críticas académicas han subrayado este punto, señalando que la especificación C2PA, por sí sola, no ofrece una robustez suficiente contra la pérdida de los metadatos en el flujo digital contemporáneo [7]. Esto quiere decir que el «quién y cuándo» —los elementos fundamentales del testimonio visual— pueden desvanecerse exactamente en el momento en que más se necesitan: durante una crisis informativa, una investigación periodística o un debate público.

Este agujero no es solo técnico; tiene repercusiones sociales y políticas. En la era de las «cheap fakes», donde los vídeos mal contextualizados superaron por unas siete veces a las deepfakes de IA en impacto [2], la capacidad de demostrar que una imagen procede de una fuente fiable se convierte en un activo crítico. Si las credenciales desaparecen, el debate puede desviarse hacia la sospecha y el escepticismo, alimentando la polarización que los autores del libro quieren contrarrestar.

Por eso, la solución no consiste en rechazar C2PA, sino en reconocer su límite y complementarlo con una capa de prueba de existencia inmutable. Un ancla basada en blockchain puede registrar el hash de la imagen y sus credenciales en el momento de la captura, asegurando que, aunque los metadatos sean borrados durante la distribución, el registro permanente persiste y es verificable por cualquier actor del ecosistema. Esta doble protección —la firma C2PA para la autenticidad inmediata y la prueba de existencia para la persistencia a largo plazo— constituye una defensa robusta contra las manipulaciones de la IA generativa y garantiza que el testimonio visual **siga siendo** fiable, incluso cuando el camino digital se vuelva incierto.

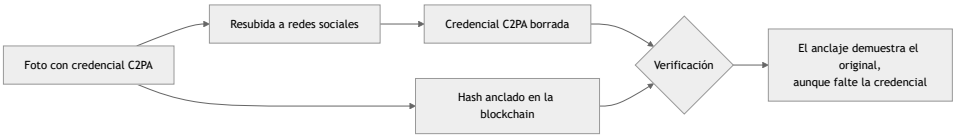


Figura 17.1 — Cuando una imagen se resube, los metadatos C2PA pueden desaparecer; el hash anclado a la cadena pública sigue demostrando que el original existía, inalterado.

El ancla que sobrevive

En un mundo donde la confianza visual se ha convertido en una mercancía escasa, el modelo de **t2p** ofrece la respuesta que el periodismo necesita para preservar la verdad de una imagen desde el momento en que se captura. La clave no es solo firmarla con las credenciales C2PA —una capa de autenticidad inmediata que ya ha movilizado a más de 5.000 miembros globales y se ha adoptado por entidades como France Télévisions y el IBC Accelerator— sino anclar su hash a una cadena pública inmutable. Esta doble protección garantiza que, aunque los metadatos sean borrados o alterados en la fase de distribución (como advierten los estudios sobre la vulnerabilidad de los metadatos de C2PA [7]), el elemento fundamental de

la prueba —el hash— persista y pueda ser verificado por cualquier actor del ecosistema sin necesidad de intermediarios.

En la AFP, el flujo editorial incorpora una marca de agua cifrada que enlaza directamente la foto publicada con el archivo original guardado en sus infraestructuras seguras [4]. Esta práctica ilustra cómo la combinación de **firma C2PA** y **ancla de prueba de existencia** transforma una simple captura en un testimonio verificable desde el primer instante. Cuando el periodista, en el campo o en el estudio, dispara con una Leica M11-P —la primera cámara que incorpora Content Credentials en su chip seguro— la imagen sale del visor ya firmada y, simultáneamente, su hash se puede enviar a una blockchain pública donde recibe un sello de tiempo inmutable. En ese momento se crea una versión «publicar con prueba», consultable por editores, plataformas sociales o auditores en cualquier momento.

Esta arquitectura resuelve el doble problema expuesto por los cheap fakes durante las elecciones —donde los vídeos mal contextualizados superaron a las deepfakes de IA por una ratio aproximada de 7:1 [2]— garantizando que la procedencia y la integridad temporal sean inalterables. Frente a incidentes como la falsa imagen de la «explosión del Pentágono» generada por IA en mayo —que provocó una breve sacudida de los mercados hasta ser desmontada por Hany Farid [1]—, el periodismo dispone ahora de una herramienta capaz de demostrar que la imagen no solo es auténtica en el momento de la captura, sino que ha sido inmutablemente registrada y puede ser rastreada hasta su origen.

Las recomendaciones conjuntas de la NSA y la CISA a principios de 2025 para el uso de Content Credentials [8] refuerzan la idea de que la seguridad visual es una cuestión de interés nacional, donde la prueba de existencia actúa como un código de confianza universal. Cualquier medio —desde grandes cadenas de televisión hasta blogs independientes— puede adoptar este marco sin inversiones masivas: solo hay que integrar el cliente t2p, que genera y registra los hash.

Así, la combinación de C2PA y t2p crea una doble barrera —una capa de autenticidad inmediata y un ancla inmutable a largo plazo— que protege las imágenes contra la erosión de confianza provocada por la IA generativa, restableciendo el papel del fotoperiodismo como testimonio fiable y ofreciendo a los periodistas una herramienta práctica para publicar con prueba.

Las instituciones se alinean

Cuando a principios de 2025 la National Security Agency (NSA) y la Cybersecurity and Infrastructure Security Agency (CISA) publicaron sus directrices que recomiendan el uso de las Content Credentials —el marco operativo de la iniciativa C2PA—, se produjo una verdadera convergencia entre seguridad nacional y periodismo. En un documento conjunto, «Strengthening Multimedia Integrity in the Generative AI Era», las agencias advertían que la integridad de los medios es una defensa crítica contra las manipulaciones basadas en IA y recomendaban adoptar la firma criptográfica en el momento de la captura o publicación de imágenes y vídeos [8]. Esta recomendación, aunque inicialmente dirigida a entidades federales, ha generado un efecto cascada: las grandes redes de noticias, los portales de streaming e incluso las redes sociales han empezado a integrar el protocolo C2PA como requisito mínimo para el contenido visual.

A la misma escala, el consorcio JPEG Trust, responsable del estándar ISO/IEC 21617-1, ha ampliado su alcance extendiendo el motor de la C2PA dentro de la especificación JPEG. Esto significa que cualquier archivo JPEG generado a partir de una cámara compatible puede contener, por defecto, una firma digital verificable y un registro de metadatos autenticados [8]. El paso de un «add-on» opcional a un componente integral del formato más utilizado del mundo consolida la credibilidad de las Content Credentials y eleva su estatus a estándar internacional. Ahora, la simple acción de crear una imagen con una cámara moderna como la Leica M11-P o los modelos Nikon, Canon y Sony que ya integran chips seguros produce automáticamente un certificado C2PA incrustado en el archivo [6].

Esta evolución normativa coincide con la entrada en vigor del EU AI Act, que impone una obligación de etiquetado para todo contenido generado o modificado por IA. El artículo 50 del reglamento exige que las plataformas y los proveedores marquen claramente si un material visual ha sido creado o manipulado por algoritmos. En este contexto, la prueba de credenciales C2PA se convierte en una respuesta directa a la obligación legal: el metadato firmado en el momento de la captura actúa como «etiqueta de confianza» y ayuda a cumplir el requisito de transparencia del AI Act. Así, el paso de buena práctica —usar C2PA para aumentar la credibilidad— se transforma en una expectativa reguladora.

Los efectos pragmáticos de este alineamiento son inmediatos. Las empresas de medios que ya han adoptado las credenciales, como hemos visto con France Télévisions en 2025 [5] o la AFP con su prototipo Nikon de certificación C2PA [4], apuestan por reducir los incidentes de difusión de imágenes falsificadas. Además, la integración directa en el estándar JPEG permite que las pequeñas publicaciones y los creadores independientes generen contenido verificable sin necesidad de inversiones tecnológicas masivas. El apoyo institucional —desde las agencias de seguridad norteamericanas hasta los organismos de normalización internacionales— convierte la firma digital en una infraestructura fundamental del paisaje mediático, estableciendo un nuevo paradigma donde la procedencia verificable es tanto una práctica recomendada como una exigencia legal.

La promesa y el peligro

En un mundo donde una fotografía ha sido durante cien años la prueba más directa de un acontecimiento —un testimonio visual que habla sin necesidad de traducción— la irrupción de la inteligencia artificial generativa está reescribiendo las reglas del juego. La promesa es clara: con los **Content Credentials** (C2PA) y un ancla inmutable en la blockchain, cada imagen puede llevar una firma digital que verifica quién la ha capturado, en qué momento y bajo qué condiciones. Esto restauraría la confianza en el periodismo visual, diferenciaría el contenido verificable del ruido manipulativo y permitiría a los fotógrafos demostrar inequívocamente su autoría y la autenticidad de sus coberturas.

Los primeros pasos ya muestran el potencial. En febrero de 2025, **la AFP** y **Nikon** presentaron una cámara prototipo que firma automáticamente cada captura con C2PA, grabando la información de procedencia en el momento mismo de la apertura del obturador [4]. Desde entonces, marcas como **Leica** (con la M11-P), **Canon**, **Sony** e incluso **Google Pixel** han integrado chips seguros que almacenan las credenciales en el hardware [6]; instituciones clave —desde la **NSA** y la **CISA** hasta el consorcio de normalización **JPEG Trust**— recomiendan el uso de estas firmas como práctica estándar desde enero de 2025 [8]. En este escenario, la imagen se convierte en un documento tan fiable como una transacción bancaria.

Sin embargo, el peligro que se esconde detrás de esta apariencia de seguridad es real y complejo. La misma información que garantiza la autenticidad puede revelar datos sensibles: coordenadas GPS, metadatos de identidad o incluso indicios sobre la fuente de una cobertura periodística. En zonas de conflicto, este rastro puede ser una pista suficiente para que las fuerzas represivas localicen y silencien a fotógrafos y activistas. El caso de la falsa «explosión del Pentágono» de mayo de 2023, analizado por **Hany Farid**, muestra cómo una simple imagen generada por IA, difundida por una cuenta que se hacía pasar por un medio, afectó brevemente a los mercados financieros, subrayando la fragilidad de un ecosistema donde la procedencia es el único filtro fiable [1].

Además, el riesgo de crear una **bifurcación del periodismo** —un mundo dividido entre contenido verificado y no verificado— puede marginar voces legítimas que no disponen de herramientas avanzadas para firmar sus imágenes. Las «cheap fakes», que superaron a las deepfakes en una proporción de 7:1 durante las elecciones de **2024**, demuestran que el problema central es la **procedencia y el contexto**, no solo la calidad visual del falseamiento [2]. Si se confía exclusivamente en el sello digital sin ningún mecanismo de auditoría independiente, se corre el peligro de una **excesiva confianza** en un certificado que puede ser eliminado o alterado; los metadatos de C2PA son vulnerables a la supresión en plataformas sociales y procesos de recodificación [7].

Para preservar la promesa sin caer en el peligro, hay que diseñar sistemas de privacidad que permitan **divulgación selectiva**. Los fotógrafos deberían tener control total sobre qué metadatos se revelan y cuándo, mediante protocolos de cifrado que separen la información sensible (como el GPS) del certificado de autenticidad. Las organizaciones mediáticas podrían establecer **políticas de anclaje** donde la prueba de existencia en la blockchain garantice la permanencia del acto, mientras los metadatos privados se mantienen en entornos protegidos y solo se liberan bajo consentimiento explícito.

En resumen, la tecnología ofrece una vía para volver a confiar en la imagen como testimonio, pero esta confianza ha de estar equilibrada con medidas rigurosas de protección de datos y un marco ético que evite la creación de un periodismo de dos velocidades. Solo así podremos garantizar que las fotos sigan siendo una voz poderosa para la verdad, sin poner en riesgo las vidas que las crean.

Esta arquitectura de anclaje no solo refuerza los medios profesionales; crea un espacio donde el periodismo ciudadano puede convertirse en testimonio legal. En Taiwán, la exministra digital **Audrey Tang** convocó a la población a grabar el propio colegio electoral, ofreciendo una cadena de vídeo que, una

vez anclada a la blockchain, podía ser contrastada al instante contra las teorías conspirativas que circulaban en redes sociales [9]. El mismo mecanismo ha encontrado un ecosistema emergente en Perú: **Voto Libre** utiliza IA para clasificar la evidencia fotográfica de fraude electoral y la registra como prueba inmutable, garantizando un reportaje «seguro, transparente y en tiempo real» que se puede auditar sin depender de intermediarios [10]. En ambos casos, una imagen anclada trasciende el simple documento visual: se convierte en una evidencia verificable de lo que realmente ha sucedido, ampliando la confianza no solo a las grandes redacciones sino también a la voz directa de la ciudadanía.

Es hora de actuar

Los medios son el primer escenario donde la ruptura de la confianza visual se hace palpable. Cada día que una redacción publica una foto sin un certificado verificable, deja abierta la puerta al engaño: el caso de la falsa «explosión del Pentágono» de mayo de 2023, generada por IA y difundida como noticia real, provocó una breve pero significativa oscilación de los mercados antes de ser desmentida por Hany Farid [1]. Como hemos visto, el primer compromiso que hay que asumir es **adoptar la captura firmada**: las nuevas cámaras Leica M11-P, Nikon, Canon y otras ya integran chips de seguridad capaces de estampar un Content Credential en el momento de la obtención de la imagen [6]. Las redacciones han de exigir que todo el material visual provenga de estos dispositivos o, en su defecto, que se procese con una herramienta certificada que añada una firma digital inalterable.

Además, la **publicación ha de ir acompañada de una prueba de existencia inmutable**. Los metadatos de C2PA pueden ser eliminados o alterados por las redes sociales y procesos de recodificación, como advierten las críticas detectadas recientemente [7]. Por tanto, cada medio ha de anclar su evidencia a una cadena de bloques pública que registre la hora exacta de captura y la firma del dispositivo; este anclaje garantiza que, aun si las credenciales son borradas, el lector puede verificar la procedencia original con un simple enlace.

Las plataformas digitales tienen una responsabilidad complementaria: **preservar y exhibir las credenciales** en lugar de eliminarlas para optimizar el almacenamiento o por motivos de privacidad. Las recomendaciones de la NSA y la CISA (enero de 2025) ya indican que los sistemas de gestión de contenido han de integrar soporte nativo para Content Credentials [8]; esto implica actualizar las API, ofrecer opciones para que los creadores decidan qué información exponer y garantizar que la capa de visualización muestre claramente el estado de verificación al público.

Los fabricantes de cámaras son el **punto de origen** de esta cadena de confianza. Han de **extender la captura en el origen con privacidad configurable**, permitiendo a los usuarios elegir qué atributos (ubicación, metadatos personales) se mantienen cifrados y cuáles se dejan visibles para el control de veracidad. El ejemplo pionero de la AFP con Nikon, que presentó una cámara prototipo con firma integrada en la captura en febrero de 2025, demuestra que este modelo es factible y ya se está desplegando en entornos profesionales [4].

La ciudadanía, finalmente, no puede quedar pasiva. En un panorama donde las «cheap fakes» superaron por una ratio de 7:1 a las deepfakes tradicionales en las elecciones de 2024, el problema central es la **procedencia y el contexto** de los contenidos [2]. Cada usuario ha de aprender a buscar e interpretar los indicadores de credibilidad —las siglas C2PA, las marcas de tiempo en blockchain— y no limitarse al valor visual. Las campañas de educación mediática han de incluir tutoriales prácticos sobre cómo verificar una imagen con herramientas gratuitas disponibles en línea.

Los reguladores, por su parte, han de establecer **estándares interoperables** que obliguen tanto a medios como a plataformas y fabricantes a seguir protocolos comunes de firma y anclaje, evitando un ecosistema de «periodismo de dos velocidades». Las iniciativas como la Content Authenticity Initiative ya cuentan con más de 5.000 miembros (como hemos visto) y han de ser reforzadas con normativas que garanticen la transparencia de las fuentes [3].

En resumen, en un mundo de imágenes sintéticas, **demostrar qué es real se convierte en defender el periodismo**. La tecnología nos ofrece las herramientas; depende de cada actor —medios, plataformas, fabricantes, ciudadanos y reguladores— adoptarlas y hacerlas visibles. El momento de probar la verdad ya ha llegado: *time2act*.

---

[1] NPR — *Fake viral images of an explosion at the Pentagon were probably created by AI* (mayo 2023). https://www.npr.org/2023/05/22/1177590231/fake-viral-images-of-an-explosion-at-the-pentagon-were-probably-created-by-ai

↩

[2] NPR / Harvard Ash Center — *AI was everywhere in 2024's elections, but deepfakes were only part of the picture.* https://ash.harvard.edu/articles/the-apocalypse-that-wasnt-ai-was-everywhere-in-2024s-elections-but-deepfakes-and-misinformation-were-only-part-of-the-picture/ ↩

[3] Content Authenticity Initiative — *5,000 members* (2025). https://contentauthenticity.org/blog/5000-members-building-momentum-for-a-more-trustworthy-digital-world ↩

[4] Nikon Rumors — *AFP validates a C2PA certification test using a prototype Nikon camera* (feb 2025). https://nikonrumors.com/2025/02/18/afp-validates-a-certification-test-of-its-photos-via-the-c2pa-standard-using-a-prototype-nikon-camera.aspx/ ↩

[5] IPTC — *C2PA news: France Télévisions, IBC «Stamping Your Content»*. https://iptc.org/news/tag/c2pa/ ↩

[6] Content Authenticity Initiative — *Leica launches world's first camera with Content Credentials.* https://contentauthenticity.org/blog/leica-launches-worlds-first-camera-with-content-credentials ↩

[7] arXiv — *Why the C2PA specifications fall short* (metadatos eliminables). https://arxiv.org/html/2604.24890v1 ↩

[8] NSA/CISA — *Content Credentials: Strengthening Multimedia Integrity* (ene 2025); JPEG Trust ISO/IEC 21617-1. https://media.defense.gov/2025/Jan/29/2003634788/-1/-1/0/CSI-CONTENT-CREDENTIALS.PDF ↩

[9] Beth Simone Noveck — *Reboot* (Yale UP, 2026), cap. 3. ↩

[10] Beth Simone Noveck — *Reboot* (Yale UP, 2026), cap. 3; Infobae (2025). https://www.infobae.com/peru/2025/06/06/blockchain-y-elecciones-2026-como-se-desarrollara-en-peru-el-voto-digital-obligatorio-para-militares-y-ciudadanos-en-el-extranjero/ ↩

Vida o muerte de los datos: salud e imagen médica

«En cuanto a las enfermedades, acostúmbrate a dos cosas: ayudar o, al menos, no hacer daño.»

— Hipócrates, Epidemias, I, XI

Era una tarde fría de octubre, y el laboratorio de oncología respiratoria de un gran hospital universitario vibraba con la rutina habitual: pacientes que esperaban los resultados de sus exploraciones, médicos que revisaban informes y técnicos que cargaban las imágenes DICOM en el sistema central. En la sala de lectura, una radióloga veterana, con más de diez años de experiencia, abrió una nueva tomografía computarizada (TC) de un hombre de 58 años que había llegado al servicio con tos persistente y pérdida de peso. La imagen en pantalla mostraba un nódulo pulmonar de 1,2 cm en el extremo superior del pulmón derecho, una pequeña sombra densa que destacaba entre el tejido sano.

Sin dudarlo, la radióloga activó el protocolo oncológico: se marcó la zona para una biopsia guiada por imagen y se programó la confirmación diagnóstica antes de cualquier tratamiento. La confianza en los datos que habían llegado a través de la red hospitalaria era total; el formato DICOM, estándar desde hace décadas, parecía una garantía de que la imagen era un testimonio fiel del cuerpo del paciente.

Pero allí dentro, una capa invisible de algoritmos podía haber alterado la esencia misma del archivo. Un grupo de investigadores de la Universidad Ben-Gurión del Néguev, junto con el centro médico Soroka, demostró en USENIX Security 2019 que una red generativa adversarial —llamada CT-GAN— es capaz de inyectar o eliminar tumores en imágenes TC y RM en milisegundos, sin dejar rastro perceptible para el ojo humano ni para los sistemas de verificación convencionales. En un experimento ciego, los radiólogos clasificaron como malignos el 99 % de los casos con tumor inyectado y como sanos el 94 % de los casos con tumor eliminado; incluso advertidos, los errores se mantuvieron alarmantemente en el 60 % y el 87 % respectivamente [1].

En este escenario, el ataque no era una ficción de ciencia ficción sino un código publicado y replicable. Alguien —quizá un actor externo con acceso a la red interna del hospital o un insider malintencionado— habría podido cargar el modelo CT-GAN en el servidor de imágenes y modificar silenciosamente el archivo DICOM antes de que llegara al terminal de la radióloga. El nódulo que ella veía podría no ser más que una ilusión digital, un artefacto generado por una red neuronal entrenada para engañar.

El impacto de una manipulación así es inmediato y potencialmente mortal: el paciente se sometería a procedimientos invasivos innecesarios, expuesto a radiaciones y a la incertidumbre psicológica de vivir con un diagnóstico falso. En la otra cara del mismo monstruo, otra imagen podría haber pasado por alto un tumor real, lo que habría retrasado el tratamiento y puesto en peligro la vida del paciente.

Esta escena no es un relato distópico; es una advertencia basada en pruebas reales que pone de relieve la fragilidad de la medicina moderna cuando los datos se vuelven vulnerables. Si no podemos confiar en la integridad de cada píxel, la esencia misma de la práctica clínica se desmorona, y la salud —el derecho más fundamental— queda a merced de una nueva forma de guerra: la guerra de los datos.

Cuando la imagen médica miente

En 2019 una investigación presentada en USENIX Security reveló un escenario inquietante para la sanidad: **CT-GAN**, una red generativa condicional capaz de inyectar o eliminar tumores pulmonares en tomografías computarizadas (TC) y lesiones cerebrales en resonancias magnéticas (RM) en solo milisegundos. En un experimento a ciegas, los radiólogos diagnosticaron como malignos la gran mayoría de los casos con tumor inyectado y consideraron sanos la gran mayoría de los casos con lesión eliminada; **como hemos visto**, el error clínico fue considerable.

El formato **DICOM** (Digital Imaging and Communications in Medicine) define la codificación, el almacenamiento y la transmisión de imágenes médicas, pero precede a la ciberseguridad moderna y **no incorpora ningún mecanismo criptográfico intrínseco**. Las imágenes viajan por redes hospitalarias, VPN o servicios en la nube a menudo sin firmas digitales que puedan garantizar su integridad. En este vacío, un atacante con acceso a la cadena de suministro —por ejemplo, un proveedor de infraestructura de TI o un insider malintencionado— puede introducir el modelo CT-GAN y modificar los datos en tiempo real, sin que ningún registro de cambios quede visible.

Las motivaciones son diversas. En el ámbito de **seguros**, una imagen falsificada podría generar coberturas para tratamientos inexistentes o, al revés, ocultar lesiones para reducir pagos. En la investigación biomédica, la manipulación de imágenes puede conducir a resultados clínicos engañosos, desviando recursos y alimentando publicaciones fraudulentas. A un nivel más siniestro, un estado o grupo hostil podría **sabotear** estudios clínicos críticos o provocar diagnósticos erróneos que pongan en peligro la vida del paciente, convirtiendo el laboratorio en una nueva línea de frente bélico [1].

Los resultados del estudio demuestran que ni las revisiones manuales ni los sistemas de alerta tradicionales son suficientes; los radiólogos, aunque informados de posibles manipulaciones, confiaron en su experiencia visual y fallaron en la mayoría de los casos. Esto expone una vulnerabilidad estructural: **la confianza ciega en la imagen como verdad absoluta**. En un ecosistema donde cada píxel puede ser alterado en milisegundos, el coste de un diagnóstico erróneo se traduce de inmediato en tratamientos inadecuados, intervenciones innecesarias y, en el peor de los escenarios, la muerte del paciente.

Para revertir esta tendencia, *time2act* propone **la prueba de existencia**: generar un hash criptográfico de cada archivo DICOM en el interior del dispositivo de adquisición y sellarlo con una autoridad de sellado temporal (TSA) conforme al RFC 3161. La huella se ancla en la blockchain pública, opcionalmente agregada en un ancla de Merkle, con ese sello de tiempo como complemento conservado fuera de cadena; esto crea una traza inmutable que cumple las regulaciones HIPAA y 21 CFR Part 11 [5]. Cualquier alteración posterior se detectaría al comparar el hash original con el nuevo valor, abriendo la puerta a auditorías automáticas y a un sistema de alerta precoz.

Como hemos visto, el ejemplo de CT-GAN ilustra cómo un dato manipulado puede convertir una imagen médica en un arma mortal. La respuesta no es solo tecnológica, sino también normativa y cultural: establecer protocolos de **cadena de custodia digital**, exigir firmas criptográficas para cada estudio y educar al personal clínico sobre la fragilidad de los formatos tradicionales. Solo así podremos garantizar que las imágenes sigan siendo testimonios fieles de la salud, y no falsificaciones que pongan en juego vidas humanas.

Médicos y pacientes sintéticos

Imaginemos un médico que, a primera hora de la mañana, recibe una llamada de una paciente que denuncia un dolor abdominal insoportable; la voz es clara y el estilo de comunicación característico, incluso menciona una anécdota de la última visita. Sin sospechar nada, el médico autoriza una receta de analgésicos fuertes y ordena programar una ecografía de urgencia. Unas horas más tarde, otro profesional detecta que el número de la seguridad social del registro no coincide con ningún expediente existente: la «paciente» era una identidad sintética generada por deepfake de audio y vídeo, alimentada por una red criminal dedicada a obtener recetas para el mercado negro [2].

Este escenario no es una excepción anecdótica; representa una amenaza emergente que supera el simple fraude farmacéutico. Las tecnologías de generación de voz e imagen —basadas en modelos de aprendizaje profundo como las redes generativas adversarias (GAN)— pueden replicar con sorprendente fidelidad la cara y el tono de un médico reconocido o de un paciente habitual. Cuando estas imitaciones se difunden a través de plataformas de telemedicina, la capa tradicional de seguridad —cortafuegos, cifrado TLS y autenticación multifactor— resulta insuficiente: ninguno de estos mecanismos «ve» una cara fabricada ni detecta una voz clonada. El peligro reside en la percepción humana; los profesionales confían en la autoridad que transmiten las expresiones faciales y el timbre de voz, y las redes maliciosas explotan esta confianza para manipular decisiones clínicas [2].

Además, el fenómeno de los «pacientes sintéticos» alimenta una cadena de fraude que empieza en la teleconsulta y se extiende hasta los sistemas de seguros. Grupos organizados pueden crear perfiles falsos con documentos digitales de identidad, historiales médicos simulados e imágenes radiológicas adulteradas; estos datos se usan para presentar reclamaciones de indemnización exageradas o para obtener reembolsos de tratamientos que nunca se han realizado. En algunos casos, una voz clonada de médico engaña al personal para que libere datos confidenciales o firme autorizaciones de procedimientos inexistentes, provocando un coste económico y una pérdida de confianza en el sistema sanitario inmensos, especialmente con la adopción masiva de la telemedicina [2].

La solución no pasa solo por reforzar las barreras técnicas, sino por instaurar una cadena de custodia digital basada en pruebas de existencia criptográficas. Cada imagen médica, registro de voz y documento clínico debería estar asociado a un hash único sellado por una autoridad temporal (TSA), como hemos visto en el RFC 3161, asegurando que el archivo nunca abandona el dispositivo original sin una marca

verificable. Este enfoque cumple las normativas de privacidad, incluida la HIPAA y la normativa 21 CFR Part 11, y crea una traza inmutable que desactiva cualquier intento de manipulación posterior a la captura [5][7].

En última instancia hay que combinar tecnología y cultura: desplegar soluciones blockchain para el almacenamiento de metadatos mínimos fuera de cadena, formar al personal clínico en la detección de anomalías de voz e imagen, y establecer protocolos de autenticación multifactor que incluyan verificaciones biométricas independientes de los datos presentados. Solo así podremos garantizar que la confianza depositada en una consulta virtual no se convierta en un arma para quien quiere jugar con la vida humana.

La integridad de la ciencia

En una era donde las revistas biomédicas son el epicentro del conocimiento clínico, la contaminación de los datos es tan mortal como un tumor inyectado en una tomografía. La detective de imágenes Elisabeth Bik ha mostrado que cerca del **3,8 %** de los más de **20.000** artículos biomédicos revisados contienen figuras problemáticas —una probabilidad de uno de cada 25 artículos— y que la mitad de estos casos revela indicios claros de manipulación deliberada [3]. Esta tasa se traduce en una erosión sistemática de la base sobre la que se toman decisiones terapéuticas, se diseñan protocolos y se destinan recursos públicos.

El neurocientífico Hoau-Yan Wang, vinculado al desarrollo del fármaco contra el Alzheimer de Cassava Sciences, fue imputado federalmente el **28 de junio de 2024** por fraude, incluyendo la fabricación de Western Blots que respaldaban resultados falsos [3]. La investigación ha revelado que se habían obtenido aproximadamente **16 millones de dólares** de financiación de los National Institutes of Health (NIH) basándose en datos manipulados, desviando recursos destinados a tratamientos para millones de pacientes.

El aumento de plataformas automatizadas como Proofig e ImageTwin, ya integradas en flujos editoriales, ofrece una esperanza concreta [3]. Estas herramientas aplican algoritmos de detección basados en análisis estadísticos de píxeles, patrones de compresión y comparaciones con bibliotecas de referencia, identificando anomalías que una revisión humana podría pasar por alto; su eficacia depende de una adopción universal y de un compromiso institucional para validar cada figura antes de la publicación.

El **peligro** es doble. En primer lugar, la ciencia deficiente alimenta decisiones clínicas equivocadas: médicos que confían en resultados falsos pueden prescribir tratamientos ineficaces o incluso nocivos, y esto pone en riesgo vidas humanas.

En segundo lugar, la financiación pública se dilapida en proyectos basados en datos no fiables, y esto reduce los recursos disponibles para investigaciones genuinas, incrementando la desconfianza del ciudadano hacia el sistema de salud.

La promesa reside en una arquitectura de integridad basada en pruebas de existencia. Mediante el uso de hash + sello de tiempo (TSA) según el RFC 3161, las imágenes y metadatos se registran fuera de cadena pero con una huella inmutable en la blockchain, cumpliendo los requisitos de privacidad de HIPAA y del 21 CFR Part 11 [5][7]. Cada archivo conserva su integridad dentro del dispositivo clínico, generando una traza de auditoría que cualquier auditor puede verificar en tiempo real.

Por tanto, el mensaje es claro: sin una capa verificable de confianza, la ciencia se convierte en un campo minado. Como hemos visto, la comunidad académica y las instituciones reguladoras han de implantar sistemáticamente estas pruebas de existencia y utilizar herramientas como Proofig o ImageTwin para filtrar cada figura antes de que llegue al lector; solo así el conocimiento generado será un pilar sólido para la salud humana, no una bomba de tiempo que amenaza vidas y financiaciones.

Sellar la verdad clínica

En un mundo donde el simple hecho de inyectar o borrar un píxel puede transformar un diagnóstico en una condena, la solución ha de ser tan rigurosa como las propias normas que regulan la salud. El patrón emergente —y ya avalado por la FDA— consiste en mantener el dato sensible totalmente fuera de la cadena de bloques y en registrar únicamente su resumen criptográfico (hash) junto con metadatos mínimos: sello de tiempo, identificador de usuario y tipo de operación. Esta pequeña huella digital se

convierte en una traza inmutable que puede ser auditada sin revelar contenido confidencial, cumpliendo o incluso superando las exigencias de auditoría de HIPAA y del 21 CFR Part 11 [5].

La mecánica es sencilla pero poderosa. Cada imagen DICOM, cada registro de historial clínico y cada archivo de un ensayo se procesa dentro del dispositivo o del servidor hospitalario; se le añade un hash SHA-256 que representa su integridad completa. Este hash se transmite a una red de bloques donde se registra con una autoridad de sellado temporal (RFC 3161) o, en entornos más avanzados, con la raíz de Merkle de una cadena privada de salud [7]. Los metadatos asociados —solo los necesarios para validar la transacción— quedan visibles en la cadena, mientras que el contenido original nunca abandona el perímetro seguro del centro médico, manteniendo así la privacidad exigida por HIPAA y facilitando una auditoría transparente: cualquier revisión puede comparar el hash almacenado con el archivo actual y detectar, en milisegundos, cualquier alteración.

En el ámbito de los ensayos clínicos este modelo crea una cadena de custodia verificable que registra quién ha generado cada dato y cuándo se ha modificado. El producto Triall ya ofrece esta funcionalidad: cada dato de un ensayo se «sella» con su hash y se vincula a un registro inmutable, asegurando que las autoridades reguladoras y los patrocinadores puedan rastrear la trayectoria de la información desde el momento de la recogida hasta la publicación final [6]. Como hemos visto, el fraude de imágenes afecta a un 3,8 % de los artículos y ha generado imputaciones por unos 16 M$ de financiación de los NIH [3].

La FDA ha reconocido esta necesidad. Su guía final de ciberseguridad para dispositivos médicos, publicada el **27 de junio de 2025**, exige que los fabricantes incluyan una lista de materia prima de software (SBOM) y documentación exhaustiva de las medidas de protección [4]. Cualquier dispositivo que emita imágenes radiológicas o datos de monitorización ha de incorporar mecanismos que demuestren que el contenido no se ha manipulado después de la adquisición.

En la práctica solo hacen falta tres pasos: (1) generar y almacenar localmente el hash de cada dato sensible; (2) enviar este hash a una cadena de bloques con un sello de tiempo certificado; (3) conservar los metadatos para auditorías futuras. Herramientas como Proofig o ImageTwin detectan automáticamente anomalías antes de que las figuras lleguen a publicación y se integran en el flujo hospitalario. Cuando estas soluciones se despliegan sistemáticamente, la confianza en las imágenes médicas pasa de una vulnerabilidad explotable a una garantía verificable.

El resultado es claro: un ecosistema donde la verdad clínica está «sellada» y no puede ser alterada sin dejar huella. En un contexto donde cada diagnóstico puede decidir entre vida o muerte, esta capa de verificación supera las normativas y ofrece una defensa real contra el engaño digital que amenaza la salud global. Es el momento de adoptarla como estándar universal y convertir la seguridad de los datos médicos en un pilar inamovible del futuro sanitario.

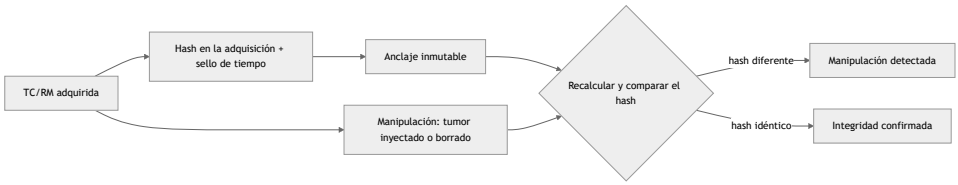


Figura 18.1 — Si se calcula el hash de la imagen en el momento de la adquisición y se ancla con sello de tiempo, cualquier manipulación posterior (un tumor inyectado o borrado) se detecta al instante.

Cómo funciona, sin que el dato salga

En el núcleo de una solución de confianza para los datos médicos hay una operación aparentemente sencilla pero extraordinariamente poderosa: calcular un hash criptográfico del archivo en el momento exacto de la adquisición. Este resumen matemático —una cadena de caracteres única que representa la totalidad del contenido— se convierte en la huella digital de la imagen, del informe radiológico o del registro clínico. Una vez generado, el hash se envía a una autoridad de sellado temporal (Timestamp Authority, TSA) conforme al protocolo que ya hemos citado, y esta emite un certificado de tiempo firmado con su clave privada, indicando que la huella existía en aquel instante y no ha sido alterada posteriormente.

Para amplificar la resistencia a manipulaciones y garantizar una verificación abierta, el hash certificado se puede anclar a una cadena pública mediante una raíz de Merkle. En este escenario, varios archivos generan nodos hijos que se agrupan en un árbol binario; cada nodo contiene el hash combinado de sus

hijos y la capa superior (la raíz) representa de forma resumida todo el conjunto de datos. Publicar esta raíz en una blockchain —donde el contenido se mantiene fuera de cadena, dejando solo la huella y los metadatos mínimos— crea una traza de auditoría inmutable que cumple con los requisitos de privacidad establecidos por HIPAA y 21 CFR Part 11 [5].

El punto clave que convierte este mecanismo en una solución viable para la salud es que el archivo original **nunca sale del dispositivo**. Solo la huella —una cadena de bytes de una longitud fija— se transmite hacia el entorno externo, ya sea al TSA o a la blockchain. Esto elimina cualquier necesidad de transferir imágenes radiológicas completas, que contienen información personal sensible, a servidores de terceros. La verificación posterior es totalmente descentralizada: cualquier parte interesada puede recalcular el hash del archivo localmente y compararlo con la huella registrada en el certificado o en la cadena pública; si coinciden, se demuestra que el contenido no ha sufrido alteraciones desde el momento de su captura.

Esta arquitectura ofrece una doble capa de seguridad. Por un lado protege la confidencialidad del paciente porque los datos clínicos permanecen dentro de los perímetros controlados del dispositivo médico o del sistema hospitalario; por otro aporta una prueba de existencia verificable para auditores, reguladores y profesionales sanitarios sin depender de ninguna entidad central que pueda negar acceso o manipular los registros. El modelo «t2p» aplicado a la salud convierte cada estudio clínico, cada diagnóstico por imagen y cada receta digital en un testimonio inmutable de su propio origen.

En la práctica, este flujo se puede integrar en los sistemas DICOM ya existentes: cuando el escáner genera una nueva tomografía, el software de gestión calcula de inmediato el hash, solicita el sello temporal y actualiza los metadatos del archivo con un enlace a la transacción blockchain. Los profesionales que revisan las imágenes pueden ver, junto al informe, un código QR o una referencia hash que les permite verificar en tiempo real la autenticidad del dato. Así, cualquier intento de inyectar tumores falsos —como demuestran los experimentos de CT-GAN, donde los radiólogos fueron engañados hasta en el 99 % de los casos— se vuelve ineficaz: sin el hash original y su sello temporal, la manipulación no podría pasar desapercibida para un auditor independiente [1] (como hemos visto).

La mecánica de la prueba de existencia combina tres principios fundamentales: **integridad criptográfica**, **temporalidad certificada** y **preservación del dominio de los datos**. Estas características aseguran que la información clínica se mantenga tanto segura como verificable, convirtiéndola en una defensa robusta contra el engaño digital que amenaza la vida de los pacientes.

La promesa y el peligro

Imagina un radiólogo que, sin saberlo, revisa una tomografía donde un tumor ha sido insertado artificialmente por una IA generativa como CT-GAN. En el estudio de USENIX Security 2019, los profesionales diagnosticaron malignidad en el **99 % de los casos** con tumores inyectados y consideraron sanos el **94 %** de los estudios donde el tumor había sido eliminado; incluso cuando se les advertía del posible engaño, el error se mantiene entre un **60 % y un 87 %** [1]. Estas cifras muestran que la confianza ciega en una imagen puede traducirse directamente en decisiones de tratamiento equivocadas, con consecuencias potencialmente letales.

La **promesa** del sello criptográfico —un hash inmutable y un sello de tiempo certificado (TSA o ancla de Merkle) que nunca abandona el dispositivo— es proporcionar una capa de autenticidad que se convierte en la piedra angular de diagnósticos fiables. Cuando cada estudio DICOM viene acompañado de un hash verificable, el radiólogo puede comprobar que la imagen no ha sido alterada desde el momento de la adquisición. Esto no solo protege al paciente ante manipulaciones malintencionadas, sino que también refuerza la **investigación**: los artículos biomédicos que incluyen figuras problemáticas representan aproximadamente un **3,8 %** de los estudios revisados, según el análisis de Bik [3]; una auditoría basada en pruebas de existencia podría detectar estas irregularidades antes de la publicación, reduciendo los costes de retractaciones y aumentando la credibilidad del campo.

En el ámbito de los **ensayos clínicos**, plataformas como Triall ofrecen cadenas de custodia que registran cada paso del proceso, desde la recogida de muestras hasta el análisis final, con un hash y una marca temporal que garantiza que ningún dato se puede suprimir o modificar sin dejar rastro [6]. Esto permite a las autoridades reguladoras —por ejemplo la FDA, que el 27 de junio de 2025 publicó una guía definitiva sobre ciberseguridad de dispositivos médicos exigiendo SBOM y documentación exhaustiva [4]— verificar la integridad de cada elemento del ensayo, evitando fraudes como el caso de los Western Blots fabricados, vinculado a unos **16 M$** de los NIH [3].

Sin embargo, el **peligro** reside en una falsa sensación de inmunidad. Un sello criptográfico no es un sustituto de la ciberseguridad de red hospitalaria; si el origen de los datos (el dispositivo o el servidor que los almacena) está comprometido, el hash puede ser generado a partir de una información ya alterada. La complejidad de integrar esta capa dentro de los flujos clínicos —que a menudo están saturados por sistemas heredados y protocolos rígidos— puede generar retrasos o errores operativos si no se dispone de una gobernanza clara sobre quién tiene autorización para verificar y validar los sellos. Un exceso de confianza en la prueba de existencia podría conducir a una **desatención** de los otros vectores de ataque, como vulnerabilidades en redes internas, software malicioso que manipula los datos antes de firmarlos o el uso indebido de claves criptográficas por parte de personal no autorizado.

Como hemos visto, el sello de tiempo y el hash constituyen una capa necesaria dentro de una estrategia integral de seguridad e integridad. Cuando se asocian a controles de red robustos, políticas de gobernanza transparentes y formación continua del personal sanitario, permiten restaurar la confianza en la medicina basada en datos —una confianza que puede marcar la diferencia entre vida y muerte para millones de pacientes.

Es hora de actuar

La integridad de los datos médicos ya no es una cuestión técnica; es un requisito vital que ha de ser adoptado como norma operativa por cada entidad del sector sanitario. Por eso, la primera responsabilidad recae sobre **hospitales y fabricantes de equipos**: el momento en que una tomografía o una historia clínica entra en el sistema ha de quedar permanentemente registrado con un hash criptográfico y anclado a un sello de tiempo (TSA) conforme al RFC 3161. Este proceso, que se completa en milisegundos, impide cualquier manipulación posterior sin dejar rastro de inconsistencia, tal como demuestra el caso CT-GAN, donde la inserción o supresión de un tumor es detectable de inmediato cuando se aplica una verificación de hash fiable [1].

Los **investigadores y las revistas científicas** han de hacer del sello de tiempo una condición para la aceptación de cualquier artículo que incluya imágenes biomédicas. Herramientas como Proofig o ImageTwin ya ofrecen servicios de auditoría de integridad; su uso sistemático debería ser tan habitual como la revisión por pares. Esto reduciría drásticamente el impacto de fraudes como los detectados por Bik, donde cerca de un 3,8 % de los artículos presentaban figuras problemáticas [3], y ayudaría a prevenir casos como la imputación federal del 28 de junio de 2024 por Western Blots fabricados, vinculada a unos 16 M$ de los NIH [3].

Los **reguladores**, liderados por la FDA con su guía final de ciberseguridad (27 de junio de 2025) y la EMA, han de incorporar explícitamente los requisitos de pruebas de existencia en las normativas de dispositivos médicos. Esto implica exigir un SBOM completo y una documentación que demuestre la trazabilidad inmutable de los archivos clínicos, tal como recomienda el patrón blockchain para salud, que combina la carga fuera de cadena con hash y metadatos mínimos en la cadena, cumpliendo HIPAA y 21 CFR Part 11 [4][5].

Las **aseguradoras** pueden convertir esta capa de integridad en un criterio de cobertura: antes de autorizar el pago de un tratamiento o una cirugía, se puede validar que los datos subyacentes no hayan sido alterados. Un sistema de verificación automatizado basado en la cadena de custodia (como el producto Triall) podría reducir los costes asociados a reclamaciones fraudulentas y aumentar la confianza de los pagadores en la autenticidad del diagnóstico [6].

Finalmente, **pacientes y profesionales** han de exigir transparencia. Cada profesional ha de poder presentar un certificado digital que demuestre que las imágenes y los informes que utiliza son exactos y no han sido modificados desde el momento de la captura. Los pacientes, por su parte, pueden solicitar acceso a este registro inmutable como derecho de información, reforzando la cultura de responsabilidad compartida.

En resumen, proteger la integridad de los datos es proteger vidas. La tecnología de pruebas de existencia ya está disponible y validada en escenarios reales; lo que falta es la adopción generalizada y la imposición reguladora. No podemos permitir que una imagen manipulada sea la causa de un diagnóstico erróneo o de una receta fraudulenta. Como hemos visto, es time2act: implementemos hash y sello de tiempo en cada punto de entrada, hagámoslo obligatorio para la investigación y exijamos trazabilidad verificable en todos los niveles del sistema sanitario. Cada segundo que esperamos supone un riesgo potencial para la vida de los pacientes.

[1] Mirsky et al. — *CT-GAN: Malicious Tampering of 3D Medical Imagery* (USENIX Security 2019). https://www.usenix.org/conference/usenixsecurity19/presentation/mirsky · resumen con cifras: https://www.pindrop.com/article/threat-deepfakes-in-healthcare/ ↩

[2] TruthScan / Pindrop — *AI-driven fraud in healthcare: deepfake doctors and synthetic patients* (2025). https://truthscan.com/blog/ai-driven-fraud-in-global-healthcare-2025-trends-and-countermeasures/ ↩

[3] STAT News — *Cassava Sciences scientist indicted (fabricated Western Blots)* (28-jun-2024); Retraction Watch / Bik. https://www.statnews.com/2024/06/28/cassava-sciences-indictment-alzheimers-hoau-yan-wang/ ↩

[4] FDA — *Cybersecurity in Medical Devices: final guidance* (Federal Register, 27-jun-2025). https://www.govinfo.gov/content/pkg/FR-2025-06-27/html/2025-11669.htm ↩

[5] HIPAA Vault — *Blockchain integration for healthcare records (audit trails)* (2025). https://www.hipaavault.com/resources/blockchain-integration-healthcare-records/ ↩

[6] Bentham/RRCT (PubMed) — *Blockchain as a Prime Guardian of clinical-trial data* (2025); Triall. https://pubmed.ncbi.nlm.nih.gov/39851126/ ↩

[7] ProofStamper — *RFC 3161 + blockchain anchoring (proof of existence)*. https://proofstamper.com/en/compare/file-timestamp-tools-2026/ ↩

Credenciales y autoría: educación e investigación

«Ni sé, ni creo que sé.»

— Platón, Apología de Sócrates (21d)

A la luz fría de una sala de cuidados intensivos del sur de Texas, el reloj del monitor marcaba las 03:17 cuando una mujer entró en la habitación con un paso seguro y un brazo lleno de papel. Llevaba una bata blanca impecable y en el pecho lucía una insignia que brillaba como si fuera de oro: «RN — Registered Nurse». El paciente, un hombre de cincuenta y siete años con una neumonía severa, miraba su mano mientras el respirador emitía su ruido constante. La enfermera se inclinó hacia la cama, revisó las constantes y, sin dudarlo, administró una dosis de antibióticos que había prescrito el médico.

El momento parecía rutinario; sin embargo, la verdad que escondía aquel uniforme era cualquier cosa menos ordinaria. Aquel título de «Registered Nurse» no provenía de una universidad acreditada ni de un programa de estudios reconocido por el estado. Era una de las más de 7.600 credenciales falsas detectadas en la operación «Nightingale», una investigación del Departamento de Justicia de Estados Unidos que desmanteló una red internacional dedicada a la fabricación y venta masiva de diplomas de enfermería falsos (DOJ 2023; fase II, 2025) [3]. Cada credencial se vendía por hasta unos 15.000 dólares, y los compradores eran tanto estudiantes como profesionales ya insertados en el mercado laboral.

El ambiente se volvió tenso —el paciente mostraba signos de reacción adversa al antibiótico. La enfermera, sin ningún registro verificable que confirmara su formación ni la fecha de obtención del título, había tomado decisiones clínicas basadas únicamente en una apariencia legal. Su «diploma» era solo un archivo digital con un hash sellado en una cadena de bloques desconocida; el documento real, si algo había, no se encontraba en la cadena, sino fuera de ella, como indica el modelo de Blockcerts del MIT, donde la etiqueta de un título se limita a un hash y una transacción sellada [5].

Este incidente encarna el hilo conductor que une este capítulo con el anterior: el peligro concreto que la falsificación de credenciales puede suponer para la vida humana. En el capítulo 18, habíamos expuesto cómo las deepfakes y la suplantación de identidad en exámenes remotos pueden comprometer la integridad académica; aquí, la misma vulnerabilidad se traduce en una amenaza directa para la salud. La pregunta que emerge es inevitable: **¿cómo podemos saber con certeza que un título —o un trabajo— es auténtico?**

En un mundo donde la IA generativa puede crear documentos de aspecto convincente y las redes de falsificación operan a escala global, la confianza tradicional en el papel firmado o en el número de registro ya no es suficiente. La respuesta ha de recurrir a sistemas que garanticen el origen y la integridad sin depender de intermediarios: credenciales verificables basadas en blockchain y pruebas de autoría que, como demuestra el modelo W3C Verifiable Credentials Data Model 2.0 (mayo-2025) [6], ofrecen una capa criptográfica de confianza que se puede auditar independientemente.

Mientras la enfermera continuaba con su atención, el monitor mostraba un ritmo cada vez más irregular. La vida de un paciente podía depender de la capacidad del sistema educativo y profesional para demostrar, sin duda, quién está realmente cualificado para curarlo. El silencio que se instaló en la sala no era solo el sonido de las máquinas; era el eco de una pregunta que debería resonar en cada aula, laboratorio y oficina: **¿qué hacemos cuando la confianza desaparece?**

La evaluación en crisis

En la primavera de 2025, las aulas del Reino Unido se convirtieron inesperadamente en una sala de experimentación a gran escala: entre las filas de bibliotecas y salas de estudio, el tránsito hacia plataformas de inteligencia artificial se disparaba. La encuesta HEPI de aquel año revelaba que el **92 % de los estudiantes del Reino Unido** ya usaban herramientas de IA para redactar ensayos, resolver problemas matemáticos o incluso generar respuestas a cuestionarios en línea. Más alarmante aún, la proporción de estudiantes que utilizaban IA **durante las evaluaciones** saltó del **53 % al 88 % en solo un año**, una evolución que supera cualquier incremento histórico de tecnologías asistenciales dentro de la educación superior.

A primera vista, estas cifras podrían sugerir una democratización del conocimiento: más estudiantes acceden a recursos avanzados y pueden mejorar la calidad de sus trabajos. No obstante, el panorama se desdibuja cuando se miran las limitaciones de las herramientas de detección actuales. El regulador australiano TEQSA en 2024 ha concluido que los métodos cuantitativos para identificar el uso de IA son «poco fiables». Un estudiante acusado puede, simplemente, negar por completo la utilización de un modelo generativo, sin dejar huella verificable; al mismo tiempo, **los usuarios hábiles son rara vez pillados**, ya que las soluciones de detección se basan en patrones superficiales y no en pruebas criptográficas.

Esta vulnerabilidad tiene consecuencias tangibles. TEQSA señala un riesgo creciente de **falsos positivos**: estudiantes inocentes son acusados injustamente de haber plagiado o de haber recurrido a la IA, lo que puede traducirse en sanciones académicas e impactar negativamente en sus trayectorias profesionales. El coste social de estos errores es evidente cuando se considera que ya **aproximadamente el 15,7 % de los estudiantes** sufría alguna forma de engaño contractual antes de la llegada masiva de la IA generativa, una cifra que se ha visto amplificada por la falta de evidencia fiable [2].

En este contexto, la respuesta no puede ser simplemente intensificar las políticas disciplinarias. La reforma de la evaluación que propone TEQSA se centra en **redefinir los criterios de verificación**, pasando de un modelo basado en suposiciones a un ecosistema donde la prueba de autoría y la integridad de los documentos sean indiscutibles. Esto implica adoptar tecnologías como las credenciales verificables almacenadas en blockchain, que permiten registrar de manera inmutable tanto la emisión del título como el momento exacto en que se creó un trabajo académico.

La transición hacia este nuevo paradigma no elimina la necesidad de una cultura ética; al contrario, ofrece una base técnica sólida para que las instituciones puedan **distinguir con claridad** entre la aportación genuina del estudiante y el apoyo de herramientas externas. En lugar de enfocarse en la persecución, los centros educativos pueden canalizar recursos hacia sistemas que garanticen la transparencia del proceso de evaluación, reduciendo así tanto los falsos positivos como las oportunidades para fraudes masivos.

En resumen, el panorama actual muestra una **erosión profunda de la confianza** en la evaluación académica, impulsada por una adopción masiva de IA y por la incapacidad de los mecanismos de detección tradicionales. La solución duradera pasa por una infraestructura de credenciales verificables que restablezca la seguridad del título y de la autoría, creando las bases de un entorno educativo resiliente ante las tecnologías emergentes.

Títulos que no valen

Imagina un documento oficial con el sello de una academia de enfermería: papel satinado, número de registro y una firma digital aparentemente auténtica. Un estudiante se enorgullece de haber conseguido aquel título tras un curso intensivo en línea, pero nadie ve que el diploma forma parte de una red clandestina como la destapada por la Operación Nightingale, una investigación conducida por el Departamento de Justicia de EE. UU.

Como hemos visto, en 2023 se descubrieron más de **7.600** diplomas y expedientes falsos en Florida; la primera oleada ya trajo **25 acusados** y la revocación de licencias en varios estados, y dejó a pacientes expuestos a profesionales no cualificados. La fase II, iniciada en 2025, añadió doce acusados más y confirmó que la falsificación sigue siendo una amenaza creciente [3]. Mientras las autoridades combaten este mercado subterráneo, las **deepfakes** —imágenes generadas por IA que superponen cara y voz de una persona sobre el cuerpo de otra— se extienden al mundo de los exámenes y entrevistas remotas. Un estudiante puede ahora hacer pasar su identidad ante una cámara de examen con una verosimilitud que engaña tanto a los algoritmos como a los supervisores humanos, y estas manipulaciones pueden ser almacenadas y reutilizadas para futuras oportunidades de evaluación, destruyendo la confianza construida a lo largo de décadas [4].

El patrón común entre ambas amenazas es claro: **la credencial y la identidad se pueden falsificar**. El título ya no es un sello fiable de competencia; la cara que aparece en la pantalla no garantiza la presencia real del candidato, exponiendo una vulnerabilidad fundamental en el modelo educativo actual, basado en documentos impresos o firmas digitales replicables y manipulables con facilidad.

La solución no pasa solo por reforzar los mecanismos de detección: hay que establecer una **infraestructura de verificación que no dependa de mirarlas**. Las credenciales verificables basadas en blockchain codifican cada título y registro de identidad con un hash único y las sellan en una

cadena inmutable, haciendo imposible la modificación sin dejar huella. Este modelo garantiza la autenticidad del documento y permite a cualquier parte interesada (universidades, entidades reguladoras u hospitales) comprobar al instante su validez sin intermediarios.

En este contexto, el fraude de credenciales y la suplantación digital son una llamada urgente a la acción: hay que adoptar sistemas descentralizados que restablezcan la confianza en la educación y la salud, para que los títulos sean realmente **títulos que valen**.

La respuesta: credenciales verificables

El primer paso hacia una educación que recupere la confianza ya se probó en el laboratorio del MIT, donde el proyecto Blockcerts puso en marcha un piloto de **111 diplomas emitidos en blockchain** en 2017. En este esquema los datos sensibles del título —nombre, fecha de obtención y programa de estudio— se mantienen fuera de la cadena; solo se incrusta en la red un **hash unidireccional** que representa el contenido completo del documento y una transacción sellada que certifica que el MIT ha creado aquel registro. Esta arquitectura es idéntica al modelo hash-ancla empleado por la prueba de autoría/existencia, donde el mismo mecanismo demuestra que alguien poseía un archivo en un momento determinado y que no ha sido alterado posteriormente [5].

En Europa, el enfoque se ha escalado a escala continental gracias a **EBSI (European Blockchain Services Infrastructure)** y al marco de las **European Digital Credentials for Learning**. Estas plataformas emiten credenciales con **sellos electrónicos eIDAS**, asegurando la validez legal y la interoperabilidad transfronteriza. Hasta ahora se han generado más de **76.000 credenciales verificables**, que pueden ser consultadas al instante por cualquier empresa u organismo regulador sin necesidad de intermediarios ni procesos manuales. La estandarización ha llegado con la **Recomendación W3C Verifiable Credentials Data Model 2.0** (mayo-2025), que define cómo empaquetar, firmar y validar estas credenciales de forma segura y compatible con cualquier infraestructura blockchain pública [6].

El valor añadido de este modelo es doble: elimina el riesgo de **diplomas falsos**, como los detectados en la operación Nightingale, donde más de **7.600 certificados de enfermería falsificados** pusieron en peligro la seguridad de los pacientes en EE. UU. (DOJ 2023; fase II con 12 acusados adicionales en 2025) [3]; y contrarresta la **suplantación vía deepfakes** y otras formas de proctoring digital que han comprometido exámenes remotos, ya que cada respuesta de un estudiante puede ser vinculada a una credencial verificable que garantiza el origen y la integridad del trabajo [4].

En la práctica, un empleador o una autoridad reguladora solo tiene que introducir el **hash** del título en la interfaz de verificación correspondiente; la cadena blockchain devuelve la huella de tiempo y la firma digital del proveedor (MIT, universidad europea, etc.), confirmando que aquel documento no se ha modificado desde su emisión. No hay que llamar a la institución, enviar correos electrónicos o esperar semanas por una respuesta oficial: la verificación se completa en segundos y es **inmutable**. Esto crea un ecosistema donde el valor del título deja de estar ligado a la reputación de la entidad emisora —que puede ser objeto de fraudes o fallos administrativos— y pasa directamente al **registro criptográfico**, que es transparente, auditable y resistente a manipulaciones.

Según el informe HEPI de 2025, como hemos visto, el uso de la IA en evaluaciones ha experimentado un aumento drástico; con credenciales verificables basadas en blockchain, las universidades pueden establecer una barrera técnica que impida que la IA produzca documentos falsificados sin dejar rastro, reforzando la confianza tanto en el emisor como en el receptor.

En definitiva, la combinación de **diplomas en blockchain**, **sellos eIDAS** y el estándar **W3C Verifiable Credentials 2.0** constituye una respuesta concreta y probada que restablece las dos formas básicas de confianza en la educación: el reconocimiento del título y la prueba de autoría. Es ahora, más que nunca, el momento de adoptar estas tecnologías descentralizadas para garantizar que nuestros títulos sean **realmente títulos que valen** [1].

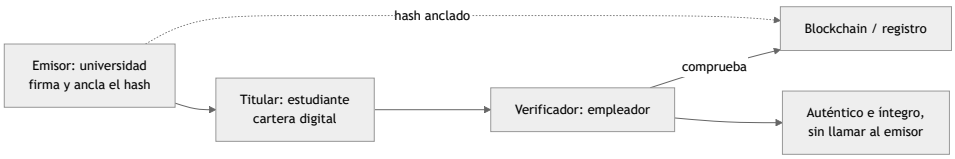


Figura 19.1 — El emisor firma y ancla el hash de la credencial; el titular la presenta; cualquier verificador comprueba su autenticidad e integridad sin intermediarios.

Probar la autoría

En un mundo donde la IA generativa puede reproducir texto con una fidelidad que desdibuja las líneas entre lo original y lo copiado, la verdadera prueba de autoría se convierte en la piedra angular de cualquier sistema educativo fiable. La solución no reside en intentar demostrar la ausencia de intervención —una tarea prácticamente imposible cuando los algoritmos son cada vez más opacos— sino en certificar **CUÁNDO** y **QUÉ** se ha creado. Esta es la premisa de la prueba de existencia: un hash único, combinado con un sello de tiempo inmutable, demuestra que el creador poseía el documento en un momento determinado, estableciendo así la prioridad de autoría antes de que el contenido llegue a cualquier revisión o publicación.

El mecanismo es sencillo pero potente. Al generar el hash —un resumen criptográfico de longitud fija— se captura el estado completo del archivo en aquel instante y se registra en una cadena de bloques pública, donde cada bloque contiene un sello de tiempo verificable por la red descentralizada. El resultado es una prueba irrefutable de que el documento existía y no había sido alterado desde aquel momento [7]. Esto ofrece dos ventajas cruciales: primero, frente al plagio, el creador puede demostrar «yo lo tenía antes», y segundo, contra las acusaciones de falsos positivos producidos por detectores poco fiables, se dispone de una evidencia objetiva que rechaza cualquier duda sobre la legitimidad de la obra.

Como hemos visto, el proyecto MIT/Blockcerts certificó 111 estudios en 2017 y la Unión Europea ha almacenado más de 76.000 credenciales hasta mayo de 2025, con el modelo W3C Verifiable Credentials 2.0, demostrando que la infraestructura para la prueba de autoría ya está operativa y escalable [5][6].

El mismo principio se aplica al trabajo intelectual de los investigadores y estudiantes. Cada artículo, cada proyecto de tesis o incluso cada código fuente puede ser «sellado» antes de ser compartido con supervisores o revisores. Esto no solo protege al autor contra acusaciones injustas, sino que también refuerza la confianza en los procesos de evaluación académica; como hemos visto, el uso de IA en evaluaciones se ha disparado recientemente [1]. En este contexto, las instituciones no pueden seguir dependiendo únicamente de detectores de autoría que son «poco fiables» y que a menudo permiten negar la responsabilidad [2].

Una prueba tangible de esta práctica se encuentra en la obra que lees ahora. Antes de publicar **time2act**, el manuscrito fue hasheado y sellado en una cadena de bloques, garantizando que nadie —ni siquiera el autor— pudiera modificarlo sin dejar huella. Este gesto no es un simple ejercicio técnico; es la manifestación concreta del principio que defiende este capítulo: **la confianza se reconstruye con pruebas verificables, no con suposiciones**.

La llamada a la acción es clara. Educadores, administradores e investigadores han de adoptar de inmediato las herramientas de prueba de existencia basadas en blockchain para todos sus productos intelectuales. Esto implica integrar soluciones como Blockcerts o EBSI en los flujos de trabajo académicos, establecer políticas que obliguen al sellado prepublicación y formar al personal en la gestión de estas credenciales digitales. Solo así podremos garantizar que los títulos y las producciones intelectuales sean realmente **títulos que valen**, y que nuestra educación recupere las dos confianzas fundamentales: el reconocimiento del título y la prueba de autoría.

La promesa y el peligro

Imagina un aula digital de una universidad europea donde una profesora acaba de publicar los resultados finales de un curso de bioingeniería. Una vez cargado el archivo en el repositorio institucional, un algoritmo genera automáticamente un *Verifiable Credential* basado en el modelo W3C 2.0 (recomendado por la W3C en mayo de 2025) y lo llama «Diploma de Bioingeniería». El estudiante que ha superado el curso recibe al instante una credencial blockchain con un hash único y un sello de tiempo verificable. Sin ningún papel, sin llamadas telefónicas al registro central, cualquier empresa o autoridad puede comprobar la validez del título en segundos: solo hay que consultar el explorador público de EBSI o el nodo nacional correspondiente.

Esta fluidez es la promesa que sustenta todo el paradigma de las credenciales digitales. Un título se convierte en un activo portable, interoperable e inmutable; la prueba de autoría, a través del mismo

mecanismo de hash + sello de tiempo, garantiza que el estudiante era el propietario del trabajo en el momento exacto de su creación (como demuestra el proyecto MIT/Blockcerts con 111 estudiantes pilotados en 2017) [5]. La verificación es instantánea y descentralizada: las empresas pueden validar miles de solicitudes de empleo sin depender de una oficina de certificación central, reduciendo costes administrativos y eliminando fraudes como los 7.600 diplomas falsos detectados en la Operation Nightingale en EE. UU. (2023-2025) [3].

No obstante, la misma infraestructura que ofrece confianza puede generar nuevos peligros. El *proctoring* invasivo, impulsado por plataformas de supervisión basadas en IA y reconocimiento facial, recoge datos biométricos de estudiantes menores de 18 años sin un marco claro de consentimiento ni control sobre el uso posterior de estos registros. La privacidad se ve amenazada cuando las instituciones almacenan imágenes, audios y patrones de comportamiento en servidores centralizados o, peor aún, en cadenas públicas sin anonimización adecuada.

Además, la equidad académica corre el riesgo de convertirse en una nueva brecha digital. Según el estudio HEPI 2025, el 92 % de los estudiantes del Reino Unido ya usan IA, y la proporción que la utiliza en evaluaciones ha subido del 53 % al 88 % en solo un año [1]. Quien no disponga de acceso a dispositivos capaces de generar o verificar credenciales blockchain quedará relegado a procesos manuales más lentos y menos reconocidos, aumentando la desigualdad entre instituciones bien financiadas y las que operan con recursos limitados.

La dependencia de un proveedor único de servicios de sellado también es una vulnerabilidad estructural. Si una empresa que controla la infraestructura clave sufre un ataque o decide modificar las condiciones del servicio, toda la cadena educativa puede ver comprometida la integridad de los títulos y las pruebas de autoría. Los riesgos de falsos positivos —y la base de engaño contractual del 15,7 % detectada en el estudio de Newton— demuestran que ningún sistema es infalible [2].

Para aprovechar la promesa sin caer en los peligros, hay que diseñar una arquitectura centrada en la privacidad y la equidad. La divulgación selectiva ha de permitir al estudiante decidir qué datos comparte con terceros; el control sobre sus credenciales ha de estar integrado en interfaces amigables que no requieran conocimientos técnicos avanzados. Además, las políticas institucionales han de incluir mecanismos de verificación descentralizada y auditorías independientes para garantizar que los proveedores mantengan unos estándares de seguridad robustos.

En resumen, la blockchain puede convertir la educación en un ecosistema donde títulos fiables y autoría justa sean la norma; pero solo si se protegen los datos personales, se alcanza equidad de acceso y se diversifica la infraestructura de confianza. Adoptar estas tecnologías ahora decidirá si nuestros sistemas educativos avanzan hacia una verdadera *trust-by-design* o se convierten en puntos débiles para el abuso y la discriminación.

Es hora de actuar

Las universidades y los centros de enseñanza superior son el primer frente donde la crisis de confianza se traduce en pérdidas concretas: diplomas falsos que llegan a las salas de operación ([3]), exámenes suplantados por deepfakes que amenazan la integridad de los procesos de selección ([4]) y una generación de estudiantes que, como hemos visto, ya el 92 % usa IA en sus tareas académicas, con un aumento de 35 puntos porcentuales en el uso para evaluaciones en solo un año ([1]). La solución no pasa por depender de detectores cada vez más sofisticados —que, como advierte TEQSA, son «poco fiables» y a menudo dejan al acusado con la posibilidad de negar su uso ([2])— sino por reconstruir el modelo de credencialización desde su núcleo.

1. Universidades y centros: emitir credenciales verificables

Adoptar los estándares abiertos como el W3C Verifiable Credentials Data Model 2.0 (mayo-2025) ([6]) permite que cada título académico se convierta en un «hash + transacción sellada» en la cadena de bloques, tal como demuestra el proyecto Blockcerts del MIT con 111 estudiantes pilotados en 2017 ([5]). Estas credenciales son inmutables, verificables al instante y compatibles con los sistemas de identidad digital europea (EBSI) que ya gestionan más de 76.000 certificados ([6]). Las universidades han de crear infraestructuras propias o unirse a redes federadas para emitir y registrar estos sellos, garantizando a la vez la privacidad de los estudiantes mediante la divulgación selectiva de datos.

2. Estudiantes e investigadores: sellar la prueba de existencia del propio trabajo

Cada artículo, proyecto o tesis ha de ser «timestamped» en una blockchain pública antes de su difusión. El mismo mecanismo que protege esta obra (hash + sello de tiempo) asegura la prioridad de autoría e impide la suplantación ([7]). Las plataformas de gestión de investigación han de integrar API que automaticen este proceso, ofreciendo al autor una prueba verificable que puede ser consultada por cualquier lector o revisor.

3. Empleadores y colegios profesionales: verificar credenciales al instante

Los procesos de contratación y acreditación han de incorporar consultas en tiempo real al registro blockchain de los títulos, eliminando la necesidad de llamadas telefónicas o documentos escaneados que se pueden falsificar. Esto reduce el riesgo de contratar profesionales con diplomas fraudulentos —un problema ya evidenciado por la Operation Nightingale ([3])— y aumenta la confianza en las competencias declaradas.

4. Reguladores y agencias de acreditación: reconocer estándares interoperables

Los organismos reguladores han de formalizar el reconocimiento oficial de las credenciales verificables, estableciendo marcos de cumplimiento que sean compatibles con eIDAS y otras normativas internacionales. Esto crea una capa de «trust-by-design» a escala macro, evitando la fragmentación del mercado educativo y asegurando que las nuevas tecnologías no se conviertan en puntos débiles para el abuso o la discriminación.

5. Plataformas educativas: integrar procedencia con privacidad

Los proveedores de aprendizaje en línea han de diseñar sistemas donde la propiedad intelectual del contenido y las credenciales de los usuarios se gestionen con divulgación selectiva, tal como recomienda el modelo de datos verificables. Esto permite que los estudiantes demuestren competencias sin revelar información personal innecesaria, alineando la privacidad con la transparencia.

Proteger la autenticidad del título y de la autoría es, en última instancia, defender el mérito mismo de la educación. Cada institución que adopte credenciales verificables y pruebas de existencia no solo refuerza la confianza de sus graduados, sino que contribuye a un ecosistema global donde la verdad académica se mantiene intacta ante las amenazas de la IA generativa. Es **time2act**: el futuro del aprendizaje depende de nuestra capacidad para construirlo hoy.

---

[1] HEPI — *Student Generative AI Survey 2025*. https://www.hepi.ac.uk/reports/student-generative-ai-survey-2025/ ↩

[2] TEQSA — *The evolving risk to academic integrity posed by generative AI* (2024). https://www.teqsa.gov.au/sites/default/files/2024-08/evolving-risk-to-academic-integrity-posed-by-generative-artificial-intelligence.pdf ↩

[3] U.S. DOJ — *Operation Nightingale: fraudulent nursing diplomas* (2023; Fase II 2025). https://www.justice.gov/usao-sdfl/pr/fraudulent-nursing-diploma-scheme-leads-federal-convictions ↩

[4] Open edX — *Proctoring in the age of AI: deepfake impersonation* (2025). https://openedx.org/blog/proctoring-in-the-age-of-ai-tackling-modern-cheating-techniques/ ↩

[5] MIT Technology Review — *Digital diplomas (Blockcerts)* (2018); MIT Registrar. https://www.technologyreview.com/2018/04/25/143311/digital-diplomas/ ↩

[6] European Commission — *EBSI Verifiable Credentials*; Europass *European Digital Credentials for Learning*; W3C VC Data Model 2.0. https://europass.europa.eu/en/european-digital-credentials-learning ↩

[7] ProofStamper / OriginStamp — *Proof of authorship via hash + timestamp*. https://proofstamper.com/en/compare/file-timestamp-tools-2026/ ↩

La verdad como arma: defensa y derechos humanos

«Juré no callar nunca, dondequiera y cuando quiera que seres humanos padezcan sufrimiento y humillación.»

— Elie Wiesel, discurso del Premio Nobel de la Paz (1986)

Era el 16 de marzo de 2022, tres semanas después de que las fuerzas rusas rompieran la frontera ucraniana e iniciaran una ofensiva que sacudía a toda Europa. Al alba, los teléfonos móviles de oficinas diplomáticas, las tabletas de los periodistas de guerra y las pantallas de medio país mostraban el mismo mensaje: un vídeo en el que el presidente Volodímir Zelenski aparecía pidiendo a sus soldados que «depongan las armas». La imagen, difundida por la cadena Ucrania 24 —que había sido pirateada aquella mañana— se proyectaba sobre el rótulo informativo de la estación de televisión y, simultáneamente, se incrustaba en su página web.

El clip era evidentemente una falsificación: resolución baja, contornos faciales difuminados y un tono de piel que no coincidía con el color natural del presidente. No obstante, en la frenética carrera informativa de una guerra activa, el vídeo se propagó por las redes sociales como una ola de desinformación, alimentando rumores y generando una primera señal de alarma: ningún líder del país llamaba a la rendición, y quizá había una ruptura interna que había que explotar.

En pocas horas, sin embargo, la respuesta oficial fue tan rápida como contundente. Zelenski publicó un vídeo —un instante ágil y auténtico donde se veía su rostro sin filtros— y, con voz clara, rechazó rotundamente la demanda: «No pensamos deponer ningún arma». El mensaje, difundido a través de los canales verificados de la Presidencia y retransmitido por las agencias internacionales, desactivó la falsificación en una jornada.

Aquel episodio se convierte hoy en el primer caso documentado de una «deepfake armada» —una falsificación audiovisual empleada directamente como arma psicológica dentro de un conflicto bélico en curso. Su impacto no se limitó a la confusión momentánea; demostró que quien controla la percepción de la verdad puede ganar una ventaja estratégica decisiva, alterando las decisiones militares y la confianza del pueblo. La guerra de información, como un frente invisible pero vital, demuestra que la verdad misma se convierte en un recurso escaso y disputado.

En este contexto, el desafío no es solo detectar los deepfakes una vez ya han circulado; la defensa duradera requiere autenticar las comunicaciones desde el momento de su creación y sellarlas con tecnologías como el hashing criptográfico y la blockchain, asegurando que cada declaración oficial, cada imagen de un testigo ocular, lleve una prueba inalterable de origen. Esta necesidad se convierte en el núcleo de nuestra propuesta: transformar la verdad en un arma defensiva para la defensa de los derechos humanos y la justicia internacional. [1]

El arma de la desinformación

En el último decenio, las operaciones de influencia han trascendido el simple envío de propaganda para convertirse en una arquitectura digital que manipula realidades y modela decisiones políticas a escala global. La campaña rusa conocida como «Doppelganger», por ejemplo, ha desplegado una red de bots y sistemas de inteligencia artificial capaces de clonar webs de medios y gobiernos occidentales, desvirtuando noticias y amplificando narrativas hostiles a Ucrania. Estas plataformas falsificadas aparecen en motores de búsqueda como resultados legítimos, engañando tanto a lectores casuales como a analistas profesionales. La Unión Europea, reconociendo la gravedad del fenómeno, ha impuesto sanciones contra las entidades vinculadas al proyecto, destacando que su objetivo no es solo desinformar sino erosionar la confianza en instituciones democráticas [2].

2024 ha marcado un punto de inflexión: una temporada electoral global que ha coincidido con la explosión de deepfakes en múltiples continentes. En Eslovaquia, días antes del voto, se difundió un audio falso atribuido a un líder político, alterando el discurso oficial e incitando al descontento social. En Estados Unidos, una llamada automatizada —un «robocall»— reproducía la voz clonada del presidente Joe Biden pidiendo explícitamente que los ciudadanos no emitieran su voto. La Federal Communications Commission (FCC) ha propuesto una multa de 6 millones de dólares al operador político responsable, Steve Kramer, por este intento de coacción electoral, un precedente que evidencia cómo las tecnologías de

síntesis vocal se convierten en armas de intimidación política [3]. En Moldavia y Taiwán, vídeos manipulados mostraban a la presidenta Maia Sandu y al candidato Lai Ching-te pronunciando declaraciones inexistentes, generando protestas y llamadas a la revocación que requirieron una respuesta institucional rápida.

Estos casos ilustran más que un simple «error de fact-check». El verdadero peligro es el que los expertos llaman el **«dividendo del mentiroso»**: cuando la capacidad de falsificar se vuelve omnipresente, el público empieza a dudar incluso de las pruebas verificadas. Esta corrosión de la fe en la evidencia crea un vacío donde cualquier afirmación —falsa o verdadera— puede ser descartada como manipulación potencial. En este contexto, la defensa de los derechos humanos se ve amenazada por una crisis de credibilidad: jueces internacionales, tribunales penales y organismos de investigación se encuentran incapaces de establecer la autenticidad de evidencias cruciales sin recursos tecnológicos avanzados.

La solución no reside únicamente en detectar deepfakes posteriores, sino en **autenticar las comunicaciones desde su origen**. La tecnología de hashing criptográfico y la inserción inmutable en blockchain ofrecen una pista verificable que puede ser consultada por cualquier parte interesada. Cuando un mensaje militar o una declaración oficial se registra con un hash único en el momento de su creación, cualquier alteración posterior es evidente y rechazada automáticamente por el sistema. Así, los actores malintencionados se ven desincentivados a crear falsificaciones, ya que la verdad documental queda «sellada» con una prueba de existencia incapaz de ser suprimida o manipulada.

En definitiva, el quinto frente —la defensa y los derechos humanos— se convierte en una batalla por preservar la confianza en la información. Solo adoptando protocolos que garanticen el origen y la integridad de los datos podremos contrarrestar el dividendo del mentiroso y transformar la verdad en un arma real contra la desinformación.

Órdenes falsas, mandos suplantados

En marzo de 2024 circuló un vídeo que parecía provenir directamente del jefe de la inteligencia militar ucraniana, Kirilo Budanov. Compuesto a partir de entrevistas previas con Budanov y con el secretario del Consejo de Seguridad y Defensa Nacional, el clip fabricaba una falsa «admisión» que atribuía a Ucrania el ataque contra la sala de conciertos Crocus City Hall. El material combinaba fragmentos de voz y de imagen reales con manipulaciones generadas por IA, hasta hacer que el resultado fuera casi indistinguible de la realidad. El episodio ilustra el peligro inminente que supone la tecnología del deepfake cuando una voz o una cara clonada se coloca sobre una orden o una confesión fabricada [4].

Esta vulnerabilidad no es solo un problema de confusión momentánea; tiene implicaciones estratégicas que pueden alterar el equilibrio de un conflicto. Una orden falsificada puede conducir a movimientos innecesarios, exponer fuerzas a emboscadas y, en el peor de los escenarios, desencadenar una escalada accidental de violencia. Por eso, la guía conjunta emitida por la NSA, el FBI y la CISA en 2023 identifica el Departamento de Defensa y la base industrial de defensa como objetivos prioritarios de ataques de suplantación, y recomienda dos ejes complementarios: (1) detectar deepfakes con herramientas avanzadas de análisis forense y (2) establecer la procedencia verificable de los medios utilizados para transmitir órdenes e informes [4].

El establecimiento de la procedencia se basa en el uso de identificadores criptográficos que aseguran que cada mensaje o documento ha sido firmado digitalmente por su emisor legítimo y que el hash resultante queda anclado a una cadena de bloques inmutable. Este modelo ya se ha puesto en práctica en proyectos como **eyeWitness to Atrocities**, donde una aplicación genera un hash criptográfico en tiempo real en el momento de la captura de evidencia, garantizando su integridad y la fecha de origen; más de 20.000 ítems verificables ya se han usado como prueba en casos judiciales [6]. De manera similar, el **Starling Lab** junto con Hala Systems ha enviado pruebas de crímenes de guerra a la Fiscalía de la CPI utilizando hash, blockchain, C2PA y Filecoin, creando un registro auditable que impide cualquier manipulación posterior [7].

El riesgo se extiende más allá del campo de batalla terrestre. La investigación sobre «deepfake geography» de 2021 demostró cómo se pueden crear imágenes satelitales sintéticas de aspecto realista, capaces de falsificar la presencia o la ausencia de actividades militares en zonas críticas [5]. El director de la National Geospatial-Intelligence Agency (NGA) ya había alertado en 2019 de que estos engaños podrían ser utilizados para ocultar movimientos de tropas, manipular negociaciones diplomáticas o justificar intervenciones armadas basadas en pruebas falsas. Si un gobierno se basa en una imagen satelital

manipulada para planificar una operación, el resultado puede ser una respuesta militar equivocada y la pérdida de vidas inocentes.

La solución, tal como proponen las autoridades norteamericanas, consiste en integrar sistemas de autenticación de extremo a extremo que combinen firmas digitales, anclaje en blockchain y protocolos de evaluación por parte de agencias certificadas independientemente. Solo con una cadena de confianza verificable desde el momento de la generación hasta el consumo final se puede garantizar que las órdenes militares no sean instrumentos de engaño, sino instrumentos fiables de una defensa responsable. En este escenario, la verdad deja de ser un lujo y se convierte en el arma más poderosa contra la desinformación bien armada.

La verdad como prueba: derechos humanos

En una tarde de octubre de 2023, en el centro de mando avanzado cerca de Járkov, un equipo del Starling Lab y Hala Systems recibió una carga digital aparentemente ordinaria. El archivo incluía miles de metadatos —marcas de tiempo, coordenadas GPS precisas, hash criptográfico generado en el momento y un enlace a la red descentralizada Filecoin donde se guardaría el contenido. No era solo un documento; era la materialización del modelo **t2p**, un registro inmutable desde el primer instante, capaz de impedir cualquier intento de manipulación.

El protocolo se basó en el precedente establecido por la aplicación *eyeWitness to Atrocities*, creada en 2015 por la International Bar Association junto con LexisNexis. Cada imagen o vídeo capturado se transforma de inmediato en un hash criptográfico, acompañado de metadatos de tiempo y coordenadas GPS; este hash sube a una cadena de confianza verificable y cualquier alteración rompe la asociación hash-archivo, revelando la falsificación con una claridad que los tribunales tradicionales no pueden ofrecer [6]. Hasta ahora se han enviado más de 20.000 ítems a la Comisión de Investigación de las Naciones Unidas, convirtiéndose en pruebas verificables en procesos judiciales relacionados con el conflicto ucraniano.

Cuando estos elementos se combinaron con la infraestructura blockchain del Starling Lab, el impacto fue exponencial. El dosier presentado a la Fiscalía de la Corte Penal Internacional (CPI) en 2022 incluía evidencias de presuntos crímenes de guerra en Járkov: publicaciones y vídeos de ataques indiscriminados, con los metadatos registrados y un hash para cada ítem. Cada pieza estaba anclada en una cadena inmutable, preservada en Filecoin según los estándares de procedencia **C2PA** y alineada con el **Protocolo de Berkeley**, adoptado en 2020 como referente global para pruebas digitales de organismos como el OHCHR [7].

Esta arquitectura no solo garantiza autenticidad, sino que crea un escudo legal que impide la manipulación informativa. En la CPI, una orden de arresto de 2017 ya había mostrado que las pruebas recogidas en las redes sociales podían ser la base de una acusación formal; ahora, con hash y blockchain, la prueba alcanza un nivel de certidumbre que supera cualquier duda sobre su integridad. La verdad deja de ser una narración subjetiva y se convierte en **un arma legal**: cada fragmento de realidad queda sellado desde el momento de la captura, inalterable hasta el tribunal.

El mensaje es claro: el modelo *t2p* no es solo una solución técnica, sino un mecanismo de defensa para derechos humanos en la era de las deepfakes y la guerra de información. Codificar la verdad con hash y anclarla a una cadena inmutable constituye una barrera infranqueable contra la falsificación que podría desencadenar pánico o justificar atrocidades, y ya ha demostrado ser capaz de salvaguardar la justicia y garantizar una voz auténtica e inalterable para las víctimas.



Figura 20.1 — Captura con hash en el origen → metadatos y geolocalización → anclaje inmutable → prueba admisible: la cadena que convierte un testimonio digital en evidencia.

La defensa responde

Las agencias de inteligencia y los aliados de la OTAN se dieron cuenta pronto de que la simple detección de deepfakes solo constituye una primera línea de defensa. El programa MediFor, impulsado por DARPA, estableció un marco para validar la integridad de imágenes y vídeos mediante análisis forenses avanzados; pero su éxito se vio limitado cuando las redes neuronales generativas empezaron a producir contenido indistinguible del original en cuestión de días. En paralelo, SemaFor —el complemento de forense

semántica— culminó en 2024 con un catálogo abierto de herramientas para la detección, atribución y caracterización de material manipulado [8], y la NATO StratCom COE mantiene una vigilancia continua sobre las nuevas técnicas de engaño digital [8].

Lo que estas iniciativas demuestran es un principio fundamental: **la detección posterior no puede revertir los daños causados por una información falsificada que ya ha circulado**. Como hemos visto con el deepfake de la «rendición» de Zelenski del 16 de marzo de 2022, un vídeo falso generó pánico e influyó en las operaciones militares antes de que cualquier herramienta forense pudiera confirmarla [1]; de manera similar, la campaña rusa «Doppelganger», que clona webs de medios occidentales con bots e IA para difundir noticias manipuladas, ha sido sancionada por la UE pero sigue demostrando que **la propagación previa a la identificación** es el verdadero motor del daño [2].

Por eso hay que **autenticar las comunicaciones y las pruebas desde el momento de su creación**, una práctica ya probada en el campo de los derechos humanos. La aplicación del hash criptográfico en el origen, tal como lo hace la app eyeWitness to Atrocities —que genera un resumen único e inmutable en tiempo real durante la captura de evidencia visual— ha permitido que más de 20.000 ítems sean verificables en casos judiciales, estableciendo un precedente directo para el concepto de «t2p» [6]. Este modelo se ha escalado a iniciativas como Starling Lab y Hala Systems, que presentaron a la Fiscalía de la CPI documentos de atrocidades con hash, blockchain y el marco C2PA, convirtiendo las pruebas en un registro inalterable y legalmente reconocible [7].

La respuesta institucional ha de evolucionar hacia una **estrategia de sellado preventivo**: cada transmisión militar, cada informe de inteligencia y cada testigo ocular se codifica con una firma digital que se registra de inmediato en una cadena inmutable. Esto impide la manipulación posterior y ofrece a jueces e investigadores un rastro verificable de procedencia —una prueba que no puede ser desmentida por el último modelo generativo.

En este contexto, el reto público establecido por SemaFor en 2024 se convierte en una llamada a la acción: **desarrollar y desplegar estándares abiertos de sellado de origen** compatibles con las infraestructuras blockchain globales. Hay que integrar estos protocolos en la cadena de mando y control (C2), asegurando que cada orden y cada informe operativo lleve una capa de autenticidad criptográfica desde el primer byte.

Así, el frente más impactante —la defensa contra la falsificación en tiempo de guerra— no se basa únicamente en detectar mentiras, sino en impedir que las mentiras **prosperen**. La verdad, codificada y anclada a una cadena inmutable, se convierte en el arma más poderosa para preservar los derechos humanos y garantizar la responsabilidad en un mundo donde la información puede ser fabricada con una sola pulsación de botón.

La promesa y el peligro

En las zonas de conflicto la verdad se convierte en un bien escaso, pero la tecnología puede convertirla en un arma imparable: la autenticación criptográfica garantiza que las órdenes en el frente sean genuinas y que las pruebas de atrocidades se puedan presentar ante los tribunales sin duda sobre su integridad. El proyecto *eyeWitness to Atrocities* (IBA + LexisNexis) ya genera un hash criptográfico en el momento de la captura y enlaza los metadatos a una cadena inmutable; más de 20.000 ítems verificados se han usado como evidencia en Ucrania, estableciendo un precedente para el marco *t2p* [6]. De manera similar, Starling Lab y Hala Systems han enviado pruebas de presuntos crímenes de guerra a la Fiscalía de la CPI con hash y blockchain, empleando estándares como C2PA y Filecoin; el Protocolo de Berkeley adoptado por el OHCHR (2020) ya preveía esta cadena de confianza [7].

Esta infraestructura no solo refuerza los tribunales, sino que impide que las potencias militares construyan pretextos falsificados para iniciar o prolongar conflictos. El deepfake de la «rendición» de Zelenski, difundido el 16 de marzo de 2022 y desmentido en horas, muestra cómo una manipulación audiovisual puede generar pánico antes de que las autoridades reaccionen [1]; si cada transmisión fuera firmada digitalmente, el impacto de estas falsificaciones se reduciría drásticamente. Lo mismo vale para la suplantación de mandos, como el deepfake del jefe de inteligencia ucraniano Budanov (2024); las recomendaciones de NSA/FBI/CISA (2023) para establecer la procedencia y la autenticidad en las comunicaciones defensivas son ahora más relevantes que nunca [4].

Sin embargo, la amenaza vinculada a esta capacidad de autenticación es profunda: la codificación y el anclaje de metadatos a una cadena inmutable pueden desanonimizar a testigos, víctimas y periodistas en

zonas de guerra si no se disponen las salvaguardas adecuadas. Un registro que revele la ubicación geográfica o la hora exacta de una grabación puede costar vidas, especialmente cuando los regímenes autoritarios tienen recursos para rastrear y perseguir disidentes. Además, estos gobiernos podrían instrumentalizar la tecnología para conferir un «sello oficial» a propaganda fabricada, como demuestra la campaña rusa «Doppelganger», que clona webs de medios occidentales con bots e IA, sancionada por la UE pero todavía capaz de usar tecnologías de verificación para legitimar falsedades [2].

Para equilibrar esta dualidad hace falta un diseño centrado en la seguridad y la privacidad. La divulgación selectiva debería permitir que solo las partes autorizadas accedan a metadatos sensibles, manteniendo la transparencia necesaria para la verificación judicial. Los protocolos han de incluir mecanismos de control del testigo, como claves temporales o credenciales descentralizadas revocables en caso de compromiso. Solo con este marco éticamente consciente y maduro podremos aprovechar la promesa de una verdad inmutable sin caer en el peligro de un control totalitario de la información.

Es hora de actuar

Las fuerzas armadas y las agencias de seguridad ya no pueden confiar únicamente en la voz del mando; han de **autenticar cada transmisión** antes de que llegue al campo de batalla. El caso del deepfake del jefe de inteligencia ucraniano Budanov, que en 2024 intentaba fabricar una falsa atribución de un ataque, ha demostrado que la falta de un mecanismo de verificación puede desencadenar decisiones estratégicas erróneas y aumentar el riesgo de escalada [4]. Por eso, las fuerzas han de incorporar firmas digitales basadas en claves temporales y credenciales descentralizadas, tal como recomiendan la NSA, el FBI y la CISA para la procedencia de las comunicaciones militares (2023). Cada orden y cada informe de inteligencia ha de llegar con un **hash criptográfico verificable** que garantice el origen y la integridad del mensaje antes de ser ejecutado.

Las organizaciones de derechos humanos y los periodistas son el frente más vulnerable a las manipulaciones. La aplicación *eyeWitness to Atrocities*, desarrollada por la IBA y LexisNexis, ha demostrado que un **hash generado en el momento de la captura** puede proporcionar una prueba de existencia inmutable; más de 20.000 ítems ya se han usado como evidencia fiable en tribunales ucranianos [6]. Este modelo ha de ser adoptado globalmente: cada foto, vídeo o testimonio grabado en zonas de conflicto ha de estar de inmediato sellado con una cadena de bloques pública y verificable. Las organizaciones han de invertir en equipos móviles que integren la tecnología C2PA y Filecoin, tal como lo hicieron Starling Lab y Hala Systems para la CPI en 2022 [7], asegurando que la fuente sea protegida pero la prueba no se pueda falsificar.

Los tribunales y las fiscalías han de ir más allá de la aceptación pasiva. Han de establecer **protocolos obligatorios** basados en el Protocolo de Berkeley (OHCHR, 2020) que exijan pruebas con hash y blockchain para cualquier documentación relacionada con crímenes de guerra. Esto implica crear guías operativas para jueces y fiscales, capacitaciones especializadas y una infraestructura judicial digital capaz de validar las pruebas en tiempo real. La primera orden de arresto basada principalmente en redes sociales (al-Werfalli, 2017) ya ha mostrado cómo las evidencias digitales pueden ser decisivas; ahora hace falta un marco formalizado para garantizar su admisibilidad y autenticidad.

Las plataformas de difusión —desde X hasta TikTok— han de asumir una responsabilidad proactiva en la preservación de la procedencia del contenido relacionado con conflictos; hay que integrar sistemas que registren metadatos, marcas de tiempo y hashes al subir un vídeo o una imagen y ofrecer herramientas para verificadores independientes. La normativa europea ya ha sancionado campañas de suplantación como la «Doppelganger» rusa [2]; las plataformas han de ir más allá del simple bloqueo y garantizar transparencia total sobre el origen del material.

Cada usuario, como primer filtro, ha de aprender a verificar antes de compartir imágenes o audios de guerra, empleando aplicaciones que muestren los hashes y la cadena de bloques asociada. El deepfake de rendición de Zelenski en 2022 —desmentido en horas pero capaz de alimentar rumores masivos— demuestra cómo la ausencia de verificación puede crear pánico y legitimar acciones violentas [1].

Los responsables políticos han de legislar estándares claros para la seguridad y la salvaguarda de estas tecnologías, estableciendo marcos éticos que impidan un control totalitario de la información mientras fomentan una verdad inmutable. **Time2act** no es solo un lema: es una llamada urgente para que la prueba de existencia sea el fundamento de la justicia y la paz.

[1] NPR — *Zelenskyy deepfake telling Ukrainians to surrender* (16-mar-2022). https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia ↩

[2] EU DisinfoLab — *Doppelganger* (campaña de desinformación rusa). https://www.disinfo.eu/doppelganger-hub/ ↩

[3] FCC — *Proposed $6M fine for AI-deepfake Biden robocall* (2024); IPI (Eslovaquia). https://www.fcc.gov/document/fcc-proposes-6m-fine-nh-robocalls ↩

[4] CISA / NSA / FBI — *Contextualizing Deepfake Threats to Organizations* (2023). https://www.cisa.gov/news-events/alerts/2023/09/12/nsa-fbi-and-cisa-release-cybersecurity-information-sheet-deepfake-threats ↩

[5] University of Washington — *Deepfake geography: AI falsifies satellite images* (Bo Zhao, 2021). https://www.washington.edu/news/2021/04/21/a-growing-problem-of-deepfake-geography-how-ai-falsifies-satellite-images/ ↩

[6] International Bar Association — *eyeWitness to Atrocities* (hash en la captura; casos en Ucrania). https://www.ibanet.org/IBA-founded-eyeWitness-to-Atrocities-marks-ten-years-of-capturing-evidence-of-human-rights-crimes ↩

[7] USC Shoah Foundation — *Starling Lab & Hala Systems file cryptographic war-crimes evidence to the ICC* (2022); Protocolo de Berkeley (OHCHR). https://sfi.usc.edu/news/2022/06/33571-starling-lab-and-hala-systems-file-cryptographic-submission-evidence-war-crimes ↩

[8] DARPA — *Semantic Forensics (SemaFor)* y *Deepfake Defense* (2024); NATO StratCom COE. https://www.darpa.mil/research/programs/semantic-forensics ↩

Créditos de carbono: el mercado del cumplimiento

«Un objetivo central de la política pública debería ser facilitar el desarrollo de instituciones que saquen lo mejor de los seres humanos.»

— Elinor Ostrom, lección Nobel (2009)

La mañana del 19 de enero de 2011, los operadores de medio continente encontraron la misma respuesta en sus pantallas: *transferencia no disponible*. No era una avería informática. Era una decisión deliberada de la Comisión Europea, que aquel día pulsó el botón de apagado del mercado de carbono más grande del mundo. Durante las semanas anteriores, unos atacantes habían vaciado cuentas de varios registros nacionales —Austria, la República Checa, Grecia, Estonia y Polonia— mediante correos de *phishing* y troyanos que robaban contraseñas. En pocos días desaparecieron más de dos millones de derechos de emisión, valorados en unos 28-30 millones de euros; el registro checo fue el más castigado, con pérdidas de unos 7 millones [11]. Aquellos derechos representaban toneladas reales de CO_2 que alguien tenía la obligación legal de compensar, y habían volado con un solo clic hacia cuentas de Alemania, Estonia y el Reino Unido.

La Comisión no tuvo más remedio que suspender las transferencias a **todos** los registros nacionales a la vez y reabrirlos de manera escalonada, solo cuando cada uno cumpliera unos mínimos de seguridad [11]. Durante días, el principal instrumento climático de Europa —un mercado que mueve decenas de miles de millones de euros— quedó congelado porque su verdad vivía en bases de datos que se podían vaciar de madrugada. La paradoja era cruel: un sistema diseñado para salvar el clima había sido secuestrado por un robo de lo más corriente.

Aquel apagado es la mejor puerta de entrada a una pregunta incómoda. Si el carbono tiene precio —y lo tiene—, ¿quién garantiza que la tonelada que se compra, se vende o se compensa existió de verdad, una sola vez, y que nadie la ha alterado después? Este capítulo trata del **mercado del cumplimiento**: los sistemas obligatorios que ponen precio a las emisiones. Funcionan, mueven el capital y ya han hecho bajar emisiones. Pero su integridad no depende del precio, sino de algo más humilde y más frágil: la confianza en los datos.

Poner precio al aire

El corazón del mercado europeo es el régimen de comercio de derechos de emisión (EU ETS), un esquema de cap-and-trade o «límite y comercio». La idea es sencilla y elegante: el estado fija un techo decreciente sobre el total de gases que se pueden emitir y reparte o subasta derechos —las llamadas EUA, European Union Allowances— en las que cada derecho equivale a una tonelada de CO_2 equivalente. Quien contamina menos de lo que le corresponde puede vender los derechos sobrantes; quien contamina más, ha de adquirirlos. El precio recompensa a quien se descarboniza y penaliza a quien se retrasa.

Veinte años después de que Paul Roberts, periodista y analista de energía, describiera en *The End of Oil* (2004) los mercados energéticos como una gran bolsa donde los precios arbitraban entre la oferta y la demanda, el ETS es quizá el mercado más ambicioso jamás construido sobre una abstracción: el derecho a no emitir. Como hemos visto, cubre aproximadamente el 40 % de las emisiones de gases de efecto invernadero de la UE y ha recaudado más de 175.000 millones de euros desde 2013. El sistema —electricidad, calor, industria pesada, aviación y, desde enero de 2024, el transporte marítimo— ha contribuido a reducir las emisiones de los sectores cubiertos alrededor de un 47 % respecto a 2005. El techo revisado apunta a una reducción del 62 % en 2030 en comparación con aquel año [1].

El precio de la tonelada, que durante años fue demasiado bajo para mover nada, hoy ya muerde; a mediados de 2026 cotizaba alrededor de los **80 euros**, tras haber llegado a casi **106 euros en febrero de 2023** [2]. Para que esta señal no se hunda cuando sobran derechos, la UE mantiene una **Reserva de Estabilidad del Mercado** que retira el excedente de circulación [5]; y para evitar la fuga de carbono hacia países sin precio del carbono, en 2026 ha entrado en escena la pieza más nueva y discutida: el **Mecanismo de Ajuste en Frontera por Carbono** (CBAM).

El CBAM estrenó su **fase definitiva el 1 de enero de 2026** [3] y hace pagar a las importaciones de productos intensivos en carbono —hierro y acero, aluminio, cemento, fertilizantes, electricidad e hidrógeno— el mismo precio de CO_2 que ya paga la industria europea. El primer precio trimestral del

certificado CBAM, publicado el 7 de abril de 2026, se fijó en **75,36 euros por tonelada**, calculado a partir de la media de las subastas de EUA del primer trimestre [4]. Las ventas y entregas de certificados no comienzan hasta febrero de 2027 y la primera declaración vence el 30 de septiembre de aquel año; un umbral mínimo de 50 toneladas al año libera al 90 % de los importadores pequeños, pero mantiene cubierto el 99 % de las emisiones incorporadas [4]. Paralelamente, la asignación gratuita de derechos a la industria se irá retirando a medida que el CBAM coja fuerza, y en la aviación ya desaparece en 2026 [5].

El **ETS2**, el nuevo mercado pensado para poner precio al carbono de los edificios y del transporte por carretera, se ha **aplazado hasta 2028**: el acuerdo político se selló en noviembre de 2025, en el marco del objetivo climático europeo para 2040, y la formalización llegó a principios de 2026 [6]. Más allá de Europa, la aviación internacional tiene su propio esquema, el **CORSIA** de la Organización de Aviación Civil Internacional: solo en 2024, los vuelos internacionales emitieron cerca de **597 millones de toneladas** de CO_2 y el sector quedó obligado a compensar unas **58 millones** [7]. Tres mercados, tres diseños diferentes; un mismo talón de Aquiles.

El crimen que secuestró el clima

Para que un mercado como este exista, una tonelada de CO_2 ha de poder cambiar de manos tan rápidamente como una acción en bolsa. Aquí reside la vulnerabilidad: un derecho de emisión es un activo puramente digital, sin peso ni textura, que se transfiere en segundos entre cuentas de toda Europa. Esta liquidez, virtuosa para el mercado, resultó ser una tentación irresistible para el crimen organizado.

Entre 2008 y 2010, una oleada de **fraude carrusel del IVA** —lo que los investigadores llaman *missing trader fraud*— infectó el mercado. El esquema era tan viejo como el comercio mismo: un defraudador compra derechos en un país sin IVA, los vende en otro cobrando el impuesto y desaparece sin ingresarlo en Hacienda, repitiendo la operación en círculo. La agencia policial europea **Europol** calculó que este fraude causó **más de 5.000 millones de euros** de pérdidas a los contribuyentes europeos y, como hemos visto, en algunos países el fraude podía llegar a casi todo el volumen del mercado [9]. El epicentro fue la bolsa francesa BlueNext, que ofrecía reembolso inmediato del IVA y vio cómo la actividad se disparaba allí a finales de 2008. En Alemania, la fiscalía cifró el agujero en unos **850 millones de euros** y, en diciembre de 2011, un tribunal condenó a seis personas a penas de entre tres y siete años y diez meses de prisión [11].

Quien mejor ha reconstruido aquel episodio es **Marius-Christian Frunza**, doctor en matemáticas por la Sorbona y antiguo responsable de estructuración en el brazo de materias primas de la Caisse des Dépôts francesa, hoy investigador del fraude financiero. En su libro *Fraud and Carbon Markets: The Carbon Connection* (Routledge, 2013) y en el artículo académico *An Assessment of Carousel VAT Fraud in the European Carbon Market* (2014), Frunza demuestra con estadística forense que la **velocidad de transferencia de un activo intangible y sin trazabilidad** lo convirtió en el vehículo perfecto para el carrusel [10]. La lección es incómoda: un mercado construido sobre simples apuntes contables, sin una capa que selle la evidencia, es vulnerable desde el origen. El robo de 2011 con el que se abría este capítulo no fue una anomalía; fue el segundo acto de una misma obra.

El regulador y la cadena de la verdad

Ante estos agujeros, la respuesta reguladora ha sido construir una arquitectura de control cada vez más exigente. Toda la credibilidad del ETS descansa en un acrónimo: **MRV**, de *Monitoring, Reporting and Verification* —seguimiento, notificación y verificación. Dos reglamentos lo sustentan, el de Seguimiento y Notificación (MRR) y el de Acreditación y Verificación (AVR), que obligan a cada instalación a medir sus emisiones, a redactar un informe y a hacerlo validar por un **verificador acreditado** independiente antes del 31 de marzo de cada año [8].

Vista de cerca, toda esta maquinaria es, en el fondo, una larga **cadena de afirmaciones de datos**. ¿Cuántas toneladas emitió aquella central? ¿Cuánto CO_2 lleva incorporado el acero que cruza la frontera con un certificado CBAM? ¿Cuánto carbono quemó aquel vuelo? Cada eslabón de la cadena es un documento —una lectura de sensor, una hoja de cálculo, un informe en PDF, un certificado— que viaja de mano en mano hasta llegar al regulador. Y cada documento es, a la vez, un punto donde la verdad se puede romper: por error, por negligencia o, como hemos visto, por dolo.

El problema es que las herramientas tradicionales para proteger esta cadena —metadatos, sellos corporativos, la auditoría anual, la fe en el registro central— son exactamente las que la digitalización ha

debilitado. Un PDF se puede editar; una hoja de cálculo, retocar; un registro central se puede piratear y, entonces, hay que apagarlo entero. La integridad del mercado del carbono se enfrenta al mismo dilema que recorre todo este libro: en un mundo donde las pruebas se pueden fabricar, **demostrar que un dato existió, intacto, en una fecha cierta** ya no es un trámite, sino la base de todo.

Pruebas que se pueden editar

Imaginemos una instalación industrial que prepara su informe anual de emisiones. El técnico descarga las lecturas de los sensores, las vuelca en una hoja de cálculo, aplica los factores de conversión y genera un PDF que el verificador firmará. Entre la lectura del sensor y la firma del verificador hay una docena de pasos en los que el número se puede «ajustar»: un decimal aquí, una hora de funcionamiento que se olvida allá. No hace falta imaginar una conspiración; basta con la presión de cerrar el ejercicio con menos toneladas de las reales, porque cada tonelada ahorrada es un derecho que se puede vender.

El verificador hace su trabajo con rigor, pero trabaja con lo que le dan: documentos que ya han pasado por manos interesadas y que nada impide retocar a posteriori. Si mañana surge una disputa —una inspección, un litigio, una sospecha de doble contabilización entre dos registros nacionales—, ¿cómo se demuestra cuál era la lectura **original** del sensor, antes de cualquier ajuste? La respuesta honesta, hoy, a menudo es que no se puede. La cadena de custodia del dato climático es tan débil como la de cualquier archivo digital. Y un mercado que mueve miles de millones sobre datos que no se pueden auditar hasta el origen es un mercado que invita al fraude.

La prueba de existencia como capa de confianza del carbono

Aquí es donde la **prueba de existencia** —la tecnología que vertebra *time2act* a través de **t2p**— entra en escena, no como bala de plata, sino como un eslabón que faltaba. La idea es atacar el problema allí donde nace: en lugar de confiar en que nadie tocará el dato después, se sella el dato en el momento exacto en que se genera.

El mecanismo es el mismo que ya conocemos de otros capítulos, aplicado ahora al carbono. El informe MRV verificado, la lectura bruta de un sensor de emisiones, el cálculo de las emisiones incorporadas de un producto CBAM o el certificado de una unidad CORSIA reciben, en origen, una **huella criptográfica SHA-512** calculada en el propio dispositivo. Esta huella se ancla a la cadena pública; complementariamente, un **sello de tiempo RFC 3161** conforme a la normativa europea eIDAS, independiente de la cadena, añade la certificación de una autoridad; a partir de aquel instante cualquier alteración posterior del PDF, de la hoja de cálculo o del registro del sensor se detecta de inmediato. Para las auditorías de campo —la inspección de una instalación o la comprobación de un proyecto de compensación—, el **GPS forense** y la **prueba de vida** añaden una capa más: sellan *dónde* y *cuándo* se tomó la muestra o la fotografía y ligan la evidencia a una persona real presente, haciendo mucho más difícil el clásico «informe de escritorio» fabricado desde un despacho.

Y todavía hay un detalle decisivo, que conecta directamente con enero de 2011 —como hemos visto—. La evidencia se puede empaquetar en un **contenedor .asice**, un formato verificable *offline*: un regulador o un comprador de acero sujeto al CBAM puede comprobar la integridad de toda la cadena **sin depender del registro central**. Es decir, sin el punto único de fallo que aquel día se había tenido que apagar. La confianza deja de vivir en una sola base de datos vulnerable y pasa a ser comprobable por cualquiera.

No es una idea marginal. El **Banco Mundial**, a través de su programa Climate Warehouse y de la plataforma **Climate Action Data Trust** —desarrollada con el gobierno de Singapur y la asociación internacional del comercio de emisiones—, ya construye exactamente esto: una capa de datos común y a prueba de manipulación, apoyada en tecnología de registro distribuido, que armoniza la información entre registros nacionales para impedir el **doble cómputo** de un mismo crédito [12]. La tesis del Banco Mundial es nítida: la integridad de los mercados de carbono de la era post-París depende de una infraestructura de datos compartida que la simple contabilidad en hojas de cálculo nunca podrá ofrecer [12].

Conviene, sin embargo, ser honesto con los límites, fieles a la dualidad de **«la promesa y el peligro»** que Don Tapscott, coautor de *Blockchain Revolution* (2016), usa para pensar la tecnología. La prueba de existencia garantiza que un dato no se ha tocado *después* de sellarlo y, combinada con un registro distribuido, ayuda a impedir el doble cómputo. Pero **no** valida que el sensor estuviera bien calibrado ni que la medición inicial fuera cierta: «basura a la entrada, basura en la cadena». Tampoco habría detenido

el fraude carrusel del IVA, que era un problema fiscal, no de integridad del dato. El sello no sustituye la auditoría ni el sentido común; solo hace que, cuando haga falta, la verdad del origen se pueda demostrar.

La promesa y el peligro

La promesa es tangible. Un mercado del carbono con evidencia sellada en el origen sería mucho más resistente al fraude, haría las auditorías más rápidas y baratas, y permitiría que un comprador, un inversor o un ciudadano comprobara por sí mismo que una tonelada compensada existió de verdad. En un sistema que ya mueve más de 175.000 millones de euros, como hemos visto, recuperar esta confianza no es un lujo: es la condición para que el precio del carbono haga el trabajo para el que fue inventado.

El peligro, como siempre, pide matiz. Una capa técnica mal diseñada puede generar una falsa sensación de seguridad —el sello certifica el *cuándo* y el *qué*, no la verdad física de la medición—. La concentración de la verificación en pocas manos, o en una sola plataforma, recrearía el mismo punto único de fallo que queremos evitar. Y la trazabilidad total, mal gobernada, puede chocar con la confidencialidad comercial legítima de las empresas. La prueba de existencia es una capa **necesaria** dentro de una arquitectura de confianza más amplia, no un atajo que nos ahorre la gobernanza.

Es hora de actuar

Para los operadores de instalaciones sujetas al ETS: sellar las lecturas de los sensores y los informes MRV en origen, antes de cualquier tratamiento, para que el dato original sea siempre demostrable. Para los importadores sujetos al CBAM: anclar el cálculo de las emisiones incorporadas de sus productos, de manera que la cifra declarada en la frontera sea auditable hasta la fábrica. Para los verificadores acreditados: exigir pruebas de existencia como parte de la cadena de custodia y no aceptar documentos que se hayan podido editar después de generarse. Para los gestores de los registros y los reguladores: avanzar hacia una capa de datos distribuida e interoperable —en la línea del Climate Action Data Trust— que haga imposible apagar todo el mercado con un solo clic, y reconocer legalmente el valor probatorio del sello.

Como vimos el 19/01/2011, Europa tuvo que apagar su mercado de carbono porque la verdad se encontraba en lugares que se podían vaciar de madrugada. Quince años después disponemos de las herramientas para evitarlo; el precio del carbono solo funcionará si podemos confiar en cada tonelada que entra en él, y demostrar esa confianza es time2act.

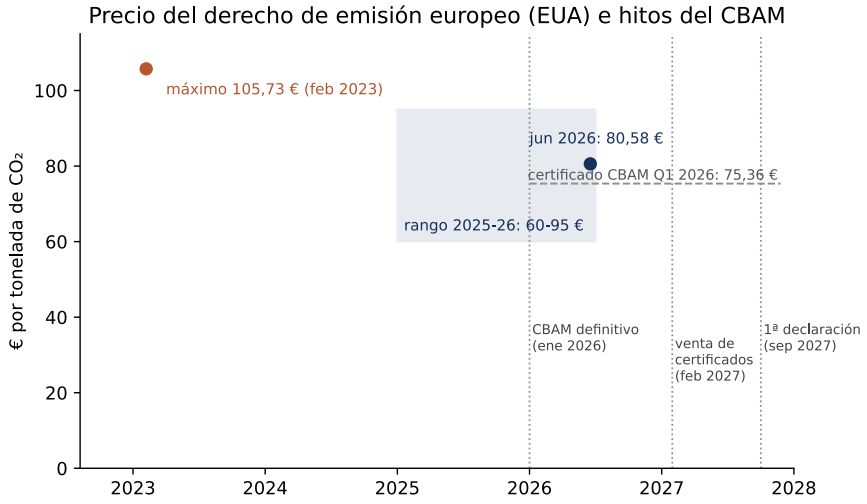


Figura 21.1 — El precio del derecho de emisión europeo (EUA) escaló hasta un máximo de 105,73 € en febrero de 2023 y se movía alrededor de los 80 € a mediados de 2026; en paralelo, el CBAM entró en fase definitiva el 1 de enero de 2026, con un primer certificado fijado en 75,36 €/t. Fuentes: Trading Economics; Comisión Europea; S&P Global.

[1] Comisión Europea — *About the EU Emissions Trading System* (cobertura ~40 %, 175.000 M€ recaudados, −47 % vs 2005, −62 % en 2030). https://climate.ec.europa.eu/eu-action/carbon-markets/about-eu-ets_en ↩

[2] Trading Economics — *EU Carbon Permits* (EUA 80,58 €/t el 19-jun-2026; máximo histórico 105,73 € en feb-2023). https://tradingeconomics.com/commodity/carbon ↩

[3] Comisión Europea (Taxation and Customs Union) — *Carbon Border Adjustment Mechanism (CBAM)* (fase definitiva desde el 1-ene-2026). https://taxation-customs.ec.europa.eu/carbon-border-adjustment-mechanism_en ↩

[4] S&P Global — *Brussels confirms first CBAM certificate price for Q1 2026 at €75.36/tCO2e* (7-abr-2026). https://www.spglobal.com/energy/en/news-research/latest-news/energy-transition/040726-brussels-confirms-first-cbam-certificate-price-for-q1-2026-at-eur7536mtco2e ↩

[5] International Carbon Action Partnership (ICAP) — *EU Emissions Trading System (EU ETS)* (MSR, factor CBAM, asignación gratuita). https://icapcarbonaction.com/en/ets/eu-emissions-trading-system-eu-ets ↩

[6] Comisión Europea — *ETS2: buildings, road transport and additional sectors* (inicio aplazado a 2028; acuerdo nov-2025). https://climate.ec.europa.eu/eu-action/carbon-markets/ets2-buildings-road-transport-and-additional-sectors_en ↩

[7] EASA — *ICAO CORSIA* (emisiones internacionales 2024 ≈ 597 $MtCO_2$; ≈ 58 $MtCO_2$ a compensar). https://www.easa.europa.eu/en/domains/environment/icao-carbon-offsetting-and-reduction-scheme-international-aviation-corsia ↩

[8] Comisión Europea — *Monitoring, reporting and verification of EU ETS emissions* (MRR y AVR; informe verificado antes del 31 de marzo). https://climate.ec.europa.eu/eu-action/carbon-markets/eu-emissions-trading-system-eu-ets/monitoring-reporting-and-verification_en ↩

[9] Europol — *Carbon Credit fraud causes more than 5 billion euros damage for European Taxpayer* (hasta el 90 % del volumen fraudulento en algunos países). https://www.europol.europa.eu/media-press/newsroom/news/carbon-credit-fraud-causes-more-5-billion-euros-damage-for-european-taxpayer ↩

[10] Marius-Christian Frunza — *Fraud and Carbon Markets: The Carbon Connection* (Routledge, 2013) y *An Assessment of Carousel VAT Fraud in the European Carbon Market* (Review of Law & Economics, 2014). https://www.routledge.com/Fraud-and-Carbon-Markets-The-Carbon-Connection/Frunza/p/book/9781138928091 ↩

[11] Comisión Europea — *Announcement: transitional measure for the EU ETS registry system* (19-ene-2011) y OCCRP — *Germany: Six Executives Stand Trial for Emissions Fraud* (~850 M€; seis condenados). https://climate.ec.europa.eu/news-your-voice/news/announcement-transitional-measure-eu-ets-registry-system-2011-01-19_en · https://www.occrp.org/en/news/germany-six-executives-stand-trial-for-emissions-fraud ↩

[12] Banco Mundial — *Why data infrastructure is key for a transparent carbon market* y plataforma *Climate Action Data Trust*. https://blogs.worldbank.org/en/climatechange/why-data-infrastructure-key-transparent-carbon-market · https://climateactiondata.org/ ↩

El mercado voluntario del carbono: promesa, fraude y la carrera por la integridad

«Si, como la verdad, la mentira no tuviera más que un rostro, estaríamos en mejores términos… Pero el reverso de la verdad tiene cien mil figuras y un campo indefinido.»

— Michel de Montaigne, Ensayos, I, 9 («De los mentirosos», 1580)

El 18 de enero de 2023, tres redacciones —*The Guardian* en Londres, *Die Zeit* en Hamburgo y el colectivo de investigación *SourceMaterial*— publicaron a la vez el resultado de nueve meses de trabajo. Habían cruzado estudios satelitales con trabajo de campo y con la ciencia académica para responder a una pregunta aparentemente técnica: los créditos de carbono que las grandes marcas compran para declararse «neutras», ¿funcionan de verdad? La conclusión sacudió a todo un sector. Más del **90 % de los créditos de selva tropical** certificados por Verra —el mayor estándar del mundo— eran probablemente **«créditos fantasma»**: no representaban ninguna reducción real de emisiones [1].

El detalle que hacía daño era la lista de compradores. Empresas como Disney, Shell, Gucci o easyJet habían comunicado productos y vuelos «carbon neutral» apoyándose en aquellos créditos. Según el análisis, la amenaza de deforestación que los proyectos decían evitar estaba sobreestimada de media alrededor de un **400 %**, y solo una pequeña fracción de los créditos examinados correspondía a reducciones reales [1]. Verra rebatió la investigación con dureza, tachándola de «manifiestamente poco fiable» y acusando a los estudios de usar «controles sintéticos» que comparaban peras con manzanas [2]. Pero el daño ya estaba hecho: cuatro meses después, el 22 de mayo de 2023, David Antonioli, consejero delegado fundador de Verra, anunciaba su salida tras casi quince años al frente [3].

Aquel terremoto resume la paradoja del mercado voluntario del carbono. Es, sobre el papel, una de las ideas más bonitas de la lucha climática: permitir que quien no puede reducir sus emisiones pague para que otro las reduzca o las absorba —plantando bosques, conservando selvas, capturando metano. Pero cuando la prueba de que esto ha pasado de verdad se reduce a unos informes que se pueden inflar, el sueño se transforma en una fábrica de coartadas. Este capítulo trata de cómo recuperar la confianza en un mercado que la necesita desesperadamente.

Cómo funciona —y cómo se rompe— el mercado voluntario

A diferencia del mercado del cumplimiento del capítulo anterior, aquí nadie obliga a nada: las empresas compran créditos **voluntariamente**, para cumplir promesas de «cero neto» o para mejorar su imagen. Un crédito equivale, nominalmente, a una tonelada de CO_2 evitada o eliminada. Cinco programas de certificación —ACR, ART, Climate Action Reserve, Gold Standard y, sobre todo, **Verra**— concentran cerca del **98 %** del mercado [8]. Verra, en solitario, ha llegado a controlar alrededor de dos tercios.

Es un mercado pequeño y volátil. Tras tocar techo hacia los **2.000 millones de dólares en 2021**, se contrajo dos años seguidos hasta los **723 millones en 2023**, con una caída del **56 % en el volumen de transacciones** respecto a 2022 y un precio medio de apenas **6,53 dólares por tonelada** [8]. Esta fragilidad de precios tiene una causa de fondo: nadie sabe a ciencia cierta qué vale un crédito porque nadie puede verificar fácilmente qué hay detrás.

Y detrás ha de haber cuatro cosas, todas difíciles de demostrar. **Adicionalidad**: que la reducción no hubiera ocurrido igualmente sin el dinero del crédito. **Línea de base**: cuánta deforestación o emisión se ha evitado *de verdad* respecto a un escenario hipotético. **Permanencia**: que el bosque siga en pie dentro de diez o treinta años, y no quemado o talado. Y **no doble cómputo**: que la misma tonelada no se venda dos veces ni la cuenten a la vez el comprador y el país donde se genera. Cada una de estas propiedades se «certifica», hoy, con documentos, fotografías e informes que se pueden manipular. Es exactamente aquí donde se ha colado el fraude.

El escándalo de los créditos fantasma

La investigación de 2023 no salió de la nada; confirmaba una sospecha que la ciencia ya apuntaba. **Patrick Greenfield**, periodista ambiental de *The Guardian* y uno de los autores del trabajo, resumió su tesis: la mayoría de los créditos de selva tropical de Verra usados por las grandes marcas no representaban reducciones reales, y el riesgo de tala que decían evitar estaba sistemáticamente inflado [1]. No era una

opinión aislada. Un estudio revisado por pares dirigido por **Alejandro Guizar-Coutiño**, investigador de la Universidad de Cambridge, había evaluado en 2022 cuarenta proyectos REDD+ en nueve países y había encontrado que sí reducían la deforestación, pero solo un **47 %** de media: reducciones reales, sí, pero muy por debajo de lo que prometían los créditos vendidos [6]. Otro estudio, publicado en *Science* en 2023 sobre veintiséis emplazamientos en seis países —con análisis detallado de la línea de base en dieciocho—, iba aún más lejos y sostenía que la mayoría de proyectos no habían reducido significativamente la deforestación, aunque este trabajo recibió una réplica formal y todavía se discute la elección de sus escenarios contrafactuales [7].

El caso que mejor ilustra el problema es **Kariba**, al norte de Zimbabue: uno de los mayores proyectos REDD+ del mundo, de cerca de 785.000 hectáreas, que había vendido créditos a gigantes como Volkswagen, Gucci, Nestlé o McKinsey. Cuando Verra lo investigó a fondo —a raíz, en parte, de un reportaje de *The New Yorker*—, la propia auditoría del certificador concluyó que se habían emitido **15.220.520 créditos en exceso de un total de 26.822.953**, es decir, un **57 % de sobreemisión** [4]. El desarrollador del proyecto, la empresa suiza South Pole, rompió el contrato con el socio local el 27 de octubre de 2023 [5]. Millones de créditos «basura» ya circulaban por el mercado, convertidos en certificados de neutralidad que nunca existieron físicamente.

El mecanismo del fraude, en el fondo, es siempre el mismo: no hay que falsificar el bosque, basta con inflar la *historia* sobre el bosque. Un escenario base exagerado, una fotografía reaprovechada, una medición tomada desde un despacho, un informe fechado después de un incendio. Todo ello, papel y píxeles que nadie puede contrastar hasta el origen.

La carrera por la integridad

Ante el descrédito, el sector ha puesto en marcha una carrera para recuperar la confianza. La pieza central es el **Integrity Council for the Voluntary Carbon Market** (ICVCM), un organismo independiente presidido por **Annette Nazareth**, antigua comisaria de la SEC norteamericana. En marzo se publicaron los **Core Carbon Principles** (CCP), una especie de sello de calidad que un crédito ha de cumplir en permanencia, medición robusta, verificación y adicionalidad. Como explicó Nazareth, la etiqueta CCP existe para que los compradores puedan distinguir los créditos que sí cumplen requisitos rigurosos [9]. En junio de 2024, el ICVCM aprobó las primeras siete metodologías con sello CCP, habilitando unos 27 millones de créditos de alta integridad [9]. En paralelo, la iniciativa **VCMI** lanzó un código de buenas prácticas para el lado de la demanda —qué puede decir y qué no una empresa que compra créditos [10].

A escala de estados, el **artículo 6 del Acuerdo de París** intenta poner orden en el comercio internacional. En la cumbre COP29 de Bakú, en noviembre de 2024, se adoptaron los estándares que hacen operativo el mecanismo de las Naciones Unidas [13]. La clave es el **ajuste correspondiente**: cada crédito autorizado para uso internacional obliga al país vendedor a restar aquella reducción de su propio inventario, de manera que la tonelada se contabiliza una sola vez. Es, en lenguaje climático, la solución contra el doble cómputo —el mismo problema que, en el mundo digital, resuelve anclar una huella única en un registro que nadie puede reescribir.

La tentación de la blockchain mal hecha

Aquí conviene una advertencia que este libro no puede ahorrarse. Cuando alguien dice «blockchain», a menudo imagina una varita mágica que lo hace todo transparente; la historia del carbono tokenizado demuestra lo contrario: **la tecnología mal aplicada empeoró el problema**.

Como hemos visto, en octubre de 2021 los proyectos Toucan y KlimaDAO lanzaron en la red Polygon la *Base Carbon Tonne*, un token que prometía equivaler a una tonelada de CO_2. En pocos meses, más de 21,6 millones de créditos migraron a la cadena. El centro de análisis **CarbonPlan** destapó el problema: sus investigadores **Danny Cullenward y Grayson Badgley**, en el estudio *Zombies on the blockchain* (abril de 2022), demostraron que casi un 28 % de aquellos créditos provenían de proyectos «zombi» —créditos viejos y de baja calidad que los compradores cuidadosos ya habían descartado, y que la tokenización había resucitado [11]. La blockchain se había convertido, decían, en un vertedero donde los peores créditos encontraban una segunda vida. El token estrella llegó a valer casi 3.900 dólares y acabó hundido en unos 20. En mayo de 2022, la propia Verra prohibió tokenizar créditos ya retirados [12].

La lección es exactamente la dualidad de **«la promesa y el peligro»** con la que Don Tapscott, coautor de *Blockchain Revolution* (2016), insiste en pensar toda tecnología. Poner una cosa «en la cadena» no la

hace verdadera; solo la hace *inmutable*. Si lo que anclas es basura, tendrás basura inmutable. La pregunta correcta no es *si* usamos la blockchain, sino **qué anclamos en ella y en qué momento**.

La prueba de existencia bien hecha: sellar la evidencia, no inventarla

Es en esta pregunta donde la **prueba de existencia** de **t2p** marca la diferencia respecto a los experimentos fallidos. La idea no es tokenizar el crédito final —el producto ya contaminado por una metodología dudosa—, sino **sellar la evidencia primaria** en el mismo instante y lugar en que se genera, antes de que nadie la pueda retocar.

En la práctica: cada fotografía de una repoblación, cada medición de una parcela de inventario, cada lectura de un sensor de campo recibe en origen una **huella SHA-512** calculada en el dispositivo, anclada a la **blockchain pública** con un **sello de tiempo RFC 3161** y acompañada de **GPS forense** y **prueba de vida** del técnico. Así queda demostrado que *esa* fotografía se tomó *en aquella coordenada*, *en aquella fecha*, por *una persona real presente*: no recuperada de Google Earth, ni generada por IA, ni fechada con trampa después de un incendio. Todo el paquete de evidencia de una monitorización —fotos, mediciones, coordenadas, firma— se puede cerrar en un **contenedor .asice verificable offline**, que un auditor, una agencia de calificación como Sylvera o BeZero, o el mismo registro pueden comprobar **sin depender de quien vende el proyecto**, incluso años después. Estas huellas se pueden encadenar con sistemas de **MRV digital** abiertos, como Open Forest Protocol, y con la trazabilidad que exige el ajuste correspondiente del artículo 6 [14].

Hay que ser, sin embargo, escrupulosamente honesto con el límite, y es un límite importante. La prueba de existencia **no resuelve la adicionalidad ni corrige una línea de base inflada** —que es el corazón del escándalo Verra y Kariba. Si la metodología es mala, el sello solo certificará, con gran fidelidad criptográfica, que alguien midió algo en un lugar y un momento. «Basura a la entrada, basura en la cadena.» Lo que aporta t2p no es validar la suposición contrafactual, sino **elevar la confianza en la evidencia de campo**: hace imposible la foto reaprovechada, la medición de despacho y el informe posfechado. La integridad climática sigue dependiendo de la buena ciencia de la línea de base y de la auditoría independiente. La tecnología es condición necesaria, no suficiente.

La promesa y el peligro

La promesa es poderosa. Un mercado voluntario donde cada pieza de evidencia esté sellada en el origen sería mucho más difícil de engañar, permitiría a un comprador comprobar por su cuenta que el bosque que financia existe y se mantiene, y volvería a hacer creíbles unos créditos que hoy se venden con descuento por culpa de la desconfianza. En un sector que ha perdido más de la mitad de su volumen en un solo año, recuperar la credibilidad es, literalmente, una cuestión de supervivencia.

El peligro tiene tres caras. La primera, la tentación de creer que la tecnología sustituye a la ciencia: ningún sello compensa una metodología mala. La segunda, el efecto placebo inverso —que una empresa compre créditos «verificados criptográficamente» para no hacer el trabajo duro de reducir sus propias emisiones; el sello certifica la evidencia, pero no la exime de descarbonizar. Y la tercera, la concentración: si la verificación y la calificación quedan en muy pocas manos, recreamos el punto único de confianza que queríamos disolver. La prueba de existencia es una herramienta al servicio de la integridad, no un sustituto de la integridad.

Es hora de actuar

Para los desarrolladores de proyectos: sellar la evidencia de campo en origen —fotos, mediciones, coordenadas— para que la calidad del proyecto sea demostrable y no haya que creerla sobre la palabra. Para las empresas compradoras: exigir créditos con evidencia anclada y etiqueta de integridad (CCP), sin usarlos para aplazar la reducción de las emisiones propias. Para los registros y estándares (Verra, Gold Standard, ICVCM): integrar la prueba de existencia y el MRV digital en sus metodologías, cerrando la puerta a la tokenización de créditos zombi. Para las agencias de calificación: usar la evidencia verificable offline como base de sus notas. Para los reguladores: hacer operativo el ajuste correspondiente del artículo 6 con infraestructura de datos a prueba de manipulación.

El mercado voluntario, nacido de una idea generosa, se ha estrellado contra su propia opacidad; tiene los años contados si no demuestra lo que promete. Como hemos visto, la diferencia entre un crédito fantasma

y un crédito real no es el discurso, sino la prueba, y generar esa prueba antes de que nadie la pueda inflar es **time2act**.

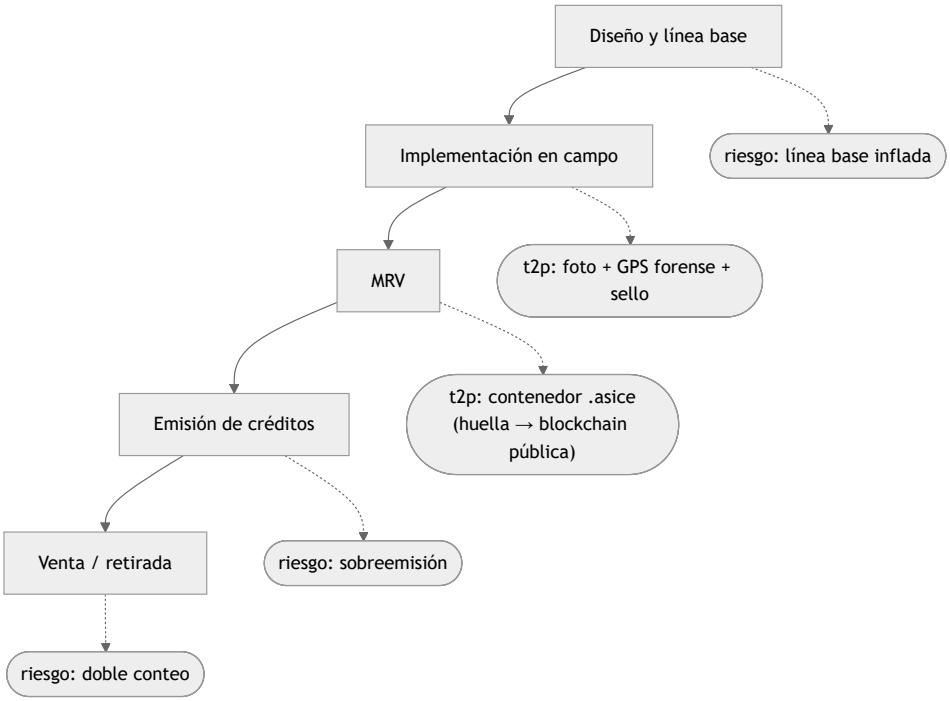


Figura 22.1 — A lo largo de la vida de un crédito —diseño y línea de base, implementación en el campo, MRV, emisión, venta y tokenización opcional— el fraude se infiltra sobre todo en la línea de base inflada y en la evidencia de campo manipulable. La prueba de existencia ancla los eslabones de evidencia (foto, medición, informe) pero no corrige una metodología defectuosa. Fuentes: The Guardian; Verra; CarbonPlan; ICVCM.

---

[1] The Guardian / Die Zeit / SourceMaterial — Patrick Greenfield, *Revealed: more than 90% of rainforest carbon offsets by biggest certifier are worthless* (18-ene-2023). https://www.theguardian.com/environment/2023/jan/18/revealed-forest-carbon-offsets-biggest-provider-worthless-verra-aoe ↩

[2] Verra — *Verra Response to Guardian Article on Rainforest Offset Credits* (réplica). https://verra.org/verra-response-guardian-rainforest-carbon-offsets/ ↩

[3] Mongabay — *Head of Verra, top carbon credit certifier, to leave in June* (dimisión de David Antonioli, 22-mayo-2023). https://news.mongabay.com/2023/05/head-of-verra-top-carbon-credit-certifier-to-leave-in-june/ ↩

[4] Verra — *Verra Acts on Kariba Project: Cancels Excess Credits and Advances Independent Review* (15.220.520 créditos en exceso de 26.822.953; ~57 %). https://verra.org/verra-acts-on-kariba-project-cancels-excess-credits-advances-independent-review/ ↩

[5] South Pole — *Statement on the Kariba REDD+ project* (27-oct-2023). https://www.southpole.com/news/statement-27october ↩

[6] Alejandro Guizar-Coutiño et al. — *A global evaluation of the effectiveness of voluntary REDD+ projects* (Conservation Biology, 2022; deforestación −47 %). https://pmc.ncbi.nlm.nih.gov/articles/PMC10086997/ ↩

[7] West et al. — *Action needed to make carbon offsets from forest conservation work for climate change mitigation* (Science, 2023; 26 emplazamientos en 6 países; resultado disputado, réplica arXiv 2312.06793). https://www.science.org/doi/10.1126/science.ade3535 ↩

[8] Ecosystem Marketplace / Forest Trends — *State of the Voluntary Carbon Market 2024* (mercado ~2.000 M$ en 2021 → 723 M$ en 2023; volumen −56 %; precio medio 6,53 $/t). https://www.ecosystemmarketplace.com/articles/report-the-voluntary-carbon-market-contracted-in-2023-driven-by-drop-off-in-transactions-for-redd-and-renewable-energy/ ↩

[9] ICVCM — *Core Carbon Principles* y *First high-integrity CCP-labelled carbon credits* (junio 2024; ~27 M de créditos). https://icvcm.org/core-carbon-principles/ · https://icvcm.org/integrity-council-announces-first-high-integrity-ccp-labelled-carbon-credits-as-assessments-continue/ ↩

[10] VCMI — *Claims Code of Practice* (28-junio-2023). https://vcmintegrity.org/launch-claims-code/ ↩

[11] CarbonPlan — Danny Cullenward y Grayson Badgley, *Zombies on the blockchain* (7-abr-2022; ~28 % de créditos zombi). https://carbonplan.org/research/toucan-crypto-offsets ↩

[12] Verra — *Verra Addresses Crypto Instruments and Tokens* (prohibición de tokenizar créditos retirados, 25-mayo-2022). https://verra.org/verra-addresses-crypto-instruments-and-tokens/ ↩

[13] S&P Global Commodity Insights — *COP29: rules for UN-led carbon market under Article 6.4 approved in Baku* (11-nov-2024). https://www.spglobal.com/commodity-insights/en/news-research/latest-news/energy-transition/111124-cop29-rules-for-un-led-carbon-market-under-article-64-approved-in-baku ↩

[14] CIFOR-ICRAF / Open Forest Protocol — *Blockchain platform offers reforestation efforts access to carbon finance* (MRV digital abierto). https://forestsnews.cifor.org/76905/blockchain-platform-offers-reforestation-efforts-access-to-carbon-finance ↩

CAE: certificar el ahorro sin hacer trampa

«Si no es correcto, no lo hagas; si no es verdad, no lo digas.»

— Marco Aurelio, Meditaciones, XII, 17

En Pordenone, en el nordeste de Italia, había una empresa de servicios energéticos que sobre el papel era un modelo de eficiencia. Desde 2013 había presentado al gestor público italiano, el GSE, casi trescientos proyectos de ahorro de energía: calderas sustituidas, aislamientos instalados, equipos renovados en casa de centenares de clientes. El GSE los validó y la empresa cobró **50.322 certificados blancos**, los títulos que premian cada kilovatio-hora ahorrado, con un beneficio de más de diez millones de euros.

Había un solo problema. La empresa no tenía oficinas, ni logística, ni empleados. Y las obras no existían. Los «clientes» eran nombres sacados de listas de una distribuidora de material termohidráulico y de una de placas solares, personas que nunca habían encargado nada. La Guardia di Finanza lo destapó y el Tribunal de Cuentas regional cifró el daño al erario público en unos **10,4 millones de euros** [10]. Era el fraude perfecto en su sencillez: certificados de un ahorro medido con precisión milimétrica… sobre instalaciones que solo existían en un PDF.

El caso de Pordenone condensa la fragilidad de uno de los instrumentos más inteligentes de la política energética europea: los **certificados de ahorro**. La idea es brillante —pagar por la energía que *no* se consume, porque el kilovatio-hora más limpio es el que no hace falta generar. Pero todo el edificio descansa sobre una prueba humilde: que la actuación de ahorro se hizo de verdad, allí donde se dice y cuando se dice. Y esa prueba, hasta ahora, era un puñado de papeles y fotografías que cualquiera podía inventar.

Pagar por la energía que no se gasta

Todo arranca de una obligación europea. La **Directiva de Eficiencia Energética** (la 2023/1791, en su artículo 8) obliga a cada estado a conseguir nuevos ahorros de energía final año tras año: un 0,8 % anual entre 2021 y 2023, un 1,3 % en 2024-2025, un 1,5 % en 2026-2027 y hasta un **1,9 % anual en 2028-2030**. La propia Comisión reconoce que la directiva refundida «más que duplica» la obligación de ahorro hacia 2028 [1]. Para España, el objetivo acumulado de ahorro de energía final de la década llega a los **53.593 ktep** [5]. Es una montaña de ahorro que alguien tiene que generar y, sobre todo, demostrar.

El instrumento que lo hace posible son los **certificados blancos**, conocidos con nombres distintos en cada país. En España son los **CAE**, los Certificados de Ahorro Energético, creados por el **Real Decreto 36/2023** de 24 de enero. La regla de oro es tan clara como un kilómetro marcado: **un CAE equivale a un kilovatio-hora de energía final ahorrado y acreditado** [2]. El sistema reparte el esfuerzo entre unos actores bien definidos: los **sujetos obligados** —las comercializadoras de gas y electricidad y los operadores de productos petrolíferos— tienen que generar unos ahorros proporcionales a sus ventas; pueden hacerlo directamente, a través de un **sujeto delegado**, o aportar dinero al Fondo Nacional de Eficiencia Energética. Cada actuación debe validarla un **verificador acreditado** por ENAC, y todo el sistema lo coordina el Ministerio para la Transición Ecológica a través de un catálogo de medidas estandarizadas [2][3].

El modelo funciona. En su primer año completo, 2024, el sistema CAE español movilizó más de **1.200 actuaciones**, certificó cerca de **2 TWh** de ahorro anual, evitó unas **500.000 toneladas de CO_2** y generó unos **230 millones de euros** en venta de certificados, con la industria como gran protagonista (un 68 % del ahorro) [4]. Francia usa el mismo principio desde 2006 con sus **CEE**, contabilizados en una unidad propia, el «kWh cumac» —energía ahorrada a lo largo de toda la vida útil del equipo—, con una obligación que para el periodo 2026-2030 llega a los **1.050 TWh cumac al año** [6]. Italia tiene sus certificati bianchi. Tres países, tres nombres, un mismo talón de Aquiles.

Quien mejor ha estudiado estos esquemas es **Louis-Gaëtan Giraudet**, economista del CIRED y de la École des Ponts y una de las autoridades europeas en certificados blancos. En trabajos como *Selling and Saving Energy: Energy Efficiency Obligations in Liberalized Energy Markets* (2020), Giraudet concluye que estos sistemas suelen tener un balance coste-beneficio positivo, pero que su integridad **depende críticamente de cómo se miden y se verifican los ahorros** frente a la línea de base [12]. Es decir: el instrumento vale exactamente lo que valga su prueba.

El fraude ataca la prueba, no la fórmula

Aquí reside la cuestión. El defraudador de ahorro energético casi nunca discute la fórmula del kilovatio-hora; lo que falsifica es **la prueba de que la actuación física existe**. Instalaciones fantasma, ahorros inflados respecto a la línea de base, facturas falsas, doble contabilización y medidas no adicionales que se habrían hecho de todos modos. Cada ataque converge en el mismo punto débil: la evidencia.

Francia es el caso de estudio más maduro y doloroso. El esquema de los CEE dio lugar al fenómeno de la «isolation à 1 euro» —el aislamiento por un euro—: empresas que captaban a particulares por teléfono prometiendo aislarles la casa «por un euro», a menudo diciéndose mandatadas por organismos oficiales. El resultado eran materiales malos, obras chapuceras o directamente inexistentes y solicitudes de certificados infladas. En el verano de 2018 la autoridad francesa de consumo y represión del fraude, la DGCCRF, controló 469 establecimientos del sector y encontró que el 56 % no respetaba plenamente las normas [8]. El goteo ha continuado: como hemos visto, el gobierno francés ha bloqueado 480 millones de euros de fraude a la transición energética, de los cuales 236 millones corresponden a los CEE [9]; y en febrero de 2025 las aduanas judiciales desarticularon una red que había desviado trece millones mediante obras ficticias y transferencias a paraísos fiscales.

Italia ha respondido con una doctrina jurídica reveladora. Su máximo tribunal administrativo, el Consiglio di Stato, ha confirmado que la asignación de un certificado blanco es un «proceso de formación progresiva»: aunque el GSE lo haya validado inicialmente, conserva el poder-deber de comprobar después que el ahorro existió de verdad y, si el beneficiario no puede probarlo con documentación, revocar el certificado y exigir su devolución [11]. En otras palabras: un certificado emitido **no es un derecho intocable**. La carga de la prueba recae, para siempre, sobre quien lo ha cobrado; y si la prueba es un archivo de fotos que nadie puede autenticar, esa carga es humo.

El regulador ya pide la prueba forense

Lo más interesante es que los reguladores ya han llegado, por la vía de los hechos, a la conclusión que vertebra este libro: que la confianza se ha de poder demostrar. La respuesta francesa al fraude lo ilustra casi literalmente. La **Ley 2025-594, de 30 de junio de 2025**, no solo elevó el techo de las sanciones —del 4 % al **10 %** de la facturación, y hasta el 12 % en caso de reincidencia—; también obligó a que determinadas operaciones de ahorro se justifiquen con **fotografías fechadas y geolocalizadas** —*horodatées et géolocalisées*— o con vídeo a distancia, pruebas que hay que conservar **seis años** y poner a disposición de los agentes de control [7].

El Estado francés, tras años de certificados falsos, ha dejado de creer en la palabra del instalador y exige por ley una **fotografía con fecha y coordenada verificables** de cada actuación. Esto es, exactamente, una prueba de existencia. Los controles de terceros sobre el terreno han subido del 10 % al 15 % entre 2023 y 2025 [9]; el regulador ha descrito el remedio, pero todavía falta la garantía de que esa fotografía, una vez tomada, no se pueda manipular ni fechar con trampa.

De requisito legal a rastro inalterable

Y aquí es donde la **prueba de existencia** de **t2p** transforma una buena intención reguladora en una garantía técnica. La ley francesa pide una foto fechada y geolocalizada; el problema es que una fecha y unas coordenadas, en un archivo corriente, también se pueden falsear. La prueba de existencia cierra esa rendija sellando la evidencia en el momento y el lugar exactos en que se genera.

El mecanismo, aplicado a una actuación de ahorro —el cambio de una caldera, un aislamiento, un motor industrial eficiente, un alumbrado LED—, es el siguiente. Se captura la evidencia completa: foto del *antes* y del *después*, lectura del contador inicial y final, factura del instalador, número de serie del equipo y firma del verificador. Cada archivo recibe en el dispositivo una **huella SHA-512**, que se ancla a la **blockchain pública** con un **sello de tiempo RFC 3161** conforme a eIDAS y con **GPS forense** que fija la coordenada de la obra. La foto del «después» incorpora, además, **prueba de vida** para impedir reaprovechar imágenes antiguas o de catálogo. Todo ello se empaqueta en un contenedor **.asice verificable sin conexión**.

El resultado ataca cada uno de los vectores de fraude. La geolocalización y la prueba de vida obligan a estar físicamente en la dirección declarada: adiós a las instalaciones fantasma de Pordenone. El sello de

tiempo y la huella delatan cualquier foto reaprovechada de otra obra o de un catálogo. Cualquier retoque posterior de una factura o de un certificado rompe la huella anclada, y la misma huella no se puede acreditar dos veces, lo que cierra la puerta al doble cómputo. Lo que la ley francesa ya exige —foto fechada, geolocalizada, conservada seis años— t2p lo convierte en un **rastro de auditoría inalterable**, verificable por el Coordinador español, por el control francés o por el GSE italiano **sin tener que confiar en el archivo del propio obligado**, y con un coste de verificación mucho más bajo que los muestreos sobre el terreno.

Conviene, como siempre, ser honesto con el límite. Anclar una prueba **no certifica que el ahorro sea real**: si el verificador acreditado avala una medida inflada, o si la línea de base está mal calculada, la cadena solo garantizará que aquel documento existía en aquella fecha y en aquel lugar, no su veracidad técnica. «Basura a la entrada, basura en la cadena.» La prueba de existencia blindará la **integridad de la evidencia y la identidad de quien la firma**, desplazando el fraude del «documento falsificable» al «perito que miente conscientemente», una conducta mucho más difícil, más rastreable y con responsabilidad nominal. No sustituye al verificador ni a la medición física; les sirve de fundamento fiable.

La promesa y el peligro

La promesa es directa y cuantificable. Un sistema de certificados de ahorro con evidencia sellada en el origen sería mucho más resistente al fraude, abarataría las verificaciones, aceleraría el pago de los certificados legítimos y protegería los miles de millones de euros públicos y privados que mueven estos esquemas. En un instrumento donde cada euro mal gastado es un euro que no compra ahorro real, la integridad de la prueba no es burocracia: es eficacia climática.

El peligro pide matiz, en la línea de la dualidad de «la promesa y el peligro» que recorre toda esta obra. Una capa técnica puede generar una falsa sensación de seguridad: el sello certifica el *cuándo* y el *dónde*, no la calidad de la medida. La geolocalización y la biometría de la prueba de vida tocan datos sensibles de instaladores y vecinos, y exigen un diseño respetuoso con la privacidad. Y si la verificación se concentra en pocas plataformas, recreamos el punto único de confianza que queríamos disolver. La prueba de existencia es una herramienta al servicio de la integridad de los certificados, no un sustituto del verificador ni del buen diseño de la línea de base.

Es hora de actuar

Para los **sujetos obligados y delegados** (comercializadoras, empresas de servicios energéticos): sellar la evidencia de cada actuación en origen, para que la calidad del trabajo sea demostrable y los certificados sean inatacables. Para los **verificadores acreditados**: exigir pruebas de existencia como base de la validación, y no aceptar fotografías o facturas que se hayan podido editar posteriormente. Para los **coordinadores y organismos de control** (MITECO, PNCEE francés, GSE italiano): reconocer el valor probatorio del sello, integrarlo en los requisitos del catálogo de medidas y reducir así el coste de los muestreos. Para los **reguladores europeos**: armonizar el requisito de prueba forense que Francia ya ha establecido por ley, antes de que cada estado reinvente la rueda.

En Pordenone, una empresa sin oficinas cobró medio centenar de miles de certificados por unas obras que no existían. La tecnología para hacer imposible aquel fraude ya existe, y un país entero empieza a exigirla por ley. Certificar el ahorro sin hacer trampa —demostrar que cada kilovatio-hora ahorrado existió de verdad— es, también aquí, **time2act**.

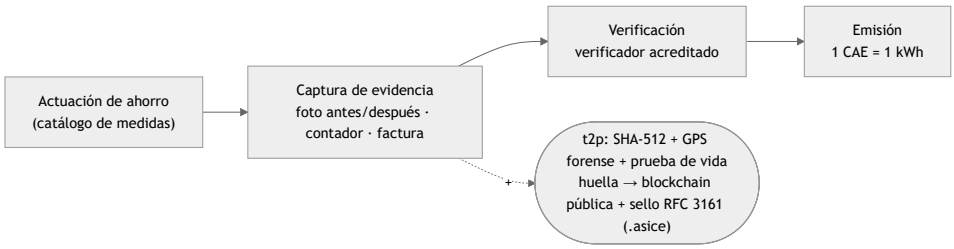


Figura 23.1 — Del catálogo de medidas a la emisión del certificado: la actuación se captura como evidencia (foto antes/después, contador, factura), se verifica y se convierte en CAE (1 CAE = 1 kWh). La prueba de existencia se inserta en el momento de capturar la evidencia —SHA-512, GPS forense, sello

RFC 3161, prueba de vida y contenedor .asice—, justo donde la ley francesa ya exige fotografías fechadas y geolocalizadas. Fuentes: BOE (RD 36/2023); Légifrance (Ley 2025-594); Funcas.

---

[1] Comisión Europea — *Energy Efficiency Directive* (Directiva 2023/1791, art. 8; nuevos ahorros hasta el 1,9 % anual en 2028-2030; «more than doubles» hacia 2028). https://energy.ec.europa.eu/topics/energy-efficiency/energy-efficiency-targets-directive-and-rules/energy-efficiency-directive_en ↩

[2] BOE — *Real Decreto 36/2023, de 24 de enero* (Sistema CAE; 1 CAE = 1 kWh de energía final acreditado; sujetos obligados/delegados, verificador, coordinador). https://www.boe.es/buscar/doc.php?id=BOE-A-2023-2027 ↩

[3] BOE — *Orden TED/845/2023, de 18 de julio* (catálogo de medidas estandarizadas de eficiencia energética). https://www.boe.es/buscar/doc.php?id=BOE-A-2023-16940 ↩

[4] Funcas — *Sistema de Certificados de Ahorro Energético (CAE): el motor que ya impulsa la transformación energética en España* (resultados 2024: ~1.200 actuaciones, ~2 TWh, ~500.000 t CO_2, ~230 M€; industria 68 %). https://www.funcas.es/articulos/sistema-de-certificados-de-ahorro-energetico-cae-el-motor-que-ya-impulsa-la-transformacion-energetica-en-espana/ ↩

[5] MITECO — *Memoria de la Orden de Obligaciones del Sistema CAE 2025* (objetivo acumulado de ahorro 2021-2030: 53.593 ktep). https://www.miteco.gob.es/content/dam/miteco/es/energia/files-1/es-ES/Participacion/Documents/aeip-fnee-2025/Memoria%20OM_Obligaciones%202025_TA.pdf ↩

[6] Légifrance — *Décret nº 2025-1048 du 30 octobre 2025* (CEE, 6.º periodo 2026-2030; 1.050 TWh cumac/año). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000052486193 ↩

[7] Légifrance — *Loi nº 2025-594 du 30 juin 2025* (sanciones hasta el 10-12 %; fotografías *horodatées et géolocalisées* o vídeo a distancia, conservadas 6 años). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000051824277 ↩

[8] DGCCRF (economie.gouv.fr) — *Rénovation énergétique : focus sur l'isolation à 1 euro* (469 establecimientos controlados; 56 % de incumplimiento). https://www.economie.gouv.fr/dgccrf/laction-de-la-dgccrf/les-enquetes/renovation-energetique-focus-sur-lisolation-1-euro ↩

[9] Hellio / Gobierno francés — *Fraude aux CEE* (480 M€ de fraude bloqueado en 2024, 236 M€ en CEE; tasa de control 10 %→15 %). https://www.hellio.com/actualites/reglementation/fraude-cee ↩

[10] ANSA / PordenoneToday — *Contributi per 10 milioni su certificati bianchi inesistenti* (292 proyectos ficticios; 50.322 TEE; daño ~10,4 M€). https://www.ansa.it/sito/notizie/cronaca/2025/06/23/contributi-per-10-milioni-su-certificati-bianchi-inesistenti_dd57abfb-77ba-483a-8f42-c240874fc308.html ↩

[11] EnergiaMercato / Consiglio di Stato — *GSE y la anulación de títulos de eficiencia energética* (doctrina de la «formación progresiva»; caso 4ESCO). https://www.energiamercato.it/notizie/project-finance/gse-conferma-la-legittimita-dellannullamento-di-titoli-di-efficienza-energetica-a-4esco ↩

[12] Louis-Gaëtan Giraudet, Matthieu Glachant y Jean-Philippe Nicolaï — *Selling and Saving Energy: Energy Efficiency Obligations in Liberalized Energy Markets* (The Energy Journal, 2020). https://ideas.repec.org/f/pgi337.html ↩

Autoconsumo y comunidades energéticas: la lectura verificable

«El sol también brilla hoy.»

— Ralph Waldo Emerson, Naturaleza (1836)

La tarde en que llega la factura, la casilla dice: «compensación de excedentes — 0 €». En la otra pantalla, la aplicación del inversor muestra un mes entero de sol contabilizado: una cifra que no se parece en nada a la de la comercializadora. El prosumidor mira las dos ventanas, una al lado de la otra: dos realidades que no cuadran, y ninguna manera de saber cuál manda.

No es una anécdota de nicho [1]: el autoconsumo fotovoltaico español ha llegado a los 9,3 gigavatios de potencia instalada —la quinta fuente de generación eléctrica del país por potencia, por delante de la nuclear. Solo en 2025 se sumaron 36.330 hogares, dentro de un total de 1.139 megavatios nuevos contando también los sectores comercial e industrial; y el objetivo del plan nacional de energía y clima es llegar a los 19 gigavatios [1]. Millones de familias y pymes han puesto ahorros en el tejado —y se han convertido, sin acabar de darse cuenta, en generadores con contabilidad energética propia.

Este capítulo cierra un círculo que el libro abrió en la Parte II: empezamos con la máquina energética, y la reencontramos ahora en los tejados —porque la transición energética también es una transición de confianza. Los certificados de ahorro energético —las actuaciones que se pagan— están en el capítulo 23; el acta de la comunidad de vecinos, en el capítulo 37; los sensores ciudadanos ambientales, en el capítulo 97; los mercados de carbono, en los capítulos 21 y 22. Pregunta clave: ¿quién tiene el contador cuando la factura no cuadra con el sol que has generado? Respuesta: la otra parte —salvo que la lectura propia tenga fecha cierta: las series del inversor y del contador selladas por lotes encadenados con **t2p**— la huella SHA-512 calculada en el dispositivo, el anclaje de la huella en la blockchain pública y el sello de tiempo RFC 3161/eIDAS complementario, dentro de un contenedor .asice [3]. Y con la simetría de siempre: el mismo rastro desarma la reclamación infundada contra la comercializadora que liquida bien.

El contador de la otra parte

El marco es claro y, en general, bien pensado [2]: el Real Decreto 244/2019 regula el autoconsumo y crea la compensación simplificada de excedentes —voluntaria, para instalaciones renovables de hasta 100 kW: la energía vertida a la red se compensa económicamente en la factura de cada mes (facturación neta mensual, no balance neto anual). El autoconsumo puede ser individual o colectivo —varios consumidores asociados a una misma instalación, con coeficientes de reparto—, y las reglas recientes han ampliado su radio hasta 5 kilómetros para plantas de hasta 5 megavatios [2]. Sobre esta base crecen las comunidades energéticas: vecinos, ayuntamientos y pymes agrupados para compartir generación.

El problema no es el marco: es la prueba. La liquidación de los excedentes se hace sobre las lecturas del contador fiscal y los sistemas de la comercializadora. El prosumidor tiene el inversor —que mide su producción en tiempo real— y su aplicación; pero cuando las dos cifras divergen, o la compensación tarda meses en aparecer, o un cambio de comercializadora pierde el hilo, la reclamación se hace contra datos ajenos: los de la otra parte.

En el modelo colectivo, la incertidumbre se multiplica: los coeficientes pactados entre vecinos, las altas y bajas de participantes, los acuerdos de asamblea —a menudo consignados en una hoja de cálculo de buena voluntad. Y en los contratos de compra de energía a largo plazo, los precios y volúmenes pactados deben contrastarse con los liquidados, una capa documental más.

La conclusión es la de este libro: la transición energética ha descentralizado la generación, pero no la prueba. Quien genera en casa merece una contabilidad energética con fecha cierta propia —no por desconfiar de nadie por sistema, sino para que cuando los números no cuadren, la conversación sea de hechos.

La prueba de existencia aplicada

Cuatro gestos —la mayoría, automáticos— convierten el tejado en un generador con contabilidad verificable [3].

1. La lectura propia, por lotes encadenados

Las exportaciones periódicas del inversor y del contador propio —producción, autoconsumo instantáneo, excedentes— se certifican con t2p por lotes: cada cierre, semanal o mensual, recibe su huella SHA-512, encadenada con la del anterior [3]. Es la misma lógica que el Estado ya impone a las facturas —el capítulo 34 lo explica— aplicada al tejado propio. El resultado: una serie fechada que nadie puede reescribir —ni siquiera el propio prosumidor, y por eso vale ante terceros.

2. La factura contrastada

Cada factura, capturada con fecha cierta al llegar; la casilla de compensación, contrastada contra la serie propia del mismo periodo [3]. Cuando no cuadran, la reclamación lleva números fechados: estos excedentes contó mi inversor, esto me compensasteis, esta es la diferencia. Y la simetría: la comercializadora que liquida bien tiene, en sus registros y en la serie del cliente, la prueba de que su factura era correcta —la reclamación infundada muere de fechas.

3. El acta de la comunidad energética

Los coeficientes de reparto, el alta y la baja de cada participante, los acuerdos de la asamblea —sellados con fecha cierta, como las actas de la comunidad de vecinos del capítulo 37 [3]. Cuando un participante discuta su porcentaje, o alguien entre a mitad de año, la historia de los acuerdos será una cadena de versiones ancladas, no una discusión de recuerdos. Las comunidades energéticas solo escalarán si la confianza entre desconocidos no depende de la buena voluntad de una hoja de cálculo.

4. El contrato congelado

El contrato de compensación, la oferta de la comercializadora el día de firmar, el PPA —el contrato de compra de energía a largo plazo— con sus precios y volúmenes: capturados y sellados en el momento [3]. Cuando las condiciones «cambien» o la letra pequeña se reinterprete, el documento de aquel día existe, exacto y fechado. El mismo gesto que el capítulo 33 aplica a la tarifa del teléfono, aplicado al contrato más largo que firma una familia.

Los límites, dichos claramente: el sello acredita series y documentos —no liquida, no tarifica y no sustituye la metrología legal: el contador fiscal es el que es, y la lectura propia contrasta, no reemplaza. Un inversor mal calibrado sella su propia desviación —mantenimiento y calibración primero. Y las discrepancias pequeñas son normales —pérdidas, momentos de medida—: el rastro sirve para las grandes y las persistentes.

La promesa y el peligro

La promesa: prosumidores que reclaman con series propias fechadas [1][3]; comunidades energéticas que crecen porque los acuerdos tienen fecha cierta; comercializadoras diligentes que resuelven reclamaciones en días porque las dos partes llevan números verificables; y la quinta fuente de generación del país [1] con la contabilidad de confianza que le corresponde.

Los peligros, mirados de frente.

El primero es **la guerra de contadores**. Si cada parte blande su serie, no hemos ganado nada. La respuesta es metodológica: equipos calibrados, metodología declarada, y la lectura propia como contraste documentado que obliga a revisar el contador fiscal —no como sustituto.

El segundo es **la sobrecarga del prosumidor**. La familia que puso placas para ahorrar no quiere una contabilidad criptográfica. El sellado ha de ser automático —la exportación periódica que se ancla sola [3] — o no será; el gesto manual es para el día de la discrepancia, no para cada día.

El tercero es **el perfil energético como intimidad**. La curva de consumo de un hogar explica cuándo duermes, cuándo cocinas, cuándo estás fuera. Las series quedan en el dispositivo o en los sistemas del prosumidor; en la cadena, solo huellas [3]; la revelación, selectiva y ante quien corresponda.

Y el cuarto es **el tecnosolucionismo solar**. Ningún hash acelera un permiso de acceso, no amplía una red saturada ni arregla una regulación lenta. La prueba de existencia hace justas las liquidaciones; que el autoconsumo llegue a los 19 gigavatios [1] es tarea de política energética.

Es hora de actuar

Que cada kilovatio generado en casa tenga su fecha cierta.

Para los prosumidores: activad la exportación periódica sellada del inversor [3]; el día que la factura no cuadre, tendréis vuestra serie —y no solo vuestra palabra.

Para las comunidades energéticas: coeficientes, altas y acuerdos con fecha cierta [3] —la confianza entre vecinos merece el mismo rastro que cualquier contrato.

Para comercializadoras y distribuidoras: anclad vuestras liquidaciones y publicadlas por huella —la reclamación infundada muere de fechas, y vuestra diligencia se vuelve argumento comercial.

Para el regulador y las autoridades de consumo: reconoced la serie propia anclada como contraste cualificado en las disputas de compensación [2]; el prosumidor no puede litigar a ciegas contra el contador de la otra parte.

Para los legisladores: la transición energética descentralizada —que ya roza los 9,3 gigavatios y aspira a los 19 [1][2]— necesita su capa de confianza: que el despliegue de las comunidades energéticas nazca con actas y liquidaciones verificables de serie.

Este libro empezó con el final del petróleo fácil; reencuentra la energía ahora en los tejados. Que la transición energética sea también una transición de confianza. Por el sol de cada tejado, **time2act**.

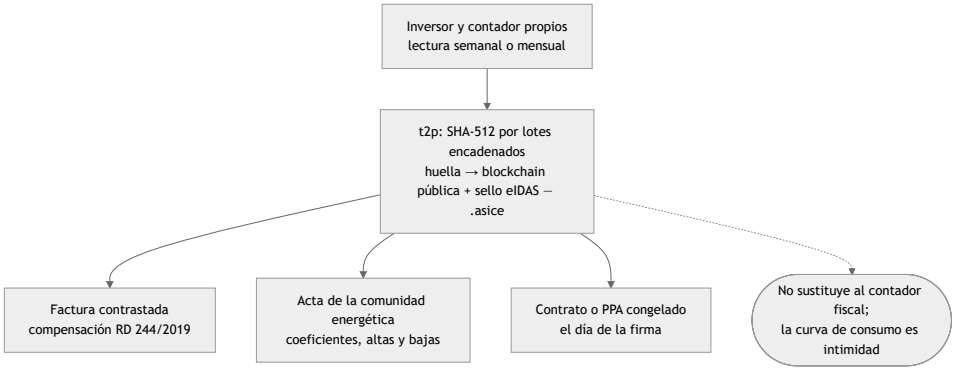


Figura 24.1 — El autoconsumo con prueba de existencia (t2p: huella SHA-512 en el dispositivo, RFC 3161/eIDAS, blockchain pública, .asice): la lectura propia del inversor y el contador sellada por lotes encadenados, la factura con compensación contrastada, el acta de la comunidad energética (coeficientes, altas y bajas con fecha cierta) y el contrato/PPA congelado el día de firmar. Contexto: 9,3 GW de autoconsumo en España (UNEF) —quinta fuente por potencia; RD 244/2019 (compensación simplificada mensual ≤100 kW; colectivo hasta 5 km). Límites: la lectura propia contrasta el contador fiscal, no lo sustituye; calibración primero; solo huellas en la cadena (la curva de consumo es intimidad). Fuentes: UNEF; BOE (RD 244/2019).

---

[1] UNEF — *El autoconsumo fotovoltaico en España alcanza los 9,3 GW instalados* (informe sobre 2025: +1.139 MW en el año, −3,7 % vs 2024; 36.330 hogares nuevos +229 MW; comercial +176 MW; industrial +679 MW; quinta fuente de generación por potencia instalada, por delante de la nuclear; objetivo PNIEC 19 GW); UNEF — *El autoconsumo sigue avanzando, superando ya el umbral de los 8 GW* (2024: +1.182 MW, acumulado 8.137 MW). https://www.unef.es/es/comunicacion/comunicacion-post/el-autoconsumo-fotovoltaico-en-espana-alcanza-los-9-3-gw-instalados · https://www.unef.es/es/comunicacion/comunicacion-post/el-autoconsumo-sigue-avanzando-superando-ya-el-umbral-de-los-8gw-instalados · https://www.eseficiencia.es/2026/02/02/autoconsumo-fotovoltaico-alcanza-9-3-gw-potencia-instalada-espana-segun-datos-unef ↩

[2] BOE — *Real Decreto 244/2019, de 5 de abril* (condiciones administrativas, técnicas y económicas del autoconsumo; compensación simplificada de excedentes ≤100 kW, voluntaria, en la factura mensual —facturación neta; autoconsumo individual y colectivo; registro administrativo); MITECO — *Preguntas frecuentes sobre autoconsumo*; UNEF — *Real Decreto 244/2019*; Puentes de Muras — *RD 244/2019: novedades* (ampliación del radio del autoconsumo colectivo hasta 5 km, plantas hasta 5 MW). https://www.boe.es/buscar/doc.php?id=BOE-A-2019-5089 · https://www.miteco.gob.es/en/energia/energia-electrica/electricidad/autoconsumo-electrico/preguntas-frecuentes-autoconsumo.html · https://autoconsumo.unef.es/real-decreto-244-2019/ · https://puentesdemuras.com/es/rd-244-2019-normativa-fotovoltaica-espana/ ↩

[3] t2p — manual de producto (certificar cualquier archivo por lotes —solo la huella viaja; captura de pantalla y de página web con imagen completa + código fuente; escáner de documentos hasta 50 páginas; foto con GPS forense; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; los CAE, en el capítulo 23; el acta de la comunidad, en el capítulo 37; la factura, en el capítulo 34. ↩

Movilidad I: flotas y empresas, evidencia sólida

«Es un error capital teorizar antes de tener datos.»

— Arthur Conan Doyle, «Un escándalo en Bohemia» (1891)

Una furgoneta de segunda mano cruza una frontera europea. En el país de origen, el cuentakilómetros marcaba 230.000 kilómetros; cuando llega al concesionario de destino, marca 150.000. En el trayecto, alguien ha conectado un pequeño aparato al conector de diagnóstico del vehículo y, en menos de un minuto, ha borrado **ochenta mil kilómetros**. El coche parece más joven, vale más, y el comprador pagará de media un 26 % de más por un vehículo que en realidad está mucho más gastado [3]. Lo más inquietante es que esta manipulación, según un estudio del servicio de estudios del **Parlamento Europeo** redactado por Enrico Pastori y Raffaele Vergnani, *Odometer manipulation in motor vehicles in the EU* (2018), «no deja ningún rastro»: la electrónica reescribe el número y la prueba del fraude se desvanece [1].

No es un caso aislado. Aquel mismo estudio cifra el coste del fraude de cuentakilómetros en la Unión Europea entre **5.600 y 9.600 millones de euros al año**, y estima que entre el **30 % y el 50 % de los coches vendidos a través de fronteras** tienen el kilometraje manipulado [1]. El Consejo Europeo de Seguridad en el Transporte lo confirma: hasta la mitad de los vehículos de segunda mano transfronterizos llevan el cuentakilómetros trucado [2].

Hasta aquí, una vieja estafa del mercado del automóvil. Pero detengámonos un momento, porque la historia da un giro que cambia todo el panorama. Aquellos mismos sensores —el cuentakilómetros, el GPS, el consumo, el registro de carga— han dejado de ser solo la ficha técnica de un coche. Hoy son la **materia prima de nuevos activos económicos**: créditos de carbono, certificados de ahorro energético (CAE) e informes de emisiones corporativas. Y si el dato que los alimenta se puede borrar en un minuto sin dejar rastro, todos estos instrumentos heredan la misma fragilidad. Este capítulo trata de cómo las flotas de empresa pueden generar evidencia climática que nadie pueda falsear.

La flota como fábrica de ahorro —y de evidencia

Una flota de empresa es, desde el punto de vista climático, una mina de ahorro. Electrificarla, formar a los conductores en conducción eficiente, optimizar rutas o cambiar a neumáticos de baja resistencia genera reducciones reales de emisiones que se pueden convertir en valor. En España, el catálogo del sistema CAE incluye cinco fichas específicas de transporte: la sustitución de neumáticos por otros más eficientes (TRA010), los sistemas de **telemetría y geoposicionamiento** en flota (TRA020), el vehículo compartido de largo recorrido (TRA030), la movilidad colaborativa urbana (TRA040) y la sustitución de un vehículo de combustión por uno eléctrico puro (TRA050) [5]. Cada actuación, recordémoslo, vale un kilovatio-hora ahorrado y acreditado.

Y el potencial es enorme, porque la tecnología ya funciona. El **International Council on Clean Transportation** (ICCT), una organización independiente de investigación sobre transporte limpio, midió en agosto de 2025 noventa y un camiones pesados eléctricos en uso real en Europa y encontró que consumen de media un **65 % menos de energía** que un diésel equivalente, con una autonomía real incluso superior a la anunciada por los fabricantes [6]. Como resume el ICCT, el problema ya no es la tecnología, sino **medir y certificar el ahorro de manera fiable**. A esta presión se añade la normativa: bajo la directiva europea de información de sostenibilidad (CSRD), las emisiones de la cadena de transporte —el llamado Alcance 3— son de obligada divulgación cuando son materiales, y están sujetas a verificación externa. Y para contarlas hay incluso un idioma común auditado, el **GLEC Framework** del Smart Freight Centre, alineado con la norma ISO 14083 [11].

El resultado es una paradoja: tenemos los vehículos, tenemos las fichas, tenemos los marcos contables y la obligación legal de reportar. Lo que falta es el eslabón más humilde de todos —la garantía de que el **dato de partida** es cierto.

Sensores que mienten

Porque la superficie de ataque de una flota conectada es enorme, cada puerta abierta puede inflar un ahorro o crear un crédito falso. El cuentakilómetros se puede retrasar —como hemos visto— y el **GPS se**

puede suplantar: en lugar de bloquear la señal, el atacante inyecta una falsa, de modo que un vehículo «aparece» por rutas eficientes que nunca ha recorrido, alimentando créditos de carbono o CAE de transporte. El **bus CAN**, la red interna que conecta los sensores del vehículo, no autentica quién envía cada mensaje; una inyección por el conector de diagnóstico o por la telemática puede hacer decir al coche lo que convenga. Las **tarjetas de combustible** son un clásico del fraude: en 2022 una investigación coordinada por Eurojust desarticuló una red entre Rumanía, Bélgica y Austria que había estafado 420.000 € con tarjetas clonadas y repostajes fantasma que viajaban por media Europa [8].

No es teoría. La empresa de ciberseguridad Upstream contabilizó **494 ciberataques** a vehículos y flotas durante 2025, el 92 % en remoto y dos de cada tres dirigidos a la telemática y la nube [7]. Incluso la recarga eléctrica tiene su flanco: el protocolo OCPP que gobierna los puntos de carga autentica cada sesión, pero las versiones débiles permiten manipular los mensajes entre el vehículo y la estación, falsificando los kilovatios-hora facturados o acreditados.

Es el caso del problema recurrente en este libro: *basura a la entrada, basura en la cadena*. Por muy sofisticado que sea el registro donde se anote finalmente el crédito, si la lectura entra ya falseada queda inmutablemente falsa. Ninguna blockchain salva un odómetro trucado.

La lección de Bélgica: sellar funciona

Por suerte, ya sabemos qué pasa cuando se sella el dato en origen, porque hay un experimento a escala real que lo demuestra. Se llama **Car-Pass** y es belga. Antes de su implantación, Bélgica sufría entre **sesenta mil y cien mil manipulaciones de cuentakilómetros al año**. El sistema es sencillo: cada vez que un coche cambia de manos, se registra oficialmente el kilometraje, y este historial sigue al vehículo para siempre. El resultado fue fulminante. En 2022, en toda Bélgica, solo se detectaron **1.344 casos** de fraude —menos del 0,2 % de los coches de segunda mano—, y el fraude en las importaciones cayó del 2,4 % en 2020 al 0,87 % en 2022 [4].

La lección es luminosa: cuando la verdad de un dato queda fijada en el momento en que se genera, y esa huella acompaña al activo para siempre, el fraude se hunde. Pero Car-Pass tiene dos limitaciones que lo hacen insuficiente para el mundo de las flotas y los créditos de carbono. Es **nacional** —un coche que entra desde otro país llega con un historial vacío o sospechoso— y es **centralizado**, una base de datos bajo una sola autoridad. Para una flota que opera en toda Europa, y para unos créditos que se venden a escala global, hace falta el mismo principio de Car-Pass pero **descentralizado, transfronterizo y verificable por cualquiera**. Y esto es, precisamente, lo que aporta la prueba de existencia.

La prueba de existencia para flotas

Apliquemos la mecánica de **t2p** al dato de una flota. La lectura en bruto —los kilómetros del odómetro, los kilovatios-hora de una sesión de carga, la traza GPS de un trayecto, el paquete del bus CAN— recibe una **huella SHA-512** calculada en el propio dispositivo de telemática, lo más cerca posible de la fuente, antes de que ningún servidor la pueda tocar. Esa huella se acompaña de **GPS forense** y **prueba de vida**, que ligan la posición y el momento al dato y delatan una ruta fantasma o un GPS suplantado al cruzar el sello con la geometría real. Se añade un **sello de tiempo RFC 3161** cualificado: y aquí hay un detalle jurídico poderoso, porque bajo los artículos 41 y 42 del reglamento europeo eIDAS, este sello tiene **presunción legal de exactitud** de la fecha y la hora. En caso de disputa, no es quien presenta la prueba quien debe demostrar que la fecha es buena; es quien la impugna quien debe demostrar que es falsa [12]. Finalmente, la huella se ancla a la **blockchain pública** y todo el paquete se cierra en un contenedor **.asice verificable sin conexión**, que un auditor de CSRD, un verificador de CAE o un organismo de créditos de carbono puede comprobar sin depender del emisor.

Es, en esencia, **Car-Pass elevado a la potencia de la blockchain**: un historial de kilometraje y de consumo incontrovertible, pero descentralizado y transfronterizo. Sellando la lectura en cada repostaje, en cada sesión de carga, en cada inspección técnica, se crea un registro que hace imposible el retroceso del cuentakilómetros, los trayectos fantasma para inflar ahorros, la manipulación de las sesiones de carga o el inflado de la línea de base de un CAE. Y encaja de manera natural con dos infraestructuras que ya llegan. La primera es el estándar de **Identidad de Vehículo** (VID) de **MOBI**, la *Mobility Open Blockchain Initiative*, un consorcio fundado en 2017 por fabricantes como BMW, Ford, General Motors, Honda y Renault, que en 2019 publicó la primera «partida de nacimiento» digital de un vehículo en blockchain y en 2024 demostró un pasaporte global de batería [9]. La segunda es el **Pasaporte de Batería** europeo, que

será obligatorio desde el 18 de febrero de 2027 para todas las baterías de vehículo eléctrico de más de dos kilovatios-hora y que registrará el estado de salud de cada batería accesible con un código QR [10].

Hay que ser honesto, también aquí, con el límite. La prueba de existencia garantiza que **el dato no ha cambiado desde que se selló**, no que el sensor dijera la verdad en aquel instante. Un odómetro trucado físicamente *antes* de la lectura, o un sensor comprometido en el hardware, seguiría sellando un valor falso. La mitigación es doble: sellar en el dispositivo de confianza más cercano a la fuente y hacerlo tan a menudo como se pueda, y cruzar señales redundantes —GPS contra consumo contra kilómetros— para que cualquier incoherencia salte a la vista. La tecnología no elimina la mentira de raíz; la hace mucho más difícil, más cara y más rastreable.

La promesa y el peligro

La promesa, para una empresa con flota, es tangible. Una evidencia sellada en origen convierte los créditos de carbono y los CAE de transporte en activos sólidos, defendibles ante un auditor y un comprador; protege a la empresa de comprar, sin saberlo, vehículos trucados; y hace que los informes de Alcance 3 que exige la CSRD dejen de ser un ejercicio de fe para convertirse en datos comprobables. En un mercado donde cada tonelada y cada kilovatio-hora se han de demostrar, la evidencia fiable es una ventaja competitiva.

El peligro pide el matiz de siempre, la dualidad de «la promesa y el peligro». La telemática y la prueba de vida recogen datos sensibles —a dónde va cada vehículo, quién lo conduce— y exigen un diseño escrupuloso con la privacidad de los trabajadores. La concentración de la verificación en pocas plataformas recrearía el punto único de confianza que queremos disolver. Y ningún sello exime del trabajo físico: medir bien, calibrar los sensores, auditar la línea de base. La prueba de existencia es el fundamento de la confianza, no un sustituto de la diligencia.

Es hora de actuar

Para los **gestores de flota**: sellar en origen las lecturas clave —kilometraje, consumo, sesiones de carga y rutas— para que los créditos, los CAE y los informes de emisiones sean demostrables e inatacables. Para los **proveedores de telemática**: incorporar el sello criptográfico al dispositivo, tan cerca del sensor como sea posible, y no en un servidor donde el dato ya se haya podido alterar. Para los **verificadores de CAE y los registros de créditos de carbono**: exigir evidencia anclada como base de la certificación y aprovecharla para abaratar los controles. Para los **auditores de sostenibilidad** (CSRD): reclamar pruebas de existencia para los datos de Alcance 3. Para los **reguladores**: extender la lógica del Car-Pass —historial de kilometraje inalterable— a escala europea y descentralizada, y reconocer el valor probatorio del sello, que su propio reglamento eIDAS ya ampara.

Una furgoneta puede rejuvenecer ochenta mil kilómetros en un minuto; pero si la lectura del cuentakilómetros queda sellada en cada cambio de manos, aquel minuto deja de existir. La diferencia entre una flota que afirma ahorrar y una flota que **demuestra** que ahorra es, cada vez más, la distinción entre un activo y una sospecha. Generar esta prueba en origen y a prueba de manipulaciones es time2act.



Figura 25.1 — La lectura de un sensor (odómetro, bus CAN, GPS, sesión de carga OCPP) se resume en una huella SHA-512 en el dispositivo, se le ligan el GPS forense y un sello de tiempo RFC 3161/eIDAS con presunción legal, se ancla a la blockchain pública y se empaqueta en un contenedor .asice verificable sin conexión, listo para emitir un CAE (fichas TRA010-TRA050), un crédito de carbono o un informe CSRD. Caja comparativa: sin sello, hasta el 30-50 % de los odómetros transfronterizos están manipulados; con un registro sellado (modelo Car-Pass), menos del 0,2 %. Fuentes: Parlamento Europeo (EPRS); Car-Pass; MITECO.

[1] Parlamento Europeo (EPRS) — Enrico Pastori y Raffaele Vergnani, *Odometer manipulation in motor vehicles in the EU* (2018; daño de 5.600-9.600 M€/año; 30-50 % en ventas transfronterizas).

https://www.europarl.europa.eu/RegData/etudes/STUD/2018/615637/EPRS_STU(2018615637_EN.pdf ↩

[2] ETSC (European Transport Safety Council) — *EU should act against mileage tampering on second-hand cars* (hasta el 50 % de los coches transfronterizos). https://etsc.eu/eu-should-act-against-mileage-tampering-on-second-hand-cars/ ↩

[3] carVertical — *The cost of odometer fraud in Europe* (2024; ~5.300 M€/año; sobreprecio medio del 26,3 %). https://www.carvertical.com/en/blog/cost-of-odometer-fraud-in-europe ↩

[4] Car-Pass (Bélgica) — *Annual report 2022* (1.344 casos en 2022, <0,2 %; importaciones 2,4 %→0,87 %). https://www.car-pass.be/en/blog/car-pass-annual-report-2022 ↩

[5] MITECO — *Catálogo de fichas CAE: sector transporte* (fichas TRA010 a TRA050). https://www.miteco.gob.es/en/energia/eficiencia/cae/catalogo-de-fichas/catalogo-vigente-de-fichas/transporte.html ↩

[6] ICCT — *Real-world use cases for zero-emission trucks: heavy tractor-trailers for goods transport in the EU* (agosto 2025; 65 % menos energía; autonomía real +11-19 %). https://theicct.org/publication/rw-use-cases-for-zet-heavy-tractor-trailers-for-goods-transport-in-the-eu-aug25/ ↩

[7] Upstream Security — *2026 Global Automotive & Smart Mobility Cybersecurity Report* (494 ciberataques en 2025; 92 % remotos; 67 % a telemática/nube). https://upstream.auto/press-releases/upstream-security-research-ransomware-attacks-on-automotive-and-smart-mobility-more-than-doubled-in-2025/ ↩

[8] Eurojust — *Suspects arrested in Romania, Belgium and Austria for defrauding EUR 420,000 using cloned fuel cards* (2022). https://www.eurojust.europa.eu/news/suspects-arrested-romania-belgium-and-austria-defrauding-eur-420000-using-cloned-fuel-cards ↩

[9] MOBI (Mobility Open Blockchain Initiative) — *Vehicle Identity (VID) standard* (2019) y *Global Battery Passport MVP* (2024). https://dlt.mobi/mobi-announces-the-first-vehicle-identity-vid-standard-on-blockchain-in-collaboration-with-groupe-renault-ford-and-bmw-among-others/ ↩

[10] Reglamento (UE) 2023/1542 — *Pasaporte de Batería digital* (obligatorio desde el 18-feb-2027 para baterías de VE e industriales de más de 2 kWh; acceso por QR). https://www.circularise.com/blogs/eu-battery-passport-regulation-requirements ↩

[11] Smart Freight Centre — *GLEC Framework v3.0 / ISO 14083:2023* (contabilidad de emisiones del transporte de mercancías). https://www.smartfreightcentre.org/en/about-sfc/news/a-solid-foundation-to-further-accelerate-freight-decarbonization-smart-freight-centre-releases-updated-glec-framework-version-30/ ↩

[12] Reglamento (UE) 910/2014 (eIDAS), artículos 41-42 — presunción legal de exactitud del sello de tiempo cualificado. https://eur-lex.europa.eu/eli/reg/2014/910/oj ↩

Movilidad II: coche compartido y particulares, repartir la confianza

«Quienquiera que sea usted... siempre he dependido de la bondad de los desconocidos.»

— Tennessee Williams, Un tranvía llamado Deseo (1947)

En Brooklyn, en agosto de 2024, la fiscalía federal del Distrito Este de Nueva York presentó cargos contra dos hombres por una estafa de una elegancia perturbadora. Eliahou Paldiel y Carlos Arturo Suárez Palacios habían programado una aplicación de **suplantación de GPS** y la habían repartido a más de ochocientos conductores de una plataforma de transporte. Con aquella herramienta, un conductor podía «aparecer» en una zona de tarifas altas —las llamadas *surge*— sin estar realmente allí. Multiplicado por centenares de conductores y miles de viajes, el engaño llegó a defraudar unos **cuarenta millones de dólares** desde noviembre de 2018 [5]. Una segunda app, llamada «Screwber», les adelantaba el destino y la tarifa de cada petición para que solo aceptaran los trayectos más rentables.

El caso es casi una parábola. Si la prueba de que un viaje ha existido es un **punto azul en un mapa**, ese punto se puede falsificar. Y toda la economía de la movilidad compartida —del coche que comparten dos vecinos al sistema de bicicletas de una ciudad— descansa, en última instancia, sobre esta prueba frágil. En el capítulo anterior vimos cómo una empresa con flota puede sellar la evidencia de sus vehículos. Ahora bajamos a la escala más difícil de todas: la del **particular** que comparte coche y que, sin ningún operador central que lo avale, quiere demostrar que un trayecto ocurrió de verdad para reclamar su parte justa de un ahorro, de un crédito o de un coste. Aquí, repartir la confianza es el problema central.

La revolución silenciosa de compartir

Compartir vehículo es una de las palancas climáticas más potentes y menos glamurosas que existen. La razón es tan simple como demoledora: un coche privado pasa parado alrededor del 95 % del tiempo. Lo subraya **Susan Shaheen**, profesora de ingeniería en la Universidad de California en Berkeley y codirectora de su Transportation Sustainability Research Center, probablemente la investigadora de referencia mundial en movilidad compartida. En un estudio de tres años sobre el servicio car2go, Shaheen y Elliot Martin encontraron que **cada vehículo compartido retiraba entre siete y once coches privados** de las calles de cinco ciudades norteamericanas, y reducía los kilómetros conducidos y las emisiones de sus usuarios [1].

Esa cifra, sin embargo, exige una cautela honesta que atraviesa toda la literatura: **el número de coches privados que sustituye uno compartido es siempre un rango, no una constante**. Un estudio europeo sobre el servicio SHARE NOW, con más de 278.000 usuarios en once ciudades, encontró una media de **3,3 coches sustituidos** —de 2,1 en Madrid y Lisboa hasta 5,3 en Bruselas—, mientras que otras ciudades llegan a cifras mucho más altas según la metodología [2]. Cualquiera que os venda un número único y redondo (el clásico «un coche compartido reemplaza a diez») os vende marketing, no ciencia.

La plataforma BlaBlaCar evitó **2,5 millones de toneladas de CO_2** en 2024, llenando más de setenta millones de asientos vacíos y transportando noventa y dos millones de pasajeros, como hemos visto [3]. En América del Norte, en 2023 se registraron **157 millones de viajes** en bicicletas y patinetes compartidos, un récord histórico [4]. Es un universo en plena expansión y cargado de potencial climático —tanto que plataformas de coche compartido entre particulares como Turo se han llegado a certificar «neutras en carbono» [11]— y genera ahorros certificables: créditos de carbono, CAE de movilidad colaborativa —recordad la ficha TRA040 del capítulo anterior— o simples repartos justos de coste, siempre que se pueda demostrar que el viaje existió.

El problema de la prueba entre iguales

Y aquí topamos con una dificultad que las flotas de empresa no tienen. Cuando una compañía sella los datos de sus camiones, hay una organización responsable detrás. Pero cuando dos desconocidos comparten un trayecto, **¿quién da fe de que ha ocurrido?** Hoy, la respuesta es la aplicación: BlaBlaCar, Turo o quien sea actúa a la vez de juez y de parte, y su «prueba» es un registro dentro de su base de datos, perfectamente editable. Para repartir un crédito entre dos particulares que no se conocen ni

se fían el uno del otro, dependemos ciegamente de un intermediario central —exactamente la dependencia que este libro, desde el primer capítulo, cuestiona.

Esta fragilidad abre la puerta a un fraude específico y barato. Se pueden inventar **viajes fantasma** para «cultivar» créditos que nunca se han generado. Dos cuentas pueden **confabularse** para intercambiarse trayectos falsos. Y, como ilustra el caso de Brooklyn, un **GPS suplantado** puede fabricar rutas enteras que no han existido. En todos los casos, el ataque no es contra la fórmula del ahorro, sino contra la prueba de que la actividad física ocurrió. Mientras esta prueba sea un punto azul editable, cualquier esquema de incentivos a la movilidad compartida nace con un agujero en el corazón.

Una moneda nueva: los créditos de movilidad

Este agujero es, precisamente, lo que ha frenado una de las ideas más fascinantes de la economía del transporte: los **créditos de movilidad negociables**. El concepto lo formalizaron los ingenieros **Hai Yang y Xiaolei Wang** en el artículo *Managing network mobility with tradable credits* (2011). La propuesta es tan elegante como equitativa: en lugar de cobrar peajes, una autoridad repartiría a cada ciudadano una cuota de créditos de movilidad, cobraría el uso de la red en créditos y dejaría que se comerciaran libremente. Quien se desplaza poco —a menudo, quien menos tiene— podría **vender** su excedente a quien se desplaza mucho, logrando los mismos objetivos que un peaje pero con neutralidad de ingresos y mucha más justicia social [6].

La idea ha generado una línea de investigación pujante. **Oded Cats**, catedrático de transporte en la Universidad Técnica de Delft, ha estudiado el diseño y la clasificación de estos esquemas y ha modelado incluso su aplicación a los viajes de larga distancia en Europa [7]. Y sin embargo, hay un hecho revelador: **hasta 2025 no se ha implementado ningún esquema de créditos de movilidad negociables a escala real**. Una revisión académica reciente del estado del arte lo confirma sin ambages: solo existen experimentos de laboratorio, juegos de simulación y modelizaciones [8]. Los incentivos que sí funcionan hoy son más modestos: en Bélgica, el «presupuesto de movilidad» corporativo ya llega a unos 18.000 trabajadores que cambian el coche de empresa por alternativas sostenibles [9]; en la Universidad de Delft, los ciudadanos «gastan» créditos simulados en una sala de juego; y en Bruselas, la Región ofrece entre 505 y 1.010 euros al año a quien da de baja la matrícula del coche a cambio de transporte público, bici o coche compartido [10] —pero todo esto son incentivos, no todavía mercados de créditos.

¿Por qué la idea no acaba de arrancar? Pesan la privacidad, el marco legal y la aceptación pública. Pero hay una pieza técnica que a menudo se olvida y que es justamente la de este libro: **sin una manera fiable de que cada ciudadano demuestre sus desplazamientos sin entregar toda su vida a una autoridad central, el sistema no es ni verificable ni aceptable**. Un mercado de créditos de movilidad necesita, antes que nada, una capa de prueba de confianza.

Repartir la confianza sin operador central

Es aquí donde la **prueba de existencia** de **t2p** aporta exactamente la pieza que falta, y lo hace con una propiedad que la distingue de todo el resto del libro. Apliquémosla a un trayecto compartido. Al cerrar el viaje, la aplicación del particular genera **en su propio dispositivo** un registro estructurado —ruta GPS forense, ocupantes, distancia, modo— y calcula una huella **SHA-512**, de modo que el dato en bruto no sale del teléfono: solo lo hace su huella. Esta huella recibe un **sello de tiempo RFC 3161** conforme a eIDAS y se ancla a la **blockchain pública**, de modo que nadie puede «crear» después un viaje pasado para inflar créditos.

Y entonces llega la clave de bóveda, la pieza que el sector de la movilidad compartida necesita más que ningún otro: la **prueba de vida**. La biometría de *liveness* liga el sello a la **persona real y presente** en aquel viaje, no a una cuenta ni a un emulador. Esto ataca de raíz la estafa de Brooklyn: un emulador puede falsear coordenadas, pero no puede superar un reto de prueba de vida anclado a la captura de la huella en aquel instante y aquel lugar. Finalmente, todo el conjunto se cierra en un contenedor **.asice verificable sin conexión**, y aquí está el giro decisivo: **dos desconocidos pueden liquidar su trayecto compartido sin confiar en ningún operador**, porque ambos pueden verificar la misma prueba de manera independiente. La confianza ya no la presta una app central; la prestan las matemáticas.

Esta capa es, en realidad, la infraestructura que faltaba para que los créditos de movilidad de Yang y Cats dejen de ser un experimento de laboratorio. Permite repartir créditos «sin operador de confianza», impide los viajes fantasma y la confabulación entre cuentas, y hace detectable cualquier reescritura retroactiva del

registro. Encaja, además, con estándares abiertos de identidad de vehículo como el VID de MOBI, la *Mobility Open Blockchain Initiative* [12].

Hay que ser, una vez más, honesto con el límite. La prueba de existencia certifica que *este registro existía, intacto, en aquel momento y ligado a esta persona*; **no** garantiza que la lectura de GPS subyacente sea físicamente cierta si el hardware o el firmware del teléfono se comprometieron antes del sellado. Un GPS suplantado a escala de hardware todavía podría pasar coordenadas falsas. La defensa real es la combinación de capas —prueba de vida, coherencia entre altitud, velocidad y ruta, y sello de tiempo—, no la cadena de bloques por sí sola. Y tampoco demuestra la **adicionalidad**: que aquel viaje compartido realmente sustituyera un coche que de verdad se habría usado. Esto sigue siendo un supuesto metodológico. La tecnología eleva la confianza en la evidencia; no inventa la verdad del mundo físico.

La promesa y el peligro

La promesa es grande y concreta para este sector: una capa de prueba entre iguales podría desbloquear por fin los mercados de créditos de movilidad, hacer justos y verificables los repartos de coste entre particulares, y convertir millones de pequeños gestos cotidianos —compartir un coche, coger la bici— en ahorro climático contabilizado y recompensado sin necesidad de un gran intermediario que se quede una parte.

Pero aquí el peligro es especialmente agudo, y tiene un nombre: **privacidad**. Se trata de sellar los desplazamientos de personas concretas. Una infraestructura que demuestre a dónde ha ido cada ciudadano puede ser, mal diseñada, la herramienta de vigilancia más perfecta jamás construida. Por eso la propiedad de que el hash se calcule en el dispositivo y de que el dato en bruto no salga de él no es un detalle técnico: es la línea que separa una herramienta de empoderamiento de una de control. La prueba de vida implica datos biométricos sensibles. Y un mercado de créditos mal pensado podría castigar a quien no tiene alternativa al coche —el vecino de un pueblo sin tren— en lugar de ayudarlo. La prueba de existencia ha de ser, en este terreno, escrupulosamente respetuosa con la privacidad y el diseño equitativo, o no será nada bueno.

Es hora de actuar

Para las **plataformas de movilidad compartida** (BlaBlaCar, Turo, operadores de bici y patinete): ofrecer a los usuarios pruebas de existencia de sus viajes que sean suyas y portátiles, no prisioneras de la base de datos de la empresa. Para los **particulares**: exigir poder demostrar los propios desplazamientos sin tener que ceder toda su localización a un tercero. Para los **diseñadores de esquemas de créditos de movilidad** (autoridades de transporte, investigadores como Cats): incorporar la capa de prueba entre iguales como fundamento, para que sus modelos salgan por fin del laboratorio. Para las **ciudades y reguladores**: construir estos sistemas con la privacidad como primer requisito, no como parche final.

Dos hombres en Brooklyn demostraron que un punto azul en un mapa no es ninguna prueba. Reconstruir la confianza a la escala más íntima de la movilidad —la del ciudadano que comparte un trayecto y quiere que cuente— exige una prueba que ni un emulador ni un intermediario interesado puedan fabricar. Repartir esta confianza, persona a persona, es la frontera más difícil y más humana de todo este libro. Y lograrla es, también, time2act.

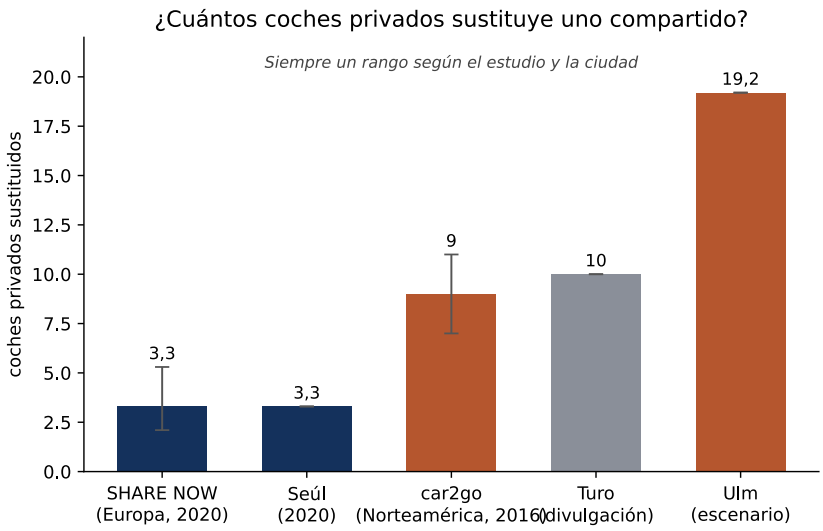


Figura 26.1 — El número de coches privados que retira de la calle un solo vehículo compartido varía enormemente según la ciudad y la metodología: de 3,3 de media en el estudio europeo de SHARE NOW hasta los 7-11 del estudio de car2go en Norteamérica, con escenarios aún más altos en algunas ciudades. La cifra de divulgación «uno por diez» es comercial, no consensuada. La lección: ningún número único; siempre un rango con su fuente. Fuentes: UC Berkeley TSRC (Shaheen y Martin, 2016); Transportation Research Part A (2020).

---

[1] Susan Shaheen y Elliot Martin (UC Berkeley, Transportation Sustainability Research Center) — *Impacts of car2go: One-Way Carsharing in North America* (2016; cada vehículo compartido retira 7-11 coches privados; VMT y GEI a la baja). https://phys.org/news/2016-07-car-mobility-decreases-greenhouse-gas.html ↩

[2] *Does free-floating carsharing reduce private vehicle ownership? The case of SHARE NOW in European cities* (Transportation Research Part A, 2020; media de 3,3 coches sustituidos; rango 2,1-5,3). https://pmc.ncbi.nlm.nih.gov/articles/PMC7544607/ ↩

[3] BlaBlaCar — *Sustainability Report 2024* (2,5 Mt CO_2 evitadas en 2024; 92 millones de pasajeros). https://newsroom.blablacar.com/news/sustainability-report-2024 ↩

[4] NACTO — *A micromobility record: 157 million trips on bike and scooter share in 2023*. https://nacto.org/latest/a-micromobility-record-157-million-trips-on-bike-and-scooter-share-in-2023/ ↩

[5] Insurance Journal (fiscalía EDNY) — *Two charged in $40M ride-hail surge-pricing GPS spoofing scheme* (caso «Fake GPS», agosto 2024). https://www.insurancejournal.com/news/east/2024/08/30/790683.htm ↩

[6] Hai Yang y Xiaolei Wang — *Managing network mobility with tradable credits* (Transportation Research Part B, 45(3), 2011, pp. 580-594). https://ideas.repec.org/a/eee/transb/v45y2011i3p580-594.html ↩

[7] Oded Cats et al. — *Design and classification of tradable mobility credit schemes* (Transport Policy, 136, 2023) y *Tradable mobility credits for long-distance travel in Europe* (Transportation Research Part A, 186, 2024). https://ideas.repec.org/a/eee/trapol/v136y2023icp59-69.html ↩

[8] Aljamal et al. — *Tradable credit scheme for mobility management: state of the art* (Transportation Research Interdisciplinary Perspectives, 2025; ninguna implementación a escala real hasta ahora). https://www.sciencedirect.com/science/article/pii/S2590198225002908 ↩

[9] Next Mobility / ONSS — *Mobility budget in Belgium: ONSS figures 2024* (18.386 trabajadores con presupuesto de movilidad; 17.030 sin coche de empresa). https://www.nextmobility.be/en/post/mobility-budget-belgium-onss-figures-2024/ ↩

[10] Bruxelles Environnement — *Prime Bruxell'Air* (ayuda de 505-1.010 €/año por dar de baja la matrícula, vigente en 2024). https://environnement.brussels/citoyen/services-et-demandes/primes-et-aides-financieres/la-prime-mobilite-bruxellair-pour-se-deplacer-autrement-dans-la-capitale ↩

[11] SCS Global Services / Turo — *Turo becomes first global carbon-neutral certified car-sharing marketplace* (2023). https://www.prnewswire.com/news-releases/turo-becomes-first-global-carbon-neutral-certified-car-sharing-marketplace-301799877.html ↩

[12] MOBI (Mobility Open Blockchain Initiative) — *Vehicle Identity (VID) standard on blockchain*. https://www.traffictechnologytoday.com/news/smart-cities/mobi-creates-the-first-vehicle-identity-standard-on-blockchain.html ↩

Retrasos de transporte: probar la hora de llegada

«No es que tengamos poco tiempo, sino que perdemos mucho.»

— Séneca, De la brevedad de la vida, I (c. 49 d. C.)

Un andén cualquiera, una puerta de embarque cualquiera. El panel salta de «+10» a «+45» sin explicaciones; la conexión se pierde; el ambiente se tensa. Meses después, la respuesta de la reclamación llega con su prosa impecable: «denegada por circunstancias operativas ajenas a la compañía». Y el viajero descubre el fondo del asunto: él tiene el recuerdo de la espera; la compañía tiene el registro —y el registro lo hace quien debería pagar.

El contexto es de actualidad [1]: el 1 de julio de 2024, Renfe recortó su compromiso voluntario de puntualidad para AVE, Avlo, Alvia, Euromed e Intercity. Desaparecieron las indemnizaciones por retrasos de 15 y 30 minutos, y el nuevo régimen paga el 50 % del billete a partir de 60 minutos y el 100 % a partir de 90 —incentivando, además, el cobro en puntos (el 200 %) o en vales (el 150 %) en lugar de euros. La justificación oficial: adaptarse a la liberalización y a la normativa europea. El debate sobre si hay que indemnizar desde los 15 minutos sigue abierto [1]. Y la lección probatoria es inmediata: cuando los umbrales suben, la frontera entre 58 y 61 minutos vale media tarifa —y la medida oficial de esa frontera la hace una de las partes.

Este capítulo trata el derecho de consumo más claro y peor provisto de prueba. La reclamación al servicio de atención de la compañía está en el capítulo 33; el reloj del proveedor de nube —el mismo patrón en otra industria—, en el capítulo 59; las flotas y la movilidad compartida, en los capítulos 25 y 26. Pregunta clave: ¿de quién es el reloj que decide si cobras? Respuesta: de quien tiene que pagar —salvo que la llegada real tenga fecha cierta en el dispositivo del viajero, con **t2p**: huella, hora cierta y ancla pública— la maquinaria del capítulo 13 [3]. Y con la simetría de siempre: el registro anclado del transportista lo protege de la reclamación inflada.

El derecho existe; la prueba, no tanto

El marco de los vuelos es de los más generosos del derecho de consumo europeo [2]: el Reglamento (CE) 261/2004 fija compensaciones de 250 euros para vuelos de hasta 1.500 kilómetros, 400 para los intraeuropeos más largos y los de 1.500 a 3.500, y 600 para los de más de 3.500; la jurisprudencia europea —la doctrina Sturgeon— equiparó el retraso de tres horas o más a la llegada con la cancelación; y el Tribunal de Justicia ha dejado una precisión preciosa para este libro: la «hora de llegada» es el momento en que se abren las puertas —un instante que el pasajero presencia con el móvil en el bolsillo. La excepción que lo tensa todo: las «circunstancias extraordinarias», que eximen a la compañía y que el viajero difícilmente puede contrastar.

El mecanismo de prueba, en cambio, es de otra época. La hora de llegada real la registran los sistemas del transportista; los paneles se actualizan y se borran; el motivo del retraso lo anuncia quien tiene que justificarlo; y la reclamación se presenta semanas después, con una tarjeta de embarque y recuerdos difusos. En el tren, lo mismo con el matiz español [1]: el compromiso es de la casa, y la medida también.

La conclusión no pide desconfiar de nadie: pide que el minuto 61 sea un hecho y no una versión. El derecho ya existe; lo que falta es que su única variable —cuánto de tarde llegaste— se pueda acreditar desde los dos lados.

La prueba de existencia aplicada

La llegada, convertida en hecho [3].

1. La llegada con lugar y hora

El gesto decisivo dura diez segundos: al abrirse las puertas —la definición del Tribunal de Justicia [2]—, una foto con el GPS forense de t2p: fijado genuino, precisión de unos 50 metros, antigüedad máxima de unos 30 segundos; una ubicación simulada bloquea la certificación [3]. Lugar y hora ciertos de la llegada real, en el dispositivo del pasajero. Y si el vuelo iba en modo avión, ningún problema: la certificación en

segundo plano se reanuda sola al recuperar cobertura, y el sello acredita el momento de la captura [3]. El minuto 61 deja de ser una discusión.

2. El panel congelado

El panel con el retraso anunciado —o el motivo alegado—, la pantalla de la app con el estado del vuelo o del tren, el correo de la cancelación: capturados y certificados con fecha [3]. Cuando la versión oficial cambie —el retraso «por causas técnicas» que después se convierte en «circunstancia extraordinaria»—, lo que se dijo en cada momento existe, exacto y fechado, y nadie lo puede reescribir a posteriori.

3. El expediente del viaje

El billete y la tarjeta de embarque, escaneados; los gastos que la compañía tenía que atender y no atendió —la comida, el hotel, el taxi— con tiques fotografiados con GPS forense [3]; todo agrupado en un proyecto y exportable como paquete .asice verificable sin conexión [3]. La reclamación a la compañía, a la agencia estatal de seguridad aérea o al juzgado de consumo llega con hechos fechados, no con una historia.

4. La simetría del transportista

El mismo mecanismo protege a quien opera bien: el registro de salidas y llegadas anclado por lotes —la lógica de la sonda del capítulo 59— y la evidencia de la circunstancia extraordinaria de verdad —el cierre de espacio aéreo, la tormenta, el incidente ajeno— sellada cuando ocurre [3]. Contra la reclamación inflada o la del pasajero que nunca voló, el transportista con registros verificables responde con fechas; y su compromiso de puntualidad, anclado y público por huella, se convierte en un argumento comercial que ningún competidor puede imitar sin cumplir [1].

Los límites, sin ambages: el sello acredita horas, lugares y documentos —no decide si una circunstancia era extraordinaria: eso lo dicen el Reglamento y el juez [2]. No sustituye la reclamación formal dentro de plazo ni el procedimiento de cada autoridad. Y la proporcionalidad manda: se documenta el viaje propio —nunca tripulaciones, empleados ni otros pasajeros.

La promesa y el peligro

La promesa: reclamaciones que se resuelven sobre horas ciertas [2][3]; pasajeros que cobran lo que el derecho europeo les reconoce sin batallas de versiones; transportistas diligentes que acreditan sus circunstancias y liquidan las reclamaciones legítimas en días; y un mercado —ahora liberalizado [1]— donde la puntualidad verificable compite.

Ahora, los peligros.

El primero es **la reclamación industrializada**. El fraude tiene dos caras: también hay pasajeros que reclaman lo que no corresponde. Precisamente por eso el expediente fechado beneficia a todos: quien voló y llegó tarde lo puede probar; quien no, no puede fabricar un GPS forense que se niega a certificar ubicaciones simuladas [3].

El segundo es **la guerra de relojes**. El pasajero con su foto contra la compañía con sus sistemas. La salida es la del capítulo 59: registros oficiales de operación anclados y públicos por huella como estándar del sector —cuando el reloj oficial es verificable, el particular solo hace falta por excepción.

El tercero es **el viaje como perfil**. Dónde estás y cuándo estás es intimidad pura. El expediente del viaje queda en el dispositivo; en la cadena, solo huellas [3]; se revela el tramo reclamado, nunca el historial de movimientos.

El cuarto peligro no es técnico, sino de mirada: confundir la prueba con el servicio. Ningún sello hace llegar el tren puntual ni evita la tormenta. La prueba hace exigible la compensación y honesta la estadística de puntualidad; el servicio lo mejoran la inversión y la gestión.

Es hora de actuar

Que el reloj del retraso tenga dos propietarios.

Para ti, viajero: la foto de la apertura de puertas [2][3] —diez segundos que valen hasta 600 euros [2]; y guarda el panel y los gastos en el mismo proyecto.

Para las compañías aéreas y ferroviarias: anclad los registros de operación y publicad la puntualidad por huella [1][3] —la reclamación infundada morirá de fechas, y vuestra fiabilidad será verificable, no publicitaria.

Para las plataformas de reclamación: incorporad el expediente sellado del pasajero como estándar de entrada [3]; ganaréis los casos con hechos, no con volumen.

Para las autoridades —aviación y ferrocarril: exigid a los operadores registros de llegadas verificables [1][2]; la protección del viajero no puede depender del reloj de quien tiene que pagar.

Para los legisladores: el debate sobre los umbrales —los 15, los 60, los 90 minutos [1]— es legítimo; lo que no lo es es que la medida del retraso sea unilateral. Que todo umbral nuevo nazca con hora de llegada verificable.

La próxima vez que el panel salte de «+10» a «+45», que tu reloj también cuente —con fecha cierta. Por cada minuto que es tuyo, **time2act**.

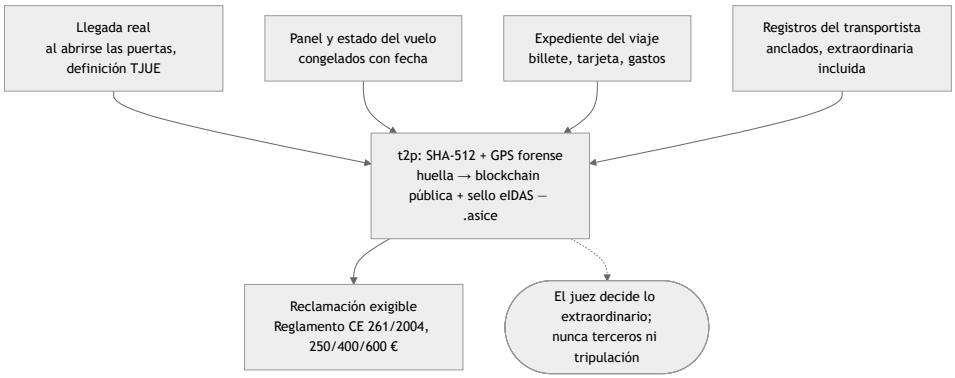


Figura 27.1 — El retraso con prueba de existencia (sellado con t2p — capítulo 13): la llegada con GPS forense al abrirse las puertas (la definición del TJUE), el panel y el estado del vuelo congelados, el expediente del viaje (billete, embarque, gastos de atención) y la simetría del transportista (registros de operación anclados; la circunstancia extraordinaria sellada cuando ocurre). Contexto: Reglamento (CE) 261/2004 (250/400/600 €; Sturgeon ≥3 h); Renfe 1-7-2024: de los 15/30 min a los 60/90 (50 %/100 %). Límites: el juez decide lo extraordinario; documentar el viaje propio, nunca terceros. Fuentes: EUR-Lex; Renfe/Newtral.

---

[1] Newtral — *Cómo cambió Renfe las indemnizaciones por retraso del AVE* (1-7-2024: eliminadas las indemnizaciones de 15 y 30 minutos para AVE, Avlo, Alvia, Euromed e Intercity; nuevo régimen 50 % a partir de 60 min y 100 % a partir de 90; devolución del 200 % en puntos o 150 % en vales; justificación: liberalización y ajuste a la legislación); Renfe — *Compromiso de puntualidad* y nota de prensa de la actualización; Xataka — *el debate sobre indemnizar desde los 15 minutos* (situación normativa abierta). https://www.newtral.es/renfe-indemnizacion-retraso-ave-gobiernos-pp-psoe/20250801/ · https://www.renfe.com/es/es/ayuda/compromiso-puntualidad · https://www.renfe.com/es/es/grupo-renfe/comunicacion/renfe-al-dia/sala-de-prensa/renfe-actualiza-compromiso-voluntario-puntualidad-ave-avlo-alvia-euromed-intercity · https://www.xataka.com/movilidad/renfe-esta-obligada-a-indemnizar-retrasos-15-minutos-a-partir-1-enero-gobierno-quiere-impedirlo ↩

[2] EUR-Lex — *Reglamento (CE) 261/2004* (compensaciones de 250/400/600 € por cancelación y, por la doctrina Sturgeon del TJUE, gran retraso ≥3 horas a la llegada; excepción de circunstancias extraordinarias; derecho de atención; jurisprudencia del TJUE: la «hora de llegada» es la apertura de puertas). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32004R0261 ↩

[3] t2p — manual de producto (foto con GPS forense —fijado genuino ~50 m / ≤30 s, la ubicación simulada bloquea la certificación; certificación en segundo plano que se reanuda al recuperar cobertura —modo avión; captura de pantalla certificada; escáner de documentos; proyectos para agrupar el expediente de un viaje; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; la reclamación de servicios, en el capítulo 33; el reloj del proveedor, en el capítulo 59. ↩

Seguros: la prueba del siniestro

«Alguien tenía que haber calumniado a Josef K., porque, sin haber hecho nada malo, una mañana fue detenido.»

— Franz Kafka, El proceso (1925), frase inicial

Un autónomo británico tenía, como todo el mundo, fotos de su furgoneta en las redes sociales: la herramienta de su oficio, aparcada frente a una obra, reluciente y sin un rasguño. En 2024, alguien tomó una de aquellas imágenes públicas, la editó digitalmente para pintarle una grieta en el parachoques y la usó para presentar una reclamación de seguro fraudulenta, con una factura de reparación falsa de más de mil libras, por un accidente que nunca había ocurrido. El equipo de fraude de la aseguradora LV= lo destapó porque la imagen era idéntica a la de las redes, pero con daños añadidos. Matt Crabtree, responsable de inteligencia de delitos financieros de LV=, advirtió de que los defraudadores usan la tecnología «para sus fines ilegales y para atacar a ciudadanos inocentes con ánimo de lucro» [6].

El caso es pequeño en el importe, pero inmenso en lo que anuncia. Durante décadas, falsificar un siniestro exigía un taller cómplice, un médico complaciente o un coche de verdad abollado. Hoy basta con una app en el móvil. Y la prueba en la que se basa todo el sistema asegurador —la fotografía del daño— se ha convertido, de golpe, en el eslabón más fácil de fabricar. Este capítulo trata de cómo volver a hacer creíble aquella fotografía: sellándola en el momento y el lugar en que se toma, antes de que la mentira entre en ella.

Un robo que pagamos todos

El fraude al seguro no es un delito sin víctimas; lo pagamos todos a través de primas más altas. Su magnitud es vertiginosa. En Estados Unidos, la **Coalition Against Insurance Fraud** (CAIF), una coalición de aseguradoras, reguladores y consumidores, publicó en 2022 —con la Colorado State University Global— el primer cálculo actualizado en veintisiete años: el fraude cuesta al país **308.600 millones de dólares al año**, el equivalente a unos 933 dólares por cada norteamericano [1]. La salud se lleva la parte más grande (unos 105.000 millones), seguida de la vida y de los daños materiales y de responsabilidad.

En Europa, la federación de aseguradoras **Insurance Europe** estima que el fraude —detectado y no detectado— equivale a alrededor del **10 % del gasto total en siniestros**, una cifra que arrastra desde un informe de 2013 y que sigue repitiendo porque es tan robusta como difícil de mejorar [2]. Los registros nacionales lo confirman año tras año. En el Reino Unido, las aseguradoras detectaron en 2024 **1.160 millones de libras** en reclamaciones fraudulentas —un 2 % más que el año anterior— repartidas en 98.400 reclamaciones, de las cuales más de la mitad eran del automóvil [3]. En España, el sector detectó en 2024 **285.407 casos sospechosos** y evitó el 63,7 %; el automóvil concentraba el 61,2 % del fraude, con un importe medio por reclamación fraudulenta evitada de 2.924 euros y un coste de investigación de apenas 43 euros por caso —un retorno de unos 68 euros por cada euro invertido en investigar [4]. Según el barómetro de la aseguradora Línea Directa, el 8,8 % de los partes de accidente de auto en España en los dos años previos eran intentos de estafa, casi cinco veces más que en 2009 [10].

La nueva frontera: el siniestro que nunca ocurrió

Estas cifras ya eran altas antes de la inteligencia artificial. Ahora, la IA generativa ha puesto una fábrica de pruebas falsas en el bolsillo de todo el mundo y el sector lo vive como un terremoto. El analista de datos de riesgo **Verisk**, junto con el National Insurance Crime Bureau, publicó en marzo de 2026 un estudio —encuesta a mil consumidores y trescientos profesionales de siniestros— con datos que hielan la sangre: el **36 % de los consumidores** norteamericanos consideraría alterar digitalmente una imagen o un documento de un siniestro aunque infringiera las normas de la aseguradora, y la cifra se dispara entre los jóvenes —un **55 % de la generación Z**, un 49 % de los millennials, frente al 12 % de los mayores [5]. El 13 % ve incluso aceptable «crear fotos de daños que nunca ocurrieron». Y desde el otro lado, el **99 % de las aseguradoras** ya ha topado con documentación manipulada o alterada con IA, y el 98 % afirma que estas herramientas están aumentando el fraude digital [5].

No es teoría. Las aseguradoras Allianz y Zurich documentaron un **aumento del 300 %** en las reclamaciones con fotos manipuladas comparando 2021-22 con 2022-23, y Allianz UK advirtió de que el

fenómeno tenía «todas las señales de convertirse en la próxima gran estafa del sector» [6]; solo en el primer semestre de 2025, Allianz destapó en el Reino Unido más de **15.800 casos** de fraude por **92,6 millones de libras** [7]. Los defraudadores compran fotos de coches siniestrados en subastas en línea, insertan con IA una matrícula real y fabrican daños de colisión. El equipo de Zurich ha pillado a muchos «observando anomalías en los metadatos de la imagen y con el análisis de nivel de error», una técnica forense que delata la edición; en un caso, la foto del vehículo llevaba marcas de tiempo anteriores a la fecha del supuesto accidente [8]. La reaseguradora **Swiss Re**, en su informe *SONAR 2025*, cifra un **aumento del 700 %** de incidentes con deepfakes en el sector fintech en 2023 y recomienda, explícitamente, combinar biometría, **detección de prueba de vida** y **marcas inalterables ancladas en blockchain** [9].

Detectar a posteriori no basta

La respuesta inmediata del sector es la detección: analizar cada imagen recibida en busca de huellas de edición —anomalías de píxel, metadatos incoherentes, nivel de error. Es un trabajo valioso y necesario, pero tiene un defecto estructural que este libro ya ha argumentado para las deepfakes: es una **carrera armamentística** que el defensor siempre corre por detrás. Cada mejora del detector empuja al defraudador hacia una IA mejor, y el día que la imagen generada no deje ningún rastro de píxel, la detección quedará ciega. Además, analizar a posteriori significa confiar en unos metadatos que el propio teléfono escribe y que cualquiera puede reescribir.

El problema de fondo es que la prueba —la foto del daño— se genera **fuera** del control de la aseguradora y **después** del hecho. El reclamante envía un JPEG por una app o un correo, y aquel JPEG puede ser una foto de stock, una imagen de un desguace, un daño preexistente o una creación de IA. Mientras la prueba nazca así, sin anclaje, toda la arquitectura del siniestro descansa sobre arena. La solución duradera no es analizar mejor la foto que llega, sino **garantizar el origen de la foto en el momento en que se toma**.

La prueba de existencia: sellar el siniestro en la escena

Es aquí donde la **prueba de existencia** de **t2p** ataca el problema desde la raíz. En lugar de examinar la imagen una vez recibida, la sella en el instante de la captura, en la escena del daño. La foto o el vídeo se **resume en una huella SHA-512 en el propio dispositivo** en el momento de tomarse; cualquier reedición posterior —añadir una grieta, alterar una matrícula— cambiaría la huella y rompería la cadena. A la huella se le añade un **sello de tiempo RFC 3161** conforme a eIDAS y un anclaje a la **blockchain pública** que fijan *cuándo* se capturó. Y aquí está la clave: esto neutraliza exactamente el truco que delataba a los defraudadores de Zurich —metadatos con fechas anteriores en años—, porque el sello proviene de una autoridad de confianza, no del EXIF manipulable del teléfono.

Se suman dos piezas que el sector necesita especialmente. El **GPS forense** acredita *dónde* se tomó la foto, lo que ayuda a descartar imágenes de subastas o daños reciclados de otro lugar. Y la **prueba de vida** liga la captura a *una persona real presente en la escena*, haciendo muy difícil que alguien suba imágenes generadas «desde detrás del ordenador», el patrón que describen Allianz y LV=. Todo ello —imagen original intacta, huella, sello, GPS, prueba de vida— se empaqueta en un **contenedor .asice verificable sin conexión**, que el perito o el auditor puede validar sin depender de la app ni de un servidor, y que es admisible como evidencia. Vale la pena subrayarlo: es precisamente la receta que Swiss Re recomienda —biometría, prueba de vida, anclaje inalterable—, convertida en producto.

Hay que ser, como siempre, honesto con el límite. La prueba de existencia demuestra que *esta* imagen existía íntegra, en *este* lugar, en *este* momento, capturada por *esta* persona viva. **No demuestra la causa ni la legitimidad del daño.** Alguien puede fotografiar con t2p después de haber provocado él mismo un accidente escenificado: el sello será impecable y el siniestro seguirá siendo fraude. Por eso la prueba de existencia **complementa, no sustituye, al perito**: elimina la capa de fraude documental y de imagen —la de crecimiento más rápido— para que la investigación humana se concentre en la causalidad y la simulación. Y solo aporta valor si la captura se hace con la app en el momento, no para siniestros ya ocurridos y documentados con fotos viejas.

La promesa y el peligro

La promesa es tangible y cuantificable. En un sector donde el fraude cuesta centenares de miles de millones, eliminar de raíz el fraude de la foto-prueba liberaría recursos enormes, aceleraría el pago de los siniestros honestos —la inmensa mayoría— y bajaría la presión sobre las primas de todos. Una foto sellada en la escena convierte la parte más vulnerable del proceso en la más sólida.

El peligro pide el matiz de siempre, la dualidad de «la promesa y el peligro». Recoger fotos geolocalizadas y biometría de prueba de vida toca datos sensibles del cliente en un momento de estrés; el diseño ha de ser escrupuloso con la privacidad y no convertir cada parte en una cesión excesiva de datos. Ningún sello exime al perito de juzgar la causa, ni a la aseguradora de tratar al cliente con confianza por defecto. Y la concentración de la verificación en pocas plataformas recrearía el punto único de confianza que queremos disolver. La prueba de existencia es una capa necesaria dentro de una arquitectura de confianza más amplia.

Es hora de actuar

Para las aseguradoras: ofrecer la captura sellada en origen como canal preferente del parte de siniestro y premiarla con una tramitación más rápida —quien no tiene nada que ocultar, sale beneficiado. Para los asegurados honestos (la inmensa mayoría): exigir poder demostrar su siniestro con una prueba que ningún algoritmo pueda poner en duda. Para los peritos e investigadores: reservar el esfuerzo humano para la causalidad y el fraude duro, dejando que la tecnología cierre la puerta al fraude de imagen. Para los reguladores: reconocer el valor probatorio del sello y fijar estándares que protejan simultáneamente la integridad de la prueba y la privacidad del cliente.

Un autónomo vio cómo la foto de su furgoneta se convertía en el arma de una estafa. La diferencia entre una imagen que cualquiera puede fabricar y una prueba sellada en la escena es, cada vez más, la clave para un sistema que se autodefiende. Volver a hacer creíble la foto del siniestro —demostrar que el daño existió, allí y entonces— es, también aquí, time2act.

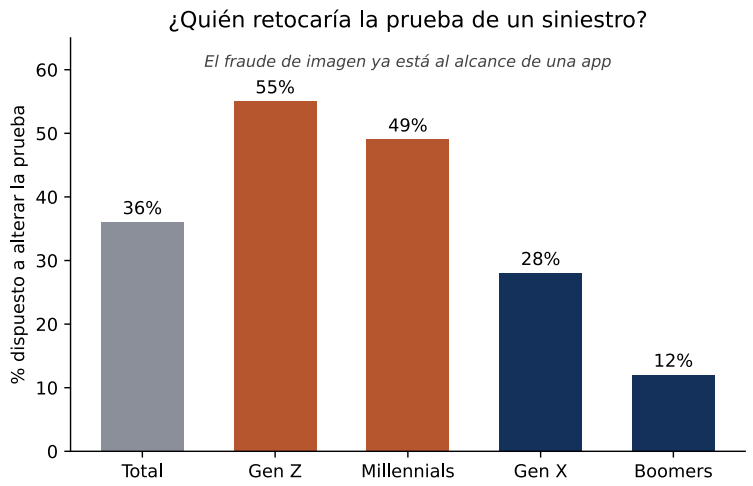


Figura 28.1 — Porcentaje de consumidores dispuestos a alterar digitalmente la imagen o el documento de un siniestro, aunque infrinja las normas de la aseguradora: un 36 % de media, pero hasta el 55 % entre la generación Z. La predisposición cae con la edad. Es el rostro del fraude de imagen por IA que el 99 % de las aseguradoras ya ha visto. Fuente: Verisk con el National Insurance Crime Bureau (2026).

[1] Coalition Against Insurance Fraud — *The Impact of Insurance Fraud on the U.S. Economy* (2022; 308.600 M$/año, ~933 $ por persona). https://insurancefraud.org/wp-content/uploads/The-Impact-of-Insurance-Fraud-on-the-U.S.-Economy-Report-2022-8.26.2022.pdf ↩

[2] Insurance Europe — *Annual Report 2023-2024* (capítulo Fraud) y *The impact of insurance fraud* (~10 % del gasto en siniestros; estimación de 2013, ~13.000 M€ referidos a 2017). https://www.insuranceeurope.eu/downloads/ar-2024-fraud/Fraud.pdf ↩

[3] Association of British Insurers (ABI) — *Fraudulent insurance claims continue to top £1 billion* (2024: 1.160 M£; 98.400 reclamaciones). https://www.abi.org.uk/news/news-articles/2025/11/fraudulent-insurance-claims-continue-to-top-1-billion/ ↩

[4] ICEA — *El sector detectó 285.407 casos sospechosos de fraude, de los que evitó un 63,7 %* (España, 2024). https://segurosnews.com/news/el-sector-detecto-285-407-casos-sospechosos-de-fraude-de-los-que-evito-un-637 ↩

[5] Verisk (con el National Insurance Crime Bureau) — *AI editing tools are fueling a new era of insurance fraud* (marzo 2026; 36 % de consumidores, Gen Z 55 %; 99 % de las aseguradoras). https://www.verisk.com/company/newsroom/ai-editing-tools-are-fueling-a-new-era-of-insurance-fraud-according-to-new-research-from-verisk/ ↩

[6] The Guardian (vía PetaPixel) — *Fraudsters are editing photos of damaged vehicles to claim insurance* (caso LV=; +300 % de fotos manipuladas, Allianz/Zurich). https://petapixel.com/2024/05/07/fraudsters-are-editing-photos-of-damaged-vehicles-to-claim-insurance/ ↩

[7] Allianz UK — *Allianz UK detects frauds totalling £93m in first half of 2025* (15.800 casos). https://www.allianz.co.uk/news-and-insight/news/allianz-uk-detects-frauds-totalling-93m-in-first-half-of-2025.html ↩

[8] Zurich Insurance — *AI poses challenges, offers tantalizing solutions to insurers fighting fraud* (metadatos + análisis de nivel de error). https://www.zurich.com/insights/business/ai-poses-challenges-offers-tantalizing-solutions-to-insurers-fighting-fraud ↩

[9] Swiss Re Institute — *SONAR 2025: How deepfakes, disinformation and AI amplify insurance fraud* (+700 %; recomienda prueba de vida y anclaje en blockchain). https://www.swissre.com/institute/research/sonar/sonar2025/how-deepfakes-disinformation-ai-amplify-insurance-fraud.html ↩

[10] Línea Directa — *VII Barómetro del Fraude al Seguro* (8,8 % de los partes de auto en España). https://www.lineadirectaaseguradora.com/-/vii-barometro-de-fraude-al-seguro ↩

Cadena de suministro: el origen verificable contra la falsificación

«No es de la benevolencia del carnicero, del cervecero o del panadero de quien esperamos nuestra cena, sino de la atención que prestan a su propio interés.»

— Adam Smith, La riqueza de las naciones, I, 2 (1776)

En el otoño de 2022, en los hospitales de Banjul, la capital de Gambia, los médicos empezaron a ver llegar bebés con una insuficiencia renal aguda que no sabían explicar. El rastro llevó a cuatro jarabes pediátricos para la tos y el resfriado, fabricados por una empresa india, Maiden Pharmaceuticals, y contaminados con dietilenglicol y etilenglicol —dos disolventes industriales tóxicos. Murieron cerca de **setenta niños**. El 5 de octubre de 2022, la Organización Mundial de la Salud emitió la Alerta de Producto Médico N°6/2022 [3]. Tres años después, en octubre de 2025, la historia se repitió en la India: el jarabe «Coldrif», con casi un 48 % de dietilenglicol, mató al menos a veinticuatro niños más, y la OMS tuvo que emitir una nueva alerta [4].

El detalle que lo cambia todo es este: en aquellos casos, **la etiqueta era auténtica y la cadena documental era «legítima»**. Los papeles estaban en orden. Lo que falló no fue el sello ni el código de barras, sino la verdad física del contenido. Es la lección más dura y más honesta de este capítulo, y conviene ponerla por delante: ninguna prueba de origen, por perfecta que sea, analiza la molécula. Pero, como veremos, esto no hace inútil la prueba de origen —la hace imprescindible para todo el resto del problema.

El fraude que entra en las cadenas legítimas

La falsificación de productos ya no se limita a bolsos de marca vendidos en el top manta; es un río que se infiltra en las cadenas de suministro legítimas y amenaza la salud. La **OCDE** y la **Oficina de Propiedad Intelectual de la Unión Europea** (EUIPO), en su informe *Mapping Global Trade in Fakes 2025*, cifran el comercio mundial de productos falsificados y pirateados en **467.000 millones de dólares** en 2021 —un **2,3 % de todas las importaciones del mundo** [1]. En la Unión Europea la proporción sube al **4,7 % de las importaciones**, unos 117.000 millones [1]; como hemos visto, lo que más alarma es el giro hacia la **falsificación peligrosa**: recambios de automóvil, cosméticos, juguetes, alimentos y medicamentos falsos que entran en el mercado como si fueran auténticos.

Los medicamentos son el caso más letal. La **Organización Mundial de la Salud** estima que **al menos uno de cada diez productos médicos** en los países de renta baja y media es subestándar o falsificado, basándose en más de cien estudios y 48.000 muestras de 88 países [2]. El despilfarro económico ronda los **30.500 millones de dólares** al año, pero el coste real se cuenta en vidas como las de Gambia. La OMS distingue el producto **subestándar** —el que no cumple las normas de calidad por mala fabricación— del **falsificado** —el que tergiversa deliberadamente su identidad, composición u origen. En ambos casos, el problema fundamental es que **no hay manera fácil de probar de dónde viene realmente lo que tenemos en las manos**.

El regulador exige coordenadas

Ante esto, Europa ha dado un giro histórico: ahora exige que el origen sea *verificable*, no solo declarado. La pieza más ambiciosa es el **Reglamento contra la deforestación**, el EUDR (Reglamento UE 2023/1115). Por primera vez, la ley obliga a aportar las **coordenadas de geolocalización de la parcela exacta** de donde proviene cada partida de siete materias primas —ganado bovino, cacao, café, aceite de palma, caucho, soja y madera— para garantizar que no salgan de tierras deforestadas después del 31 de diciembre de 2020 [5]. La mecánica es reveladoramente concreta: para parcelas de más de cuatro hectáreas hace falta un **polígono** de coordenadas que dibuje su perímetro; para las más pequeñas basta con un punto con seis decimales; todo se envía en formato GeoJSON al sistema de información de la Unión. Las fechas de aplicación quedan fijadas el **30 de diciembre de 2026** para los grandes y medianos operadores y el **30 de junio de 2027** para los más pequeños [6]. Es, en una frase, el desplazamiento de la prueba «del papel a la tierra».

No es el único ejemplo. La **Directiva de Medicamentos Falsificados**, en vigor desde febrero de 2019, obliga a que la mayoría de medicamentos de receta lleven un **identificador único** —un código 2D con producto, número de serie, lote y caducidad— y un dispositivo antimanipulación, verificados contra un repositorio central europeo antes de dispensarlos [7]. Y en el mundo del lujo, el **Aura Blockchain Consortium**, como hemos visto, ya ha registrado más de **cincuenta millones de productos** en una cadena de bloques que da al comprador acceso directo a la historia y la prueba de autenticidad de su pieza [8][9]. Tres respuestas diferentes, una misma intuición: la confianza ha de poder demostrarse.

Por qué el sello por sí solo no salva (y por qué aun así hace falta)

Llegados aquí, hay que ser implacablemente honesto, porque este capítulo toca vidas. La serialización de un medicamento demuestra que **la caja** es auténtica, no que **la molécula** de dentro lo sea. En Gambia, una foto sellada de la fábrica no habría detectado el disolvente tóxico. Es el principio que recorre todo el libro, aquí en su forma más literal: «basura a la entrada, basura en la cadena». Una prueba de existencia de una parcela **equivocada**, o de un lote correcto con un contenido adulterado, sigue siendo una mentira bien sellada.

¿Por qué, entonces, vale la pena? Porque la inmensa mayoría del fraude de la cadena de suministro **no** es el envenenamiento deliberado, sino la **retrodatación** de certificados, la **sustitución de documentos**, la falsificación del origen y la reutilización de fotos de otra parcela o de otro año. Contra todo esto, sellar el acto de origen es demoledor: eleva el coste de mentir, fija responsabilidades con nombre y fecha, y deja un rastro que un auditor puede seguir hasta la fuente. La prueba de existencia no sustituye el control de calidad físico —el que habría salvado a los niños de Gambia—; lo **complementa**, cerrando la puerta al fraude documental para que la inspección se concentre en lo que de verdad importa: el contenido.

La prueba de existencia en el origen

Apliquemos la mecánica de **t2p**. En el punto de origen —la parcela, la cosecha, la fábrica, el lote— se toma una fotografía georreferenciada y se sella en el instante: una **huella SHA-512** calculada en el dispositivo, un **GPS forense** que fija las coordenadas, un **sello de tiempo RFC 3161** conforme a eIDAS y un anclaje a la **blockchain pública**. Para el EUDR, esto significa fotografiar la parcela con su polígono o su punto de seis decimales y convertir la captura en **evidencia inalterable** del momento y del lugar exactos. La **prueba de vida** puede ligar la evidencia a la persona que hace la inspección o la cosecha —el inspector, el agricultor—, reduciendo el fraude porque «nadie puede sellar esto sin estar allí». Y todo el conjunto se empaqueta en un **contenedor .asice verificable sin conexión**, que un agente de aduanas, un auditor o un comprador puede comprobar sin conexión y sin confiar en la palabra del proveedor.

Lo más importante es que la prueba de existencia **no compite** con la serialización ni con los pasaportes digitales; los complementa. El código 2D del medicamento y el pasaporte de Aura dicen *qué* producto es; el sello de origen de t2p añade la capa que falta: *este lote se fotografió aquí, en esta fecha, con esta persona presente*. Es la diferencia entre tener una etiqueta de confianza y tener la **prueba del acto** que aquella etiqueta resume. Para el consumidor de lujo que escanea su bolso y ve su historia, y para el agente de aduanas que verifica un contenedor de café, la promesa es la misma: poder comprobar el origen sin tener que creer a nadie.

La promesa y el peligro

La promesa es enorme y transversal. Una cadena de suministro con el origen sellado sería mucho más resistente a la falsificación documental, cumpliría el EUDR con evidencia real en lugar de declaraciones, protegería las marcas honestas y, sobre todo, daría al ciudadano el derecho de comprobar qué compra. En un comercio donde las falsificaciones mueven cerca de medio billón de dólares, recuperar la confianza en el origen es una ventaja competitiva y una cuestión de salud pública.

El peligro pide el matiz de siempre, en la dualidad de «la promesa y el peligro». El primero, ya explicado: el sello certifica el acto, no la calidad física; presentarlo como garantía de seguridad sería peligroso y falso. El segundo, la carga que puede recaer sobre los pequeños productores del Sur global, para quienes geolocalizar cada parcela puede ser una barrera; el diseño ha de ser inclusivo, no un nuevo muro. Y el tercero, la privacidad y la concentración: quien controla la capa de verificación no puede convertirse en un

nuevo intermediario único. La prueba de existencia es una herramienta necesaria dentro de una arquitectura más amplia que incluye, siempre, el control físico.

Es hora de actuar

Para los **productores y agricultores**: sellar el acto de origen —parcela, cosecha, lote— para que la trazabilidad sea demostrable y defendible ante el EUDR y los compradores. Para los **importadores y marcas**: exigir evidencia anclada como base de la diligencia debida, no aceptar certificados retrodatados. Para los **reguladores y aduanas**: reconocer el valor probatorio del sello e integrarlo en los sistemas de información, sin olvidar nunca el control físico del producto. Para los **consumidores**: poder escanear y comprobar el origen de lo que comen, toman o visten. Y para todos, recordar la lección de Gambia: el origen verificable es necesario, pero la seguridad del producto exige también analizar su contenido.

Setenta niños murieron con una etiqueta auténtica en la mano. Ninguna tecnología debería arrogarse el poder de evitar toda tragedia, pero sí podemos hacer que mentir sobre el origen sea mucho más difícil y rastreable. Demostrar de dónde viene de verdad una cosa —y quién se hace responsable— es, también aquí, time2act.

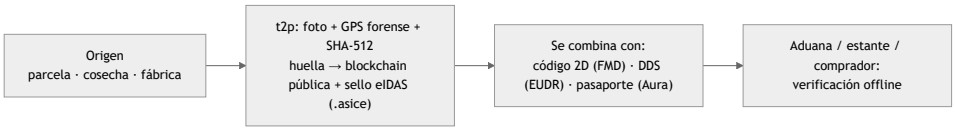


Figura 29.1 — En el punto de origen (parcela, cosecha, fábrica) se captura una foto georreferenciada que se sella con GPS forense, sello de tiempo eIDAS y huella SHA-512, y se empaqueta en un contenedor .asice verificable sin conexión. Esta capa de prueba del acto de origen se combina con la serialización (código 2D del FMD), la declaración de diligencia debida del EUDR o el pasaporte digital de Aura, hasta la verificación final en la aduana o en el estante. Fuentes: EUDR (UE 2023/1115); EMA; Aura Blockchain Consortium.

---

[1] OCDE / EUIPO — *Mapping Global Trade in Fakes 2025* (falsificaciones: 467.000 M$ en 2021, 2,3 % de las importaciones mundiales; UE 4,7 %). https://www.oecd.org/en/publications/mapping-global-trade-in-fakes-2025_94d3b29f-en.html ↩

[2] Organización Mundial de la Salud — *Substandard and falsified medical products* (≥1 de cada 10 en los países de renta baja/media; ~30.500 M$/año). https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products ↩

[3] OMS — *Medical Product Alert Nº6/2022* (Gambia; jarabes de Maiden Pharmaceuticals contaminados con dietilenglicol). https://www.who.int/news/item/05-10-2022-medical-product-alert-n-6-2022-substandard-(contaminated-paediatric-medicines ↩

[4] OMS — *Medical Product Alert Nº5/2025* (India; jarabe «Coldrif» de Sresan Pharmaceuticals). https://www.who.int/news/item/13-10-2025-medical-product-alert-n-5-2025--substandard-(contaminated-oral-liquid-medicines ↩

[5] EUR-Lex — *Reglamento (UE) 2023/1115* (EUDR; coordenadas de geolocalización de parcelas; 7 materias primas; fecha de corte 31-dic-2020). https://eur-lex.europa.eu/eli/reg/2023/1115/oj/eng ↩

[6] Comisión Europea (Access2Markets) — *Delay until December 2026 — implementation of the EUDR* (segunda prórroga, Reg. UE 2025/2650; aplicación 30-dic-2026 / 30-jun-2027). https://trade.ec.europa.eu/access-to-markets/en/news/delay-until-december-2026-and-other-developments-implementation-eudr-regulation ↩

[7] EMA — *Falsified medicines: overview* (Directiva 2011/62/UE; identificador único 2D obligatorio desde el 9-feb-2019). https://www.ema.europa.eu/en/human-regulatory-overview/public-health-threats/falsified-medicines-overview ↩

[8] Aura Blockchain Consortium — *About* (fundado en 2021 por LVMH, Prada y Cartier; >50 M de productos registrados). https://auraconsortium.com/about ↩

[9] WWD — *Aura Blockchain crosses 50 million products* (LVMH, Prada, OTB; septiembre 2024). https://wwd.com/business-news/technology/aura-blockchain-crosses-50-million-products-lvmh-prada-otb-1236606994/ ↩

Consumo: reseñas falsas, precios inflados y garantías con reloj

«La publicidad trata de relaciones sociales, no de objetos. Su promesa no es de placer, sino de felicidad: felicidad juzgada desde el exterior por los demás.»

— John Berger, Modos de ver (1972)

Antes de comprar nada, haces lo que hace todo el mundo: lees las reseñas. Cinco estrellas, «me ha cambiado la vida», miles de valoraciones que parecen la voz colectiva de una multitud satisfecha. Lo que quizá no sabes es que detrás de aquella unanimidad puede haber una industria. En julio de 2022, Amazon demandó a los administradores de más de 10.000 grupos de Facebook dedicados a orquestar reseñas falsas a cambio de productos gratuitos o dinero: un solo grupo, «Amazon Product Review», tenía más de 43.000 miembros; en otro se pagaban 10 dólares por reseña; la trama operaba en las tiendas de Estados Unidos, el Reino Unido, Alemania, Francia, Italia, España y Japón, y esquivaba la detección de Meta cambiando letras de las palabras sensibles [2]. Desde 2020, Amazon había reportado más de 10.000 grupos a Meta; solo la mitad habían sido eliminados [2].

Este capítulo trata la capa de información sobre la que el consumidor decide. De dónde viene físicamente el producto se explica en el capítulo 29; quién paga los anuncios que nadie ve, en el capítulo 56; qué hay de verdad dentro de la comida, en el capítulo 101. Aquí las preguntas son las del carrito de la compra: ¿puedo creer estas estrellas? ¿este descuento es real? y si se rompe, ¿podré demostrar cuándo y cómo? La respuesta del libro: devolver la fecha cierta a las tres señales —la reseña con compra acreditada, la serie de precios sellada y la cronología de garantía— con **t2p**: la huella SHA-512 en el dispositivo, el anclaje de la huella en la blockchain pública y el sello de tiempo RFC 3161/eIDAS complementario, dentro de un contenedor .asice [5]. Ni el mercado ni el consumidor deberían discutir nunca más sobre recuerdos.

La opinión fabricada

La demanda de Amazon puso cifras a un secreto conocido: las opiniones se fabrican en masa y se venden como un producto más. Grupos organizados con decenas de miles de miembros, tarifas por reseña, técnicas de evasión para burlar los filtros de las plataformas [2] —la profesionalización completa de un fraude que decide compras cada segundo.

La respuesta regulatoria ha llegado. En Estados Unidos, la norma final de la FTC —anunciada el 14 de agosto de 2024, en vigor desde el 21 de octubre de 2024— prohíbe comprar o vender reseñas falsas, las reseñas de «insiders» sin revelar la relación, las webs de reseñas «independientes» controladas por la propia empresa, la supresión selectiva de reseñas negativas y la compraventa de indicadores falsos de influencia social, con sanciones de hasta 51.744 dólares por infracción [1].

Pero la ley, por sí sola, no resuelve el problema epistemológico: el lector sigue sin poder distinguir, estrella a estrella, quién ha tocado el producto y quién cobra por opinar. Y con la IA generativa, el coste de fabricar mil opiniones verosímiles —con toques humanos, detalles de uso inventados y tono de vecino sincero— tiende a cero.

La salida no es creer menos: es poder verificar más. Si cada reseña puede ir ligada a una prueba de compra sellada —el justificante con huella en el dispositivo del comprador, sin revelar su identidad [5]—, la plataforma puede distinguir, y el lector filtrar, la opinión de quien compró de verdad. Puedes comprar mil opiniones; no puedes fabricar mil compras selladas antes de escribirlas. La estrella deja de ser un acto de fe.

El descuento que no lo era

La segunda señal fabricada es el precio «de antes». La OCU lo ha medido en sus análisis del Black Friday, y el panorama es desolador: solo uno de cada tres productos se abarata de verdad; en categorías como relojes inteligentes, cámaras y auriculares, los precios suben de media un 13 % las semanas previas a la campaña; el 43 % de los productos dispara el precio durante la campaña misma; el ahorro medio anunciado es del 23 %, pero los precios reales salen de media un 3 % más caros [3]. Y el dato reglamentario: en el 99 % de los casos, el «precio anterior» indicado no es el menor de los últimos 30 días,

como exige la normativa de rebajas —muchos comercios usan como referencia un «precio recomendado por el fabricante» que a menudo nunca ha sido el precio real de venta [3].

La OCU puede detectarlo porque hace lo que ningún consumidor puede hacer solo: monitorizar los precios desde principios de septiembre [3]. Y aquí es exactamente donde la prueba de existencia cambia el juego: la norma existe, pero su verificación es inaccesible para el ciudadano —habría que haber vigilado el precio cada día.

La serie de precios anclada lo hace por todos: si los precios se registran con capturas selladas —cada precio, cada día, con fecha cierta [5]—, por la plataforma misma, por observatorios de consumo o por la ciudadanía organizada, el «precio anterior» se convierte en un hecho verificable en un clic, y el descuento falso, en una infracción demostrable. El cartel del «–70 %» deja de ser una declaración de fe: o resiste la serie, o retrata a quien lo cuelga. Y para el comercio honesto, el mismo sello es marketing —el descuento verificable vale más que el inflado de al lado.

La garantía con reloj

La tercera señal es la promesa de que, si falla, responderán. El marco español vigente es de los más protectores de Europa: desde el 1 de enero de 2022 —transponiendo las directivas europeas—, la garantía legal mínima es de tres años para los bienes (dos para contenidos y servicios digitales); durante los dos primeros años se presume que el defecto es de origen (un año para productos de segunda mano); los fabricantes deben garantizar recambios durante diez años desde que el producto deja de fabricarse; y el plazo para reclamar es de cinco años [4].

En la práctica, sin embargo, la garantía es una carrera de pruebas contra el reloj. ¿Cuándo compraste? —el tique ha desaparecido entre facturas. ¿Cómo llegó? —el rasguño «ya estaba» o «lo has hecho tú». ¿Cuándo avisaste del defecto? —dentro de la presunción de los dos años, o fuera. ¿Cuántas veces se ha reparado? Cada pregunta sin prueba es una reclamación que muere ante el servicio posventa.

La aplicación de la prueba de existencia es directa. El tique y la factura, sellados el día de la compra, fijan con fecha cierta el inicio de los tres años [4][5]: el papel perdido deja de ser fatal. El estado del producto en la entrega —cuatro fotos o treinta segundos de vídeo con huella en el momento— es el equivalente consumidor del inventario de alquiler: ni el transportista ni el comprador pueden reescribir cómo llegó la caja. Y cada aviso al vendedor, anclado, fija si el defecto apareció dentro de la presunción [4]. La garantía deja de ser una batalla de memoria: no más luchas contra el reloj —ahora el reloj trabaja para ti.

La prueba de existencia aplicada

Una compra cualquiera, tres sellos de diez segundos —el tique, la caja abierta, el primer aviso— y ninguna discusión posible meses después.

1. La reseña con compra acreditada

El comprador real sella el justificante de compra en su dispositivo y publica la reseña acompañada de la prueba: la huella que acredita que la compra existe, sin revelar ni el nombre ni los datos del comprador [5]. La plataforma marca estas opiniones con un distintivo verificable; el lector filtra por «compra acreditada»; y el mercado negro de reseñas pierde su materia prima [2]. La norma de la FTC pone las multas [1]; la prueba de existencia pone el mecanismo que las hace casi innecesarias.

2. La serie de precios que no miente

Observatorios de consumo, plataformas honestas o la ciudadanía organizada registran los precios con capturas selladas —cada precio, cada día, con fecha cierta [5]. Cuando llega la campaña de descuentos, el «precio anterior» se contrasta contra la serie anclada: si el 99 % de los carteles no resiste la regla de los 30 días [3], que lo tenga que demostrar la serie, no la paciencia del comprador. La transparencia de precios deja de depender de la buena fe del cartel.

3. La caja abierta con fecha cierta

El día que llega el paquete, treinta segundos de vídeo o cuatro fotos selladas en el momento: el estado del producto, el número de serie, el contenido de la caja [5]. Si el producto llegó dañado, la prueba existe desde el minuto uno y el reembolso no admite dilaciones; si el comprador reclama un daño que él mismo

causó, la ausencia de prueba coetánea lo retrata. La guerra diaria del comercio electrónico —los daños de transporte, el fraude de devoluciones— se resuelve sobre imágenes con integridad acreditada, en las dos direcciones: el consumidor honesto cobra antes, y el tramposo topa con la criptografía.

4. El reloj de la garantía

La compra sellada activa los tres años con fecha cierta [4][5]; el primer aviso de defecto, anclado, fija si el problema apareció dentro de la presunción de los dos años [4]; y cada reparación sucesiva queda fechada, de modo que el producto que encadena averías dentro de garantía —el candidato a sustitución o reembolso — lleva su propia cronología. Para el vendedor diligente, el mismo registro es la defensa contra la reclamación extemporánea. La garantía más larga de Europa [4] vale lo que valga su prueba —y ahora la prueba es automática.

Los límites, dichos con claridad: el sello acredita que la compra, la foto o el aviso existían en una fecha — no acredita que la reseña sea sincera (un comprador real también puede cobrar por opinar), ni que el producto sea bueno, ni resuelve quién tiene razón en un defecto técnico: eso lo hacen peritos, plataformas y tribunales de consumo. Y la reseña con compra acreditada ha de preservar siempre el anonimato del comprador: acreditar la compra, nunca identificar a la persona [5].

La promesa y el peligro

La promesa: un mercado donde las estrellas tienen compra detrás [1][2], los descuentos resisten la regla de los 30 días [3] y la garantía de tres años se ejerce sin guardar tiques en una caja de zapatos [4]. Confianza de consumo con base verificable: más barata para el honesto, más cara para el tramposo.

Los peligros, con la misma claridad.

El primero es **el anonimato del comprador**. Acreditar la compra no puede significar identificar a la persona. Si el distintivo de «compra acreditada» exigiera nombre y perfil, habríamos cambiado reseñas falsas por vigilancia de consumidores. El diseño correcto: la prueba criptográfica de la compra viaja; la identidad, nunca [5].

El segundo es **la censura por verificación**. Si las plataformas solo publicaran reseñas con compra acreditada, silenciarían voces legítimas —el regalo recibido, la compra en otra tienda, la experiencia de servicio. El distintivo ha de filtrar y ponderar, no censurar: opinión libre para todos, peso verificable para quien la acredite.

El tercero es **el sello comprado**. El fraude se adapta: vendedores que «venden» productos a precio simbólico para cosechar compras acreditadas, series de precios selladas por tiendas fantasma. El sello acredita hechos, no buena fe —la vigilancia de patrones (compras masivas, precios imposibles) sigue siendo tarea de plataformas y reguladores [1][3].

Y el cuarto es **el tecnosolucionismo de consumo**. Ninguna huella hará los productos mejores ni los precios más justos; eso lo hacen la competencia, la inspección de consumo y las normas que ya existen [1][3][4]. El sello solo garantiza que las reglas del juego se puedan verificar. Un mercado puede ser perfectamente transparente y perfectamente caro.

Es hora de actuar

El consumidor decide con señales; que las señales vuelvan a ser de fiar.

Para ti, consumidor: sella el tique el día de la compra, la caja el día de la entrega y el primer aviso de defecto [4][5]; ante un descuento espectacular, recuerda el dato —solo uno de cada tres es real [3]; y ante mil estrellas unánimes, busca la compra acreditada [2].

Para las plataformas de comercio y reseñas: implantad la reseña con compra acreditada y anónima [1][2][5] y publicad series de precios ancladas —la credibilidad es vuestro producto.

Para los comercios honestos: el descuento verificable contra la serie sellada [3][5] es vuestro mejor argumento contra el cartel inflado de al lado.

Para las autoridades de consumo: exigid la regla de los 30 días contra series de precios ancladas [3] y aceptad la cronología sellada —compra, desembalaje, avisos— como prueba preferente en las

reclamaciones de garantía [4].

Para los reguladores: la norma de la FTC marca el camino [1]; completadla con el mecanismo —presunción de validez para la compra acreditada anónima y sanciones para los indicadores sociales fabricados.

Diez dólares por reseña, 43.000 miembros en un solo grupo [2]: la confianza del consumidor se había convertido en mercancía. Que vuelva a ser lo que era —una señal honesta entre desconocidos. Por el carrito de la compra de cada día, **time2act**.

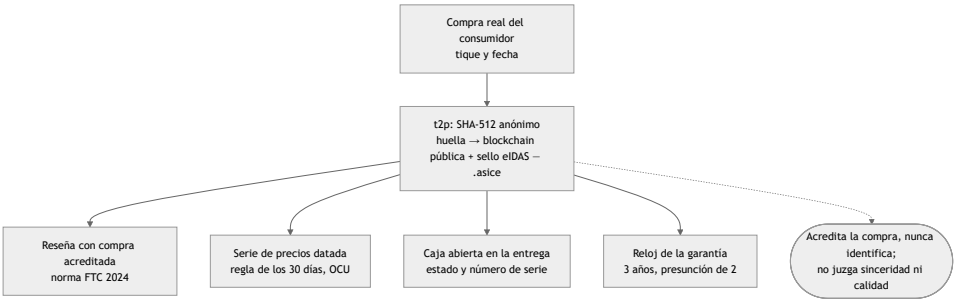


Figura 30.1 — La capa de información del consumidor con prueba de existencia: la reseña con compra acreditada y anónima (el justificante sellado en el dispositivo; el mercado negro de reseñas se queda sin materia prima), la serie de precios con fecha cierta (la regla del menor precio de los 30 días se vuelve verificable) y el reloj de la garantía (compra, unboxing y avisos sellados activan y acreditan los 3 años legales). Límites: el sello no juzga la sinceridad ni la calidad; la acreditación de compra nunca puede identificar al comprador. Fuentes: FTC (norma 2024); Amazon vs. grupos de Facebook; OCU (Black Friday); CEC/Consumo (garantía de 3 años).

---

[1] Federal Trade Commission — *FTC Announces Final Rule Banning Fake Reviews and Testimonials* (14 de agosto de 2024; en vigor el 21 de octubre de 2024; hasta 51.744 $ por infracción; prohíbe la compraventa de reseñas, las reseñas de insiders sin revelación, las webs de reseñas controladas, la supresión selectiva y los indicadores falsos de influencia social); Federal Register — *Trade Regulation Rule on the Use of Consumer Reviews and Testimonials*. https://www.ftc.gov/news-events/news/press-releases/2024/08/federal-trade-commission-announces-final-rule-banning-fake-reviews-testimonials · https://www.federalregister.gov/documents/2024/08/22/2024-18519/trade-regulation-rule-on-the-use-of-consumer-reviews-and-testimonials ↩

[2] Infobae — *Amazon demanda a miles de grupos de Facebook por publicar reseñas falsas* (19 de julio de 2022; más de 10.000 grupos; EE. UU., Reino Unido, Alemania, Francia, Italia, España y Japón); Marketing4eCommerce — *Amazon denuncia a los administradores de más de 10.000 grupos de Facebook* («Amazon Product Review», más de 43.000 miembros; 10 $ por reseña; más de 10.000 grupos reportados a Meta desde 2020, la mitad eliminados); La Nación — *Amazon demanda a los administradores de 10.000 grupos de Facebook*. https://www.infobae.com/america/agencias/2022/07/19/amazon-demanda-a-miles-de-grupos-de-facebook-por-publicar-resenas-falsas/ · https://marketing4ecommerce.net/amazon-reviews-falsas/ · https://www.lanacion.com.ar/tecnologia/amazon-demanda-a-los-administradores-de-10000-grupos-de-facebook-por-promover-resenas-falsas-nid19072022/ ↩

[3] OCU — *Black Friday: descuentos que no son reales* (solo 1 de cada 3 productos se abarata; subidas medias del 13 % en las semanas previas en categorías como relojes inteligentes, cámaras y auriculares; el 43 % de los productos dispara el precio; ahorro anunciado del 23 % vs precios reales un 3 % más caros; en el 99 % de los casos el «precio anterior» no es el menor de los últimos 30 días; monitorización desde septiembre); Público — *La trampa del Black Friday: precios inflados, rebajas ficticias*. https://www.ocu.org/consumo-familia/compras-online/noticias/bf-precios-rebajados · https://www.publico.es/sociedad/trampa-black-friday-precios-inflados-rebajas-ficticias-fiebre-compras-detiene.html ↩

[4] Centro Europeo del Consumidor en España (Ministerio de Consumo) — *España amplía la garantía legal mínima de dos a tres años* (desde el 1 de enero de 2022; transposición de las Directivas (UE) 2019/770 y 2019/771; presunción de origen del defecto ampliada de 6 meses a 2 años —1 año para segunda mano—; recambios durante 10 años; prescripción de 3 a 5 años); OCU — *Garantía de los productos: se amplía el plazo*. https://portal-cec.consumo.gob.es/en/comunicacion/noticias/2022/espana-amplia-la-garantia-legal-minima-de-dos-tres-anos · https://www.ocu.org/consumo-familia/derechos-consumidor/noticias/novedades-garantia ↩

[5] t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; acreditación sin identificación —la prueba de compra viaja, la identidad nunca; contenido en el dispositivo y revelación voluntaria). Véanse los capítulos 13 y 15; el origen del producto, en el capítulo 29. ↩

La segunda mano entre particulares: el estado del artículo, con fecha cierta

«La máxima es: doveriai, no proveriai — confía, pero verifica.»

— Ronald Reagan (con Gorbachov), firma del Tratado INF (1987)

El comprador abre la caja que acaba de llegar. Dentro, donde tenía que haber una consola, hay un ladrillo envuelto en papel de periódico. En la otra punta del país, un vendedor recibe una devolución «por defectos» y descubre que el móvil devuelto no es el que envió: otra carcasa, una pantalla con marcas de años. Dos víctimas del mismo vacío: entre desconocidos, el estado de un objeto en un momento dado no lo puede probar nadie.

Y el vacío es de país entero [1]: solo Wallapop tiene más de 19 millones de usuarios activos en España, y el mercado de segunda mano entre particulares mueve más de 13.000 millones de euros anuales. La cara oscura: las estafas en estas plataformas son el grueso de los más de 412.000 fraudes informáticos registrados en 2024, las denuncias crecieron un 60 % en 2025, y la Guardia Civil alerta periódicamente de las campañas [1].

Este capítulo trata el contrato más informal de la economía: la compraventa entre desconocidos. Las reseñas falsas y la garantía del comercio están en el capítulo 30; el cliente ante la gran compañía, en el capítulo 33; el anuncio falso de alquiler, en el capítulo 36; y el pago fuera de plataforma engañado —recuperar una transferencia— se trata en el capítulo 69. Pregunta clave: ¿cómo se prueba en qué estado estaba un objeto cuando cambió de manos? Respuesta: documentándolo con fecha cierta en los dos extremos del viaje —el vídeo antes de enviar y el vídeo al abrir— con **t2p**: la tríada del capítulo 13 —huella en el dispositivo, hora cierta y ancla en la cadena [3]. La simetría es total: el mismo gesto desarma el paquete que no es el prometido y el «cambiazo» de la devolución.

Las estafas simétricas

El repertorio está documentado [1], y vale la pena mirarlo de frente.

El **pago fuera de plataforma**: el anuncio con fotos impecables y un precio demasiado bueno, y la insistencia en cobrar por Bizum o transferencia «para ahorrar comisiones». Pagado el dinero, no llega nada —o llega cualquier cosa— y el comprador ha perdido la protección de la plataforma por el camino: el pago ya vive fuera de su marco de garantías. (El componente bancario —recuperar la transferencia engañada— es materia del capítulo 69.)

El **fraude por triangulación y el «cambiazo»**: el estafador compra con envío, recibe el artículo en buen estado y presenta inmediatamente una queja alegando defectos —aprovechando la protección que retiene el pago hasta que el comprador valida. Pide la devolución, se queda el artículo bueno y devuelve otro destartalado. El vendedor honesto se queda sin dinero y sin su producto —y ante la plataforma, solo tiene su palabra.

El **phishing del «confirma el pago»**: el enlace que imita la interfaz de la plataforma y pesca credenciales; y las **etiquetas de envío fraudulentas** y suplantaciones que visten el engaño de legitimidad [1].

El diagnóstico probatorio: la compraventa entre particulares no tiene factura ni garantía comercial —el vicio oculto civil es el único recurso de fondo— y toda la evidencia vive en fotos de anuncio sin fecha fiable, chats y seguimientos ambiguos. Cuando la plataforma arbitra, decide con esto: palabras e imágenes que cualquiera puede fabricar o reutilizar. El desconocido honesto no tiene manera de distinguirse del desconocido estafador —y esta es exactamente la clase de problema que la fecha cierta resuelve.

La prueba de existencia aplicada

Diez segundos en cada extremo del viaje [3].

1. El artículo documentado antes de enviar

El vendedor filma el artículo con t2p antes de empaquetar: el estado general, el número de serie, comprobando su funcionamiento si procede —con la fecha y la hora sobreimpresas en el vídeo y el GPS forense del lugar [3]. Treinta segundos que fijan un hecho: este objeto, en este estado, existía así en este momento. La foto del anuncio puede ser vieja o de otro; el vídeo certificado, no.

2. El precintado en plano secuencia

El artículo entrando en la caja, el cierre, la etiqueta de envío pegada —un solo plano, sin cortes, certificado [3]. Es el gesto que desarma el «dentro no había nada»: el contenido y el paquete quedan ligados en un mismo vídeo fechado. Para los artículos de valor, es la diferencia entre una disputa perdida y una cerrada en cinco minutos.

3. La apertura simétrica

El comprador hace el mismo gesto en el otro extremo: el paquete cerrado con la etiqueta visible, la apertura, el contenido —en plano secuencia certificado [3]. Si dentro está el ladrillo, el vídeo lo acredita con fecha y lugar; si el artículo es el prometido, también. Y contra el «cambiazo» [1], la pareja de vídeos —el precintado del vendedor y la apertura del comprador, y los de la devolución en sentido contrario— convierte el arbitraje en una comparación: qué salió, qué llegó, qué se devolvió.

4. El expediente de la disputa

El anuncio capturado con fecha —las fotos y la descripción que se prometieron—, el chat con el acuerdo, el justificante de pago, el seguimiento del envío: agrupados en un proyecto [3] y exportables como paquete .asice verificable sin conexión. Para el arbitraje de la plataforma, para la denuncia a la Guardia Civil [1], para la reclamación civil: hechos fechados en lugar de capturas discutibles.

Y un primo hermano de esta economía entre particulares que merece su párrafo: el préstamo entre familia y amigos. El «te lo presté» que años después se convierte en «era un regalo» ha roto más amistades que ninguna estafa. El acuerdo breve sellado en el momento de dejar el dinero —el importe, el pacto de devolución, dos líneas con fecha cierta [3]— protege al prestamista y, sobre todo, protege la relación: cuando los términos son un hecho, la memoria no tiene que hacer de árbitro.

Los límites, antes de que nadie se haga ilusiones: el sello acredita estados y momentos —no decide si el precio era justo ni si el defecto era vicio oculto: eso lo valoran la plataforma, el perito o el juez. La proporcionalidad manda: la venta de 10 euros no necesita expediente; la de 500, quizá sí —que cada uno calibre. Y nunca se graba al repartidor ni a ningún tercero: se documenta el objeto, no las personas.

La promesa y el peligro

La promesa: disputas que se resuelven por comparación de vídeos fechados y no por la intuición de un moderador [1][3]; el «cambiazo» que deja de ser rentable porque el artículo devuelto se contrasta con el precintado; vendedores y compradores honestos que se distinguen de los estafadores con un gesto de diez segundos; y un mercado de 13.000 millones [1] que gana la confianza que le faltaba para crecer.

Los peligros, sin ambages.

El primero es **el teatro probatorio**. El estafador también puede filmar: un vídeo con el artículo bueno y el envío de otro. Por eso el método importa: el plano secuencia sin cortes hasta la etiqueta, el GPS forense que no admite ubicaciones simuladas [3], y la pareja simétrica de vídeos —un teatro tiene que engañar a las dos cámaras y a las dos fechas a la vez, y eso ya no es un timo barato.

El segundo es **la fricción que mata la venta**. Si vender un libro de segunda mano exige un rodaje, nadie lo hará. La respuesta es la proporcionalidad: el gesto corto para las ventas normales, el expediente completo para las valiosas —y las plataformas integrándolo para que cueste un clic.

El tercero es **la plataforma como juez opaco**. Los arbitrajes internos deciden con reglas propias y sin apelación real. El rastro verificable les pone fácil decidir bien; el paso de fondo es que valoren evidencia anclada por encima de capturas —y que lo digan en sus normas.

Y una última trampa: fiarse de que la herramienta vigile por ti. Ningún sello sustituye la prudencia elemental: pagar dentro de la plataforma, desconfiar del Bizum a desconocidos y de los enlaces de «confirmación» [1]. La fecha cierta protege la transacción legítima; la estafa del pago por fuera se combate no picando.

Es hora de actuar

Que el desconocido honesto gane siempre.

Para vendedores y compradores: el gesto de diez segundos en cada extremo —el artículo, el precintado, la apertura [3]; y para las ventas que valen, el expediente entero.

Para las plataformas: integrad la evidencia con fecha cierta en vuestros arbitrajes [1][3] —resolveréis más rápido, expulsaréis a los profesionales del «cambiazo» y vuestro sello de confianza será algo más que marketing.

Para los transportistas: el peso y el estado del paquete en la admisión, anclados —vuestra parte de la cadena también cuenta.

Para la Guardia Civil y las autoridades de consumo: las denuncias crecen un 60 % al año [1]; el expediente .asice del ciudadano es la diferencia entre archivar e investigar.

Para los legisladores: la compraventa entre particulares es la economía real de millones de personas [1]; que la protección del consumidor digital reconozca la evidencia anclada —de las dos partes— como prueba cualificada.

El próximo paquete que envíes o recibas, que lleve su momento de verdad grabado. Por un mercado de vecinos donde el desconocido honesto gane siempre, **time2act**.

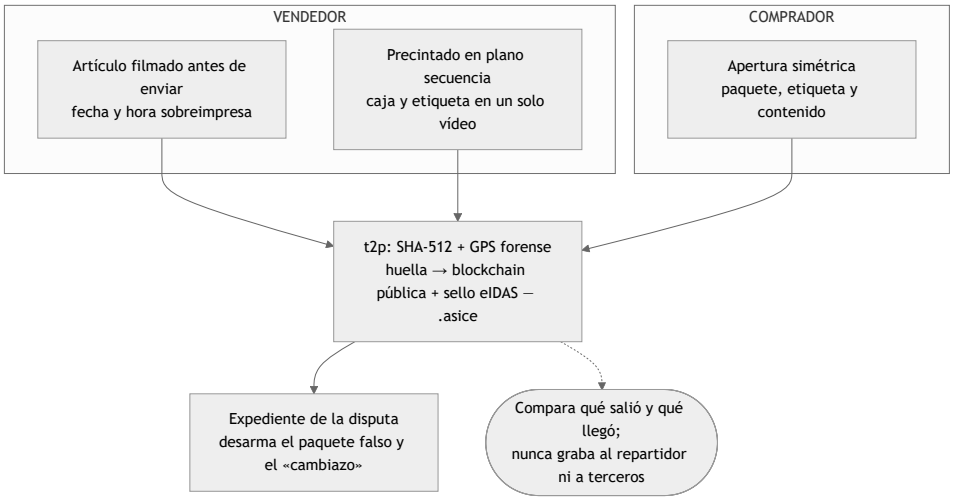


Figura 31.1 — La segunda mano entre particulares con prueba de existencia (sellado con t2p — capítulo 13): el artículo filmado antes de enviar (fecha/hora sobreimpresa + GPS forense), el precintado en plano secuencia, la apertura simétrica del comprador y el expediente de la disputa (anuncio capturado, chat, pago, seguimiento). Simetría total: desarma el paquete falso Y el «cambiazo». Contexto: >19 M de usuarios en Wallapop; >13.000 M€/año; las estafas de segunda mano, grueso de los >412.000 fraudes informáticos de 2024 (+60 % de denuncias en 2025). Límites: proporcionalidad según valor; el vicio oculto lo valora el perito; nunca grabar a terceros. Fuentes: Guardia Civil/prensa especializada.

---

[1] Digital Perito — *Estafas en Wallapop y Vinted: cómo denunciar con pruebas* (>19 millones de usuarios activos en Wallapop en España; mercado de segunda mano >13.000 M€ anuales; las estafas de plataformas de segunda mano como grueso de los >412.000 fraudes informáticos de 2024; +60 % de denuncias en 2025); Público — *Así operan los estafadores en plataformas de segunda mano* (tipologías: pago fuera de plataforma, triangulación/«cambiazo» aprovechando la protección al comprador, phishing, etiquetas fraudulentas, suplantación); OKDiario / Genbeta — alertas de la Guardia Civil y trucos de detección. https://digitalperito.es/blog/estafas-wallapop-vinted-como-denunciar-pruebas-2026/ · https://www.publico.es/sociedad/asi-operan-estafadores-plataformas-segunda-mano-vinted-wallapop.html · https://okdiario.com/curiosidades/fraude-que-arrasa-plataformas-segunda-mano-guardia-civil-lanza-advertencia-sobre-vinted-wallapop-15912396 · https://www.genbeta.com/seguridad/estas-estafas-wallapop-comunes-varios-trucos-para-pillarlas-rapidamente ↩

[2] Marco civil de la compraventa entre particulares (vicio oculto; ausencia de garantía comercial de consumo). Véase el capítulo 30 para la garantía B2C y el capítulo 36 para la estafa del anuncio falso.

[3] t2p — manual de producto (vídeo con fecha/hora sobreimpresa; foto con GPS forense —fijado genuino ~50 m / ≤30 s, la ubicación simulada bloquea la certificación; captura de pantalla certificada; certificar cualquier archivo; proyectos para agrupar el expediente de una venta; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; el pago engañado, en el capítulo 69. ↩

El alquiler de cosas: el estado al recoger y al devolver

«No seas prestatario ni prestamista, / pues el préstamo a menudo se pierde a sí mismo y pierde al amigo.»

— William Shakespeare, Hamlet, I, 3 (c. 1600)

El aeropuerto, la cola del mostrador de alquiler, la vuelta rápida al coche con la hoja de daños en la mano —«¿este rasguño ya está?»— y la devolución con prisa: el buzón de llaves, el avión. Tres semanas después, el correo: «cargo por daños: 460 €», con dos fotos hechas quién sabe cuándo.

No es mala suerte: es un patrón documentado [1]. El informe oficial sobre prácticas irregulares de compañías españolas de alquiler describe indemnizaciones desproporcionadas —de 300 a 1.000 euros por rasguños o desperfectos pequeños— cargadas directamente a la tarjeta del depósito, con el carácter y la cuantía fijados unilateralmente por la empresa; y el Centro Europeo del Consumidor documenta los cargos posteriores por limpieza o daños menores decididos en revisiones hechas sin la presencia del consumidor, que queda obligado a asumirlos sin conocimiento expreso [1]. Ha habido condenas: un líder europeo del sector fue condenado a devolver daños cobrados indebidamente [1].

Y la ironía que da pie al capítulo: el propio CEC recomienda devolver el coche con la oficina abierta, revisarlo con el personal y «hacer fotografías del interior y el exterior… podrán servir como prueba» [1]. El regulador ya ha entendido que esto va de pruebas; lo que falta es que las fotos del consumidor valgan tanto como la inspección de la empresa.

Este capítulo trata el contrato sobre el estado de una cosa. El inventario bilateral del piso alquilado está en el capítulo 36; el estado de la cosa vendida entre particulares, en el capítulo 31; el coche compartido entre iguales, en el capítulo 26; el cargo que vuelve y la reclamación a la compañía, en el capítulo 33; la devolución del recibo a la tarjeta, en el capítulo 69. Pregunta clave: ¿cómo se discute el estado de una cosa en dos momentos si ninguno de los dos momentos tiene registro oponible? Respuesta: con el vídeo de estado en los dos extremos del alquiler —al recoger y al devolver— sellado con **t2p** —la mecánica de siempre, la del capítulo 13 [2]. Y con la simetría de siempre: el mismo rastro protege a la empresa honesta del cliente que niega el golpe.

La asimetría del mostrador

El problema, pieza a pieza. La **hoja de daños inicial**: un dibujo con cruces que el cliente firma con prisa, a menudo sin luz ni tiempo para repasarlo. La **franquicia y el depósito**: la tarjeta retenida que permite cobrar primero y discutir después. La **inspección de devolución**: cuando la oficina está cerrada o el cliente ya vuela, el estado lo determina la empresa sola, sin contrapeso [1]. El **precio del desperfecto**: baremos internos, no presupuestos —el rasguño valorado en centenares de euros según una tabla que el cliente no ha visto nunca [1]. Y la **distancia**: el turista extranjero que no volverá para reclamar.

La extensión B2B reproduce el mismo esquema con importes más grandes: el alquiler de maquinaria de obra y de equipos profesionales —el estado inicial de la retroexcavadora, las horas de uso, el daño «descubierto» a la devolución— a menudo entre empresas que se necesitarán la una a la otra la temporada siguiente.

El diagnóstico probatorio: el alquiler es un contrato sobre el estado de una cosa en dos momentos —y ninguno de los dos momentos tiene, hoy, un registro que valga para las dos partes. Las fotos del cliente no tienen fecha oponible; la inspección de la empresa no tiene al cliente delante. Cuando el cargo llega, la discusión es la de siempre: tu palabra contra su tarjeta.

La prueba de existencia aplicada

Dos minutos en cada extremo del alquiler [2].

1. La vuelta de recogida

Antes de salir del aparcamiento, la vuelta completa filmada con t2p: la carrocería entera, las llantas, el interior, el cuadro con los kilómetros y el nivel de combustible —con la fecha y la hora sobreimpresas y el

GPS forense del aparcamiento (fijado genuino, precisión de unos 50 metros; una ubicación simulada bloquea la certificación) [2]. Cada rasguño preexistente, documentado; la hoja de cruces, escaneada y sellada. Dos minutos que valen exactamente lo que la empresa quiera reclamar después.

2. La vuelta de devolución

El mismo gesto al devolver —y aquí es donde se gana o se pierde todo: en la devolución fuera de horas, con el buzón de llaves y nadie de la empresa delante [1], el vídeo certificado del estado final es la única inspección con fecha cierta que existirá. El cargo de tres semanas después [1] topa con un hecho: así estaba el coche el día que lo devolví, a esta hora, en este aparcamiento.

3. El contrato y el cargo

El contrato, el inventario de estado y las condiciones de la franquicia, escaneados y sellados al firmar [2]; y cuando el cargo tardío llega, la reclamación fechada —a la empresa, al mediador de consumo, y si hace falta la devolución del recibo al banco, el camino que el capítulo 69 explica. El expediente .asice —vueltas, contrato, cargo, reclamación— verificable sin conexión por cualquiera [2].

4. La simetría del arrendador honesto

La empresa —o el particular que alquila su máquina— que documenta con el cliente delante tiene la misma protección: la inspección de entrega y la de devolución, filmadas y selladas, con el cliente presente o notificado [2]. Contra el cliente que niega el golpe nuevo, la pareja de vídeos responde; y el baremo del desperfecto, publicado y anclado por adelantado, convierte el precio del rasguño en una condición conocida, no en una sorpresa. En el B2B de la maquinaria, este expediente bilateral es sencillamente la diferencia entre conservar un cliente y perderlo en un pleito.

Los límites, negro sobre blanco: el sello acredita estados y momentos —no valora si el desperfecto es uso normal o daño, ni si el precio es proporcionado: eso lo dicen el contrato, el mediador y el juez [1]. La vuelta filmada ha de ser completa y con luz —un vídeo oscuro sella su propia inutilidad. Y la proporcionalidad de siempre: el patinete de diez euros no necesita expediente; el coche con franquicia de 1.200, sí.

La promesa y el peligro

La promesa: consumidores que devuelven el coche fuera de horas con la tranquilidad de un hecho fechado [1][2]; cargos tardíos que mueren al ver el expediente; empresas honestas que liquidan daños reales con evidencia bilateral y se desmarcan de las malas prácticas que ensucian el sector [1]; y el alquiler de cosas —del coche de vacaciones a la retroexcavadora— funcionando sobre estados verificables.

Y los peligros, uno por uno.

El primero es **el vídeo de mala fe**: filmar esquivando el golpe que ya has hecho. El método lo combate: la vuelta completa en plano secuencia, la fecha sobreimpresa, el GPS del aparcamiento [2] —y la pareja de vídeos: el que esconde un golpe en su vuelta, lo enseña en la del otro extremo.

El segundo es **la fricción del mostrador**. Si recoger un coche exige un ritual, el cliente no lo hará. Dos minutos, un gesto guiado —y las empresas que lo integren en su propio proceso (la vuelta conjunta filmada) lo convertirán en argumento de venta.

El tercero es **el baremo unilateral que sobrevive**. La prueba del estado no arregla el precio abusivo del rasguño [1]: eso es tarea del regulador de consumo y de los jueces. La fecha cierta hace la disputa limpia; la justicia del baremo es otra batalla.

Queda el cuarto: la tentación de delegarlo todo en el sello. Ningún sello sustituye devolver el coche con la oficina abierta cuando se puede [1], ni leer la franquicia antes de firmar. La prueba es para cuando la prudencia no basta.

Es hora de actuar

Que el estado de la cosa tenga dos testigos: uno en cada extremo.

Para ti, que alquilas: la vuelta de dos minutos en los dos extremos [2] —y si devuelves fuera de horas, no te la saltes nunca: es la única inspección que tendrás.

Para las empresas de alquiler: inspecciones bilaterales filmadas y baremos publicados por huella [1] [2] —el cargo documentado se cobra sin discusión, y el sector se limpia de la fama que lo acompaña.

Para el alquiler profesional y de maquinaria: el expediente de entrega y devolución como anexo estándar del contrato [2]; los pleitos de estado son los más evitables de vuestro negocio.

Para las autoridades de consumo y el CEC: ya recomendáis las fotos [1]; el paso siguiente es reconocer la evidencia con fecha cierta del consumidor como contrapeso formal de la inspección unilateral.

Para los legisladores: la revisión sin el cliente presente y el cargo unilateral a la tarjeta [1] son el agujero; que todo cargo por daños exija evidencia de estado verificable de los dos momentos.

El próximo buzón de llaves de aeropuerto, que no sea un acto de fe. Dos minutos de vídeo, y el coche devuelto queda devuelto —para ambos. Por el alquiler sin sorpresas, **time2act**.

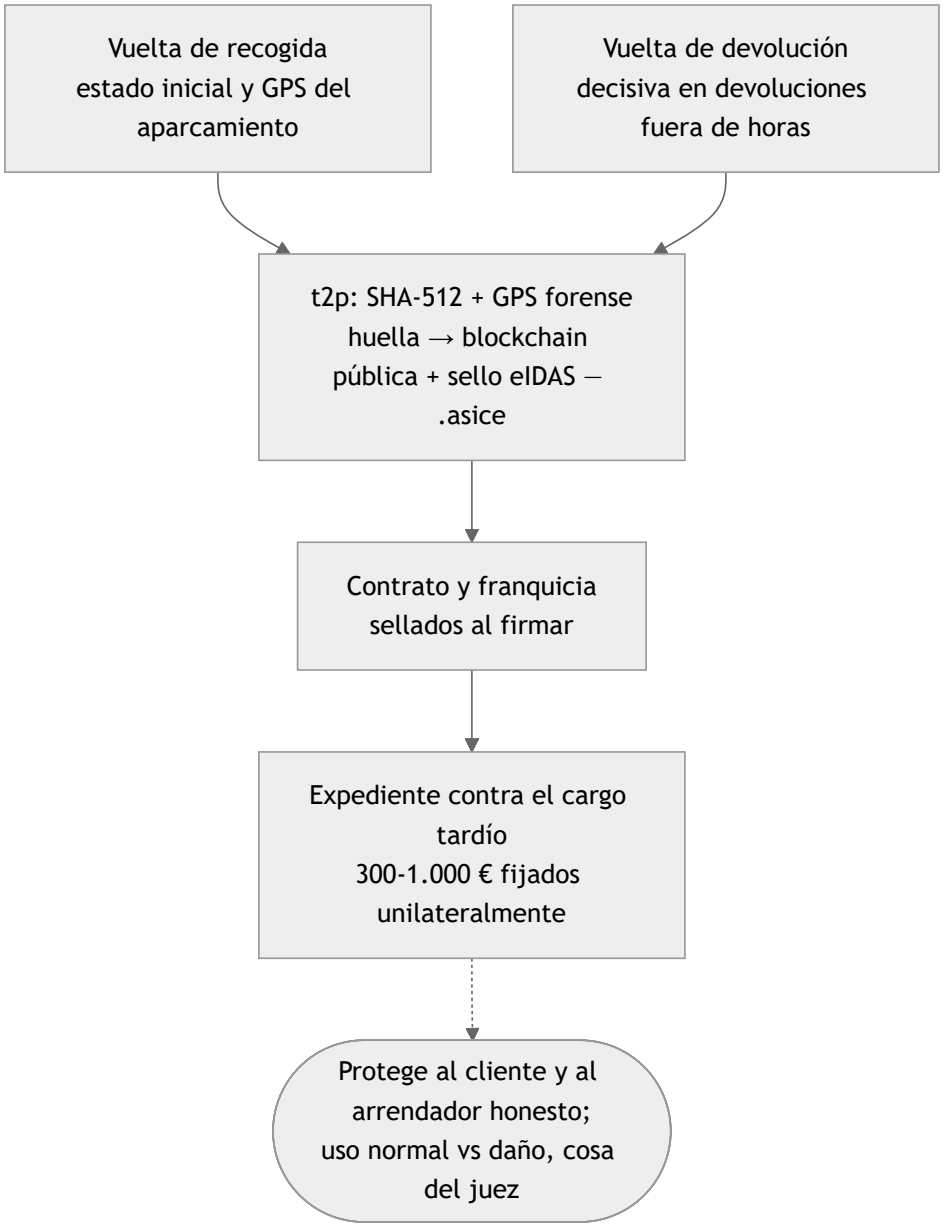


Figura 32.1 — El alquiler de cosas con prueba de existencia (sellado con t2p — capítulo 13): la vuelta de recogida filmada (fecha/hora sobreimpresa + GPS forense del aparcamiento), la vuelta de devolución —decisiva en devoluciones fuera de horas —, el contrato y la franquicia sellados, y el expediente contra el cargo tardío. Simetría: la inspección bilateral protege a la empresa honesta del cliente que niega el golpe; extensible al alquiler de maquinaria B2B. Contexto: prácticas irregulares documentadas (cargos de 300-1.000 € fijados unilateralmente; revisiones sin el cliente); el CEC ya recomienda fotos —faltaba la fecha cierta. Límites: uso normal vs daño y precios, cosa del contrato y el juez. Fuentes: Consumo/DSCA; CEC-España.

[1] Dirección General de Consumo (DSCA) — *Prácticas irregulares de compañías españolas de alquiler de coches* (indemnizaciones desproporcionadas de 300 a 1.000 € por rasguños o desperfectos pequeños, cargadas a la tarjeta del depósito con cuantía fijada unilateralmente); CEC-España (Centro Europeo del Consumidor) — *Alquiler de vehículos: derechos y recomendaciones* (cargos posteriores por limpieza o daños menores; revisiones sin la presencia del consumidor; recomendaciones: devolver con la oficina abierta, revisar con el personal, pedir justificante y «hacer fotografías del interior y el exterior como prueba»); AEA — *Líder europeo del rent-a-car condenado a devolver el importe de unos daños cobrados indebidamente*.
https://www.dsca.gob.es/sites/default/files/consumo_masinfo/PRACTICAS_IRREGULARES_ALQUILER_COCHES.pdf · https://portal-cec.consumo.gob.es/sites/default/files/documentos/Folleto_Alquiler_Coches.pdf · https://portal-cec.consumo.gob.es/en/comunicacion/noticias/2021/cec-espana-recuerda-los-derechos-de-las-personas-consumidoras-cuando · https://aeaclub.org/rent-a-car-reclamacion-coche-alquiler-cobro-indebido/ ↩

[2] t2p — manual de producto (vídeo con fecha/hora sobreimpresa; foto con GPS forense —fijado genuino ~50 m / ≤30 s, la ubicación simulada bloquea la certificación; escáner de documentos; proyectos para agrupar el expediente de un alquiler; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; el inventario del piso, en el capítulo 36; el estado de la cosa vendida, en el capítulo 31; el cargo a la tarjeta, en el capítulo 69. ↩

El cliente contra la compañía: la baja, la permanencia y el call center

«Si el pilar principal del sistema es vivir en la mentira, no es extraño que la amenaza fundamental contra él sea vivir en la verdad.»

— Václav Havel, El poder de los sin poder (1978)

La música de espera, un cuarto de hora largo, y por fin una voz: «llame mañana, que ahora el sistema no me funciona». Al día siguiente, otra voz: «le paso con el departamento de retenciones». Una oferta, una promesa —«le mantenemos el precio y la baja queda anotada»— y la sensación de haber terminado. Tres meses después, el cargo sigue llegando, y el servicio de atención al cliente responde con toda la tranquilidad del mundo: «no consta ninguna solicitud de baja». Nadie recuerda exactamente qué se dijo; solo queda un acuerdo verbal que nunca se ha materializado.

Es la queja de consumo más cotidiana del país, y el desequilibrio que la alimenta es estructural: la compañía graba cada llamada «para garantizar la calidad del servicio» —pero la grabación la tiene ella; el código de la reclamación lo genera su sistema; el registro de la baja vive en sus servidores. Cuando la disputa llega, el cliente aporta su memoria; la compañía, su base de datos. La Ley 10/2025 acaba de dar derechos nuevos al consumidor [1] —pero un derecho sin prueba propia es un derecho que depende de la buena fe del otro.

Este capítulo trata la relación probatoria del cliente con la gran compañía de servicios: la baja, la permanencia, el cargo que vuelve, la promesa del call center. Las reseñas, los precios y la garantía del producto están en el capítulo 30; la relación con la Administración pública, en el capítulo 44; la licitud y la técnica de grabar las conversaciones propias —la STC 114/1984—, en el capítulo 75; la voz clonada que llama haciéndose pasar por ti, en el capítulo 68. Pregunta clave: ¿cómo se ejerce un derecho cuando toda la evidencia vive en casa del adversario? Respuesta: documentando cada gestión en el momento con **t2p** —el paquete probatorio que el capítulo 13 desgrana pieza a pieza [3]— de modo que la fecha cierta quede, por fin, también del lado del cliente. Y con la neutralidad de siempre: el mismo rastro acredita a la compañía diligente que atiende bien y tramita a tiempo.

Derechos nuevos, prueba vieja: la Ley 10/2025

La novedad legislativa es de primer orden [1]: la Ley 10/2025, de 26 de diciembre, de servicios de atención a la clientela —publicada en el BOE el 27 de diciembre de 2025, con doce meses para que las empresas se adapten— impone obligaciones concretas y medibles. Atender el 95 % de las llamadas en menos de tres minutos de media. Asignar a cada consulta, queja, reclamación o incidencia un código identificativo que permita seguir su estado. Responder las reclamaciones en quince días como máximo —y en solo cinco los cargos no autorizados. Avisar con quince días de antelación de cada renovación automática, facilitando la cancelación. Hacer la baja sencilla, sin laberintos: basta con el DNI y el número de contrato. Y prohibir la atención exclusivamente automatizada: el cliente tiene derecho a un operador humano.

Sobre el papel, es un antes y un después. Pero míralo con los ojos de este libro y verás el agujero: la ley da derechos; no da pruebas. ¿Quién acredita que la llamada duró cuarenta y siete minutos? ¿Que la baja se pidió el día 3 y no el 28? ¿Que el cargo era no autorizado y se comunicó dentro de plazo? ¿Que la renovación llegó sin aviso? El código de seguimiento lo genera y lo custodia la compañía; el expediente entero vive en sus bases de datos. Un derecho sin prueba propia se ejerce por cortesía del adversario —y la cortesía, en un call center con objetivos trimestrales, no es una garantía procesal.

Cuando el cargo vuelve: los casos

Las sanciones existen, y dibujan el mapa del problema [2].

Vodafone fue multada con 20.000 euros por cobrar a una consumidora servicios de terceros que ella había desconectado: vulneró hasta tres veces su derecho de desconexión y obstruyó la inspección de consumo; acabó asumiendo la responsabilidad y pagando 20.100 euros con la reducción legal. Movistar recibió una multa de 20.000 euros después de que una gestora de cobros acosara a una consumidora por una deuda falsa de 1.741 euros —tres líneas que nunca había contratado. Y Telefónica arrastra una multa de 765.000 euros, confirmada por el Tribunal Supremo, por limitar el derecho de sus clientes a recibir la factura en

papel. En la misma lista de agravios, las asociaciones de consumidores mantienen denunciadas las penalizaciones por baja anticipada que consideran cláusulas abusivas [2].

La lección común es la de este libro: todas estas sanciones llegaron porque alguien pudo documentar lo que pasaba —y a menudo tras años de lucha. Por cada caso que acaba en multa, ¿cuántos mueren en la primera llamada, cuando el cliente no puede probar ni siquiera que llamó? La normativa de consumo reconoce el derecho a la baja en la misma forma en que se contrató; lo que falta es que el hecho de pedirla deje un rastro verificable en manos de quien la pide.

La prueba de existencia aplicada

El mismo teléfono que hace la gestión puede sellarla [3].

1. La baja sellada

El cliente hace la gestión y la documenta en el momento: la grabación de su propia llamada —conversación propia, lícita, como explica el capítulo 75—, la captura de pantalla certificada del formulario de baja enviado o del chat con el bot, el correo de confirmación escaneado [3]. Cada pieza recibe su huella SHA-512 en el dispositivo y su fecha cierta. La solicitud de baja del día 3 se convierte en un hecho, diga lo que diga el sistema de la compañía el día 28 —y el certificado PDF con código QR se adjunta a la reclamación de consumo tal cual.

2. El contrato y sus versiones

Las condiciones publicadas el día que contrataste, capturadas con el navegador integrado de t2p —la imagen completa de la página y su código fuente, empaquetados y certificados [3]; el contrato escaneado, hasta 50 páginas en un único PDF; y cada modificación unilateral, capturada con su fecha. Cuando la tarifa «para siempre» sube al octavo mes, la comparación es aritmética: esto decías, esto dices.

3. La llamada y la promesa

La promesa verbal —«le mantenemos el precio un año más si se queda»— grabada por quien la recibe, con el modo de audio que sigue en segundo plano [3], y sellada al colgar. La oferta de retención que después «no consta» deja de ser indemostrable. Y los proyectos de la app agrupan el expediente entero del caso —llamadas, capturas, correos— ordenado y fechado [3].

4. El expediente del cliente — y la simetría

Cuando la reclamación llega a consumo o al juzgado, el cliente exporta el paquete .asice: cada pieza con su huella, su sello de tiempo y las instrucciones de verificación, comprobable por cualquiera sin confiar en nadie [3]. Y la simetría de siempre: la compañía diligente —la que atiende en dos minutos, tramita la baja el día 3 y responde en cinco días— tiene en sus propios registros anclados la mejor defensa contra la reclamación infundada y la mejor evidencia de cumplimiento de la Ley 10/2025 [1].

Y los límites, que también los hay: el sello acredita gestiones —qué pediste, cuándo, qué te respondieron—, no da la razón de fondo: si la penalización era procedente o la tarifa correcta, lo dirán la ley y el juez. La grabación es siempre de conversaciones propias, nunca de terceros, y la protección de datos del teleoperador exige proporcionalidad: se documenta la gestión, no se persigue a la persona que atiende. Y ninguna huella sustituye la reclamación formal dentro de plazo.

La promesa y el peligro

La promesa: el cliente que ejerce los derechos de la Ley 10/2025 con el expediente en la mano [1][3]; reclamaciones de consumo que se resuelven sobre hechos fechados y no sobre versiones; malas prácticas —el cargo que vuelve, la baja que «no consta» [2]— que dejan de ser rentables porque dejan rastro; y la compañía honesta que se distingue con pruebas, no con eslóganes.

Los peligros, con la misma franqueza.

El primero es **la guerra de grabaciones**. Si cada llamada se convierte en un campo de minas probatorio, la relación se degrada para todos. La respuesta es la proporcionalidad: se documenta la gestión que importa —la baja, el cargo, la promesa contractual—, no cada interacción humana; y la

grabación propia es un escudo para la disputa, nunca un instrumento de acoso contra el trabajador que atiende.

El segundo es **la asimetría que persiste**. El cliente con herramientas sigue siendo más débil que la compañía con departamento jurídico. La prueba nivela la disputa concreta; la protección real es colectiva —asociaciones de consumidores, autoridades con régimen sancionador, y la Ley 10/2025 aplicada de verdad [1][2].

El tercero es **el tecnosolucionismo del ticket**. Ningún sello hace que te cojan el teléfono en tres minutos ni que la baja sea sencilla: eso lo tiene que hacer cumplir el regulador. La prueba hace el incumplimiento visible y reclamable; que tenga consecuencias es tarea de quien sanciona.

Y el cuarto es **la privacidad del expediente**. El expediente del cliente contiene su vida de consumo: ha de quedar en su dispositivo —solo huellas en la cadena [3]—, revelarse selectivamente ante el órgano que corresponda, y no convertirse nunca en un perfil comercializable.

Es hora de actuar

Que la palabra del cliente pese tanto como la base de datos de la compañía.

Para ti, cliente: documenta las gestiones que importan —la baja, el cargo no autorizado, la promesa de tarifa— en el momento y con fecha cierta [3]; y reclama dentro de plazo: la Ley 10/2025 te da quince días de respuesta máxima, y cinco para los cargos no autorizados [1].

Para las asociaciones de consumidores: recomendad el expediente sellado como práctica estándar de reclamación [2][3]; cada caso documentado es jurisprudencia en potencia.

Para las compañías: anclad vuestros registros de atención —el código de seguimiento de la Ley 10/2025 [1] con fecha cierta verificable es vuestra prueba de cumplimiento y el fin de la reclamación infundada.

Para las autoridades de consumo: valorad la evidencia anclada del consumidor como lo que es —fecha cierta neutral— y exigid a las compañías registros igualmente verificables [1][2].

Para los legisladores: el despliegue de la Ley 10/2025 [1] es la ocasión: que el código identificativo de cada reclamación lleve sello de tiempo cualificado, y que el registro de la baja sea verificable por las dos partes.

La próxima vez que una voz diga «llame mañana», que el mañana tenga fecha cierta. Por el cliente que cumple y por la compañía que atiende, **time2act**.

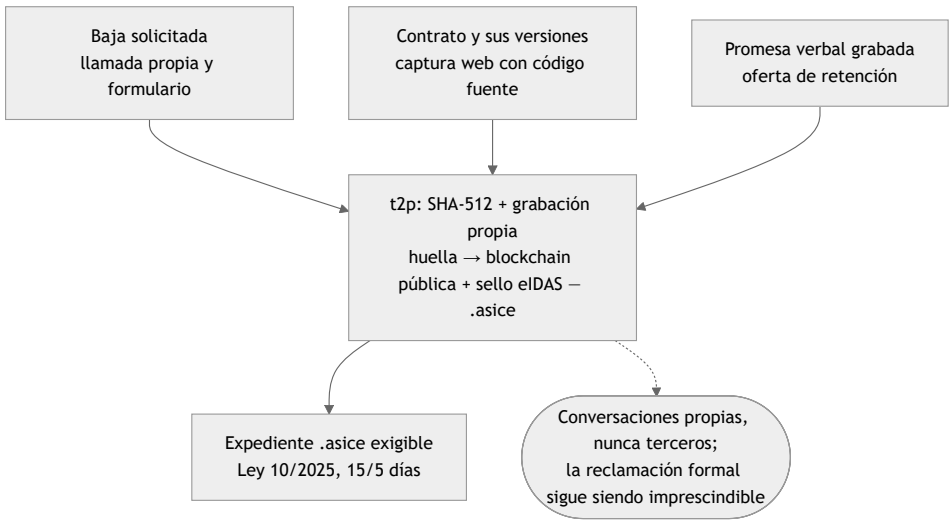


Figura 33.1 — El cliente ante la compañía con prueba de existencia (sellado con t2p — capítulo 13): la baja sellada (grabación de la llamada propia, captura certificada del formulario), el contrato y sus versiones (captura web con código fuente), la promesa verbal grabada y el expediente .asice exportable a consumo. La Ley 10/2025 da los derechos (3 minutos, código de seguimiento, 15/5 días, baja simple); la fecha cierta los hace exigibles —y acredita a la compañía diligente. Límites: conversaciones propias, proporcionalidad con el teleoperador, la reclamación formal sigue siendo imprescindible. Fuentes: BOE (Ley 10/2025); FACUA (multas Vodafone/Movistar/Telefónica).

[1] BOE — *Ley 10/2025, de 26 de diciembre, por la que se regulan los servicios de atención a la clientela* (BOE 27-12-2025; 12 meses de adaptación; 95 % de llamadas en <3 minutos; código identificativo de seguimiento; respuesta en 15 días —5 para cargos no autorizados; aviso 15 días antes de renovaciones automáticas; baja sencilla con DNI y número de contrato; prohibición de atención exclusivamente automatizada); La Moncloa — *Ley de Servicios de Atención a la Clientela: objetivos y medidas*; Sepín — *Novedades de la Ley 10/2025.* https://www.boe.es/buscar/act.php?id=BOE-A-2025-26698 · https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/derechos-sociales-consumo-agenda-2030/paginas/2025/ley-servicios-atencion-al-cliente.aspx · https://blog.sepin.es/blog/2026/01/14/novedades-ley-10-2025-servicios-atencion-clientela/ ↩

[2] FACUA — *Multa de 20.000 euros a Vodafone: cobró a una socia de FACUA servicios de terceros que había desconectado* (vulneración del derecho de desconexión hasta tres veces; obstrucción a la inspección; 20.100 € con reducción); FACUA — *Multa a Movistar por acosar a través de una gestora de cobros a una socia por una deuda falsa* (1.741 € por líneas nunca contratadas); FACUA — *El Supremo confirma la multa de 765.000 € a Telefónica por limitar el derecho a recibir facturas en papel*; Xataka Móvil — *FACUA denuncia a Telefónica por la penalización por baja anticipada.* https://facua.org/noticias/multa-de-20-000-euros-a-vodafone-cobro-a-una-socia-de-facua-servicios-de-terceros-que-habia-desconectado/ · https://www.facua.org/es/noticia.php?Id=9279 · https://facua.org/noticias/el-supremo-confirma-la-multa-de-765000-de-la-junta-de-andalucia-a-telefonica-por-limitar-el-derecho-a-recibir-facturas-en-papel/ · https://www.xatakamovil.com/conectividad/facua-denuncia-a-telefonica-por-la-penalizacion-por-baja-anticipada-en-movistar-fusion ↩

[3] t2p — manual de producto (grabación de audio en segundo plano; captura y grabación de pantalla certificadas con verificación de la app en primer plano; captura de página web con imagen completa + código fuente; escáner de documentos hasta 50 páginas; proyectos para agrupar capturas por caso; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión; solo huellas en la cadena). Véanse los capítulos 13 y 15; la licitud de grabar conversaciones propias, en el capítulo 75; la voz clonada, en el capítulo 68. ↩

La factura y la morosidad: el reloj del cobro

«Recuerda que el tiempo es dinero.»

— Benjamin Franklin, «Consejos a un joven comerciante» (1748)

Un taller de carpintería en un polígono cualquiera. El pedido —muebles a medida para una cadena de restaurantes— sale por el muelle por la tarde, con el albarán firmado de cualquier manera sobre el capó de la furgoneta. La factura se envía por correo electrónico al día siguiente. Y comienza la espera: «la semana que viene», «está pendiente de validación», «no nos consta». Mientras tanto, las nóminas del taller no esperan: la caja adelanta lo que el cliente grande no paga.

La escena tiene ley desde hace veinte años —y la ley tiene datos que dan vergüenza [2]. La Ley 3/2004 fija plazos máximos de pago entre empresas: 60 días naturales como máximo pactado, 30 por defecto desde la recepción de la mercancía o del servicio; establece un interés de demora automático —sin necesidad de aviso, y que el primer semestre de 2025 era del 11,15 %— y 40 euros fijos de costes de cobro por factura. La realidad, según el informe de 2025 de la Plataforma Multisectorial contra la Morosidad: el 85 % de las grandes compañías incumple los plazos legales, financiándose en parte a costa de sus proveedoras; las Administraciones Públicas pagan de media a 70 días —más del doble de su límite de 30—, y el sector privado, a 67 [2].

¿Por qué una ley con intereses automáticos se incumple masivamente y casi nadie los reclama? Porque reclamar exige probar: la fecha de la entrega, la fecha de recepción de la factura, el inicio exacto del cómputo. Y estas fechas viven en papeles de parte, correos discutidos y albaranes que se pierden. Este capítulo trata el desierto probatorio entre la emisión y el cobro —y cómo la fecha cierta lo atraviesa. La financiación del comercio internacional —cartas de crédito, conocimientos de embarque— está en el capítulo 54; la evidencia contable para el auditor, en el capítulo 55; el pedigrí de la mercancía misma, en el capítulo 29; el cliente particular ante la compañía, en el capítulo anterior. Pregunta clave: ¿cuándo empieza, exactamente, el reloj del cobro? Respuesta: cuando la entrega y la factura tienen fecha cierta oponible entre privados —la huella SHA-512 en el dispositivo, el anclaje de la huella en la blockchain pública y el sello de tiempo RFC 3161/eIDAS complementario de **t2p**, dentro de un contenedor .asice [3]. Y el Estado, sin decirlo con estas palabras, acaba de dar la razón a esta tesis: se llama VeriFactu.

VeriFactu: el Estado construye media prueba

El Real Decreto 1007/2023 —desarrollo de la ley antifraude— impone una arquitectura nueva a todos los programas de facturación, los llamados SIF [1]. Cada factura debe generar un registro normalizado con una **huella encadenada**: el hash de cada registro incorpora el hash del anterior, formando una cadena donde cualquier alteración retrospectiva canta. Cada registro se firma electrónicamente, y la factura lleva un **código QR** que permite contrastarla con la Agencia Tributaria. Hay dos maneras de cumplir: la modalidad «Verifactu» —envío inmediato y voluntario de los registros a la AEAT— o la conservación inalterable de la cadena a disposición de la Inspección [1].

El calendario, tras el aplazamiento de un año aprobado por el Real Decreto-ley 15/2025, de 2 de diciembre: obligatorio el 1 de enero de 2027 para las sociedades y el 1 de julio de 2027 para el resto de obligados. Las sanciones no son simbólicas: hasta 50.000 euros por ejercicio para quien use software no conforme, y hasta 150.000 para los fabricantes que lo vendan [1].

Detente un momento en lo que esto significa para la tesis de este libro: el Estado español impone por ley hashes encadenados, registros inalterables y verificación por código QR. Es, pieza por pieza, la arquitectura de la prueba de existencia —aplicada al antifraude fiscal. Ya no es una propuesta teórica: es BOE.

Y ahora, la precisión sobre lo que VeriFactu no hace —porque aquí empieza este capítulo. Primero: protege a Hacienda, no al acreedor —el registro acredita que la factura se emitió y no se ha alterado, no que el cliente la recibió ni que te debe dinero. Segundo: no acredita la entrega —el albarán, la recepción de la mercancía, el momento en que arranca legalmente el plazo de pago quedan fuera de la cadena. Y tercero: no es una fecha cierta pensada para ser oponible entre privados en un juzgado —es una prueba dirigida a la Administración tributaria. La capa que falta —la que mira al acreedor y al deudor, no al contribuyente— es exactamente la que la prueba de existencia neutral añade [3].

La prueba de existencia aplicada

La misma pyme que emite la factura puede sellar todo el trayecto del cobro [3].

1. El albarán con lugar y hora

En el muelle de descarga, el transportista o el técnico fotografía el albarán firmado con t2p: el GPS forense exige un fijado genuino —precisión de unos 50 metros, antigüedad máxima de unos 30 segundos; una ubicación simulada bloquea la certificación del todo [3]— y la huella SHA-512 con sello de tiempo hace de la entrega un hecho: qué se entregó, dónde y cuándo. Si el polígono no tiene cobertura, la certificación en segundo plano se reanuda sola al recuperarla, y el sello acredita el momento de la captura [3]. El «no nos llegó la mercancía» topa con un acta que ninguna de las dos partes puede reescribir.

2. La factura con doble fecha cierta

La factura, escaneada y sellada al emitirse —hasta 50 páginas en un único PDF certificado [3]— y, sobre todo, su envío capturado: el correo con la factura adjunta, certificado con pantalla y fecha [3]. Emisión y entrega, ambas con fecha cierta. El clásico «no me ha llegado la factura» —el comodín que para relojes— deja de funcionar: la factura existía tal día y se envió tal otro, y el certificado con código QR se lo dice a quien lo quiera comprobar.

3. El reloj que arranca solo

Con la entrega fechada y la factura entregada, el cómputo de la Ley 3/2004 [2] ya no se discute: 30 o 60 días desde un hecho cierto, el interés de demora automático —el 11,15 %— y los 40 euros por factura, calculables al céntimo desde el día exacto. La reclamación de intereses, que hoy casi ninguna pyme hace porque no puede fijar el día uno, se vuelve aritmética. Y la posición negociadora cambia: quien debe sabe que el contador corre —y que está acreditado.

4. El requerimiento y el monitorio

Cuando hay que reclamar, cada paso queda fechado: el requerimiento de pago enviado y capturado, la promesa de pago del cliente guardada con fecha, y el expediente entero —albarán, factura, envío, requerimientos— exportado como paquete .asice verificable sin conexión [3], listo para el procedimiento monitorio o para el fondo que compra la cartera. Y la simetría de siempre: el cliente que pagó a tiempo tiene en su propio registro anclado la prueba contra la reclamación duplicada o el interés mal calculado.

Los límites, dichos claramente: el sello acredita fechas y documentos, no la calidad del trabajo ni la razón de fondo de una disputa comercial —si la mercancía era defectuosa, lo dirá el perito. VeriFactu [1] y t2p [3] se complementan pero no se confunden: uno mira a Hacienda, el otro mira a las partes. Y ninguna huella cobra una factura: convierte el crédito en exigible —que no es poco—, pero el cobro final depende del juzgado y de la solvencia del deudor.

La promesa y el peligro

La promesa: pymes que reclaman los intereses que la ley les reconoce desde hace veinte años, porque por fin pueden fijar el día uno [2][3]; morosos que pagan antes porque el contador acreditado corre; monitorios que se resuelven sobre expedientes verificables; y un país donde VeriFactu [1] habrá normalizado una idea más grande que el antifraude: que los registros económicos llevan hash encadenado y fecha cierta —el paso cultural hacia la prueba de existencia universal.

Los peligros, con la misma franqueza.

El primero es que **el poder de mercado no se cura con hashes**. La pyme a menudo no reclama intereses por miedo a perder al cliente grande, no por falta de prueba. La fecha cierta quita la excusa probatoria, pero el desequilibrio es económico: hacen falta regímenes sancionadores de morosidad y observatorios públicos que hagan la reclamación innecesaria —que pagar tarde salga caro por defecto.

El segundo es **el VeriFactu-solucionismo**. Cumplir con Hacienda no es pagar a tiempo: una empresa puede tener todos los registros encadenados del mundo y pagar a 120 días. Confundir el antifraude fiscal con la protección del acreedor sería leer mal la reforma [1].

El tercero es **la carga sobre la micropyme**. Si documentar el cobro se convierte en burocracia añadida, el autónomo no lo hará. La herramienta ha de ser el gesto de diez segundos en el muelle [3], no un departamento administrativo —y el grueso del esfuerzo, la cadena fiscal, ya lo hace el software de facturación por obligación legal [1].

Y el cuarto es **el rastro como arma de presión**. El mismo expediente que protege al acreedor puede servir para acosar al deudor de buena fe con reclamaciones industrializadas. El contrapeso es doble: la neutralidad de la prueba —también acredita quién pagó— y el control judicial del monitorio.

Es hora de actuar

Que cada factura lleve su reloj, y cada reloj su día uno.

Para pymes y autónomos: sellad el trayecto entero —el albarán con GPS forense, la factura enviada, los requerimientos [3]; el día que reclaméis, el reloj de la Ley 3/2004 [2] tendrá día uno acreditado.

Para gestorías y asesores: incorporad el expediente de cobro anclado al servicio estándar; VeriFactu [1] ya os lleva a la cadena de hashes fiscal —ofreced al cliente la capa entre partes.

Para las grandes empresas pagadoras: anclad vuestras recepciones y pagos —la prueba de que pagáis a tiempo es vuestro mejor argumento ante el informe anual de morosidad [2].

Para las Administraciones: pagar a 70 días con un límite de 30 [2] es insostenible; con registros de recepción y pago anclados y publicados por huella, el periodo medio dejará de ser una cifra discutida.

Para los legisladores: el régimen sancionador de la morosidad, pendiente desde hace años, tiene ahora la infraestructura probatoria lista [1][2][3]; y que la factura electrónica B2B en despliegue incorpore la fecha cierta de recepción, no solo de emisión.

Para que cobrar a tiempo deje de ser un privilegio, **time2act**.

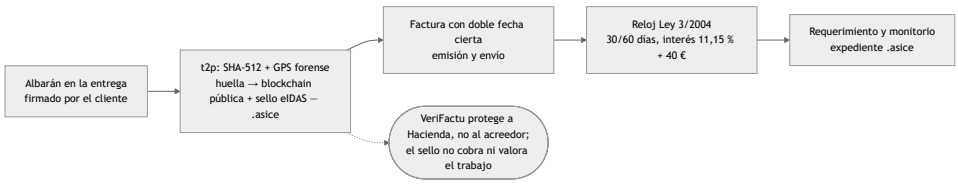


Figura 34.1 — El reloj del cobro con prueba de existencia (sellado con t2p — capítulo 13): el albarán fotografiado con GPS forense en la entrega, la factura con doble fecha cierta (emisión y envío), el cómputo automático de la Ley 3/2004 (30/60 días; interés de demora 11,15 % + 40 €) y el expediente .asice para el monitorio. Contexto: VeriFactu (RD 1007/2023, aplazado a 2027 por el RD-ley 15/2025) ya impone registros de facturación con hash encadenado y QR —el Estado construye media prueba de existencia; t2p añade la capa oponible entre privados. Límites: el sello no cobra facturas ni valora el trabajo; VeriFactu protege a Hacienda, no al acreedor. Fuentes: AEAT; BOE; PMcM 2025 (85 % de grandes incumplidoras; AAPP a 70 días).

---

[1] AEAT — *Sistemas Informáticos de Facturación (SIF) y VERI*FACTU *(RD 1007/2023: registro de facturación normalizado con huella encadenada —cada registro contiene el hash del anterior—, firma electrónica y QR de verificación; modalidades «Verifactu» de envío inmediato voluntario y conservación inalterable; FAQ oficial); Guía Fiscal* — Verifactu 2026-2027 *y Davisa* — Guía Verifactu 2026* (calendario aplazado por el RD-ley 15/2025, de 2 de diciembre: 1-1-2027 sociedades, 1-7-2027 resto; sanciones de hasta 50.000 €/ejercicio para usuarios y 150.000 € para fabricantes). https://sede.agenciatributaria.gob.es/Sede/iva/sistemas-informaticos-facturacion-verifactu.html · https://sede.agenciatributaria.gob.es/Sede/iva/sistemas-informaticos-facturacion-verifactu/preguntas-frecuentes/sistemas-verifactu.html · https://guiafiscal.es/autonomos/verifactu-2026-guia/ · https://www.davisa.es/guia-verifactu-2026/ ↩

[2] BOE — *Ley 3/2004, de 29 de diciembre, de medidas de lucha contra la morosidad en las operaciones comerciales* (60 días naturales de máximo pactado entre empresas, 30 por defecto desde la recepción; interés de demora automático; 40 € de costes de cobro por factura; AAPP 30 días —Ley 15/2010); Togas — *Los intereses de demora en el primer semestre de 2025: 11,15 %* (Resolución del Tesoro de 30-12-2024); PMcM / Revista Limpiezas — *Informe sobre morosidad 2025* (el 85 % de las grandes compañías incumple los plazos; AAPP a 70 días de media, +3 en 2025; sector privado a 67). https://www.boe.es/buscar/act.php?id=BOE-A-2004-21830 · https://togas.biz/articulos/articulo-profesionales--los-intereses-de-demora-en-las-operaciones-comerciales-en-el-primer-semestre-de-2025-quedan-fijados-en-un-11-15-por-resoluci-n-de-30-de-diciembre-de-2024-de-la-secretar-a-general-del-tesoro-y-financiacion-internacional/ · https://www.revistalimpiezas.es/actualidad/normativa-limpiezas/informe-morosidad-pmcm-el-85-de-las-grandes-companias-incumple-los-plazos-de-pago-y-se-financia-en-parte-a-costa-de-las-pymes-segun-la-pmcm_20260417.html · https://pmcm.es/informe-morosidad-estudio-plazos-pago-espana-2024/ ↩

[3] t2p — manual de producto (foto con GPS forense —fijado genuino ~50 m / ≤30 s, la ubicación simulada bloquea la certificación; certificación en segundo plano que se reanuda al recuperar cobertura; escáner de documentos hasta 50 páginas en un PDF; captura de pantalla y de correo certificadas; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión; solo huellas en la cadena). Véanse los capítulos 13 y 15; el comercio internacional, en el capítulo 54; la auditoría, en el capítulo 55. ↩

Inmobiliario: el estado de la propiedad y el registro de la tierra

«El primero que, tras haber cercado un terreno, se le ocurrió decir "esto es mío" y encontró gentes bastante simples para creerle, fue el verdadero fundador de la sociedad civil.»

— Jean-Jacques Rousseau, Discurso sobre el origen de la desigualdad (1755)

Un día cualquiera, un propietario descubre que su casa se ha puesto a la venta. Él no la ha vendido; alguien ha falsificado una escritura —a menudo una *quitclaim deed*, la escritura de renuncia norteamericana— y la ha presentado en el registro para transferirse una propiedad que no es suya. La oficina de Boston del FBI alertó en abril de 2025 del aumento de este fraude, y la asociación del sector asegurador de títulos, la **American Land Title Association** (ALTA), documentó que el 28 % de sus empresas habían sufrido intentos de **suplantación de vendedor** en 2023, con un objetivo predilecto: el **suelo sin edificar** (un 85 % de los casos), porque no vive nadie que se dé cuenta [5][6]. En muchos de aquellos intentos, los defraudadores usan credenciales de notario falsas —un 43 %— o usurpan reales.

El fraude inmobiliario moderno, fijémonos, no ataca tanto la cadena de títulos como **la identidad del firmante** y **el estado de la cosa**. Y aquí, el sistema tiene un agujero que este capítulo quiere llenar. Pero conviene empezar con una distinción que el lector tiende a confundir y que atraviesa todo el capítulo: una cosa es el **título legal** —el que crea o transfiere la propiedad, competencia exclusiva del registro y del notario— y otra, bien distinta, es la **evidencia**: la prueba de que un documento o un estado físico existían, íntegros, en un momento, un lugar y a cargo de una persona. La prueba de existencia no sustituye el registro. Aporta la capa de evidencia con fecha cierta que hoy falta o es discutible.

La propiedad insegura

El problema de fondo es sorprendentemente masivo. El Banco Mundial, en un trabajo de sus expertos Laura Tuck y Wael Zakout, calcula que solo alrededor del 30 % de la población mundial tiene sus derechos sobre la tierra y la vivienda legalmente registrados; es decir, cerca del 70 % no dispone de un título documentado [1]. Y la inseguridad no afecta únicamente a los países pobres. La iniciativa Prindex, la mayor encuesta global sobre percepción de seguridad de la tenencia, encontró en 2024 que unos 1.100 millones de adultos —el 23 %, frente al 19 % de 2020— temen perder su tierra o casa; en Estados Unidos esta inseguridad percibida ha subido del 13 % al 25 % en cuatro años, y golpea sobre todo a jóvenes e inquilinos [2]. Un informe de la FAO de 2026 lo confirma: solo un 35 % de la tierra del mundo está formalmente documentada [3].

Donde hay opacidad, hay fraude. El FBI registró en 2025 más de 12.000 víctimas de fraude inmobiliario en Estados Unidos, con pérdidas de unos 275 millones de dólares, un 59 % más que el año anterior [4]. Entre 2019 y 2023 el fraude inmobiliario dejó 58.141 víctimas y 1.300 millones de dólares en pérdidas [6]. Y en el otro extremo de la escala —el de los millones sin título—, la inseguridad no se mide en dólares robados sino en familias que pueden ser desahuciadas de la tierra que trabajan porque no pueden probar su propiedad.

Pioneros y fracasos: Georgia, Suecia, Honduras

Ante esto, algunos estados han hecho de la necesidad una virtud. El caso pionero es la **República de Georgia**, un país postsoviético marcado por la corrupción registral. En 2016, su Agencia Nacional de Registro Público, con la empresa Bitfury y con el economista **Hernando de Soto** —el gran teórico del capital muerto de los pobres sin título— como padrino del proyecto, inició el anclaje a la cadena de bloques de Bitcoin de la huella de cada certificado de propiedad. En 2018, cerca de 1,5 millones de títulos estaban sellados de manera que, en palabras de la propia agencia, «nadie, ni siquiera el Estado, puede alterar su marca de tiempo» [7]. En 2017 el piloto se amplió a compraventas, hipotecas y alquileres [8]. La paradoja es bella: un Estado que da a sus ciudadanos una prueba que él mismo ya no puede falsificar.

Suecia fue por un camino parecido: su registro, el Lantmäteriet, con la empresa ChromaWay, calculó que sellar las transacciones inmobiliarias podía ahorrar más de **100 millones de euros al año** al contribuyente y reducir el tiempo entre la firma y la transferencia de tres a seis meses a unos pocos días [9]. Pero no todas las historias acaban bien, y aquí hay una lección. Honduras anunció en 2015, con la

empresa Factom, el primer registro nacional de tierras «a prueba de manipulación» —motivado, precisamente, porque algunos funcionarios pirateaban la base de datos estatal para robarse fincas. A finales de aquel año, el proyecto se encalló por «cuestiones políticas» y no se desplegó nunca [10]. La tecnología prometía blindar la propiedad; la falta de voluntad política la dejó en una carta de intenciones. Es la prueba de que el sello es condición necesaria, pero no suficiente: hace falta que el registro, el notario o el tribunal lo acepten.

La prueba de existencia aplicada

Veamos cómo **t2p** llena el vacío de la evidencia en tres escenarios muy diferentes.

El primero, cotidiano y universal: las **disputas por la fianza del alquiler**. El clásico «ya estaba roto / no, lo rompiste tú» es una de las causas más frecuentes de litigio entre propietario e inquilino, hasta el punto de que diecisiete estados norteamericanos exigen por ley un informe del estado de la vivienda a la entrada para poder retener legalmente la fianza. Con **t2p**, el inquilino o el gestor fotografía el estado del piso y lo sella al instante: **huella SHA-512** en el dispositivo, **GPS forense** que prueba qué piso y cuándo, **sello de tiempo** eIDAS, **prueba de vida** que liga la captura a una persona real presente —adiós a las fotos viejas recicladas— y todo empaquetado en un **contenedor .asice** que la otra parte o un juez pueden verificar sin conexión.

El segundo: **escrituras, contratos y due diligence**. Sellar la huella de un borrador de escritura, de un contrato de arras o de un informe de tasación les da **fecha cierta**, haciendo imposible la retrodatación. En el vector de suplantación del vendedor, capturar con prueba de vida y GPS el momento de la identificación añade un rastro que las credenciales de notario falsificadas no pueden fabricar después.

El tercero, el más transformador: los **contextos de registro débil**, como hemos visto. Donde no hay un registro fiable, sellar fotografías georreferenciadas de la ocupación, las mejoras y los lindes crea un **historial verificable de posesión**. No es un título —eso solo lo puede crear el Estado—, pero sí una evidencia con fecha cierta, oponible, en el espíritu de lo que hizo Georgia. Es, para millones de familias, la diferencia entre una posesión muda y una posesión que se puede demostrar.

Hay que decir los límites con claridad, fieles a la dualidad de «la promesa y el peligro». «Basura a la entrada, basura en la cadena»: si la foto miente o el documento de origen es falso, la cadena solo certifica que aquella mentira existía íntegra en aquel instante. La prueba de existencia demuestra existencia, integridad, tiempo, lugar y persona; **no** demuestra la verdad física previa —que el muro estuviera bien antes, o que el vendedor sea el dueño real—. Y, como en Honduras, su valor pleno solo aparece cuando el registro, el notario o el tribunal aceptan esta evidencia.

La promesa y el peligro

La promesa es doble. Para los países ricos, cerrar la puerta al fraude de escrituras y a las disputas de fianza, y dar fecha cierta a cada documento inmobiliario. Para los países con registros débiles, ofrecer a centenares de millones de personas una manera de acreditar su posesión sin esperar a que el Estado construya un catastro perfecto. En ambos casos, más seguridad jurídica con menos coste y menos intermediarios.

El peligro pide matiz. El primero, la confusión peligrosa entre evidencia y título: vender la prueba de existencia como si transfiriera la propiedad sería un fraude en sí mismo. El segundo, la privacidad: las fotos geolocalizadas del interior de una vivienda y la biometría de prueba de vida son datos sensibles que exigen un diseño escrupuloso. Y el tercero, la lección de Honduras: sin voluntad política y reconocimiento institucional, la mejor tecnología se queda en una promesa. La prueba de existencia es una capa necesaria dentro de una arquitectura que incluye, siempre, el registro y la ley.

Es hora de actuar

Para los **arrendatarios y propietarios**: sellar el estado de la vivienda a la entrada y a la salida, evitando que una disputa de fianza se resuelva por la voz más fuerte. Para los **compradores y las aseguradoras de título**: exigir evidencia con fecha cierta y prueba de vida del vendedor, cortando la suplantación. Para los **registros y notarios**: reconocer el valor probatorio del sello e integrarlo, como hizo Georgia. Para los **gobiernos con registros débiles**: ofrecer una capa de evidencia de posesión mientras se construye el

catastro, sin obligar a la población a esperar. Para los **reguladores**: proteger simultáneamente la integridad de la prueba y la privacidad de los hogares.

Un propietario puede descubrir un día que su casa se ha «vendido» sin él. Millones de familias viven toda la vida sin poder demostrar que la tierra que trabajan es suya. Entre la propiedad verificable y la basada en la confianza de un documento manipulable se dibuja cada vez más la frontera de la seguridad. Dar a cada uno la prueba de lo que es suyo —o del estado en que lo recibió— es, también aquí, **time2act**.

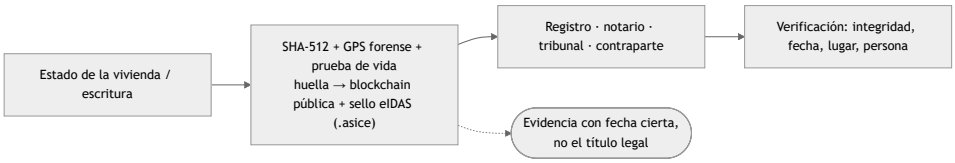


Figura 35.1 — El estado de la vivienda (alquiler) o un documento (escritura, contrato) se captura y se sella en el dispositivo con SHA-512, GPS forense, sello de tiempo eIDAS y prueba de vida, se ancla a la blockchain pública y se empaqueta en un contenedor .asice verificable sin conexión, listo para el registro, el notario, el tribunal o la otra parte. La prueba de existencia aporta evidencia con fecha cierta, no el título legal (que crea el registro). Barra de contexto: ~70 % de la población mundial sin título registrado; ~1.100 M de personas inseguras sobre su propiedad; Georgia, ~1,5 M de títulos anclados. Fuentes: Banco Mundial; Prindex; Exonum/Bitfury.

---

[1] Banco Mundial — Laura Tuck y Wael Zakout, *7 reasons for land and property rights to be at the top of the global agenda* (~30 % de la población con título registrado). https://blogs.worldbank.org/en/voices/7-reasons-land-and-property-rights-be-top-global-agenda ↩

[2] Prindex — *Tenure insecurity on the rise* (2024; ~1.100 M de adultos, 23 %, inseguros sobre su tierra/vivienda). https://www.prindex.net/news-and-stories/tenure-insecurity-on-the-rise/ ↩

[3] FAO (informe SOFA, vía UN News) — *Global report highlights slow progress in expanding secure land tenure* (~35 % de la tierra documentada; >1.100 M temen perderla). https://news.un.org/en/story/2026/02/1167037 ↩

[4] FBI IC3 (vía National Association of Realtors) — *Online real estate fraud climbed to $275M in 2025* (12.368 víctimas). https://www.nar.realtor/magazine/real-estate-news/online-real-estate-fraud-climbed-to-275m-in-2025-fbi-says ↩

[5] American Land Title Association (ALTA) — *Seller Impersonation Fraud Attempts Increase, Study Shows* (julio 2024; 28 %; suelo sin edificar 85 %; credenciales de notario falsas 43 %). https://www.alta.org/news-and-publications/news/20240730-Seller-Impersonation-Fraud-Attempts-Increase-Study-Shows ↩

[6] FBI Boston (vía ALTA) — *FBI Boston Issues Quit Claim Deed Fraud Warning* (abril 2025; fraude inmobiliario 2019-2023: 58.141 víctimas / 1.300 M$). https://www.alta.org/news-and-publications/news/20250410-FBI-Boston-Issues-Quit-Claim-Deed-Fraud-Warning ↩

[7] Exonum / Bitfury — *The story of Georgia* (NAPR; ~1,5 M de títulos anclados a Bitcoin; «nadie puede alterar la marca de tiempo»). https://exonum.com/story-georgia ↩

[8] Eurasianet — *Georgia authorities use blockchain technology for developing land registry* (ampliación feb-2017; Hernando de Soto, asesor). https://eurasianet.org/georgia-authorities-use-blockchain-technology-for-developing-land-registry ↩

[9] Computer Weekly — *Sweden trials blockchain for land registry management* (Lantmäteriet + ChromaWay; >100 M€/año de ahorro). https://www.computerweekly.com/news/450421958/Sweden-trials-blockchain-for-land-registry-management ↩

[10] CoinDesk — *Blockchain land title project stalls in Honduras* (Factom; encallado por cuestiones políticas, 2015). https://www.coindesk.com/markets/2015/12/26/blockchain-land-title-project-stalls-in-honduras ↩

Alquiler y vivienda: el estado de las cosas, con fecha cierta

«La casa es nuestro rincón del mundo. Es —se ha dicho con frecuencia— nuestro primer universo.»

— Gaston Bachelard, La poética del espacio (1957)

Estás ante un portal inmobiliario conocido y el cursor se detiene sobre un anuncio que parece un regalo: piso bonito, bien situado, claramente por debajo del precio del barrio. El «propietario» escribe con urgencia —hay más interesados, hace falta una señal para reservarlo— y no hay manera de visitarlo antes: está fuera, por trabajo. Solo un número de cuenta donde transferir el dinero. Así empezó, para una víctima que buscaba piso en el centro de Valladolid, la historia que la Guardia Civil acabó bautizando como Operación ISLEDA (2026): una trama de «estafa inmobiliaria a escala nacional», con anuncios falsos repartidos por el país y víctimas por toda España; tres detenidos de entre 19 y 34 años en San Fernando (Cádiz); y un detalle que retrata la época —las cuentas bancarias receptoras se habían abierto con documentación personal robada en estafas previas de ofertas de trabajo falsas. Delitos: estafa, blanqueo y organización criminal [1]. El patrón es siempre el mismo: precio-gancho, propietario que no da la cara y prisa para que pagues antes de poder comprobar nada [2].

El capítulo 35 trató la propiedad: el título, el registro, la tierra. Este capítulo trata lo que pasa dentro: la vida del contrato de alquiler, donde casi todo se discute a posteriori. Si el piso existía. Cómo estaba el día que recibiste las llaves. Cuándo avisaste de la humedad. Cuándo entró el ocupante. La pregunta clave: ¿cómo se prueba el estado de las cosas cuando cada parte recuerda una versión diferente? La respuesta no puede ser la memoria: es la fecha cierta en el momento —**t2p**: la huella SHA-512 de cada foto, acta y mensaje, calculada en el dispositivo, con sello de tiempo RFC 3161/eIDAS y anclaje a la blockchain pública dentro de un contenedor .asice [5]. Y con neutralidad total: la misma herramienta ampara al inquilino, al propietario y a cualquiera que actúe de buena fe.

El piso que no existe

La mecánica de la estafa de los anuncios falsos está bien documentada: pisos inexistentes —o que no son de quien los anuncia— publicados con fotos atractivas y precios por debajo de mercado para generar cola de víctimas; un «propietario» que a menudo dice estar en el extranjero; y comunicación rápida con presión para pagar una reserva o la primera mensualidad antes de ninguna visita [1][2]. La Operación ISLEDA, conocida en la primavera de 2026, mostró su madurez industrial: víctimas por todo el territorio, anuncios distribuidos por el país, identidades robadas para abrir las cuentas receptoras y una estructura de organización criminal [1].

La asimetría de fondo explica por qué funciona. Para montar la estafa solo hacen falta fotos bonitas, un texto persuasivo y una dirección de correo; el coste es insignificante al lado de la recaudación. En cambio, para demostrar que eres el propietario de verdad, hoy no hay ningún gesto sencillo: el inquilino no puede distinguir al anunciante legítimo del impostor hasta que es demasiado tarde, y el propietario honesto compite contra pisos fantasma más baratos que el suyo.

La salida estructural es el anuncio verificable. El propietario real puede sellar la oferta —vinculada a su acreditación de titularidad, la cadena registral del capítulo 35— con fecha cierta [5]; el portal puede mostrar el distintivo del anuncio acreditado; y el inquilino aprende la regla inversa: oferta sin sello y con prisa, sospecha por defecto [2]. El estafador puede copiar las fotos, pero no puede acreditar ni la titularidad ni la continuidad en el tiempo. Sin el distintivo, su anuncio deja de competir; con la regla aprendida, deja de cobrar.

La guerra de la fianza

Cuando el contrato se acaba, empieza la otra batalla. El marco es claro sobre el papel: la fianza se ha de devolver en el plazo de un mes desde el final del contrato, y pasado el plazo devengan intereses legales [3]; los motivos válidos de retención son tasados —deudas de renta o suministros, y daños que excedan el deterioro normal por el uso [3]. Una pintura desgastada por el tiempo no justifica retener nada; una baldosa rota o una puerta forzada, sí.

La clave, sin embargo, es procesal: los tribunales suelen fallar a favor del inquilino cuando el arrendador no aporta pruebas suficientes —facturas, informes de desperfectos— que justifiquen la retención; y a favor del propietario cuando acredita gastos reales por mal uso [3]. Traducido: la fianza no la gana quien tiene razón, sino quien tiene pruebas.

Y aquí aparece el ritual que falta. Los expertos recomiendan formalizar un acuerdo de liquidación firmado, con comprobación detallada del inventario en la entrega de llaves [3]; en la práctica se hace poco, tarde y sin fecha fiable —fotos sueltas en el móvil de cada uno, mensajes dispersos, recuerdos enfrentados.

La versión sellada del ritual lo arregla de raíz: el día de las llaves, las dos partes fotografían la vivienda —cada estancia, cada desperfecto preexistente— y sellan las imágenes y el acta en el momento, desde los dos dispositivos: huella SHA-512, fecha cierta, anclaje [5]. El día de la salida, el mismo recorrido. La discusión sobre «cómo estaba el piso» desaparece: queda la comparación entre dos series de imágenes con integridad acreditada. Ni el inquilino puede negar el agujero que hizo, ni el propietario puede atribuirle la grieta que ya estaba.

Las 48 horas y los 15 días

La ocupación es el conflicto más envenenado del mercado, y su nuevo marco legal ha convertido el tiempo en el elemento central. La Ley Orgánica 1/2025, de eficiencia del servicio público de justicia, en vigor desde el 3 de abril de 2025, hace que el allanamiento de morada (artículo 202 del Código Penal: ocupar el domicilio habitual de alguien) y la usurpación de inmueble (artículo 245: ocupar una propiedad que no es domicilio habitual) se tramiten por juicio rápido, con plazos de resolución del orden de quince días; si la ocupación se detecta dentro de las primeras 48 horas, las fuerzas de seguridad pueden desalojar sin esperar orden judicial, como delito flagrante; y en esta vía se suprime el informe previo de vulnerabilidad [4].

Fijémonos de qué pende toda la vía rápida: de fechas. ¿Cuándo entró el ocupante? ¿Cuándo lo descubrió el propietario? ¿El inmueble era domicilio habitual o segunda residencia? ¿Cuándo se denunció? Cada respuesta mueve el caso de un artículo a otro, de una vía a otra, del desalojo inmediato al procedimiento largo. Y hoy estas preguntas se responden con testimonios e indicios —el material probatorio más frágil que existe.

Con prueba de existencia, se responden con cronología. El propietario de una vivienda vacía puede establecer la línea de base con pruebas de estado periódicas —la visita mensual, la foto con fecha cierta [5] —; si un día encuentra la puerta forzada, el descubrimiento queda fechado al minuto y la denuncia lleva hora anclada: la flagrancia de las 48 horas y el juicio de quince días [4] trabajan sobre hechos fechados, no sobre estimaciones.

Y la simetría es imprescindible, y hay que decirla con el mismo énfasis: la misma herramienta protege al inquilino legítimo de ser tratado como ocupante. El contrato, los recibos de renta y los pagos de suministros sellados en su dispositivo son su cronología de posesión legítima [5], el escudo contra el desalojo abusivo o la acusación infundada. La fecha cierta no tiene bando: distingue la ocupación ilegal de la posesión legal, sea cual sea el lado que lo tenga que probar.

Humedades, averías y el reloj

La tercera guerra del alquiler no es ni la entrada ni la salida: es el mientras tanto. La mancha de humedad que crece, la caldera que falla en invierno, la reparación que «ya vendrá». Jurídicamente, estas disputas son cronologías puras: cuándo se avisó al propietario, por qué canal, qué respondió, cuánto tardó la reparación, cómo evolucionó el daño mientras tanto. Quien no puede fechar el aviso, no puede exigir; quien no puede fechar la respuesta, no se puede defender.

Imaginemos la secuencia con prueba de existencia. El inquilino detecta la humedad en noviembre y envía el aviso sellado —huella y fecha cierta del mensaje [5]. La respuesta del propietario, también sellada, llega al día siguiente: inspección la semana que viene. El técnico documenta el daño con fotos fechadas; la reparación queda registrada; y si la mancha vuelve en enero, la serie fotográfica anclada muestra la progresión entera. Ninguna de las dos partes depende ya de la memoria: el inquilino que avisó a tiempo puede exigir; el propietario que reparó diligentemente puede demostrarlo; y el que calló —sea quien sea— queda retratado por su propio silencio, porque los vacíos de la cronología también tienen fecha [5].

En un contrato de tracto sucesivo, la justicia es cuestión de reloj. Y el reloj, para ser justo, ha de poder ser auditado por cualquiera: eso es exactamente lo que aporta el sello.

La prueba de existencia aplicada

Una entrega de llaves cualquiera: dos móviles que fotografían las mismas estancias, diez minutos de ritual —y un año de disputa ahorrado.

1. El inventario sellado

El día de la entrada, inquilino y propietario recorren el piso juntos: fotos de cada estancia y de los desperfectos preexistentes, un acta breve de inventario, y todo sellado en el momento desde los dispositivos de ambas partes —huella SHA-512, fecha cierta, anclaje a la blockchain pública [5]. El día de la salida, el mismo recorrido. La fianza se liquida sobre la comparación de dos series de imágenes con integridad acreditada, no sobre recuerdos: los tribunales ya premian a quien aporta pruebas [3]; el sello hace que ambas partes las tengan, de la misma calidad, desde el primer día.

2. El anuncio verificable

El propietario legítimo sella la oferta con su acreditación de titularidad (capítulo 35) y el portal la distingue con el distintivo de anuncio verificado [5]. Ante el piso «demasiado barato» con propietario en el extranjero y prisas [1][2], el inquilino aplica una regla de tres palabras: sin sello, sin dinero. La Operación ISLEDA necesitó una denuncia, una investigación y meses de trabajo policial para desmantelar la trama [1]; un mercado de anuncios acreditados la habría dejado sin víctimas desde el primer clic.

3. La cronología de la posesión

Para el propietario de una vivienda vacía: pruebas de estado periódicas y selladas que establecen la línea de base; si un día encuentra la puerta forzada, el descubrimiento queda anclado al minuto, la denuncia también, y la vía rápida de la LO 1/2025 —las 48 horas, el juicio en unos quince días [4]— trabaja sobre una cronología indiscutible [5]. Para el inquilino legítimo: el contrato, los recibos y los suministros sellados son el escudo que impide que nadie lo pinte como ocupante. La misma huella sirve a las dos caras del conflicto: esa es exactamente su virtud.

4. El diálogo con fecha cierta

El aviso de avería sellado, la respuesta del propietario sellada, la progresión del daño en serie fotográfica anclada [5]: la disputa de humedades deja de ser un «te lo dije» contra un «no me lo dijiste». Quien avisó a tiempo puede exigir; quien reparó diligentemente puede demostrarlo; y el silencio de quien no hizo ni una cosa ni la otra queda fechado con la misma precisión que todo lo demás.

Hay que decir también qué no hace el sello: acredita el estado y el momento, pero no reparte culpas ni interpreta la Ley de Arrendamientos Urbanos —eso lo hacen los jueces; una foto sellada no sustituye la inspección física cuando hace falta un perito; y las imágenes del interior de un hogar son datos íntimos — solo la huella se ancla, el contenido queda en los dispositivos de las partes y se revela únicamente en caso de disputa [5].

La promesa y el peligro

La promesa es un mercado de alquiler donde el anuncio falso no encuentra víctimas [1][2], la fianza se liquida en diez minutos de comparación y no en meses de guerra [3], la ocupación y la posesión legítima se distinguen por cronología [4], y las reparaciones tienen un reloj que ambas partes pueden auditar. Menos juzgados, menos miedo, más confianza entre desconocidos —en el contrato más cotidiano que existe.

Los peligros exigen la misma honestidad.

El primero es **el desequilibrio de poder**. Si solo una parte sella, la herramienta se convierte en arma. Un mercado donde los grandes tenedores documentan industrialmente y el inquilino vulnerable no, agrava la asimetría que ya existe. Por eso el ritual ha de ser bilateral por diseño —el inventario sellado desde los dos dispositivos— y la herramienta, gratuita o de coste insignificante para la parte débil.

El segundo es **la privacidad del hogar**. Las fotos de tu casa son el mapa de tu intimidad. Ninguna imagen ha de salir del dispositivo: solo huellas en la cadena, revelación solo ante disputa, revocabilidad cuando el contrato se acaba y ningún registro central de interiores [5].

El tercero es **la barrera burocrática**. Si el sello se convierte en un requisito más para acceder a un piso —una «puntuación de documentación» que expulsa a quien menos tiene—, habremos empeorado el problema que queríamos resolver. El sello ha de resolver disputas, no filtrar personas: sencillo, gratuito y opcional para quien alquila.

Y el cuarto, dicho sin ambages: **esto no es política de vivienda**. Ninguna huella baja el precio del alquiler ni construye ningún piso. La crisis de la vivienda es de precios, de oferta y de políticas públicas; este capítulo solo limpia la capa de conflictos que la hace aún más cruel. Confundir las dos cosas sería vender humo sobre el techo de la gente.

Es hora de actuar

En el contrato más importante de la vida cotidiana, la memoria no puede ser la única prueba.

Para los inquilinos: sella el inventario de entrada aunque el propietario no lo haga; guarda con fecha cierta el contrato, los recibos y cada aviso de avería [3][5]; y ante un anuncio con prisa y precio-gancho, sin sello ni visita, ni un euro [1][2].

Para los propietarios: inventario sellado bilateral el día de las llaves [3]; para los pisos vacíos, la prueba de estado periódica [4][5]; y acredita tu anuncio —el distintivo te distingue del estafador que copia tus fotos [1].

Para los portales inmobiliarios: implantad el distintivo de anuncio verificado con sello de titularidad y fecha cierta [1][2][5]; el coste es mínimo y el mercado entero gana credibilidad.

Para administradores de fincas y cámaras de la propiedad: estandarizad el acta de inventario sellada como servicio básico del alquiler profesionalizado [3].

Para jueces y cuerpos policiales: valorad la cronología sellada en la vía rápida de la LO 1/2025 [4] — las 48 horas y los quince días necesitan fechas fiables más que ninguna otra cosa.

Para los legisladores: dad presunción de autenticidad al inventario sellado bilateral, y velad para que ninguna herramienta probatoria se convierta nunca en barrera de acceso a la vivienda.

La víctima de Valladolid perdió el dinero por un piso que no existía [1]. Que el próximo anuncio falso no encuentre a nadie a quien engañar, y que la próxima fianza se devuelva sin guerra. Por un mercado donde el estado de las cosas tenga fecha cierta, **time2act**.

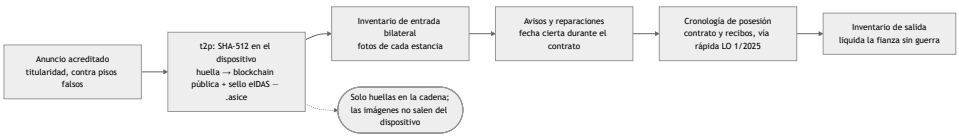


Figura 36.1 — El ciclo del alquiler con prueba de existencia: el anuncio acreditado (titularidad + sello, contra la estafa del piso inexistente), el inventario de entrada sellado bilateralmente, los avisos y reparaciones con fecha cierta durante el contrato, la cronología de posesión (contrato y recibos del inquilino; pruebas de estado periódicas del propietario; vía rápida LO 1/2025) y el inventario de salida que liquida la fianza sin guerra. Solo las huellas SHA-512 se anclan a la blockchain pública (RFC 3161/eIDAS, .asice); las imágenes del hogar no salen nunca de los dispositivos. Fuentes: Guardia Civil (Op. ISLEDA); Idealista/Maldita; LO 1/2025.

[1] Libertad Digital — *Cae en Cádiz una red criminal por una «estafa inmobiliaria a nivel nacional»* (6 de mayo de 2026; Operación ISLEDA; 3 detenidos de 19-34 años en San Fernando; destapada en Valladolid; cuentas abiertas con identidades robadas en falsas ofertas de trabajo; estafa, blanqueo y organización criminal); Cádiz Directo — *La Guardia Civil destapa en San Fernando una trama nacional de falsas viviendas de alquiler*. https://www.libertaddigital.com/andalucia/2026-05-06/san-fernando-cadiz-valladolid-guardia-civil-detiene-tres-hombres-acusados-de-estafa-inmobiliaria-conocido-portal-web-alquiler-y-venta-de-pisos-utilizaban-sus-datos-para-cuentas-falsas-victimas-por-todo-el-pais-destapado-en-valladolid-1b-7400307/ · https://www.cadizdirecto.com/cadiz/la-guardia-civil-destapa-en-san-fernando-una-trama-nacional-de-falsas-viviendas-de-alquiler ↩

[2] Idealista/News — *La última estafa en los anuncios de alquiler y los consejos para no caer en ella* (precios-gancho, propietarios «en el extranjero», pagos antes de la visita); Maldita.es — *Anuncios de alquiler falsos e inmobiliarias fantasma: cómo reconocer timos inmobiliarios*. https://www.idealista.com/news/inmobiliario/vivienda/2022/11/18/800160-la-ultima-

estafa-en-los-anuncios-de-alquiler-y-los-consejos-para-no-caer-en-ella · https://maldita.es/malditobulo/20230830/inmobiliaria-fantasma-alquiler-piso-fraude-verano/ ↩

[3] Idealista/News — *Todo lo que tienes que saber sobre la devolución de la fianza del alquiler* (plazo de un mes; intereses legales; acuerdo de liquidación con inventario); Ático Jurídico — *Devolución de la fianza del alquiler* (los tribunales exigen pruebas a quien retiene: facturas, informes); Fotocasa Life — *Cómo proceder si no nos devuelven la fianza del alquiler*. https://www.idealista.com/news/inmobiliario/vivienda/2022/07/03/797535-todo-lo-que-tienes-que-saber-sobre-la-devolucion-de-la-fianza-del-alquiler · https://aticojuridico.com/devolucion-fianza-alquiler/ · https://www.fotocasa.es/fotocasa-life/alquiler/como-proceder-si-no-nos-devuelven-la-fianza/ ↩

[4] Housage — *Ley antiokupas 2025: desalojo en 15 días, cómo funciona y a quién no protege* (LO 1/2025 en vigor el 3 de abril de 2025; allanamiento art. 202 CP y usurpación art. 245 CP por juicio rápido; desalojo policial dentro de las primeras 48 horas; supresión del informe de vulnerabilidad en esta vía); Blegal — *La Ley 1/2025 agiliza el desalojo de okupas*; Vento Abogados — *Juicio rápido por okupación: la nueva regulación de la LO 1/2025*. https://housage.es/articulos/actualidad-inmobiliaria/ley-antiokupas-2025-desalojo-en-15-dias-como-funciona-y-a-quien-no-protege/ · https://www.blegal.eu/la-reforma-de-la-ley-organica-1-2025-agilizara-los-juicios-rapidos-para-facilitar-el-desalojo-de-okupas/ · https://vento.es/juicio-rapido-por-okupacion/ ↩

[5] t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; el contenido no sale nunca del dispositivo; revelación voluntaria; los vacíos de la serie quedan fechados). Véanse los capítulos 13 y 15; para la titularidad y el registro, el capítulo 35. ↩

La comunidad de propietarios: actas, derramas y acuerdos con fecha cierta

«Las ciudades tienen la capacidad de proporcionar algo para todo el mundo, solo porque, y solo cuando, son creadas por todo el mundo.»

— Jane Jacobs, Muerte y vida de las grandes ciudades (1961)

La junta anual, en el vestíbulo o en el local de debajo de la escalera: sillas plegables, el libro de actas bajo el brazo del administrador, la discusión eterna sobre la derrama del ascensor. Se alzan manos, el recuento se hace deprisa, alguien protesta y otro ya habla del punto siguiente. Tres semanas después llega el acta —y más de uno de los presentes no reconoce lo que en ella se dice que se votó.

Millones de personas viven en régimen de propiedad horizontal, y toda su vida colectiva —obras, dinero, normas— pende de una cadena documental fragilísima: una convocatoria que quizá llegó, una votación que nadie registró, un acta redactada después por una sola persona, un libro de actas que vive en un cajón. Cuando hay confianza, todo funciona; cuando se rompe —y en una comunidad se rompe a menudo—, todo se convierte en «tu palabra contra la del presidente».

Este capítulo trata la democracia más pequeña del país y su memoria. El título de propiedad y el registro están en el capítulo 35; la vida del contrato de alquiler, en el capítulo 36; la relación con la Administración, en el capítulo 44; y si alguna vez hay que desempatar una plaza de aparcamiento por sorteo, el capítulo 45 explica cómo hacerlo de manera irrefutable. Pregunta clave: ¿cómo se gobierna un edificio cuando la única memoria oficial la redacta y la custodia una sola mano? Respuesta: dando fecha cierta a cada pieza —la convocatoria, el acta, las cuentas, la comunicación— con **t2p**: hash en el dispositivo, sello de tiempo y ancla pública —el trípode del capítulo 13 [3]. Al alcance de cualquier vecino —y del administrador honesto, que es el primer beneficiado.

El libro de actas en una sola mano

El caso real que lo ilustra [1]: un administrador de fincas de Gijón, condenado a un año y medio de prisión —condena confirmada— por apropiarse de 2.984,04 euros de la cuenta de la comunidad. El método: maniobras engañosas en el libro de actas, haciendo firmar a los expresidentes documentos que supuestamente resolvían trámites con el banco; para encubrirse, aportó recibos de obra y cerrajería que no correspondían a ningún gasto comunitario. Y el detalle que importa a este libro: el fraude solo se descubrió cuando cambiaron el presidente y el tesorero, y el nuevo equipo repasó las cuentas minuciosamente.

El delito es la excepción —la inmensa mayoría de administradores hacen bien un trabajo ingrato—, pero la arquitectura que lo permitió es la norma: el libro de actas como única memoria oficial, redactada y custodiada por una sola parte; las cuentas que solo se miran cuando alguien sospecha; las firmas que se piden «por un trámite». El Código Penal le pone nombre cuando todo ha pasado —la apropiación indebida del artículo 253 [1]—; lo que no hay es nada que lo haga visible antes.

Y el conflicto civil es mucho más frecuente que el penal. La Ley de Propiedad Horizontal permite impugnar los acuerdos contrarios a la ley, lesivos o abusivos [2] —pero impugnar exige probar qué se convocó, qué se dijo y qué se votó exactamente. Sin registro, la impugnación es un acto de fe; y la defensa de la junta que lo hizo todo bien queda igualmente a merced de los recuerdos.

La prueba de existencia aplicada

La misma junta, el mismo administrador —y cada pieza de la vida comunitaria con fecha cierta [3].

1. La convocatoria que consta

La convocatoria con el orden del día, escaneada y sellada al enviarse —y el envío mismo capturado con fecha cierta: el correo, el tablón o el buzón fotografiado con GPS forense [3]. El «a mí no me llegó» y el «se convocó fuera de plazo» dejan de ser discutibles: la convocatoria existía tal día, decía esto y se comunicó por este canal. Protege al vecino —y protege a la junta que convoca bien.

2. El acta del mismo día

La votación, contada en voz alta y —si la junta lo acuerda— grabada [3]; el acta, redactada y sellada el mismo día o al día siguiente, no tres semanas después. Cada acta recibe su huella SHA-512 con sello de tiempo, y el libro de actas se convierte en una cadena de versiones ancladas que nadie —ni administrador, ni presidente, ni vecino— puede reescribir retroactivamente [3]. La impugnación de la LPH [2] pasa a discutir el fondo, no los hechos; y la maniobra del caso de Gijón [1] —tocar el libro a posteriori— se vuelve imposible de hacer en silencio.

3. La derrama trazable

El expediente de la obra, agrupado en un proyecto de la app [3]: los presupuestos recibidos —escaneados, hasta 50 páginas cada uno—, el acuerdo de aprobación con su acta sellada, las facturas, las certificaciones. Cada euro de la derrama, del voto al pago, con fecha cierta. Las cuentas anuales, contrastables por cualquier vecino sin pedir permiso —y el administrador honesto, blindado: sus registros anclados son su auditoría permanente.

4. La comunicación fehaciente de vecindario

Las comunicaciones que importan —el requerimiento al administrador, el aviso del desperfecto que después será siniestro, la queja formal— enviadas y capturadas con fecha cierta [3], sin burofax ni notario para cada minucia. Y cuando el conflicto escala, el expediente entero se exporta como paquete .asice verificable sin conexión [3], listo para el abogado o el juzgado.

Los límites, para no vender humo: el sello acredita convocatorias, actas y cuentas —no resuelve el fondo de ninguna disputa vecinal: si la derrama era justa o la obra necesaria, lo deciden las mayorías y, si hace falta, el juez [2]. La grabación de juntas exige el acuerdo de la propia junta y proporcionalidad: se documenta la decisión colectiva, nunca la vida de los vecinos. Y las actas contienen datos personales: la publicación es por huella; el contenido queda en la comunidad.

La promesa y el peligro

La promesa: comunidades donde la confianza no depende de la memoria de nadie [1][3]; impugnaciones que discuten el fondo sobre hechos ciertos [2]; administradores honestos con la mejor credencial de la profesión —registros verificables—; y la democracia más pequeña del país funcionando, por fin, con la trazabilidad que exigimos a las grandes.

Ahora toca mirar los peligros.

El primero es **la comunidad vigilada**. Si cada escalera se convierte en un campo de grabaciones cruzadas, se habrá perdido más de lo que se gana. La línea es nítida: se documentan los actos de gobierno —convocatoria, votación, acta, cuentas— por acuerdo colectivo; nunca la convivencia, nunca los vecinos entre sí.

El segundo es **la guerra de bloqueos**. El vecino pleiteante con herramientas puede inundar la comunidad de impugnaciones documentadas. El contrapeso es la misma simetría: la junta que lo hace bien tiene el expediente que lo prueba, y la impugnación infundada muere de hechos.

El tercero es **la brecha digital del rellano**. La comunidad es de todos, también de quien no tiene móvil inteligente. Ningún sistema puede excluir: el papel sigue valiendo —se escanea y se ancla—, y quien certifica es la comunidad como órgano, no cada vecino por su cuenta.

El cuarto peligro vive en el propio rellano: esperar que la técnica haga de buen vecino. Ninguna huella arregla la comunidad envenenada ni paga la derrama de quien no puede. La fecha cierta pacifica la capa de los hechos; la convivencia y la solidaridad entre vecinos son —y serán— trabajo humano.

Es hora de actuar

Diez minutos de acuerdo en la primera junta ahorran años de discusiones.

Para presidentes y juntas: acordad el protocolo —convocatorias, actas y cuentas selladas [3]; es una votación corta que cambia la vida de la comunidad.

Para los administradores de fincas: anclad el libro de actas y las cuentas que gestionáis [1][3] —vuestro trabajo bien hecho merece ser indiscutible, y la profesión entera gana cuando el fraude no tiene dónde esconderse.

Para los vecinos: guardad con fecha cierta lo que os afecta —la convocatoria, el aviso del desperfecto, la comunicación al administrador [3]; el día de la impugnación [2], los hechos valdrán más que los recuerdos.

Para los colegios de administradores: haced del registro anclado un estándar profesional y un sello de calidad —el caso de Gijón [1] es el contraejemplo que la profesión no se puede permitir.

Para los legisladores: la Ley de Propiedad Horizontal ya admite juntas telemáticas [2]; el paso natural es el libro de actas electrónico con fecha cierta verificable —la fe pública de la vida comunitaria, a coste de céntimos.

En la próxima junta, cuando se alcen las manos, que el recuento tenga fecha cierta —y que la discusión del año que viene sea sobre el ascensor, no sobre qué se votó. Por la democracia del rellano, **time2act**.

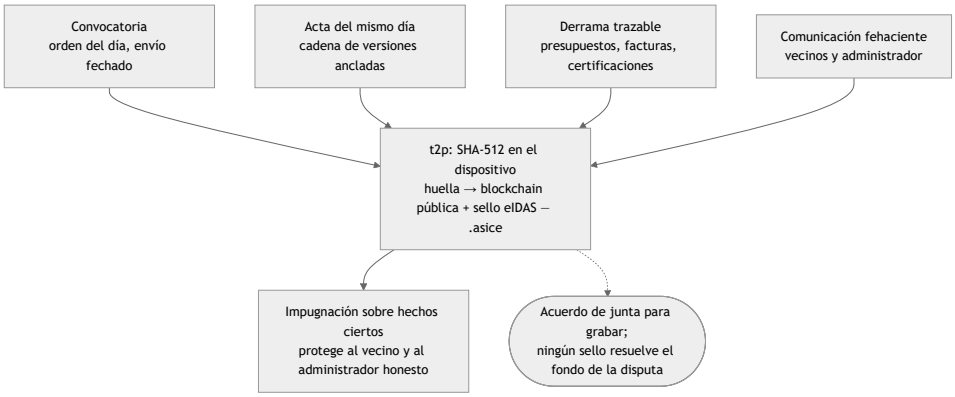


Figura 37.1 — La comunidad de propietarios con prueba de existencia (sellado con t2p — capítulo 13): la convocatoria con fecha cierta de envío, el acta sellada el mismo día (libro de actas como cadena de versiones ancladas), la derrama trazable (presupuestos, acuerdo, facturas, certificaciones en un proyecto) y la comunicación fehaciente entre vecinos y administrador. Simetría: protege al vecino que impugna y al administrador honesto. Límites: acuerdos de junta para grabar, publicación solo por huella (datos personales), y ningún sello resuelve el fondo de las disputas (LPH). Fuentes: condena de Gijón (art. 253 CP); Ley de Propiedad Horizontal.

---

[1] Vecindia — *Condenado administrador de fincas por apropiación indebida* (Gijón: 1 año y medio de prisión confirmados; 2.984,04 € de la cuenta comunitaria; maniobras engañosas en el libro de actas haciendo firmar a expresidentes; recibos de obra y cerrajería falsos para encubrirse; descubierto al cambiar presidente y tesorero); ADADE — *El Tribunal Supremo ratifica la condena por apropiación indebida a un administrador de fincas*; El Derecho — *Responsabilidad penal del administrador de fincas* (art. 253 CP). https://vecindia.es/comunidades-de-propietarios/condenado-administrador-fincas-apropiacion-indebida/ · https://www.adade.es/comunicacion/sala-de-prensa/el-tribunal-supremo-ratifica-la-condena-por-apropiacion-indebida-a-un-administrador-de-fincas · https://elderecho.com/cuando-puede-concurrir-responsabilidad-penal-en-el-administrador-de-fincas-por-su-actuacion-en-una-comunidad-de-propietarios/ ↩

[2] Ley de Propiedad Horizontal (impugnación de acuerdos contrarios a la ley, lesivos o abusivos; convocatorias y actas; juntas telemáticas habilitadas por reforma reciente); Mundojurídico — *Responsabilidad del administrador de la Comunidad*; Oliva-Ayala — *Falsedad documental y certificaciones de juntas*. https://mundojuridico.info/responsabilidad-del-administrador-de-la-comunidad/ · https://www.oliva-ayala.es/wp-content/uploads/2024/03/Alcacer-2024-LLPenal-Falsedades.pdf ↩

[3] t2p — manual de producto (escáner de documentos hasta 50 páginas en un PDF certificado; grabación de audio; captura de pantalla y correo certificadas; foto con GPS forense; proyectos para agrupar el expediente de una obra; certificar cualquier archivo —solo la huella viaja; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; la propiedad y el registro, en el capítulo 35; el alquiler, en el capítulo 36. ↩

Reformas en casa: el anticipo, la obra y la prueba

«Cuando construimos, pensamos que construimos para siempre.»

— John Ruskin, Las siete lámparas de la arquitectura (1849)

La cocina, a medio hacer: encimeras arrancadas, tubos a la vista, una capa de polvo sobre cada superficie. En el centro del desorden, un teléfono que ya no contesta. El último mensaje decía: «el anticipo está pagado, los materiales encargados —vuelvo mañana». La fecha de regreso se repite desde entonces: siempre mañana.

No es una excepción: es un guion documentado [1]. La Guardia Civil y la policía investigan periódicamente el mismo patrón: el anuncio atractivo en un portal digital, el presupuesto sospechosamente barato, el primer pago por adelantado «para la compra de materiales», y la desaparición. En Vigo y su comarca, una sola investigación contó al menos seis víctimas con pérdidas de hasta 10.000 euros cada una; en otros casos, las pérdidas acumuladas han superado los 77.000 euros; y en Guadalajara, un vecino perdió los ahorros ante un falso albañil de internet hasta que la Guardia Civil acorraló al estafador en Madrid [1].

Y el matiz que da pie al capítulo entero: por cada estafador hay centenares de profesionales honestos que sufren el mismo vacío de prueba desde el otro lado —el cliente que regatea la última factura alegando defectos, los «extras» que sí se pidieron de palabra, la reputación de un oficio entero manchada por los que huyen. Este capítulo trata el contrato más caro que una familia firma sin firmar casi nada. La derrama y la obra común del edificio están en el capítulo 37; el cobro del profesional, en el capítulo 34; la construcción industrial, en el capítulo 94; el seguro del hogar, en el capítulo 28. Pregunta clave: ¿cómo se discute una obra cuando todo lo que hay son WhatsApps, un PDF sin firmar y recuerdos? Respuesta: dando fecha cierta a cada paso —el presupuesto, el estado inicial, las fases, los pagos, la recepción— con **t2p**: la cadena huella–hora–ancla descrita en el capítulo 13 [3]. Protege a la familia del estafador —y al profesional honesto, del cliente que no quiere pagar.

El contrato que nunca se escribe

Mucho más frecuente que la estafa penal es el conflicto ordinario, y todos han oído una versión: el presupuesto verbal que crece —«han salido cosas»—; la calidad prometida que nadie puede contrastar; los plazos que se alargan sin fecha; los pagos que van por delante del trabajo hecho; los «extras» nunca pactados por escrito; la obra que queda a medias con la relación rota. El marco está —el Código Civil regula el contrato de obra, y la normativa de consumo exige presupuesto previo y factura cuando el cliente es consumidor [2]— pero la evidencia típica de una reforma doméstica es un PDF sin firmar, una cadena de WhatsApps y transferencias sin concepto.

La reforma tiene todas las características del conflicto perfecto: importe alto, duración larga, especificaciones que evolucionan, dos partes sin hábito documental —y un objeto, la casa, que cambia cada día borrando el estado anterior. Cuando llega la discusión, ni el cliente puede probar qué se pactó ni el profesional puede probar qué hizo. Y lo peor: el estado inicial de la vivienda —la pared que «ya estaba agrietada», el parqué que «ya estaba rayado»— desaparece físicamente bajo la propia obra, para siempre.

Los derechos existen; los hechos, no. Cada mensaje se puede borrar, cada transferencia queda sin concepto, cada acuerdo verbal vive en dos memorias que divergen. Lo que falta no es más normativa: es que lo que se pacta y lo que se hace dejen rastro fechado en manos de ambos.

La prueba de existencia aplicada

Cinco minutos el primer día, diez segundos en cada hito [3].

1. El presupuesto y sus versiones

El presupuesto aceptado —y cada modificación pactada después— escaneado y sellado con t2p el día que se pacta: hasta 50 páginas en un único PDF certificado [3]. Los «extras» dejan de ser una discusión: o tienen fecha y documento, o no existen. Protege al cliente del presupuesto que crece solo —y al profesional del cliente que «no recuerda» haber pedido el cambio.

2. El estado inicial: la foto que protege a ambos

Antes del primer golpe de maza, un recorrido fotográfico por la vivienda con GPS forense [3]: las paredes, los suelos, las ventanas, aquello que ya estaba estropeado. Es la evidencia que la obra destruirá físicamente —y la única defensa contra las dos acusaciones simétricas: «me habéis estropeado el parqué» y «esto ya estaba así». Cinco minutos que valen todo el conflicto.

3. Las fases con hitos: pagar contra hechos

Cada hito de obra —el derribo acabado, la instalación pasada, el alicatado hecho— documentado con fotos y un vídeo corto con fecha y hora sobreimpresas [3], y el pago correspondiente ligado al hito en el mismo proyecto de la app: presupuesto, fase, evidencia, justificante. El anticipo deja de ser un acto de fe: se paga contra hechos documentados —el patrón que desarma la estafa del anticipo [1], porque quien no piensa volver no quiere hitos.

4. La recepción firmada

La obra acabada —o cada fase— se recibe con la firma fuerte de t2p: el vídeo-selfie con retos de vida y verificación biométrica, de ambas partes [3]. La recepción fechada cierra el perímetro de la responsabilidad: los defectos que aparezcan después se discuten sobre el estado recibido y documentado, no sobre memorias. Y el expediente entero —presupuesto, estado inicial, fases, pagos, recepción— se exporta como paquete .asice verificable sin conexión [3]: para la reclamación de consumo, la vía civil o la denuncia [1].

Los límites, como siempre, por adelantado: el sello acredita documentos, estados y momentos —no valora la calidad técnica de la obra: eso lo hacen los peritos y, si hace falta, el juez [2]. No sustituye elegir bien —referencias, profesionales identificables, desconfianza del presupuesto imposible [1]. Y la proporcionalidad manda: el fontanero que viene una hora no necesita expediente; la reforma de 30.000 euros, sí.

La promesa y el peligro

La promesa: familias que pagan contra hechos y no contra promesas [1][3]; profesionales honestos blindados ante el mal cliente —y un oficio que recupera la reputación que los estafadores le roban; conflictos de extras y plazos que se resuelven mirando documentos fechados [2]; y la estafa del anticipo, cada vez más difícil: quien no piensa volver no acepta hitos.

Los peligros, que no son pocos.

El primero es **el cliente-expediente**: quien documenta obsesivamente para construir excusas de no pagar. La simetría lo desarma: si cada fase tiene evidencia y recepción firmada, el impago final se queda sin relato —el mismo rastro que protege al cliente, lo obliga.

El segundo es **la fricción en el pequeño oficio**. El autónomo que hace tres trabajos al día no puede administrar expedientes. El gesto ha de ser el de diez segundos —la foto del hito, el escaneo del presupuesto [3]— y, bien mirado, es el mismo que ya hace por WhatsApp: solo que con fecha cierta y sin depender de un chat.

El tercero es **el estafador que también documenta**: el teatro del profesional falso con fotos bonitas. El rastro no sustituye la prudencia: el patrón de la estafa es previo a la obra —el precio imposible y la prisa por el anticipo [1]— y ningún sello valida un presupuesto; valida que existía.

Y aún un cuarto: creer que documentar bien es construir bien. Ninguna huella hace buena una obra ni honesto un oficio. La calidad la hacen las manos y los materiales; la prueba solo garantiza que, si sale mal, la discusión sea de hechos. Y la mejor regla sigue siendo antigua: no pagar nunca mucho por delante de lo que hay hecho.

Es hora de actuar

Que la confianza se gane con hitos, no con promesas.

Para las familias: el ritual de los cinco minutos —presupuesto sellado, estado inicial fotografiado, pagos contra hitos [3]; y ante el precio imposible con prisa por el anticipo, la respuesta es no [1].

Para los reformistas y los gremios: el expediente fechado es vuestro mejor comercial —presupuesto, fases y recepción firmada [3] os blindan del mal cliente y os distinguen del estafador que os mancha el oficio [1].

Para los administradores de fincas: exigid el expediente verificable en las obras que superviséis —la derrama del capítulo 37 y la reforma privada comparten la misma lógica.

Para las autoridades de consumo y la Guardia Civil: el expediente .asice de la víctima [1][3] es la diferencia entre una denuncia archivable y una investigación con hechos.

Para los legisladores: la normativa de consumo ya pide presupuesto previo y factura [2]; el paso natural es reconocer el presupuesto y la recepción con fecha cierta como prueba cualificada de lo que se pactó.

Que la próxima cocina a medio hacer tenga, al menos, un expediente entero —y que el profesional que acaba el trabajo pueda cobrarlo sin discutir recuerdos. Por las casas que se reforman y los oficios que las levantan, **time2act**.



Figura 38.1 — La reforma con prueba de existencia (sellado con t2p — capítulo 13): el presupuesto y sus versiones sellados el día de pactarse, el estado inicial fotografiado con GPS forense (la prueba que la obra borra), las fases con hitos —pagar contra hechos documentados— y la recepción firmada con vídeo-selfie de las dos partes. Simetría: protege a la familia de la estafa del anticipo y al profesional honesto del cliente que no quiere pagar. Contexto: investigaciones de la Guardia Civil (Vigo: ≥6 víctimas de hasta 10.000 €; pérdidas >77.000 € en algún caso). Límites: la calidad la valoran los peritos; proporcionalidad; no pagar por delante de los hechos. Fuentes: prensa/Guardia Civil; normativa de consumo.

---

[1] Atlántico — *Investigan varias estafas en reformas de viviendas en Vigo y su comarca* (al menos seis víctimas; hasta 10.000 € cada una; constructor que inicia obras y desaparece); Liberal de Castilla — *Un vecino de Guadalajara pierde sus ahorros ante un falso albañil de internet* (Guardia Civil; estafador localizado en Madrid); Telemadrid — *Destapamos al presunto estafador de las reformas*; Allende Abogados — *Estafas en reformas* (patrón: oferta digital atractiva, presupuesto barato, anticipo «para materiales», desaparición; pérdidas que superan los 77.000 € en algunos casos). https://www.atlantico.net/articulo/vigo/investigan-estafa-reformas-menos-media-docena-victimas/20221017222637946245.html · https://www.liberaldecastilla.com/un-vecino-de-guadalajara-pierde-sus-ahorros-ante-un-falso-albanil-de-internet-la-guardia-civil-acorrala-al-estafador-en-madrid/ · https://www.telemadrid.es/programas/la-redaccion/Destapamos-presunto-estafador-reformas-2-2339786043--20210510052540.html · https://www.allendeabogados.com/estafas-reformas/ ↩

[2] Marco del contrato de obra (Código Civil) y normativa de consumo aplicable a reformas con consumidores (presupuesto previo y factura). Véase el capítulo 34 para el cobro del profesional y el capítulo 37 para la obra común. ↩

[3] t2p — manual de producto (escáner de documentos hasta 50 páginas en un PDF certificado; foto con GPS forense —fijado genuino ~50 m / ≤30 s; vídeo con fecha/hora sobreimpresa; proyectos para ligar presupuesto, fases, evidencias y pagos; firma con vídeo-selfie, retos de vida y biometría; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; la derrama, en el capítulo 37; la factura, en el capítulo 34. ↩

Activos del mundo real: tokenizar con pruebas, no a ciegas

«Cada hombre tiene una propiedad en su propia persona… El trabajo de su cuerpo y la obra de sus manos son propiamente suyos.»

— John Locke, Segundo tratado del gobierno civil, V, §27 (1689)

El 20 de marzo de 2024, el gestor de activos más grande del mundo hizo un gesto que sacudió Wall Street. BlackRock lanzó su primer fondo tokenizado, el BUIDL, sobre la red pública Ethereum: letras del Tesoro norteamericano, efectivo y repos puestos dentro de un token que se puede mover en una cadena de bloques. En doce meses, el fondo superó los **mil millones de dólares** [4][5]. Su consejero delegado, **Larry Fink**, lo había anunciado en su carta anual a los inversores como «la próxima generación de los mercados»: convertir acciones, bonos e inmuebles en tokens digitales negociables, capaces de «democratizar el rendimiento».

Pero en aquel gesto había un detalle que contiene toda la tensión de este capítulo. El token vive en la cadena; los bonos reales que lo avalan, no. Siguen en un custodio, **fuera de la cadena**, y el token solo *apunta* a ellos. El propio Fink lo admitió con una franqueza reveladora: para que esto escale, dijo, hay que resolver la verificación de identidad —saber quién hay al otro lado y que el token esté realmente avalado [10]. Esta es la pregunta del capítulo: cuando tokenizamos el mundo real, ¿el token apunta a una **promesa** o a una **prueba**?

La gran apuesta —y su agujero

La promesa económica es vertiginosa, aunque nadie se pone de acuerdo en la cifra. La consultora **BCG**, con la bolsa de mercados privados ADDX, proyectó en 2022 en su informe *Relevance of On-chain Asset Tokenization* que el mercado crecería cincuenta veces, hasta unos **16,1 billones de dólares en 2030** — un 10 % del PIB mundial [1]. **McKinsey**, como hemos visto, preveía unos **2 billones** en 2030, con un rango de 1 a 4 [2]; la diferencia —ocho veces— no es un detalle técnico: refleja cuánta basura están dispuestas a admitir y la velocidad real de la adopción. Standard Chartered proyecta unos **30,1 billones** en 2034 [9].

La realidad actual es más modesta y reveladora. A mediados de 2025, el mercado de RWA tokenizados —sin contar las stablecoins— era de unos **24.000 millones de dólares**, un 380 % más que tres años antes [3]. El segmento más grande no eran los bonos del Tesoro, sino el **crédito privado** (unos 14.000 millones), seguido de los Tesoros (unos 7.000) y del oro tokenizado (unos 4.000). Este oro ilustra bien el problema y la solución: el token PAXG está avalado por barras con número de serie guardadas en las cámaras de Brink's en Londres, y desde febrero de 2025 la auditoría KPMG emite atestaciones mensuales que verifican el aval onza por onza [6]. La pregunta es: ¿y si la atestación se pudiera falsear o retrodatar? Todo el edificio descansa, una vez más, sobre una prueba.

El problema del oráculo

Aquí reside la fragilidad estructural de toda la tokenización, y tiene nombre técnico: el **problema del oráculo**. El token está en la cadena, pero el valor está fuera —la barra de oro, la escritura, el bono, el informe de custodia—, y alguien tiene que hacer de puente entre ambos mundos. El **Consejo de Estabilidad Financiera** (FSB), organismo que coordina la regulación financiera global, lo advirtió con claridad en su informe *The Financial Stability Implications of Tokenisation* (octubre de 2024): la tokenización «depende a menudo de proveedores externos, como custodios para guardar los activos de referencia y oráculos para recoger sus datos», lo que «introduce nuevos puntos de vulnerabilidad» y puede provocar un «desajuste entre el precio del token y el valor del activo de referencia» [7]. La agencia de calificación **Moody's** añadió que muchos emisores y proveedores tecnológicos tienen un «historial limitado» y que un fallo de oráculo puede interrumpir los pagos aunque el código funcione perfectamente [8].

No es un miedo abstracto. En marzo de 2022, la stablecoin Cashio, en la red Solana, se hundió cuando un atacante explotó un error que le permitía acuñar tokens «avalados»… sin ningún colateral real [8]. Es la imagen literal del principio que recorre este libro: «basura a la entrada, basura en la cadena». Un token

perfectamente válido en la cadena que no estaba avalado por nada. Y aquí conviene recordar la lección ya explicada con los créditos de carbono: cuando se tokeniza sobre un subyacente no verificado, la cadena se llena de «créditos zombi». Trasladado a los activos del mundo real, el mismo error se repetiría a escala de billones.

Tokenizar a ciegas o tokenizar con pruebas

La conclusión es nítida y es la tesis del capítulo. La blockchain no hace verdadero lo que tokeniza; lo hace *negociable e inmutable*. Si lo que hay debajo es una promesa sin prueba, tendremos una promesa inmutable —que es exactamente lo peor: una mentira que se vende con la apariencia de la certeza criptográfica. La diferencia entre un mercado de 2 billones sólidos y uno de 16 billones inflados no la marca la tecnología del token, sino **la calidad de la prueba de lo que hay debajo**. Tokenizar a ciegas es repetir el error de los zombis; tokenizar con pruebas es la condición para que esta revolución financiera no acabe en una crisis de confianza.

La prueba de existencia bajo el token

Es aquí donde **t2p** aporta la pieza que falta. No resuelve la custodia ni la legalidad —eso corresponde al custodio, al auditor y al registro—, pero **sella la evidencia documental que un token debería referenciar**, de manera verificable sin conexión. El mecanismo es el de siempre, aplicado al respaldo. El documento que constituye el respaldo del token —la escritura, el informe de tasación, el certificado de custodia o de auditoría, la póliza, la fotografía de la barra con su número de serie— recibe una **huella SHA-512** calculada en el dispositivo, se ancla a la **blockchain pública** y se acompaña de un **sello de tiempo RFC 3161** conforme a eIDAS. Para los activos físicos, la captura lleva **GPS forense** y fecha sellados: «esta foto del activo se tomó aquí, este día». Y la **prueba de vida** liga la evidencia a una persona real —el tasador, el custodio, el firmante—, resolviendo precisamente la verificación de identidad que Fink señalaba como cuello de botella.

Todo se empaqueta en un **contenedor .asice verificable sin conexión**, sin depender de t2p ni de la cadena del token. Y aquí está el giro: el token RWA puede **apuntar a la huella de un .asice** en lugar de apuntar a una promesa. El comprador deja de confiar en que hay un bono detrás; puede **comprobar por sí mismo** que la evidencia existía íntegra en aquel momento, lugar y persona. Esto cierra la puerta a la sustitución o la posedición del documento de respaldo, a reutilizar el mismo informe para varios tokens y a la opacidad sobre *cuándo* existía la prueba. Convertir «confía en que hay un activo» en «aquí tienes el sello de la evidencia, verifícalo» es, en sí mismo, una transformación del riesgo.

Hay que ser, como siempre, escrupulosamente honesto con el límite, porque aquí es especialmente peligroso olvidarlo. La prueba de existencia demuestra que **un registro existió, íntegro, en un momento, lugar y persona**; **no** demuestra que la barra siga en la cámara, que no se haya pignorado dos veces, ni que el token confiera un derecho legal sobre ella. La custodia, la auditoría independiente del inventario y la exigibilidad legal del derecho siguen siendo imprescindibles. t2p refuerza la **capa de evidencia**, no sustituye al custodio ni al auditor; es complementario, por ejemplo, a sistemas de prueba de reservas que verifican el respaldo conectándose a los custodios. Es, en una frase, la diferencia entre tokenizar a ciegas y tokenizar con pruebas.

La promesa y el peligro

La promesa es inmensa: una tokenización apoyada en evidencia verificable podría abrir a los pequeños inversores activos hoy ilíquidos —inmuebles, fondos privados, infraestructuras—, hacer los mercados más rápidos y transparentes, y hacerlo sin sacrificar la confianza. En un mercado que podría valer billones, que cada token apunte a una prueba y no a una promesa es la diferencia entre una revolución y una burbuja.

El peligro pide el matiz de siempre, en la dualidad de «la promesa y el peligro». El primero, ya dicho: confundir el sello de la evidencia con la garantía del derecho legal o de la custodia sería un fraude peor que el que se quiere evitar. El segundo, la falsa sensación de seguridad que puede dar una capa técnica brillante sobre un activo malo. Y el tercero, la concentración: si la verificación de la evidencia queda en muy pocas manos, recreamos el intermediario único que la blockchain prometía disolver. La prueba de existencia es una capa necesaria dentro de una arquitectura que incluye, siempre, el custodio, el auditor y el regulador.

Es hora de actuar

Para los **emisores y tokenizadores**: anclaje de la evidencia del respaldo —tasaciones, certificados de custodia, fotos serializadas— para que cada token apunte a una prueba verificable, no a una promesa. Para los **custodios y auditores**: sellar sus atestaciones en origen, impidiendo que se puedan retrodatar ni reutilizar. Para los **inversores**: exigir poder comprobar la evidencia del subyacente antes de comprar y desconfiar del token que solo ofrece una promesa. Para los **reguladores** (FSB, supervisores nacionales): reconocer el valor de la capa de evidencia y cerrar el vacío del oráculo antes de que el mercado llegue a los billones anunciados.

BlackRock puso bonos del Tesoro dentro de un token, pero los bonos siguen fuera de la cadena. Toda la tokenización del mundo real depende de aquel hilo invisible entre el token y la prueba de lo que lo respalda. Hacer que ese hilo sea verificable por cualquiera —tokenizar con pruebas, no a ciegas— es, también aquí, time2act.

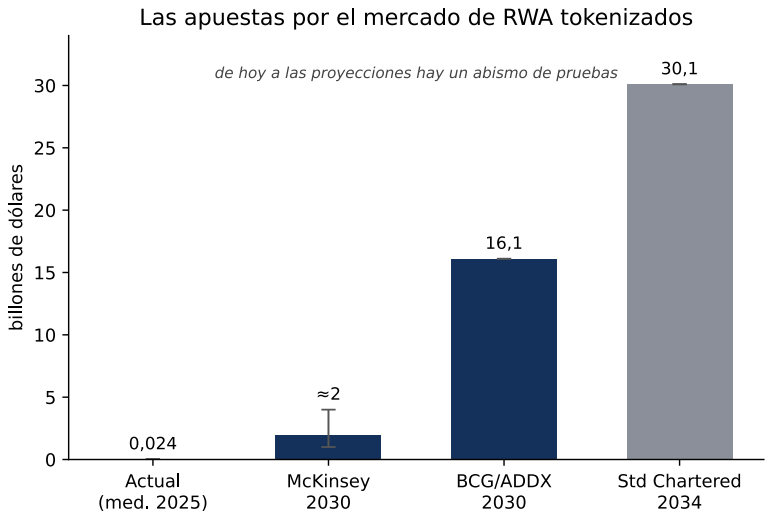


Figura 39.1 — Las dos proyecciones de referencia para el mercado de RWA tokenizados en 2030 difieren unas ocho veces: el escenario prudente de McKinsey (~2 billones de dólares, rango 1-4) y el optimista de BCG/ADDX (~16,1 billones); el punto de partida real era de unos 24.000 millones a mediados de 2025. La distancia depende, en el fondo, de cuánta «basura» se admita: del vacío entre el token y la prueba de su respaldo —el problema del oráculo— que la prueba de existencia ayuda a cerrar. Fuentes: McKinsey (2024); BCG/ADDX (2022); CoinDesk/RWA.xyz (2025).

[1] BCG y ADDX — *Relevance of On-chain Asset Tokenization in 'Crypto Winter'* (2022; ~16,1 billones $ en 2030, ~10 % del PIB mundial). https://www.bcg.com/publications/2022/relevance-of-on-chain-asset-tokenization ↩

[2] McKinsey — *From ripples to waves: the transformational power of tokenizing assets* (2024; caso base ~2 billones $, rango 1-4, excluye stablecoins). https://www.mckinsey.com/industries/financial-services/our-insights/from-ripples-to-waves-the-transformational-power-of-tokenizing-assets ↩

[3] CoinDesk (informe RedStone / Gauntlet / RWA.xyz) — *Real-world asset tokenization market has grown almost fivefold in 3 years* (~24.000 M$; crédito privado ~14.000 M$). https://www.coindesk.com/business/2025/06/26/real-world-asset-tokenization-market-has-grown-almost-fivefold-in-3-years ↩

[4] BlackRock / BusinessWire — *BlackRock Launches Its First Tokenized Fund, BUIDL, on the Ethereum Network* (20-mar-2024). https://www.businesswire.com/news/home/20240320771318/en/BlackRock-Launches-Its-First-Tokenized-Fund-BUIDL-on-the-Ethereum-Network ↩

[5] Securitize / PR Newswire — *BlackRock's BUIDL surpasses $1B in AUM* (marzo 2025). https://www.prnewswire.com/news-releases/blackrock-usd-institutional-digital-liquidity-fund-buidl-tokenized-by-securitize-surpasses-1b-in-aum-302401480.html ↩

[6] Paxos — *PAXG transparency* (barras serializadas en Brink's Londres; atestaciones mensuales de KPMG). https://www.paxos.com/paxg-transparency ↩

[7] Financial Stability Board — *The Financial Stability Implications of Tokenisation* (octubre 2024; custodios y oráculos como nuevos puntos de vulnerabilidad). https://www.fsb.org/2024/10/the-financial-stability-implications-of-tokenisation/ ↩

[8] Moody's (vía CoinDesk) — *Tokenized fund adoption grows but brings technology risks* (2024; fallos de oráculo, historial limitado). https://www.coindesk.com/markets/2024/01/15/tokenized-fund-adoption-grows-but-brings-technology-risks-

moodys ↩

[9] Standard Chartered y Synpulse — *Trade finance to play substantial role in $30.1 trillion tokenised real-world assets market by 2034.* https://www.sc.com/en/press-release/trade-finance-to-play-substantial-role-in-usd-30-1-trillion-tokenised-real-world-assets-market-by-2034/ ↩

[10] InvestmentNews — *Larry Fink takes aim at investment inequality* (carta anual 2025 de BlackRock; la verificación de identidad como condición). https://www.investmentnews.com/alternatives/larry-fink-takes-aim-at-investment-inequality/259910 ↩

Autoría creativa: probar quién lo hizo primero en la era de la IA

«Porque las obras maestras no son nacimientos únicos y solitarios; son el fruto de muchos años de pensar en común [...] de modo que tras la voz única está la experiencia de la multitud.»

— Virginia Woolf, Una habitación propia (1929)

El 4 de abril de 2023, un usuario anónimo que se hacía llamar *ghostwriter977* subió una canción a las plataformas de streaming. Se titulaba «Heart on My Sleeve» y sonaba como una colaboración inédita entre Drake y The Weeknd, dos de los artistas más grandes del planeta. No lo era: sus voces habían sido clonadas con inteligencia artificial. La canción se propagó como la pólvora —solo en TikTok acumuló unos **quince millones de visualizaciones**— hasta que, el lunes siguiente, plataforma a plataforma, desapareció. En YouTube quedaba el cartel: «Este vídeo ya no está disponible por una reclamación de copyright de Universal Music Group» [7]. La discográfica consiguió retirarla alegando que entrenar y generar IA con las voces de sus artistas vulneraba sus acuerdos y la ley.

La escena contiene toda la inquietud de este capítulo. Dos de los músicos más poderosos del mundo quedaron, durante unos días, a merced de un anónimo, y la canción ni siquiera contenía sus grabaciones: solo sus voces sintéticas. Para un creador sin el ejército jurídico de una multinacional —una ilustradora, un fotógrafo, un guionista, un músico independiente—, la pregunta es aún más angustiosa: ¿cómo demuestro que **una obra es mía y que existía antes** de que una máquina se la tragara o de que alguien la copiara? Este capítulo trata de eso: de volver a hacer demostrable la autoría en la era de la copia infinita.

La maquinaria que se traga la autoría

El caso de la canción es la punta de un iceberg de litigios que están redefiniendo la creación. El **New York Times** demandó a OpenAI y Microsoft en diciembre de 2023 por haber copiado «millones» de sus artículos sin permiso ni pago para entrenar sus modelos; como prueba, adjuntó un anexo de 127 páginas que alinea, columna contra columna, párrafos del diario y salidas casi idénticas de GPT-4 —la demostración visual de que el modelo «memorizaba» el periodismo que supuestamente solo había «aprendido» [1]. El caso avanza poco a poco: en enero de 2026, un juez obligó a OpenAI a entregar a los demandantes una muestra de veinte millones de registros de conversaciones de ChatGPT [2]. **Getty Images** llevó a Stability AI a los tribunales de Londres por haber procesado millones de sus imágenes sin licencia [3][4]. Y un grupo de artistas demandó a Stability, Midjourney y DeviantArt por haber alimentado los generadores con su obra.

Una de aquellas artistas es **Karla Ortiz**, ilustradora que ha dado forma a personajes de Marvel. En julio de 2023 declaró ante el Comité Judicial del Senado de Estados Unidos una frase que resume el agravio de toda una profesión: sobre la práctica totalidad de su obra ingerida por los modelos, «nunca me han preguntado, nunca me han acreditado, nunca me han compensado ni un céntimo» [6]. No es un rechazo a la tecnología. Como subraya la propia Getty —que sí licencia su catálogo a desarrolladores de IA respetando los derechos—, el conflicto no es la IA en sí, sino **el consentimiento y la licencia** [3]. Y en Hollywood, la huelga de actores de SAG-AFTRA, la más larga de la historia contra los estudios, se saldó con un acuerdo que exige consentimiento informado y compensación justa antes de crear una «réplica digital» de un intérprete [8].

El creador y la prueba de prioridad

Bajo todos estos casos hay un mismo problema, y es de **prioridad temporal**: demostrar que un tema, una ilustración, un guion o una foto existían, firmados por ti, *antes* de que un modelo los ingiriera o de que alguien los copiara. Y aquí la ley ha dado una pista decisiva. La Oficina de Copyright de Estados Unidos estableció en enero de 2025 que **la autoría humana es el fundamento del copyright**: una obra generada enteramente por IA no es registrable, y la simple elección de instrucciones, por detallada que sea, no basta para crear una obra protegible [10]. La consecuencia es profunda: en un mundo inundado de contenido sintético, el valor se desplaza hacia **quién creó qué, y cuándo**. La prueba de la autoría humana y de su fecha se convierte en el activo central.

Por qué la etiqueta por sí sola se borra

La industria ya ha intentado responder con una buena idea: las **Content Credentials** del estándar **C2PA**, una coalición bajo la Linux Foundation que incluye a Adobe, la BBC, Google, Microsoft, OpenAI o Sony. Funcionan como una «etiqueta nutricional» del contenido digital: un manifiesto firmado criptográficamente e incrustado en el archivo que registra quién lo creó, cuándo, con qué herramientas y con qué historial de edición [9]. Es una herramienta valiosa y necesaria. Pero tiene un talón de Aquiles confirmado, y es demoledor: **la mayoría de redes sociales recomprimen las imágenes al subirlas y borran el manifiesto**. WhatsApp, iMessage o Facebook reescriben el archivo y eliminan las credenciales; una captura de pantalla, un cambio de formato o un reescalado bastan para romperlas. La propia C2PA lo reconoce y ha introducido «credenciales duraderas» con marca de agua invisible, pero admite que el sistema «depende del cumplimiento de todo el ecosistema», algo poco realista en un entorno abierto. La etiqueta, pues, viaja dentro del archivo y se pierde con él. Falta un ancla independiente.

La prueba de existencia: sellar la obra al nacer

Es aquí donde **t2p** aporta exactamente esa ancla. En lugar de escribir la prueba *dentro* del archivo —de donde se puede borrar—, la fija *fuera*, en una cadena pública. En el momento de la creación, se calcula la **huella SHA-512** de la obra —el `.wav` de la maqueta, el `.psd` por capas, el `.raw` de la foto, el guion— **en el propio dispositivo, sin que el archivo salga**: un detalle crucial para el creador que aún no ha publicado y no quiere subir su obra inédita a ningún servidor. Esa huella se ancla a la **blockchain pública** con un **sello de tiempo RFC 3161** conforme a eIDAS, creando una **fecha cierta de autoría** verificable por cualquiera, que sobrevive aunque el creador cambie de plataforma o desaparezca. El **GPS forense** y la **prueba de vida** ligan el momento de creación a un lugar y a una persona viva —útil contra las disputas de «quién lo hizo primero» y contra las réplicas sintéticas, porque vinculan la obra a un autor humano real. Y todo se empaqueta en un **contenedor .asice verificable sin conexión** que un tribunal o un comprador pueden comprobar por su cuenta.

La clave es que t2p **no compite con C2PA, la completa**. Las Content Credentials aportan la trazabilidad legible dentro del archivo; la prueba de existencia aporta el **ancla inmutable** que sobrevive aunque el manifiesto se borre o alguien haga una captura de pantalla: el hash en la cadena sigue demostrando que aquel archivo exacto existía en tal fecha, lugar y persona. La pareja natural es esta: credenciales para la trazabilidad, prueba de existencia para el ancla. Y el **marketplace NFT** añade un historial de procedencia y de licencias que no se puede editar a posteriori, útil para licenciar legítimamente a quien sí quiera entrenar con consentimiento —el modelo Getty: licencia, no expolio.

Hay que decir los límites sin ambages, fieles a la dualidad de «la promesa y el peligro». «Basura a la entrada, basura en la cadena»: la prueba de existencia demuestra **cuándo, qué, dónde y quién** selló, no que la obra sea **original o no infractora**. Si selláis un plagio, tendréis un plagio con fecha cierta. Tampoco resuelve la cuestión jurídica de fondo —si entrenar con obra protegida es o no uso legítimo—, que decidirán los tribunales y los reguladores. Y la autoría humana que exige la ley sigue siendo un requisito separado: el sello prueba precedencia, no convierte en registrable lo que la ley no protege. Finalmente, anclar antes de publicar solo ayuda si se hace antes de la filtración; no rebobina lo que ya se ha expoliado.

La promesa y el peligro

La promesa es inmensa para millones de creadores. Una capa de prueba de autoría en el origen les daría, por primera vez, una manera barata y universal de demostrar la prioridad de su obra, de defenderse ante un tribunal y de licenciarla en sus términos en lugar de verla expoliada. En una economía creativa amenazada por la copia infinita, poder decir «esto es mío, y lo puedo probar» es recuperar el poder de negociar.

El peligro pide matiz. El primero, no confundir precedencia con originalidad: el sello no limpia un plagio ni resuelve por sí solo la autoría legal. El segundo, la carga para los creadores menos tecnológicos, que el diseño ha de hacer trivialmente fácil para no excluir a nadie. Y el tercero, la privacidad: la prueba de vida y la geolocalización del acto creativo son datos sensibles que hay que proteger. La prueba de existencia es una herramienta de empoderamiento del creador, no un atajo que sustituya a los tribunales ni a la ley.

Es hora de actuar

Para los **creadores** (músicos, ilustradores, fotógrafos, guionistas): sellar la obra en el momento de crearla, antes de compartirla, para tener fecha cierta de autoría. Para las **plataformas**: dejar de destruir las credenciales de procedencia al subir el contenido y reconocer el ancla independiente. Para los **desarrolladores de IA**: licenciar la obra con consentimiento —el modelo Getty— en lugar de expoliarla, usando el rastro de procedencia para identificar y compensar a los autores. Para los **reguladores y tribunales**: cerrar el marco legal del consentimiento y el uso justo, y reconocer el valor probatorio del sello de autoría.

Dos de los músicos más grandes del mundo quedaron indefensos ante una voz sintética; el creador individual lo está aún más. La diferencia entre una obra que cualquiera puede reclamar o copiar y una obra que nace con una prueba de autoría inalterable es, cada vez más, la diferencia entre crear y ser expoliado. Como hemos visto, demostrar quién lo hizo primero —y que era humano— es, también aquí, time2act.

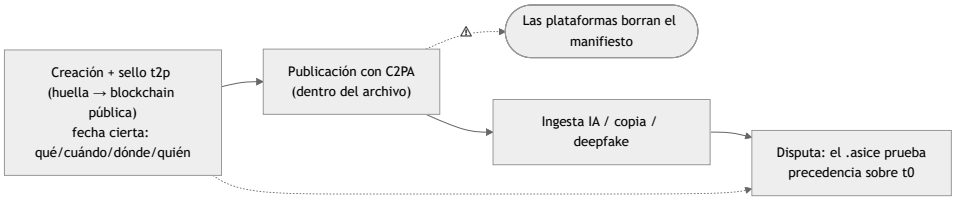


Figura 40.1 — En el momento de crear (t0), la obra se sella con huella SHA-512 en el dispositivo, ancla a la blockchain pública, sello de tiempo eIDAS, GPS y prueba de vida: fecha cierta de qué, cuándo, dónde y quién. Al publicarla (t1), las credenciales C2PA pueden borrarse al subirla a las redes; cuando un modelo la ingiere o alguien la copia (t2), el contenedor .asice todavía demuestra que el archivo existía intacto en t0, antes de t2. La prueba de existencia demuestra precedencia, no originalidad. Fuentes: C2PA; U.S. Copyright Office; casos NYT, Getty, Andersen.

---

[1] NPR — *The New York Times sues OpenAI and Microsoft for copyright infringement* (27-dic-2023; anexo de 127 páginas con salidas de GPT-4). https://www.npr.org/2023/12/27/1221821750/new-york-times-sues-chatgpt-openai-microsoft-for-copyright-infringement ↩

[2] Bloomberg Law — *OpenAI must turn over 20 million ChatGPT logs, judge affirms* (enero 2026). https://news.bloomberglaw.com/ip-law/openai-must-turn-over-20-million-chatgpt-logs-judge-affirms ↩

[3] Getty Images — *Getty Images statement* (acción contra Stability AI; consentimiento y licencia, enero 2023). https://newsroom.gettyimages.com/en/getty-images/getty-images-statement ↩

[4] Judiciary of England and Wales — *Getty Images v Stability AI [2025] EWHC 2863 (Ch)* (nov 2025; desestima la mayor parte de las reclamaciones de copyright). https://www.judiciary.uk/judgments/getty-images-v-stability-ai/ ↩

[5] Copyright Alliance — *Andersen v. Stability AI* (Sarah Andersen, Kelly McKernan, Karla Ortiz; discovery desde agosto 2024). https://copyrightalliance.org/andersen-v-stability-ai-copyright-case/

[6] Karla Ortiz — *Testimony before the U.S. Senate Judiciary Committee* (12-jul-2023; «nunca me han preguntado, acreditado ni compensado»). https://www.judiciary.senate.gov/imo/media/doc/2023-07-12_pm_-testimony-_ortiz.pdf ↩

[7] Variety — *AI-generated fake Drake/The Weeknd song 'Heart on My Sleeve'* (abril 2023; retirada por Universal Music Group). https://variety.com/2023/music/news/fake-ai-generated-drake-weeknd-collaboration-heart-on-my-sleeve-1235585451/ ↩

[8] Wikipedia — *2023 SAG-AFTRA strike* (14-jul a 9-nov-2023; consentimiento para la «réplica digital»). https://en.wikipedia.org/wiki/2023_SAG-AFTRA_strike ↩

[9] C2PA / Content Authenticity Initiative — *Content Credentials* (manifiesto firmado; las plataformas lo borran al recomprimir). https://c2pa.org/ ↩

[10] U.S. Copyright Office — *Copyright and Artificial Intelligence, Part 2: Copyrightability* (29-ene-2025; la autoría humana como fundamento). https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf ↩

Patentes y prior art: la publicación defensiva con fecha cierta

«Se puede resistir la invasión de los ejércitos; no se puede resistir la invasión de las ideas.»

— Victor Hugo, Historia de un crimen (1877)

Hay una escena que se repite en los despachos de abogados de patentes de todo el mundo. Un inventor independiente llega con un sobre cerrado, amarillento por los años. Dentro está la descripción de su invento, que él mismo se envió por correo certificado hace tiempo, convencido de que aquel matasellos era una especie de **«patente del pobre»** que protegería su idea. Ahora un competidor ha patentado algo parecido, y el inventor quiere hacer valer su sobre. El abogado tiene que explicarle, con tacto, que aquel gesto repetido durante décadas **nunca protegió nada**: enviarse un sobre a uno mismo no establece ningún derecho de patente ni es una prueba reconocida por los tribunales [5]. Y todavía hay una noticia peor: desde 2013, en Estados Unidos, ni siquiera la fecha importa frente a quien presentó primero la solicitud.

Esta escena contiene el nudo de este capítulo. La propiedad industrial es una carrera cara e implacable, y la mayoría de inventores —los autónomos, las pequeñas empresas, los investigadores— no se pueden permitir correr en ella. Pero existe una jugada poderosa y poco conocida que les cambia las reglas: en lugar de patentar, **publicar con fecha cierta** para impedir que nadie más lo patente. Y aquí la prueba de existencia ofrece una herramienta casi hecha a medida.

La carrera de quien presenta primero

Para entender la jugada, hay que conocer el terreno. El 16 de marzo de 2013, Estados Unidos abandonó el viejo sistema de «primero en inventar» y adoptó el de **«primero en presentar»** (*first-invention-to-file*), con la entrada en vigor de la America Invents Act. Como resume la propia oficina de patentes norteamericana, la **USPTO**, a partir de aquella fecha «la fecha de la invención es irrelevante»: lo que cuenta es quién presenta antes la solicitud [1]. El sistema premia la velocidad y el capital, no la paternidad de la idea.

Según las estimaciones del sector, redactar una solicitud de patente de utilidad en Estados Unidos cuesta entre 9.000 y 17.000 dólares, y hay que presupuestar **entre 15.000 y 25.000 dólares** antes de que la patente se conceda, sin contar las tasas de mantenimiento que se extienden durante toda su vida [3]. Para una gran corporación es calderilla; para un inventor individual, una barrera a menudo infranqueable. Existe una vía oficial más económica para fijar la fecha —la solicitud provisional, que por unos centenares de dólares otorga el estatus de «patent pending» durante doce meses—, pero no se examina y caduca si no se presenta después la solicitud completa [4].

Un concepto clave abre una puerta. La **Organización Mundial de la Propiedad Intelectual** (WIPO) define el **estado de la técnica** —el *prior art*— como toda información puesta a disposición del público en cualquier lugar del mundo antes de la fecha de presentación; para que una invención sea patentable, ha de aportar una característica nueva que no esté ahí [2]. Y aquí viene el giro decisivo: la WIPO recuerda que **divulgar públicamente una invención antes de presentar la solicitud puede destruir su novedad** y hacerla impatentable —salvo que la ley prevea un «periodo de gracia», presente en Estados Unidos o Canadá pero no en Europa, y en China solo de manera muy restringida [2]. Esta espada de doble filo es precisamente el arma defensiva.

Publicar para defenderse

Si divulgar destruye la novedad, se puede divulgar a propósito para impedir que otro lo patente. Es la **publicación defensiva**: difundir deliberadamente una descripción de la invención para que entre en el dominio público y se convierta en prior art, derrotando cualquier solicitud de patente posterior de un tercero sobre la misma idea. No da derechos exclusivos —una vez publicada, la invención ya no se puede patentar—, pero evita los costes de una patente y, sobre todo, impide que un competidor te la quite y te cobre por su uso.

No es una idea marginal; es una industria. **Technical Disclosure Commons**, una plataforma **gratuita** operada por Google, permite a cualquiera publicar una divulgación técnica que el sistema **fecha**

automáticamente y que **Google Patents indexa**, de modo que un examinador la encontrará al evaluar una solicitud rival [6]. **IP.com** ofrece una base de datos de prior art donde cada publicación se cierra con un **sello de tiempo criptográfico** —del servicio Surety AbsoluteProof— que protege su integridad y su fecha. Y **Research Disclosure**, el servicio decano del sector, publica divulgaciones defensivas desde 1960. Todo este material se puede buscar en bases gigantescas: el Espacenet de la Oficina Europea de Patentes superó los **160 millones de documentos** en abril de 2025, y el PATENTSCOPE de la WIPO ronda los 128 millones [9][10]. Como explican los abogados de patentes Richard Coller y Alexander Covington en un trabajo de referencia sobre la estrategia, la publicación defensiva no sustituye nunca el valor de una patente para una innovación importante, pero es una manera muy rentable de bloquear competidores cuando hay que tomar decisiones difíciles de presupuesto [8].

Fijémonos en un detalle, porque es la clave de todo: IP.com ya sella sus publicaciones con una marca de tiempo criptográfica y un archivo validable por cualquiera. Es, en esencia, un **notario digital** que congela el contenido y la fecha. Y aquí es donde entra t2p, generalizando aquel servicio a cualquier persona.

La prueba de existencia para la invención

La mecánica de **t2p**, aplicada a la invención, es sencilla y potente. El inventor toma el documento de divulgación —la memoria técnica, los planos, el código, el cuaderno de laboratorio donde consta la concepción— y calcula su **huella SHA-512** en el dispositivo, sin que el documento salga. Esa huella se ancla a la **blockchain pública** con un **sello de tiempo RFC 3161** conforme a eIDAS, y todo se empaqueta en un **contenedor .asice verificable sin conexión**. El **GPS forense** y la **prueba de vida** pueden ligar el momento a un lugar y a una persona real.

El resultado demuestra, de manera inalterable y verificable globalmente, que **aquel contenido exacto existía íntegro en aquella fecha**, opcionalmente en aquel lugar y por aquella persona. Es, en la práctica, dos cosas a la vez: una **publicación defensiva instantánea y barata con fecha cierta** —si, además, el contenido se hace público en aquella fecha—, y una **prueba de la fecha de concepción** para disputas entre coinventores, entre empresa y empleado o entre socios. Ante el presupuesto de quince a veinticinco mil dólares de una patente, el coste de un sellado es marginal. Y contra la retrodatación, es impenetrable: nadie puede fabricar después un documento «de aquella fecha», porque la huella anclada y el sello son inmutables.

Hay que decir los límites con toda la crudeza, fieles a la dualidad de «la promesa y el peligro», porque aquí confundirse sale caro. La prueba de existencia **no demuestra novedad, patentabilidad, utilidad ni que el invento funcione**: eso lo decide el examinador contra todo el prior art mundial. Tampoco convierte un documento privado en prior art por sí sola: para bloquear a un tercero, la divulgación ha de ser **accesible al público** —un hash anclado sin publicar el contenido prueba *posesión en una fecha*, no *disponibilidad para el público*. Y en Europa, donde no hay periodo de gracia, publicar **también destruye tu propia novedad**: la fecha cierta no sustituye la decisión estratégica entre patentar y publicar, solo la hace más sólida una vez tomada. «Basura a la entrada, basura en la cadena»: el sello prueba fecha y contenido, no que la idea sea realmente tuya ni original.

La promesa y el peligro

La promesa es profundamente democratizadora. Una herramienta de fecha cierta barata pone al alcance del inventor individual una jugada —la publicación defensiva— que hasta ahora dominaban las grandes corporaciones con departamentos de patentes. Permite proteger la prioridad de una idea, bloquear que un gigante la patente y resolver disputas de autoría, todo por una fracción del coste del sistema. En una economía de la innovación donde la velocidad y el capital lo deciden todo, significa devolver un poco de poder a quien crea.

El peligro pide matiz. El primero, ya dicho: confundir el sello con una patente o con una prueba de novedad sería un error costoso; la prueba de existencia es precedencia, no patentabilidad. El segundo, la tentación de sellar sin publicar y creerse protegido contra terceros, cuando solo la divulgación pública crea prior art oponible. Y el tercero, la decisión irreversible: publicar defensivamente cierra para siempre la puerta a patentar aquella invención. La prueba de existencia es una herramienta al servicio de una estrategia, no un sustituto del consejo experto sobre cuándo patentar y cuándo publicar.

Es hora de actuar

Para los **inventores individuales y las pequeñas empresas**: sellar la concepción con fecha cierta y, cuando la jugada sea defensiva, publicar la divulgación para bloquear patentes ajenas a una fracción del coste. Para los **departamentos de I+D**: integrar el sellado en el flujo de trabajo, para tener prueba de prioridad de cada idea antes de decidir qué se patenta y qué se publica. Para las **plataformas de publicación defensiva**: ofrecer el anclaje independiente como complemento a su sello. Para las **oficinas de patentes**: reconocer e indexar estas divulgaciones fechadas como prior art de pleno derecho.

El inventor del sobre amarillento confió su idea a un gesto que no protegía nada. Hoy, cualquier persona puede dejar constancia inalterable de que una idea era suya en una fecha cierta y convertirla en una muralla contra quien la quiera patentar. Demostrar quién la concibió primero —y hacerlo al alcance de todos— es, también aquí, **time2act**.



Figura 41.1 — El inventor sella el documento de divulgación con huella SHA-512, ancla a la blockchain pública y sello de tiempo eIDAS (fecha cierta, integridad y autoría), por un coste marginal ante los 15.000-25.000 dólares de una patente. Si además lo publica (Technical Disclosure Commons, IP.com, web), se convierte en prior art indexado por Espacenet o Google Patents; cuando llega la solicitud de un rival, el examinador encuentra la divulgación fechada y la rechaza por falta de novedad. El sello prueba fecha y contenido, no la patentabilidad —que decide el examinador. Fuentes: USPTO; WIPO; Technical Disclosure Commons.

---

[1] USPTO — *America Invents Act (AIA): Frequently Asked Questions* (primero en presentar desde el 16-mar-2013; «la fecha de la invención es irrelevante»). https://www.uspto.gov/patents/laws/america-invents-act-aia/america-invents-act-aia-frequently-asked ↩

[2] WIPO (Organización Mundial de la Propiedad Intelectual) — *Patents: Frequently Asked Questions* (prior art; la divulgación previa destruye la novedad; el periodo de gracia no es universal). https://www.wipo.int/en/web/patents/faq_patents ↩

[3] BitLaw — *What does a patent application cost?* (redacción 9.000-17.000 $; presupuestar 15.000-25.000 $ antes de la concesión). https://www.bitlaw.com/guidance/patent/what-does-a-patent-application-cost.html ↩

[4] USPTO — *Fee Schedule* (solicitud provisional: fija fecha, 12 meses; tasas oficiales). https://www.uspto.gov/sites/default/files/documents/USPTO-fee-schedule_current.pdf ↩

[5] McLane Middleton — *Know the Law: Is the 'Poor Man's Patent' Real?* (sin valor legal; obsoleta desde el first-to-file de 2013). https://www.mclane.com/insights/know-the-law-is-the-poor-mans-patent-real/ ↩

[6] Technical Disclosure Commons — *FAQ* (gratuito; fecha de publicación automática; indexado por Google Patents). https://www.tdcommons.org/faq.html ↩

[7] IP.com — *Publishing Disclosures to the Prior Art Database* (sello de tiempo mediante Surety AbsoluteProof). https://kb.ip.com/pad/knowledge-base/publishing-disclosures-to-the-prior-art-database-pad/

[8] Richard Coller III y Alexander Covington (IPWatchdog) — *Defensive Publications: A Cost-Effective Tool to Supplement Your Patent Strategy* (2020). https://ipwatchdog.com/2020/05/25/defensive-publications-cost-effective-tool-supplement-patent-strategy/ ↩

[9] Oficina Europea de Patentes (EPO) — *Espacenet reaches 160 million patent documents* (abril 2025). https://agip-news.com/news.aspx?id=76074&lang=en ↩

[10] WIPO — *PATENTSCOPE* (~128 millones de documentos de patente; 5,4 M de solicitudes PCT). https://patentscope2.wipo.int/ ↩

Secretos empresariales: probar sin revelar

«Nadie puede guardar un secreto si no se concede un pequeño margen de disimulo, que es, por así decirlo, la cola o el rastro del secreto.»

— Francis Bacon, Ensayos, «De la simulación y el disimulo» (1625)

Uno de los ingenieros estrella del proyecto de coche autónomo de Google —el que se convertiría en Waymo— se descarga miles de archivos confidenciales en su portátil antes de marcharse. Funda una empresa de camiones autónomos, Otto. Uber la compra a los pocos meses. Y Waymo demanda a Uber: años y fortunas de investigación conducen ahora por el carril de al lado. En 2018, Uber cierra el asunto con un acuerdo que la prensa valoró en unos 245 millones de dólares en acciones [1]. En marzo de 2020, Anthony Levandowski se declara culpable de robo de secretos comerciales; en agosto, el juez William Alsup lo condena a dieciocho meses de prisión con una frase para los anales: «el crimen de secretos comerciales más grande que he visto jamás». Y el epílogo de novela: el 20 de enero de 2021, el último día de su mandato, el presidente Trump lo indultó [1].

Si esto le pasó a Google —con los mejores abogados y sistemas del mundo—, qué no pasa cada semana a escala pequeña: el comercial que se va con la lista de clientes, el socio que sale con el procedimiento de fábrica, el proveedor que «reinventa» el diseño que le enseñaste bajo acuerdo de confidencialidad. Y la víctima descubre entonces el nudo del secreto empresarial: para defenderlo ante un juez tiene que probar qué tenía, desde cuándo y que lo protegía —sin revelarlo una segunda vez por el camino.

Este capítulo trata el único activo que se defiende ocultándolo —y que por eso tiene el peor problema probatorio del derecho. Es el espejo del capítulo 41: la patente protege publicando; el secreto, ocultando. La autoría creativa está en el capítulo 40; los registros que un atacante no puede reescribir, en el capítulo 57; y el alertador que revela ilícitos —que no es un ladrón de secretos— en el capítulo 62. Pregunta clave: ¿cómo pruebas que tienes algo que no puedes enseñar? Respuesta: con el depósito sellado por huella de **t2p** —la SHA-512 calculada en el dispositivo, el sello de tiempo RFC 3161/eIDAS, el anclaje a la blockchain pública [3]—, donde solo la huella viaja y el contenido no sale nunca de casa: posesión con fecha cierta, perímetro exacto, y ninguna revelación. Y con la simetría que hace el capítulo honesto: la misma herramienta defiende al exempleado o al competidor acusado injustamente, que puede probar su desarrollo independiente previo.

Tres requisitos y un nudo

El marco es la Ley 1/2019, de secretos empresariales —transposición de la directiva europea— y es exigente [2]: para que una información sea secreto protegible ha de cumplir tres requisitos. Ha de ser secreta —no generalmente conocida ni fácilmente accesible en los círculos que trabajan con este tipo de información. Ha de tener valor empresarial precisamente por ser secreta. Y ha de haber sido objeto de medidas razonables de su titular para mantenerla en secreto. Fórmulas químicas, procesos productivos, bases de datos, estrategias, listas de clientes, algoritmos, know-how: todo cabe —si cumples los tres requisitos.

El nudo probatorio vive en el tercero. Sin medidas razonables demostrables, no hay secreto protegible: la información puede ser valiosísima y haberse filtrado igualmente, y el juez te dirá que no la protegías lo suficiente. La documentación de las medidas se convierte, pues, en parte del propio secreto —y su ausencia, en la trampa clásica de la empresa descuidada.

Los otros dos hilos del nudo: para litigar tienes que delimitar qué era exactamente el secreto —y cada palabra de más que revelas en el proceso es secreto que muere, de modo que la redacción ha de ser quirúrgica; y tienes que probar la prioridad temporal —que tú lo tenías antes—, como en las patentes del capítulo 41, pero sin ningún registro público donde apuntarla: aquí la fecha se la ha de procurar el propio titular.

Y el equilibrio que la propia ley impone —y que este libro suscribe [2]: la protección no se extiende a la experiencia y las competencias que el trabajador adquiere honestamente durante su carrera, ni puede servir para restringir su movilidad. La frontera entre «nuestro know-how» y «su oficio» es la línea de combate de casi todos estos litigios —y sin hechos fechados, cada bando dibuja en ella lo que quiere.

La prueba de existencia aplicada

Aquí la prueba de existencia juega su partido perfecto, porque es la única que prueba sin enseñar [3].

1. El depósito sellado

La empresa certifica con t2p los archivos que son su secreto —la fórmula, el código, la base de clientes, el procedimiento—: la huella SHA-512 se calcula en el dispositivo y solo la huella se ancla; el contenido no sale nunca de casa [3]. El resultado es triple: posesión con fecha cierta —lo tenías el día X—; perímetro exacto —byte a byte, qué es y qué no es tu secreto—; y una medida razonable en sí misma: un protocolo de custodia fechado es exactamente lo que el tercer requisito pide [2]. El día del litigio, la revelación es selectiva y ante el juez —las medidas de confidencialidad procesales de la ley ayudan [2]— y el certificado con código QR acredita que aquello es lo que existía aquel día.

2. La cronología del know-how

Cada versión del desarrollo —el cuaderno de laboratorio, las iteraciones del código, los ensayos— sellada en el momento [3]. La cadena de fechas ciertas dibuja el camino propio: cuando el competidor aparezca con «el mismo» producto, tu cronología prueba anterioridad y desarrollo independiente. Como en el capítulo 41, la precedencia es el corazón de la disputa —pero aquí sin publicar nada.

3. La salida del empleado

El momento de riesgo máximo, documentado con neutralidad: el acta de devolución de equipos y credenciales, escaneada y sellada —hasta 50 páginas en un PDF [3]—; el inventario de accesos que tenía, anclado; el recordatorio del NDA, entregado con fecha cierta. Sin dramas ni sospechas: un trámite de diez minutos que protege a las dos partes —la empresa, si después aparecen sus archivos donde no corresponde; y el extrabajador, que tiene acta de lo que devolvió y de cuándo.

4. El NDA con perímetro — y la defensa del inocente

El NDA firmado con la firma fuerte de t2p —vídeo-selfie con retos de vida y verificación biométrica [3]— y, como anexo, el perímetro del secreto definido por huella: el receptor sabe exactamente qué archivos no puede usar, sin que el contenido viaje. Y la simetría que hace este capítulo honesto: el exempleado que monta su empresa, o el competidor que desarrolló su solución por su cuenta, tiene en su propia cadena de sellos la mejor defensa contra la acusación infundada [2][3] —su conocimiento previo, fechado antes de cualquier contacto.

Los límites, dichos claramente: el sello no hace secreta una información que ya es pública, ni decide si aquello era secreto protegible o experiencia profesional —eso lo dirá el juez con la ley en la mano [2]. No sustituye la seguridad real —controles de acceso, cifrado, prevención de fugas—: acredita lo que tenías, no impide que te lo roben; para los registros del ataque, capítulo 57. Y nunca puede servir para sellarlo todo y reclamarlo todo: el perímetro inflado se vuelve en contra en el proceso.

La promesa y el peligro

La promesa: litigios de secretos que se resuelven por fechas ciertas y perímetros exactos en lugar de por testimonios y sospechas [1][2][3]; el tercer requisito —las medidas razonables— cumplido por diseño y demostrable con un certificado; pymes que protegen su know-how sin pagar lo que cuesta una guerra procesal; y trabajadores que cambian de trabajo con su bagaje documentado y la conciencia tranquila.

Los peligros, mirados de frente.

El primero es **la caza del exempleado**. El mismo expediente que protege el secreto puede industrializar la amenaza contra quien se va: cartas intimidatorias con anexos sellados para congelar la competencia. El contrapeso es triple: el equilibrio expreso de la ley —la experiencia honesta y la movilidad no se tocan [2] —, la simetría de la prueba —el desarrollo independiente del demandado también se fecha [3]— y los jueces mercantiles castigando el abuso procesal.

El segundo es **el perímetro inflado**. Sellarlo todo y decir que todo es secreto no prueba medidas razonables: prueba desorden. El secreto protegible es el que se delimita, se custodia y se trata como tal —el sello documenta la disciplina, no la sustituye.

El tercero es **el secreto contra el interés público**. Ningún depósito sellado convierte en secreto aquello que la ley obliga a revelar, ni puede usarse contra el alertador que denuncia un ilícito —esta frontera es del capítulo 62, y es sagrada.

Y el cuarto es **el tecnosolucionismo de la caja fuerte**. La huella no evita la filtración: la detecta y la fecha. Quien confunda el depósito con la seguridad acabará con un secreto perfectamente documentado… y perfectamente robado. Cifrado, accesos mínimos y cultura interna siguen siendo la primera línea.

Es hora de actuar

Que lo que no se puede enseñar se pueda probar.

Para empresas y fundadores: inventariad vuestros secretos, delimitadlos y depositad sus huellas con fecha cierta [2][3]; el día que lo necesitéis, «medidas razonables» será un certificado, no un alegato.

Para los departamentos legales y asesores de PI: NDA con perímetro por huella y actas de salida ancladas como práctica estándar [3]; y recordad al cliente el equilibrio de la ley: el secreto se defiende, el exempleado no se persigue [2].

Para los trabajadores y emprendedores que se van: sellad vuestro bagaje previo y vuestro desarrollo independiente [3] —vuestra libertad profesional vale una cadena de fechas.

Para los jueces mercantiles: el depósito por huella con revelación selectiva resuelve la paradoja del proceso de secretos [2]; exigidlo —y castigad tanto el robo como la acusación estratégica.

Para los legisladores: la ley de 2019 puso los tres requisitos [2]; el paso siguiente es reconocer expresamente el depósito de huella con fecha cierta como medida razonable y como prueba cualificada de posesión.

Que el próximo Levandowski [1] encuentre huellas donde esperaba niebla —y que el próximo inocente tenga fechas donde esperaba sospechas. Por el conocimiento que vale precisamente porque no se ve, **time2act**.

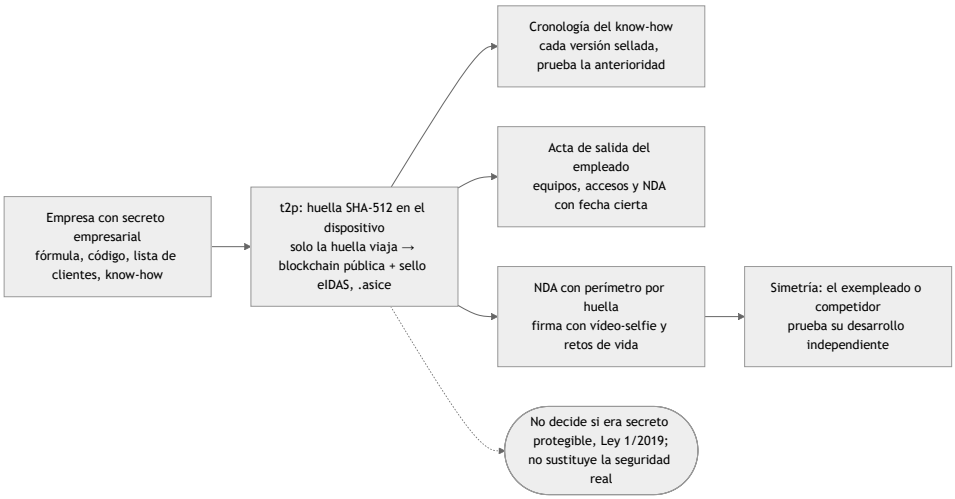


Figura 42.1 — El secreto empresarial con prueba de existencia (t2p: huella SHA-512 en el dispositivo —el contenido no sale nunca—, RFC 3161/eIDAS, blockchain pública, .asice): el depósito sellado (posesión + perímetro + medida razonable del tercer requisito de la Ley 1/2019), la cronología del know-how versión a versión, el acta de salida del empleado y el NDA con perímetro por huella y firma con vídeo-selfie. Simetría: la cadena de fechas del acusado inocente prueba el desarrollo independiente. Espejo del capítulo 41: la patente protege publicando; el secreto, ocultando —y por eso solo la prueba que no revela lo puede defender. Fuentes: caso Waymo/Uber/Levandowski; Ley 1/2019.

[1] CNBC — *Trump pardons Anthony Levandowski, the engineer who stole self-driving car secrets from Google* (miles de archivos descargados antes de marcharse; Otto comprada por Uber; acuerdo Waymo-Uber de 2018 valorado por la prensa en ~245 M$ en acciones; culpabilidad en marzo de 2020; 18 meses de prisión —juez William Alsup: «the biggest trade secret crime I have ever seen»; indulto total el 20-1-2021, último día de mandato); TechCrunch — *Former Google engineer Anthony Levandowski among list of last-minute Trump pardons*; Wikipedia — *Anthony Levandowski* (acuerdo global de 2022: 25-30 M$). https://www.cnbc.com/2021/01/20/anthony-levandowski-pardoned-after-stealing-trade-secrets-from-google.html · https://techcrunch.com/2021/01/19/former-google-engineer-anthony-levandowski-among-list-of-last-minute-trump-pardons/ · https://en.wikipedia.org/wiki/Anthony_Levandowski ↩

[2] BOE — *Ley 1/2019, de 20 de febrero, de Secretos Empresariales* (transposición de la Directiva (UE) 2016/943; tres requisitos: secreto + valor empresarial + medidas razonables; alcance: fórmulas, procesos, bases de datos, listas de clientes, algoritmos, know-how; equilibrio: no cubre la experiencia y competencias adquiridas honestamente por el trabajador ni puede restringir su movilidad; medidas de confidencialidad procesales); Garrigues — *Aprobada la ley que protege los secretos empresariales*. https://www.boe.es/buscar/act.php?id=BOE-A-2019-2364 · https://www.garrigues.com/en_GB/new/law-will-protect-trade-secrets-has-been-approved ↩

[3] t2p — manual de producto (certificar cualquier archivo —solo la huella viaja, el contenido no sale nunca del dispositivo; escáner de documentos hasta 50 páginas; firma con vídeo-selfie, retos de vida y biometría; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice con revelación selectiva verificable sin conexión). Véanse los capítulos 13 y 15; el prior art y la patente, en el capítulo 41; los registros de un ataque, en el capítulo 57; los alertadores, en el capítulo 62. ↩

Govtech: contratación pública y registros a prueba de manipulación

«Pero ¿quién vigilará a los propios vigilantes?»

— Juvenal, Sátiras, VI, 347-348 (c. 100 d. C.)

En junio de 2020, una alianza insólita —el Foro Económico Mundial, el Banco Interamericano de Desarrollo y la Procuraduría General de Colombia— anunció un experimento que parecía salir de una metáfora. Querían poner en una cadena de bloques la fase de licitación del **Programa de Alimentación Escolar**, que compra las comidas para los niños más vulnerables del país y donde, históricamente, se había filtrado la corrupción. La idea era sencilla y conmovedora: hacer que nadie pudiera robar, en silencio y a posteriori, el dinero de la comida de los niños. El prototipo funcionó sobre la red pública Ethereum y registró automáticamente cada modificación o intervención. Pero sus impulsores fueron honestos con los límites, y su conclusión vale para todo este capítulo: «la tecnología no puede resolver del todo aquello que está en el corazón del comportamiento humano» [8].

Aquel experimento toca el nervio de este último frente. La contratación pública es, como dice la propia OCDE, la actividad gubernamental más vulnerable a la corrupción, por el volumen de dinero y la discrecionalidad que mueve. Y la confianza que los ciudadanos depositan en ella —que sus impuestos compren escuelas, puentes y comidas reales— descansa, una vez más, sobre pruebas que se pueden manipular. Este capítulo trata de cómo hacer que aquella confianza se pueda *demostrar*, y de hacerlo con la humildad que el experimento colombiano ya aprendió.

El gasto más vulnerable

La magnitud de lo que está en juego cuesta de imaginar. La contratación pública mundial supera los **13 billones de dólares al año**, cerca del 13-15 % del PIB global; es, de lejos, la mayor palanca económica en manos de los estados [1]. Y una parte estremecedora se evapora. El **Banco Mundial** calcula que los gobiernos malgastan alrededor de **una cuarta parte** de este gasto por ineficiencia y corrupción, y que una contratación sólida podría liberar un **millón de millones —un billón— de dólares al año**, lo que llama «el billón oculto» [2]. El propio Banco Mundial sigue el progreso del gobierno digital en todo el mundo con su GovTech Maturity Index, que cubre 198 economías [10]. En el sector de la construcción el agujero es aún más brutal: la iniciativa de transparencia de la infraestructura **CoST** estima que **entre el 10 % y el 30 % del valor de una obra pública** se pierde por mala gestión y corrupción [3].

Buena parte de esta pérdida tiene un mecanismo con nombre propio. La OCDE, en sus directrices contra la **licitación colusoria** —el *bid rigging*—, advierte de que cuando las empresas se ponen de acuerdo para amañar un concurso, eliminar aquella colusión podría abaratar los precios de los contratos un **20 % o más** [4]. Las formas son conocidas: ofertas de cobertura, supresión o rotación de ofertas, reparto del mercado, a menudo con la complicidad de un infiltrado dentro del organismo contratante. El resultado global de esta erosión lo mide cada año **Transparency International** con su Índice de Percepción de la Corrupción: el de 2025 marcó una media mundial de apenas **42 sobre 100, un mínimo histórico**, con más de dos tercios de los países suspendidos [5].

Transparencia no es lo mismo que prueba

Ante esto, los estados han ensayado dos estrategias que conviene no confundir, porque ilustran la diferencia exacta entre *ver* y *demostrar*.

La primera es la **transparencia**: abrir los datos para que todos los puedan mirar. El mejor ejemplo es **ProZorro**, el sistema de contratación abierta que Ucrania construyó en 2016 con el lema «todos lo ven todo». Según la organización Open Contracting Partnership, ha ahorrado al erario unos **6.000 millones de dólares**, y la comunidad ciudadana de vigilancia Dozorro llegó a detectar irregularidades en más de 33.000 licitaciones [6]. Es una herramienta poderosísima —un país en guerra demostró que el arma anticorrupción era abrir los datos, no esconderlos—, pero tiene un límite: la transparencia deja ver lo que hay publicado, pero no garantiza por sí sola que aquel registro no se haya alterado ni fechado con trampa.

La segunda estrategia ataca precisamente este límite: la **integridad a prueba de manipulación**. El pionero es Estonia, que después de los ciberataques estatales de 2007 se convirtió, en 2012, en el primer

país del mundo en poner la cadena de bloques en producción para blindar sus registros, con la tecnología **KSI** de la empresa Guardtime. El diseño es elegante y es, ya lo veremos, el mismo de t2p: **a la cadena solo se envía la huella del documento, nunca el dato original**, que no sale del servidor del Estado [7]. Así, Estonia puede demostrar matemáticamente que ningún funcionario ha reescrito a posteriori un historial médico, un asiento de propiedad o un acta judicial. Transparencia es dejar ver; prueba de integridad es poder demostrar que lo que se ve no se ha tocado.

La prueba de existencia aplicada al dinero público

Es aquí donde **t2p** garantiza la integridad de Estonia sin que ningún ayuntamiento o agencia tenga que montar una cadena de bloques nacional, con tres puntos de anclaje.

El primero, el sello de las ofertas y los pliegos, contra la retrodatación. Al presentar una oferta o publicar un pliego, se calcula la **huella SHA-512** del documento en el dispositivo, se ancla a la **blockchain pública** y se le añade un **sello de tiempo RFC 3161** cualificado conforme a eIDAS. Esto fija criptográficamente que *aquel documento exacto existía en aquella hora*, de modo que nadie pueda antedatar una oferta, sustituir un pliego después de la apertura ni alterar un sobre sin que la huella y la fecha cambien. Además, el **artículo 41 del reglamento eIDAS** otorga al sello de tiempo cualificado una presunción legal de exactitud de la fecha y de la integridad de los datos [9], cosa que la transparencia de ProZorro no garantiza por sí sola.

El segundo, **el sello de los registros públicos**, al estilo de Estonia pero como servicio: cada asiento o versión de un expediente —una adjudicación, una modificación contractual, un acta— se resume en una huella y se ancla; cualquier reescritura posterior queda matemáticamente detectable por un auditor externo.

Y el tercero, el más distintivo, donde el dinero público de verdad aterriza: **el sello de la obra entregada**. Un funcionario o un ciudadano captura la **fotografía de la infraestructura entregada** —el puente, el aula, la comida escolar— con **GPS forense, fecha y prueba de vida** del operador, todo empaquetado en un **contenedor .asice verificable sin conexión**. Así, un auditor puede comprobar independientemente que *el dinero compró algo real, en aquel lugar, en aquella fecha*, atacando directamente la pérdida observada en la obra pública («como hemos visto»). Es el paso que cierra el círculo: de la oferta sellada a la verificación ciudadana de lo que se construyó.

Hay que decir el límite con la misma honestidad que tuvo el experimento colombiano, fieles a la dualidad de «la promesa y el peligro». La prueba de existencia demuestra que **un registro existió íntegro en un momento, lugar y por una persona determinados**; **no** demuestra la verdad física de lo que hay detrás ni la honestidad de la decisión. Si la oferta sellada ya estaba amañada por colusión, si la foto con GPS muestra una obra mala presentada como buena, o si el funcionario que da fe de ella es cómplice, t2p sellará fielmente un dato corrupto. Lo que hace —y no es poco— es **encarecer y hacer detectable la manipulación a posteriori y la retrodatación**, creando una cadena de custodia auditable. No sustituye la investigación de la competencia, ni el control de calidad de la obra, ni el juicio sobre el fondo de la adjudicación. «La tecnología no puede resolver del todo el comportamiento humano», como reconocieron en Colombia; pero puede cerrar muchas de las puertas por donde se escapa el dinero.

La promesa y el peligro

La promesa se mide en aquel «billón oculto». Una contratación donde las ofertas, los registros y las obras estén sellados y sean verificables por cualquier ciudadano haría mucho más difícil la retrodatación, la sustitución de expedientes y la obra fantasma, y devolvería a la ciudadanía una herramienta para comprobar que sus impuestos compran lo que dicen que compran. Como hemos visto, este sector mueve 13 billones de dólares; recuperar esta confianza es, literalmente, recuperar recursos para hospitales y escuelas.

El peligro pide el matiz de siempre. Primero, el sello no limpia una decisión corrupta ni una obra mala; confundir la integridad del registro con la honestidad del fondo sería una peligrosa falsa seguridad. Segundo, la vigilancia: una infraestructura que selle cada acto de la administración ha de servir para controlar el poder, no a los ciudadanos, y exige un diseño garantista. Tercero, la concentración: quien opere la capa de verificación no puede convertirse en un nuevo portero único de lo que es público. La prueba de existencia es una herramienta al servicio de la rendición de cuentas, no un sustituto de la política honesta ni del control democrático.

Es hora de actuar

Para los **organismos de contratación**: sellar ofertas, pliegos y adjudicaciones en origen, para que la integridad temporal del proceso sea demostrable y la retrodatación sea imposible. Para los **órganos de control y auditoría**: exigir el sello de la obra entregada —foto, GPS, fecha— como base de la fiscalización, para comprobar que el dinero ha adquirido algo real. Para la **ciudadanía y el periodismo**: reclamar poder verificar por su cuenta tanto los datos abiertos como su integridad. Para los **gobiernos y reguladores**: combinar la transparencia de datos al estilo ProZorro con la prueba de integridad al estilo estonio, y reconocer el valor probatorio del sello que el reglamento eIDAS ya ampara.

En Colombia intentaron impedir que alguien robara, en silencio, la comida de los niños. Descubrieron que la tecnología no lo cura todo —y tenían razón—, pero también que hacer cada movimiento del dinero público verificable por cualquiera es una de las murallas más efectivas contra la corrupción. Que el ciudadano pueda demostrar que sus impuestos compraron algo real es, en este último frente y como en todos los demás, **time2act**.

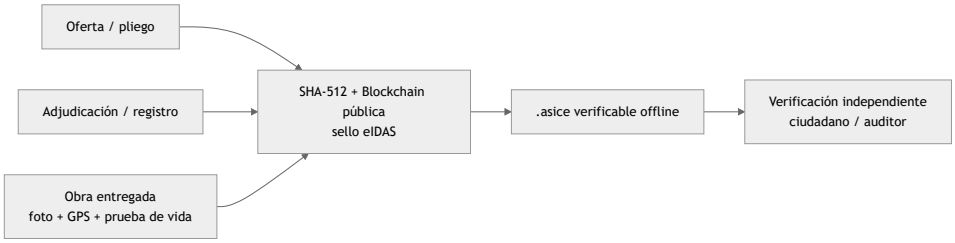


Figura 43.1 — Cada paso del dinero público —la oferta o el pliego, la adjudicación registrada y la obra entregada (foto con GPS y fecha)— se resume en una huella SHA-512, se ancla a la blockchain pública y recibe un sello de tiempo RFC 3161/eIDAS, con prueba de vida en la obra; todo se empaqueta en un contenedor .asice que un ciudadano o un auditor puede verificar de manera independiente y sin conexión. Contexto: contratación pública mundial ≈13 billones de dólares al año; entre el 10 % y el 30 % de la obra pública se pierde por corrupción y mala gestión. La prueba de existencia demuestra integridad, momento, lugar y persona —no la honestidad de la decisión ni la calidad de la obra. Fuentes: Banco Mundial; CoST; OCDE; eIDAS art. 41.

[1] Spend Network / Banco Mundial — *The $13 trillion global value of public procurement* (~13-15 % del PIB; menos del 3 % en datos abiertos). https://www.spendnetwork.com/13-trillion-the-global-value-of-public-procurement/ ↩

[2] Banco Mundial — *The hidden $1 trillion: halting waste in public procurement* (~una cuarta parte malgastada; ~1 billón $/año). https://blogs.worldbank.org/en/voices/hidden-1-trillion-halting-waste-public-procurement ↩

[3] CoST – Infrastructure Transparency Initiative — *This is why construction is so corrupt* (10-30 % del valor de la obra pública; ~6 billones $/año hacia 2030). https://infrastructuretransparency.org/2016/02/05/this-is-why-construction-is-so-corrupt/ ↩

[4] OCDE — *Guidelines for Fighting Bid Rigging in Public Procurement (2025 Update)* (la colusión puede encarecer los contratos un 20 % o más). https://www.oecd.org/en/publications/2025/09/oecd-guidelines-for-fighting-bid-rigging-in-public-procurement-2025-update_127880ea.html ↩

[5] Transparency International — *Corruption Perceptions Index 2025* (media mundial 42/100, mínimo histórico; Dinamarca 89, octavo año a la cabeza). https://www.transparency.org/en/news/cpi-2025-findings-insights-corruption ↩

[6] Open Contracting Partnership — *The impact of ProZorro in Ukraine* (~6.000 M$ ahorrados; Dozorro, 33.000+ licitaciones). https://www.open-contracting.org/impact-stories/impact-ukraine/ ↩

[7] e-Estonia — *KSI Blockchain* (primer Estado con blockchain en producción, 2012; Guardtime; solo se ancla la huella). https://e-estonia.com/solutions/cyber-security/ksi-blockchain/ ↩

[8] World Economic Forum — *Exploring Blockchain Technology for Government Transparency to Reduce Corruption* (Colombia, Programa de Alimentación Escolar, BID, 2020). https://www.weforum.org/publications/exploring-blockchain-technology-for-government-transparency-to-reduce-corruption/ ↩

[9] EUR-Lex — *Reglamento eIDAS (UE 910/2014), artículo 41* (presunción legal de exactitud del sello de tiempo cualificado). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG ↩

[10] Banco Mundial — *GovTech Maturity Index* (198 economías; cuatro áreas de madurez del gobierno digital). https://www.worldbank.org/en/programs/govtech/gtmi ↩

El ciudadano ante la Administración: el reloj del silencio

«El concepto de "secreto de oficio" es la invención específica de la burocracia, y nada es defendido por la burocracia tan fanáticamente como esta actitud.»

— Max Weber, Economía y sociedad (póst., 1922)

Ante una pantalla que repite la misma frase implacable a cualquier hora del día o de la noche —«No hay citas disponibles»—, alguien actualiza por enésima vez la página de cita previa de extranjería. Mañana, igual. La semana que viene, igual. Lo que aquella persona no ve es que las citas existen: las capturan bots en el mismo instante de publicarse y se revenden por WhatsApp entre 50 y 350 euros, con casos de hasta 600 —un mercado negro entero levantado sobre un trámite gratuito. La abogacía, las ONG y el Defensor del Pueblo lo han denunciado: la institución ha instado al Ministerio del Interior a corregir las «demoras excesivas» y recibe quejas constantes —cerca de 3.000 en un año, con más de 163.000 solicitudes de asilo en 2023 desbordando el sistema [2]. El Gobierno ha anunciado que perseguirá a las mafias de la reventa [2]. Pero el problema de fondo es más profundo que las mafias: cuando el acceso a la Administración es una lotería opaca, el ciudadano no puede ni siquiera demostrar que lo ha intentado.

Este capítulo trata la relación probatoria del ciudadano con el procedimiento administrativo: qué presentaste, cuándo te lo notificaron, cuándo vencía el plazo. La contratación pública —la Administración por dentro— está en el capítulo 43; la identidad digital, en el capítulo 47. Pregunta clave: ¿cómo corre el ciudadano una carrera de relojes si solo una parte controla el cronómetro? Respuesta: con fecha cierta propia en cada paso —la presentación, la notificación, el vencimiento, la cita— mediante **t2p**: la huella SHA-512 en el dispositivo, el anclaje de la huella en la blockchain pública y el sello de tiempo RFC 3161/eIDAS complementario, dentro de un contenedor .asice [3]. Y con neutralidad: el mismo rastro que protege al ciudadano acredita la diligencia de la Administración que hace bien su trabajo y del funcionario honesto.

La arquitectura de los plazos

El procedimiento administrativo español —la Ley 39/2015, de 1 de octubre— es una máquina de relojes. Con carácter general, la Administración tiene tres meses para resolver y notificar (artículo 21.2), salvo que la norma del procedimiento establezca un plazo diferente. Si el plazo vence sin resolución, aparece el silencio administrativo: la ficción jurídica que convierte la nada en un «sí» o en un «no» según el procedimiento, con efectos desde el vencimiento; y su existencia se puede acreditar con un certificado que el órgano competente debe expedir de oficio en quince días —y, si no lo hace, a petición del interesado [1].

Las notificaciones electrónicas tienen su propio reloj, y es implacable: desde la puesta a disposición en el buzón electrónico, el interesado tiene diez días naturales para acceder a ella; si no lo hace, la notificación se entiende rechazada y el procedimiento continúa como si la hubiera recibido [1]. Diez días de vacaciones mal elegidas pueden costar un recurso no presentado, una sanción firme, una subvención perdida.

El diagnóstico probatorio: todo este edificio pende de fechas —cuándo presentaste, cuándo pusieron a disposición, cuándo vence— y las fechas las custodia mayoritariamente una de las partes. El ciudadano tiene resguardos que acreditan que presentó algo, pero no siempre qué exactamente; tiene un buzón cuyo registro de acceso es del sistema, no suyo; y tiene un vencimiento de silencio que debe calcular y acreditar él mismo. En una relación ya bastante desequilibrada en poder y en medios, la asimetría probatoria es la tercera carga.

La cita que nunca está

El caso de extranjería merece mirada propia, porque es el paradigma del punto de acceso opaco. El cuadro verificado: un sistema crónicamente colapsado; bots que acaparan las citas en el momento de publicarse; reventa por WhatsApp entre 50 y 350 euros, hasta 600 [2]; denuncias de la abogacía, las ONG y el Defensor del Pueblo, con miles de quejas anuales; más de 163.000 solicitudes de asilo en 2023, por encima de la capacidad del sistema; y el anuncio gubernamental de perseguir a las mafias [2].

Pero el análisis ha de ir más allá del escándalo: el mercado negro es el síntoma; la enfermedad es la opacidad del punto de acceso. Nadie —ni el ciudadano, ni el Defensor, ni a menudo la propia

Administración— puede auditar cuántas citas se publicaron, cuándo, y quién las capturó en cuánto tiempo. Sin registro verificable de la disponibilidad, todo son sospechas: el ciudadano no puede demostrar que lo intentó cien veces; la Administración no puede demostrar que publicó las citas que dice; y el bot prospera exactamente en esta oscuridad.

La respuesta estructural es la disponibilidad auditable. Si cada publicación de citas y cada asignación quedan ancladas —cuántas, cuándo, asignadas en cuánto tiempo [3]—, el acaparamiento automatizado se vuelve visible a simple vista: ningún humano coge doscientas citas en tres segundos. El ciudadano puede acreditar sus intentos fechados, la persecución de las mafias [2] trabaja sobre datos y no sobre anécdotas, y la reforma se puede exigir con cifras. La transparencia del punto de acceso no resuelve el colapso de fondo —hacen falta medios [2]—, pero convierte un agujero negro en un problema medible.

La prueba de existencia aplicada

Una solicitud cualquiera, un registro electrónico cualquiera —y, por primera vez, un expediente del que el ciudadano tiene su propia cronología completa.

1. La presentación con contenido sellado

El ciudadano que presenta una solicitud, un recurso o una alegación sella en su dispositivo el documento completo y el justificante de presentación, juntos [3]: la huella SHA-512 del qué y la fecha cierta del cuándo. Si alguna vez el expediente «pierde» un anexo, si se discute qué versión se presentó, si el resguardo oficial solo acredita un asiento genérico —la copia sellada cierra la discusión. Y la simetría funciona: la Administración que ancla sus propios registros tiene la misma protección ante el ciudadano que alega haber presentado lo que nunca presentó. Nadie puede negar la presentación; nadie puede inventarla.

2. El reloj del silencio

La presentación sellada activa el cronómetro con fecha cierta: tres meses —o el plazo que corresponda [1] — contados desde un hecho indiscutible. Al vencimiento, el ciudadano tiene la cronología completa para exigir el certificado de silencio [1] o para ir al contencioso: la solicitud existía, decía esto, se presentó aquel día, y el silencio venció este otro. El silencio administrativo deja de ser una niebla procesal para convertirse en un hecho fechado —y la Administración diligente, que resuelve dentro de plazo, tiene en sus propios registros anclados la prueba de su puntualidad.

3. La notificación con rastro neutral

El reloj más peligroso —los diez días de la notificación electrónica [1]— merece un rastro que no dependa de ninguna de las dos partes: la puesta a disposición anclada (cuándo, exactamente, apareció en el buzón) y el acceso anclado (cuándo, exactamente, se entró en él) [3]. Contra el «rechazada por no acceder» que llega en el peor momento, el ciudadano puede acreditar qué había —o no había— en su buzón y cuándo; contra el «nunca me llegó» de mala fe, la Administración puede acreditar la puesta a disposición al segundo. La indefensión y la picaresca mueren de la misma medicina.

4. La cita auditable

El registro anclado de la disponibilidad de citas [2][3]: cada lote publicado, cada asignación, con hora exacta. El ciudadano que lleva semanas intentándolo puede acreditar sus intentos fechados; el análisis del registro hace visible el acaparamiento automatizado —las capturas instantáneas y masivas que ninguna mano humana puede hacer—; y el mercado negro pierde su activo principal: la opacidad. Para la Administración, el mismo registro es la defensa: si publica lo que dice que publica, los datos la avalan.

Los límites, dichos con claridad: el sello no resuelve expedientes ni pone más funcionarios en la ventanilla —el colapso de extranjería es un problema de recursos y de política [2] que ninguna huella arregla; no sustituye los registros oficiales ni la fe pública —los complementa con un rastro verificable por ambas partes; y la fecha cierta no interpreta el derecho: acredita hechos para que abogados, jueces y el propio procedimiento trabajen sobre seguro.

La promesa y el peligro

La promesa: un ciudadano que corre la carrera de relojes con cronómetro propio [1][3]; puntos de acceso sin agujeros negros, donde la cita que hoy se revende a 350 euros [2] vuelve a ser un trámite gratuito y auditable; y una Administración que puede demostrar su diligencia con el mismo rastro que la obliga. Menos indefensión, menos picaresca, menos contenciosos sobre hechos —y más energía para el fondo de los expedientes.

Los peligros, con la misma claridad.

El primero es **la burocracia del sello**. Si acreditar cada paso se convierte en una carga más —un trámite sobre el trámite—, habremos empeorado la relación que queríamos sanar. El sellado ha de ser automático e invisible: el registro que ancla solo, la aplicación que sella al presentar —nunca un requisito añadido que expulse a quien menos medios tiene, porque la brecha digital ya expulsa a bastante gente.

El segundo es **la desconfianza institucionalizada**. Este capítulo no es una enmienda a los funcionarios. Si el rastro neutral se presenta como arma contra la Administración, se vivirá como agresión y morirá en un cajón; su virtud es la simetría —protege al ciudadano del expediente perdido y al funcionario honesto de la acusación injusta. Rastro de hechos, nunca vigilancia de los empleados públicos.

El tercero es **el espejismo de la ventanilla perfecta**. Ningún anclaje crea citas donde no las hay [2] ni acorta plazos que la ley permite agotar. La transparencia hace el problema medible y exigible; la solución sigue siendo política: medios, plantillas, simplificación.

Y el cuarto es **la vigilancia del ciudadano**. La cronología administrativa de una persona —qué solicita, qué recurre, cuándo— dibuja su vida. Los rastros han de ser de cada expediente y para sus partes, nunca un perfil central consultable; solo huellas en la cadena, contenido en los sistemas de cada uno, y acceso regulado por el procedimiento [3].

Es hora de actuar

La relación más desigual del derecho merece, al menos, un reloj compartido.

Para ti, ciudadano: sella lo que presentas —documento y justificante, juntos [3]; anota y ancla los vencimientos [1]; y si el sistema te dice que no hay citas, que tus intentos queden fechados [2].

Para abogados y gestores administrativos: incorporad la cronología sellada a cada expediente —la presentación, la notificación, el vencimiento del silencio [1][3]; es la diferencia entre alegar y acreditar.

Para las administraciones: anclad vuestros registros y notificaciones [3] —el rastro neutral es vuestra mejor defensa ante la picaresca y vuestra mejor credencial ante el ciudadano; y publicad la disponibilidad de citas de manera auditable [2].

Para el Defensor del Pueblo y los órganos de control: exigid registros anclados de disponibilidad y asignación de citas [2] —las 3.000 quejas anuales merecen datos, no respuestas tipo.

Para los legisladores: reconoced la presentación y la notificación selladas como prueba cualificada [1] [3], imponed la auditabilidad de los puntos de acceso masivos [2] y velad para que ningún rastro se convierta en perfil ciudadano centralizado.

Que la próxima persona que actualice la página de citas a medianoche sepa —y pueda demostrar— si la cita no estaba o si se la habían quitado; y que el reloj del procedimiento, por fin, marque la misma hora para todos. Por la ventanilla de cada día, **time2act**.

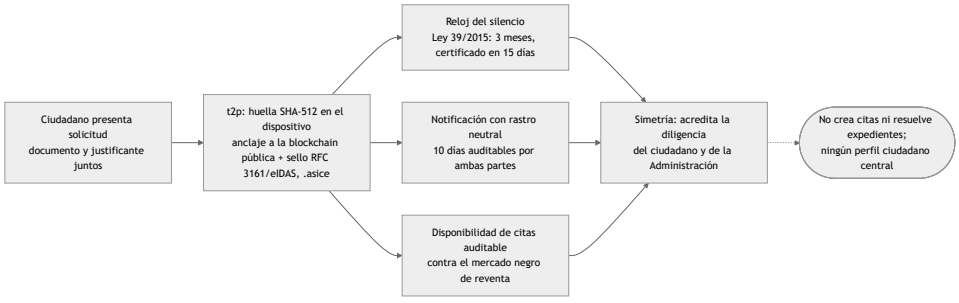


Figura 44.1 — La relación ciudadano-Administración con prueba de existencia (huella SHA-512 en el dispositivo, sello de tiempo RFC 3161/eIDAS, blockchain pública, .asice): la presentación con contenido sellado (qué y cuándo), el reloj del silencio administrativo con vencimientos fechados (Ley 39/2015: 3 meses; certificado en 15 días), la notificación con rastro neutral (los

10 días auditables por ambas partes) y la disponibilidad de citas auditable (contra el mercado negro de la cita previa). Simetría: el mismo rastro acredita la diligencia de la Administración. Límites: no crea citas ni resuelve expedientes; ningún perfil ciudadano central. Fuentes: Ley 39/2015; Defensor del Pueblo (citas de extranjería).

---

[1] BOE — *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas* (art. 21: plazo general de tres meses para resolver y notificar; silencio administrativo con efectos desde el vencimiento; certificado acreditativo del silencio expedido de oficio en 15 días; notificaciones electrónicas: 10 días naturales desde la puesta a disposición, transcurridos los cuales se entiende rechazada); Administrativando — *Silencio administrativo: qué es y cuáles son sus efectos*; Conceptos Jurídicos — *Silencio administrativo en España*. https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10565-consolidado.pdf · https://administrativando.es/silencio-administrativo/ · https://www.conceptosjuridicos.com/silencio-administrativo/ ↩

[2] Noticias Jurídicas — *El mercado negro de citas para extranjería: venta de citas para asilo internacional* (bots que acaparan citas; reventa; sistema desbordado); OKDiario — *El caos en la web de Extranjería impulsa a las mafias que cobran hasta 350 € por cita* (reventa por WhatsApp de 50 a 350 €, hasta 600 €); Parainmigrantes — *El problema de la cita previa llega al Defensor del Pueblo* (quejas constantes, ≈3.000 en un año; >163.000 solicitudes de asilo en 2023; «demoras excesivas»); Iberoeconomía — *España perseguirá a las mafias que revenden citas para trámites públicos*. https://noticias.juridicas.com/contenido-patrocinado/articulo/19314-el-mercado-negro-de-citas-para-extranjeria:-venta-de-citas-para-asilo-internacional/ · https://okdiario.com/espana/caos-web-extranjeria-impulsa-mafias-que-cobran-300-cita-cada-inmigrante-13835137 · https://www.parainmigrantes.info/el-problema-de-la-gestion-de-la-cita-previa-para-tramites-de-extranjeria-llega-al-defensor-del-pueblo/ · https://iberoeconomia.es/inmigracion/espana-perseguira-a-las-mafias-que-revende-citas-para-tramites-publicos/ ↩

[3] t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; contenido en los sistemas de cada parte, solo huellas en la cadena; rastro verificable por ambas partes). Véanse los capítulos 13 y 15; la contratación pública, en el capítulo 43. ↩

El azar verificable: sorteos que nadie puede cargar

«Babilonia no es otra cosa que un infinito juego de azares.»

— Jorge Luis Borges, «La lotería en Babilonia», Ficciones (1941)

Una sala municipal llena de gente que no suele coincidir: familias con carpetas, un notario con la suya, un bombo —o un programa informático— y una lista. Se reparten viviendas protegidas, y el azar decidirá quién tiene una y quién sigue esperando. Es uno de los rituales más antiguos y más delicados de la administración pública. En España, el azar decide cosas mayúsculas: la adjudicación de viviendas protegidas se hace ante notario, según el procedimiento de cada administración [2]; el orden de actuación de miles de opositores y la composición de sus tribunales salen de un sorteo público de letras con procedimientos reglados —incluso con el sistema «espejo» que invierte el orden del DNI para que el alfabeto no beneficie siempre a los mismos [1]. Y, sin embargo, la sospecha siempre encuentra rendija: en Los Llanos de Aridane (La Palma), el sorteo de cuarenta viviendas acabó impugnado, con el ayuntamiento pidiendo que se resolviera «con prontitud y máxima transparencia» [2]. No hace falta ningún fraude para que un sorteo pierda legitimidad: basta con la duda razonable de quien no ha tenido suerte.

Este capítulo trata el azar público: cómo se reparte por sorteo de manera que nadie pueda cargar los dados —ni sospecharlo. La contratación pública está en el capítulo 43; las urnas, en el capítulo 48. Pregunta clave: ¿puede un sorteo ser tan verificable como un recuento? Respuesta: sí, con dos piezas. La primera, el compromiso previo sellado con **t2p**: la lista de participantes y la regla de adjudicación, ancladas antes de que rueden los dados —huella SHA-512, sello de tiempo RFC 3161/eIDAS, blockchain pública [3]. La segunda, el azar público verificable: balizas como drand, que generan valores aleatorios que nadie puede predecir ni sesgar [4]. El resultado: un sorteo recomputable —cualquier vecino con un ordenador puede comprobar que el resultado es exactamente la regla aplicada a la lista. El notario no pierde su trabajo; gana el mejor instrumento de su historia.

El bombo y la sospecha

La lotería tradicional resolvió el problema de la confianza con física: bombos transparentes, bolas visibles, acto público, cámaras. Cualquiera puede ver girar el bombo, y esta exhibición material es toda la garantía —y durante décadas ha sido suficiente.

Pero el modelo no escala a los sorteos administrativos. Las listas ya no son decenas de bolas sino miles de nombres que cambian hasta el último día, gestionados en hojas de cálculo o en programas que solo el personal técnico puede inspeccionar; y el acto público a menudo se reduce a extraer una letra o una semilla —todo lo que pasa antes y después es invisible [1][2]. La transparencia cubre el momento de la extracción; la sospecha vive en todo lo que lo rodea.

Los dos puntos débiles de cualquier sorteo administrativo tienen nombre. El primero es **la lista**: ¿quién estaba, exactamente, cuando rodaron los dados? Un participante añadido tarde, un excluido indebidamente, un duplicado —ningún notario puede detectarlo si la lista es un archivo que nadie ha fijado públicamente antes. El segundo es **el azar**: ¿de dónde sale el número? Si lo genera un ordenador de la administración convocante, la confianza es ciega; si sale de un bombo, hay que estar en la sala para creerlo.

El caso de Los Llanos ilustra el coste de la duda —y la precisión importa: una impugnación, no un fraude demostrado [2]. Cuando un sorteo se discute, todo se detiene: las familias esperan, la administración se defiende, y la legitimidad del mecanismo entero queda tocada. El problema de fondo no es que los sorteos sean sucios; es que no pueden demostrar que son limpios. Y en un libro sobre pruebas, esta distinción lo es todo.

El azar que nadie puede cargar

La solución moderna tiene dos mitades, y el orden entre ellas es sagrado.

La primera mitad es **el compromiso previo**. Antes de que rueden los dados, se fija todo lo que no ha de poder cambiar: la lista completa de participantes con sus números, las bases y la regla exacta de

adjudicación —cómo se pasa del número aleatorio al orden de la lista. Todo esto se sella con t2p —huella SHA-512, fecha cierta, anclaje a la blockchain pública [3]— y la huella se publica. Consecuencia: nadie puede añadir, quitar ni reordenar candidatos a posteriori sin que la huella cante; y todos pueden guardarse la lista y comprobar que es la que era.

La segunda mitad es **el azar público verificable**. El número aleatorio no lo genera ni la administración ni ningún proveedor suyo, sino una baliza pública: drand, el faro de aleatoriedad de la League of Entropy —una coalición que incluye a Cloudflare, la EPFL, Kudelski Security, Protocol Labs y la Universidad de Chile, con miembros posteriores como la Fundación Ethereum—, que emite a intervalos fijos valores aleatorios imparciales, impredecibles y verificables por cualquiera, combinando la entropía de múltiples operadores independientes con criptografía de umbral: ni un actor ni dos confabulados pueden sesgar el resultado [4]. Sus aplicaciones declaradas incluyen, precisamente, loterías y elecciones [4].

Y la suma es **la recomputabilidad**. Se anuncia por adelantado qué ronda futura de la baliza se usará —nadie conoce todavía su valor; llega el valor; se aplica la regla comprometida a la lista comprometida; y el resultado lo puede rehacer cualquiera: con la lista publicada, la regla publicada y el valor público de drand, cada persona puede reproducir el sorteo entero en su ordenador y obtener exactamente el mismo resultado [3][4]. La confianza deja de ser un acto de fe en una sala: es una comprobación al alcance de todos.

La prueba de existencia aplicada

El mismo salón de actos, las mismas familias —y una hoja con tres huellas publicadas que cualquiera puede comprobar desde el móvil.

1. La vivienda protegida recomputable

El sorteo de viviendas [2] con el protocolo completo: la lista de solicitantes admitidos, sellada y publicada por huella —los datos personales no se exponen [3]; las bases y la regla de adjudicación, selladas; la ronda futura de drand, anunciada [4]; y, llegado el día, una adjudicación recomputable por cualquiera. En un caso como el de Los Llanos [2], la sospecha —en el sentido que fuera— se podría comprobar en cinco minutos, en una dirección o en la otra: o los números cuadran para todos, o no cuadran para nadie. El notario certifica el compromiso previo y el acta final: fe pública sobre hechos verificables.

2. Las oposiciones con dados públicos

La letra del orden de actuación y los sorteos de tribunales [1], extraídos de una ronda de drand anunciada por adelantado [4] en lugar de un bombo en una sala de Madrid: el mismo ritual, pero verificable desde cualquier punto del país por cada opositor. Los procedimientos correctores —el sistema «espejo» del DNI [1]— se publican como parte de la regla comprometida, y el conjunto se vuelve recomputable. Ningún opositor tendrá que preguntarse nunca más si la letra salió como dicen que salió: podrá rehacer la extracción él mismo.

3. La asignación sensible

La misma receta sirve para toda asignación aleatoria que reparta cosas valiosas o cargas: plazas escolares cuando hay que desempatar, turnos y destinos, muestras de inspección —qué empresas audita este año la administración: un sorteo recomputable impide tanto el favor como la persecución—, o el orden de una lista de espera. Regla fija, lista sellada, azar público [3][4]: allí donde la arbitrariedad puede vestirse de azar, la recomputabilidad la desnuda. Si alguien sale quinto en la muestra de auditoría, todos pueden verificar que aquel quinto es el resultado directo del cálculo —y no de una llamada.

4. El acta que sobrevive

Cada sorteo deja su acta anclada: la lista comprometida, la regla, el valor aleatorio usado, el resultado [3]. Años después —cuando llegue el recurso, la revisión o la sospecha retrospectiva—, el expediente entero se puede reverificar sin depender de la memoria de ningún funcionario ni de la continuidad de ningún sistema informático. El azar pasa; su prueba, no.

Y la versión doméstica del mismo problema, que cada Navidad llena juzgados de paz: el décimo compartido. La participación dicha de palabra —«vas con medio»— vale lo que valga la memoria cuando toca. La foto del décimo con la lista de participantes y las cantidades, sellada antes del sorteo [3], convierte

la costumbre más querida del país en un pacto con fecha cierta: diez segundos que ahorran la disputa que ningún premio merece.

Los límites, dichos con claridad: el sello y la baliza hacen el sorteo limpio, no la política justa —quién puede participar, cuántas viviendas se construyen o cuántas plazas se ofrecen son decisiones humanas que ninguna criptografía mejora; la recomputabilidad exige publicar regla y lista, y la protección de datos se ha de respetar con la publicación por huella y la seudonimización [3]; y el notario y el acto público siguen teniendo todo el sentido —la fe pública y el ritual comunitario son parte de la legitimidad, ahora con matemática debajo.

La promesa y el peligro

La promesa: sorteos públicos que cualquiera puede recomputar [3][4], impugnaciones que se resuelven en minutos y no en años [2], y un patrimonio de legitimidad para la administración que reparte. Cuando el azar es verificable, la mala suerte no deja resentimiento institucional —solo mala suerte.

Los peligros, con la misma claridad.

El primero es **el ritual vaciado**. Si el sorteo recomputable sustituye el acto público en lugar de reforzarlo, se pierde la dimensión comunitaria que legitima el reparto —la sala llena, el notario, el momento compartido. La tecnología ha de acompañar el ritual, no escamotearlo: el acto se hace, y además se puede comprobar desde casa.

El segundo es **la complejidad como nueva opacidad**. Para el ciudadano medio, «criptografía de umbral» puede ser tan impenetrable como una hoja de cálculo municipal. Si solo cuatro expertos pueden recomputar, habremos cambiado una fe por otra. Hacen falta verificadores públicos sencillos —la web donde cualquiera pega su número y lo comprueba— y pedagogía del mecanismo: la verificabilidad teórica no basta; hace falta la practicable.

El tercero es **la semilla capturada**. El azar público lo es si la baliza es realmente independiente y el compromiso es realmente previo. Anunciar la ronda después de conocer su valor, o usar una «baliza» controlada por el convocante, sería el fraude viejo con traje nuevo [4]. El orden de los pasos —primero el compromiso sellado, después el azar— es todo el mecanismo: invertirlo lo anula.

Y el cuarto es **el tecnosolucionismo distributivo**. Ningún sorteo limpio resuelve la escasez que lo obliga. Si hay cuarenta pisos para mil familias [2], la criptografía garantiza que el reparto sea limpio —no que sea suficiente. La transparencia del mecanismo nunca ha de servir para naturalizar la penuria de lo que se reparte.

Es hora de actuar

Si el azar decide vidas, que sea un azar que todos puedan comprobar.

Para las administraciones que sortean: adoptad el protocolo completo —lista y regla selladas antes, baliza pública después, acta anclada siempre [3][4]; y ofreced el verificador sencillo, para que comprobar no exija ingeniería.

Para los notarios: certificad compromisos previos y actas finales [2][3] —la fe pública gana su mejor instrumento desde el papel timbrado.

Para los opositores y solicitantes: guardaos la lista y la huella publicadas [3]; el día del sorteo, recomputad —o exigid poder hacerlo [1][4].

Para los juzgados contenciosos: ante una impugnación de sorteo [2], pedid el paquete verificable —compromiso, azar, acta; donde lo haya, la resolución es aritmética; donde no, la sospecha tiene base.

Para los desarrolladores cívicos: construid los verificadores abiertos —la web de recomputación de un clic [4]; la transparencia practicable es código, y es poco.

Para los legisladores: imponed el compromiso previo sellado y el azar público verificable en todo sorteo administrativo que reparta bienes o cargas [1][2][3][4] —y que la recomputabilidad sea un derecho de cualquier participante.

En la próxima sala llena de familias con carpetas, que la mala suerte —porque seguirá existiendo— no deje nunca más el regusto de la sospecha: solo el número que salió, comprobable por todos, incluso por quien se va sin piso. Por un azar de todos, **time2act**.

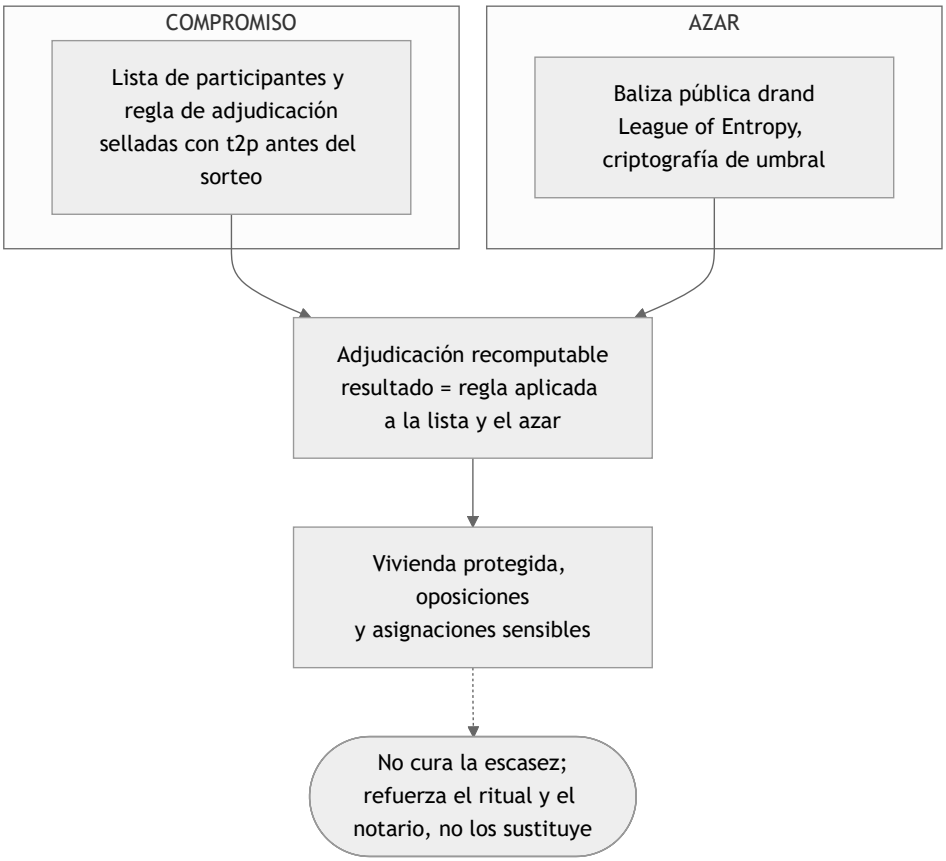


Figura 45.1 — El sorteo que nadie puede cargar, en dos mitades: el compromiso previo (lista de participantes y regla de adjudicación selladas con t2p —huella SHA-512, RFC 3161/eIDAS, blockchain pública— y publicadas por huella ANTES del sorteo) y el azar público verificable (baliza drand de la League of Entropy: valores imparciales, impredecibles y verificables, generados por criptografía de umbral entre operadores independientes). Resultado: adjudicación recomputable por cualquiera —resultado = regla(lista, azar). Límites: el sorteo limpio no cura la escasez; el ritual público y el notario se refuerzan, no se sustituyen. Fuentes: sorteos de oposiciones y de vivienda protegida; drand/League of Entropy.

---

[1] AFAPNA — *Oposiciones 2026: sorteo de letras de tribunales y aspirantes*; OpositaTest — *Sorteo por letra del orden de actuación en oposiciones* (sorteo público de letras; procedimientos reglados posteriores; sistema «espejo» de inversión del orden del DNI); USTEA — *Resultado del sorteo para la designación de vocales de los tribunales*. https://afapna.es/educa/oposiciones-2026-sorteo-letras-de-tribunales-y-aspirantes/ · https://blog.opositatest.com/dudas-letra-del-orden-de-actuacion-de-los-opositores/ · https://educacion.ustea.org/oposiciones-2026-resultado-del-sorteo-para-la-designacion-de-vocales-de-los-tribunales/ ↩

[2] esPúblico — *La notificación en el procedimiento de adjudicación de viviendas protegidas mediante sorteo* (sorteo ante notario según el procedimiento de cada administración; posibilidad de impugnación); elDiario.es (Canarias Ahora) — *Los Llanos espera que la impugnación del sorteo de las 40 viviendas se resuelva «con prontitud y máxima transparencia»*. https://www.administracionpublica.com/adjudicaciondeviviendasprotegidas/ · https://www.eldiario.es/canariasahora/lapalmaahora/municipios/los_llanos_de_aridane/los-llanos-espera-impugnacion-sorteo-viviendas-resuelva-prontitud-maxima-transparencia_1_4583333.html ↩

[3] t2p — manual de producto (huella SHA-512; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; compromiso previo por huella —los datos personales no se exponen—; actas ancladas y reverificables). Véanse los capítulos 13 y 15; la integridad electoral, en el capítulo 48. ↩

[4] Cloudflare / League of Entropy — *Distributed Randomness Beacon* (drand: baliza de aleatoriedad distribuida y públicamente verificable; miembros fundadores: Cloudflare, EPFL, Kudelski Security, Protocol Labs y Universidad de Chile; valores imparciales, impredecibles y verificables a intervalos fijos; criptografía de umbral; aplicaciones: loterías y elecciones); PR Newswire — *The League of Entropy launches production drand network* (primera baliza pública verificable en producción); GitHub — *drand/drand*. https://www.cloudflare.com/leagueofentropy/ · https://www.prnewswire.com/news-releases/the-league-of-entropy-launches-production-drand-network-providing-the-first-publicly-verifiable-distributed-randomness-beacon-301109096.html · https://github.com/drand/drand ↩

Oposiciones y exámenes: la prueba sellada antes

«Convengo con usted en que hay una aristocracia natural entre los hombres. Sus fundamentos son la virtud y el talento.»

— Thomas Jefferson, carta a John Adams (28-10-1813)

Un sábado por la mañana, en un aula grande de cualquier ciudad: centenares de personas que llevan años preparando este día, el sobre que se abre ante todos, el ritual de siempre. Y la pregunta que nadie puede responder con pruebas: este examen, ¿lo ha visto alguien antes?

El caso que lo hace urgente está documentado [1]. En la oferta pública de empleo de Osakidetza —el servicio vasco de salud— de 2016-2017, las denuncias sindicales por filtraciones en Anestesia y Angiología destaparon un escándalo: un informe encontró indicios de filtración en 19 exámenes de hasta 12 especialidades médicas. Dimitieron el consejero de Salud, Jon Darpón, la directora general de Osakidetza y dos directivos más; la Fiscalía investigó. Y el final, ocho años después: en diciembre de 2024, la jueza archivó la causa «al no existir indicios racionales de la comisión del ilícito» —provisional solo para dos investigados de una especialidad [1]. El archivo ni exoneraba ni condenaba: ocho años de sospecha, carreras destruidas, miles de opositores dejados con la duda —y ninguna manera de probar nada, en ninguna dirección.

La lección es la misma que la de la disputa de la ayuda en Somalia del capítulo 50: cuando no hay registros verificables, ni la acusación ni la defensa pueden probar nada —y la duda se lo come todo, culpables e inocentes por igual.

Este capítulo es el hermano natural del capítulo 45: allí, el sorteo recomputable; aquí, el mismo patrón —el compromiso previo— aplicado a la propia prueba. Los títulos, las credenciales y la IA en los exámenes están en el capítulo 19; el procedimiento administrativo, en el capítulo 44; quien denuncia una filtración desde dentro, en el capítulo 62. Pregunta clave: ¿cómo se sabe que las preguntas no han circulado, que la plantilla no se ha tocado y que tu hoja es la que entregaste? Respuesta: sellándolo todo antes con **t2p** —la huella SHA-512 del examen y de la plantilla, ancladas con fecha cierta ANTES de la convocatoria (solo las huellas: el contenido no sale de la custodia), y la hoja de respuestas del candidato, fechada al salir [2]. Protege al opositor del tribunal sucio —y al tribunal limpio, de la sospecha infinita.

Los tres momentos donde se rompe la confianza

El primero es **antes del examen**. El contenido se redacta, se imprime, se custodia —y pasa de mano en mano entre redactores, revisores y tribunal. Cada transferencia es una oportunidad para que una copia circule o una versión se altere sin dejar rastro. La cadena de custodia es, en esencia, una cadena de confianza personal; y cuando la sospecha llega —como en el caso vasco [1]—, no hay manera de reconstruir ni qué existía en qué momento ni quién accedió a ello.

El segundo es **la plantilla de respuestas**. Se publica, llegan las impugnaciones, se anulan preguntas —rutina legítima del contencioso. Pero también es el momento donde una plantilla se puede «ajustar»: si la versión publicada difiere de la que existía el día del examen —aunque solo en un par de preguntas—, las consecuencias mueven plazas enteras. Y sin una prueba inmutable del contenido original, nadie puede demostrar si ha habido retoque o no: todo pende de la palabra del tribunal.

El tercero es **la hoja de respuestas**. El opositor entrega su hoja y se va con las manos vacías. Si la corrección se equivoca, si la hoja «se pierde», si la lectura óptica falla —su versión no existe en ninguna parte, y la verdad queda huérfana.

El sistema pide fe tres veces. Y la fe, como enseñó Osakidetza [1], cuando se rompe no se repara con investigaciones: solo con registros que existieran desde el principio.

La prueba de existencia aplicada

El patrón del capítulo 45 —compromiso previo, revelación después— aplicado al contenido de la prueba [2].

1. El examen sellado antes

El tribunal certifica el examen definitivo con t2p el día que lo cierra: la huella SHA-512 se ancla con fecha cierta —y solo la huella: el contenido no sale de la custodia [2]. Nadie ve nada; pero desde aquel momento, el examen que se reparta el día D se puede contrastar contra la huella previa: ni sustituciones de última hora, ni «versiones» que nadie sabe de dónde salen. Y cada acceso a la custodia —quién abrió el sobre digital, cuándo— deja su registro fechado: la cadena de custodia deja de ser una cadena de palabras.

2. La plantilla comprometida

La plantilla de corrección, sellada antes del examen [2]. Las impugnaciones y las preguntas anuladas siguen siendo posibles —son derecho de los opositores— pero pasan a ser transparentes: la plantilla original tiene fecha; cada revisión posterior, también; y el «cambio silencioso de respuesta correcta» se vuelve imposible de hacer sin dejar rastro. El tribunal que lo hace todo bien tiene, por primera vez, la prueba positiva de que no tocó nada.

3. La hoja de respuestas fechada

Al salir del aula, el opositor fotografía su copia autocopiativa —o el resguardo que el sistema le dé— con t2p: su versión de las respuestas, con fecha cierta del mismo día [2]. Contra el error de corrección, la lectura óptica defectuosa o la hoja extraviada, ya no está indefenso: tiene lo que entregó, fechado antes de conocer la plantilla. Y donde el procedimiento no da copia, esta es la reforma barata que hay que exigir.

4. El expediente de impugnación — y la simetría

Cuando haya que impugnar, el expediente .asice lo lleva todo: la huella previa del examen y la plantilla, la hoja de respuestas fechada, las publicaciones oficiales capturadas con sus fechas [2] —una cronología verificable para el tribunal administrativo o el contencioso. Y la simetría que el caso vasco reclama a gritos [1]: el tribunal limpio puede probar que el examen no circuló y que la plantilla no se tocó —la sospecha infinita, que también destruye inocentes, muere de fechas. Osakidetza en positivo.

Los límites, porque los hay: el sello acredita integridad y fechas —no la calidad de las preguntas ni la justicia de la puntuación: eso es del tribunal y, si hace falta, del juez. El compromiso previo protege el contenido, no impide la filtración humana —quien ha visto el examen lo puede contar: la custodia física y las personas siguen contando, y el registro de accesos las hace responsables. Y la implantación ha de ser institucional —el opositor solo puede fechar su hoja: el resto es tarea de quien convoca.

La promesa y el peligro

La promesa: oposiciones donde la integridad de la prueba es un hecho verificable y no un acto de fe [1][2]; impugnaciones que discuten el fondo —si la pregunta era válida— sobre plantillas fechadas; opositores que conservan su versión; tribunales limpios blindados contra la sospecha; y el próximo Osakidetza [1] resuelto en días —en una dirección o en la otra— en lugar de ocho años de sombra.

Y ahora, los peligros, sin edulcorar.

El primero es **el sello como teatro**: certificar el examen y dejar la custodia física como estaba. La huella previa solo vale si lo que se reparte se contrasta de verdad contra ella, y si los accesos quedan registrados —el compromiso previo es un sistema, no un trámite.

El segundo es **la impugnación industrializada**. Si cada opositor tiene expediente, los contenciosos se pueden multiplicar. El contrapeso es el mismo mecanismo: contra plantillas fechadas y exámenes íntegros, la impugnación infundada muere de hechos —litigará menos quien menos razón tenga.

El tercero es **la filtración que ningún hash detiene**: quien ve el examen lo puede memorizar y contar. La prueba de existencia fecha y delimita responsabilidades —quién accedió a ello, cuándo—; la confidencialidad humana es otra capa, y el capítulo 62 explica qué hacer cuando alguien, desde dentro, ve que se rompe.

Hay un cuarto peligro, más silencioso: que el juego limpio haga olvidar el juego justo. Ningún sello hace justas las plazas, ni buenas las preguntas, ni cortas las listas de espera. La prueba de existencia garantiza el juego limpio; que el juego valga la pena es tarea de quien diseña las convocatorias.

Es hora de actuar

Que la pregunta «¿esto lo ha visto alguien antes?» tenga respuesta.

Para los tribunales y órganos convocantes: examen y plantilla sellados antes, accesos registrados, contraste público el día D [2] —vuestra integridad merece ser demostrable, no solo cierta.

Para los opositores: fotografiad y fechad vuestra copia de respuestas al salir [2]; y exigid a las convocatorias el compromiso previo —es una línea en el pliego de bases que lo cambia todo.

Para los sindicatos y las academias: la reivindicación barata y transversal: ningún examen sin huella previa [1]; quien se niegue, que explique por qué.

Para los tribunales contenciosos: ante una impugnación, pedid el paquete verificable —examen previo, plantilla fechada, hoja de respuestas [2]; donde lo haya, la resolución es comparación; donde no, la sospecha tiene base.

Para los legisladores: después de Osakidetza [1] —ocho años para archivar sin culpables—, que la normativa de acceso a la función pública incorpore el compromiso previo sellado como requisito de toda convocatoria: cuesta céntimos y vale la confianza de millones.

En la próxima aula de examen, cuando se abra el sobre, que la pregunta «¿esto lo ha visto alguien antes?» tenga respuesta —una huella con fecha, comprobable por todos los que se juegan la vida en ello. Por las plazas que se ganan estudiando, **time2act**.

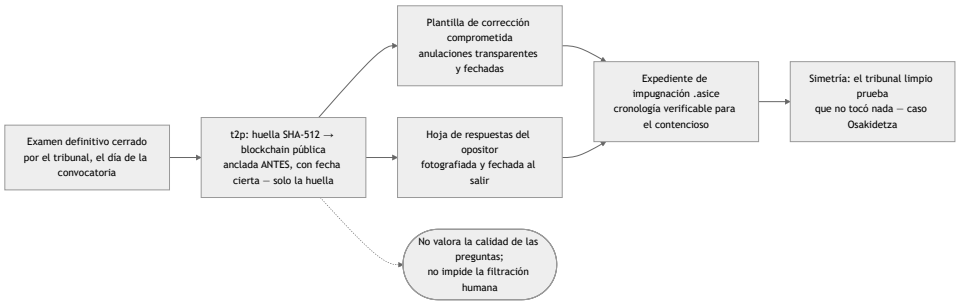


Figura 46.1 — La prueba sellada antes (t2p: huella SHA-512 —solo la huella se ancla, el contenido no sale de la custodia—, RFC 3161/eIDAS, blockchain pública, .asice): el examen certificado antes de la convocatoria con accesos registrados, la plantilla de corrección comprometida antes del examen (las anulaciones, transparentes y fechadas), la hoja de respuestas del opositor fechada al salir, y el expediente de impugnación verificable. Simetría: el tribunal limpio puede probar que no tocó nada —el caso Osakidetza (19 exámenes con indicios de filtración, dimisiones, ocho años y archivo por falta de pruebas) resuelto en días, en cualquier dirección. Patrón: el compromiso previo del capítulo 45, aplicado al contenido. Fuentes: Redacción Médica; Deia; elDiario.es.

---

[1] Redacción Médica — *Un informe revela filtraciones de 19 exámenes en hasta 12 OPE de Osakidetza* (OPE 2016-2017 del servicio vasco de salud; denuncias sindicales en Anestesia y Angiología; indicios en 19 exámenes de 12 especialidades; dimisiones del consejero de Salud Jon Darpón, la directora general de Osakidetza y dos directivos de RRHH); Deia — *Archivan la causa por las presuntas filtraciones en la OPE de Osakidetza en 2018 por falta de pruebas* (diciembre de 2024: archivo «al no existir indicios racionales de la comisión del ilícito», provisional para dos investigados de Cirugía Plástica); elDiario.es — *La Justicia cierra sin culpables la investigación* y *Ocho años del inicio de la investigación… sin fecha para el juicio.* https://www.redaccionmedica.com/autonomias/pais-vasco/un-informe-revela-filtraciones-de-19-examenes-en-hasta-12-ope-de-osakidetza-4796 · https://www.deia.eus/actualidad/sociedad/2024/12/12/archivan-causa-filtraciones-ope-osakidetza-9042604.html · https://www.eldiario.es/euskadi/justicia-cierra-responsabilidad-investigacion-filtraciones-oposiciones-medicas-vascas_1_11896007.html ↩

[2] t2p — manual de producto (certificar cualquier archivo —solo la huella viaja, el contenido no sale nunca de la custodia; foto con fecha cierta; escáner de documentos; captura de publicaciones oficiales con fecha; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; el sorteo de tribunales, en el capítulo 45; las credenciales, en el capítulo 19; los alertadores, en el capítulo 62. ↩

Identidad digital: la prueba de que existes

«Su ser es ser percibido.»

— George Berkeley, Principios del conocimiento humano, §3 (1710)

El 28 de septiembre de 2017, en una aldea del distrito de Simdega, en el estado indio de Jharkhand, una niña dalit de once años llamada Santoshi Kumari murió pidiendo arroz a su madre. Hacía casi ocho días que apenas comía. La tarjeta de racionamiento de su familia —el derecho a la cuota de alimento subvencionado— había sido cancelada porque no estaba vinculada a **Aadhaar**, el sistema de identidad biométrica de la India, y durante seis meses no habían podido retirar su grano [8]. El gobierno lo disputó, alegando malaria; la campaña por el derecho a la alimentación documentó decenas de muertes por inanición ligadas a fallos del sistema [8].

Empezamos por esta tragedia porque contiene la advertencia más importante de este capítulo, y de toda la Parte que ahora abrimos. La identidad es el derecho que precede a todos los demás: sin una prueba de que existes, no hay cuenta bancaria, ni voto, ni escuela, ni atención médica, ni ayuda. Pero una identidad **mal diseñada** —centralizada, obligatoria, sin alternativa— puede matar. Este capítulo trata de cómo dar a centenares de millones de personas la prueba de que existen, y de cómo hacerlo **sin** convertir aquella prueba en un arma contra ellas.

Ochocientos millones de invisibles

La dimensión del problema es abrumadora. Según la iniciativa **Identification for Development** (ID4D) del **Banco Mundial**, cerca de **800 millones de personas** —una de cada diez— no tienen ninguna prueba oficial de identidad; la cifra ha bajado desde 2017, pero más de la mitad de quienes no la tienen son **niños cuyo nacimiento no se registró nunca** [1]. **UNICEF** lo confirma desde el otro extremo: **150 millones de niños menores de cinco años** son «invisibles» porque nadie los ha inscrito al nacer, y la mitad viven en el África subsahariana [3]. Al otro lado del espectro está la **apatridia**: el Alto Comisionado de las Naciones Unidas para los Refugiados (**UNHCR**) contabiliza oficialmente 4,4 millones a finales de 2024, pero advierte de que la cifra real llega probablemente a los diez millones; el grupo más grande son los rohinyás, casi 1,8 millones de personas sin ninguna nacionalidad reconocida [2].

Esta gente no «no existe»; **existen**, trabajan, aman y mueren, pero ningún Estado lo reconoce. El objetivo 16.9 de los Objetivos de Desarrollo Sostenible se fijó precisamente esto: identidad jurídica para todos antes de 2030. Pero la pregunta clave no es *si* damos identidad, sino *cómo*.

Dos maneras de dar identidad

Hay dos caminos; la diferencia entre ambos es la lección de Santoshi.

El primero es el modelo **centralizado y biométrico**, ejemplificado por Aadhaar. Con unos **1.340 millones de titulares vivos** —más del 99,9 % de los adultos indios— y más de 170.000 millones de autenticaciones, es el sistema de identidad más grande de la historia [6]. Ha incluido a mucha gente antes excluida del sistema financiero. No obstante, en octubre de 2023 los datos personales de unos **815 millones de indios** —números de Aadhaar, pasaportes, teléfonos, direcciones— se pusieron a la venta en la web oscura, filtrados desde una base de datos de tests de covid [7]. La dependencia de una sola «fuente de verdad» biométrica excluye: las tasas de fallo de autenticación oscilan entre el 6 y el 12 %, y en Rajastán, en julio de 2017, uno de cada tres titulares no pudo retirar su grano por fallos repetidos de la huella [9]. La economista **Reetika Khera**, del Instituto Indio de Tecnología de Delhi, resume sin paliativos que el Estado no debería tratar la identidad biométrica como la única fuente de verdad, porque lo que se vende como «ahorro» a menudo es la denegación de derechos por fallos del sistema, no fraude eliminado [9]. El Tribunal Supremo de la India, que avaló Aadhaar en 2018, lo hizo con un voto discrepante memorable del juez Chandrachud [9].

El segundo camino es una arquitectura nueva y descentralizada, donde **la persona controla su propia identidad**. El consorcio de estándares **W3C** ha publicado las piezas técnicas: los **identificadores descentralizados** (DID), recomendación oficial de 2022, y las **credenciales verificables** (Verifiable Credentials), estándar desde mayo de 2025, que describen un ecosistema de tres partes —quién emite, quién posee y quién verifica— criptográficamente seguro y respetuoso con la privacidad [5]. Europa va de

la mano: el reglamento **eIDAS 2.0** obliga a cada Estado miembro a ofrecer una **cartera de identidad digital** (EUDI Wallet) antes de finales de 2026, con **divulgación selectiva** incorporada —por ejemplo, probar que eres mayor de edad sin revelar tu fecha de nacimiento, función ya pilotada en al menos seis estados [4]. Estonia, con su e-ID para el 99 % de la población, demuestra desde hace años que se puede hacer bien. La diferencia con Aadhaar no es la tecnología; es **quién custodia la prueba**.

La prueba de que existes

Es en este segundo camino donde **t2p** aporta una pieza fundamental: la **prueba de existencia de una persona**. El mecanismo aplica la lógica de todo el libro al caso más básico de todos. La aplicación captura un gesto de **prueba de vida** —un vídeo o un reto activo, resistente a las deepfakes—, opcionalmente un rasgo biométrico, y calcula su **huella SHA-512** en el propio dispositivo. Esa huella se ancla a la **blockchain pública** con un **sello de tiempo RFC 3161** conforme a eIDAS y un **GPS forense**, y se empaqueta en un contenedor **.asice verificable sin conexión**. El resultado, en lenguaje llano: *esta persona estaba viva, era ella, estuvo en este lugar, en este instante*. Un testimonio firmado y fechado para alguien que no tiene papeles.

Además, cuando una ONG, un médico de campo o una escuela emite una **credencial verificable** —«ha completado este curso», «ha recibido esta vacuna»—, su huella se puede anclar para que el titular la lleve **en su propio dispositivo**, la presente con divulgación selectiva y la verifique cualquiera sin tener que contactar con quien la emitió. Es crucial para quien lo pierde todo en un desplazamiento: la prueba viaja con la persona, no en un registro que puede arder o que puede ser pirateado. La diferencia con el modelo Aadhaar es exactamente esta: **el titular conserva la prueba**, no un repositorio central que puede filtrarse o denegar el acceso.

La promesa y el peligro

Y aquí, más que en ningún otro capítulo de este libro, el peligro pide que lo digamos antes que la promesa. Una prueba de existencia **no es un estatus legal**; solo los Estados otorgan nacionalidad, ciudadanía y derechos jurídicos. t2p puede demostrar que una persona existe, quién es y dónde se encuentra, pero **no la convierte en ciudadana ni resuelve la apatridia**. Confundir las dos cosas sería un engaño cruel.

Un peligro aún más grave, como hemos visto con los 815 millones de registros filtrados y las muertes por fallo de autenticación, es que centralizar la biometría puede vigilar y matar poblaciones vulnerables. Por eso el diseño ha de ser radicalmente diferente: **descentralizado, con la prueba en manos del titular, voluntario y con una alternativa no biométrica siempre disponible**. Una prueba de existencia nunca puede ser un requisito excluyente para acceder a servicios; si alguien declara un nombre falso, la cadena solo certifica que aquel dato se capturó íntegro, no su verdad. La tecnología es buena solo si sirve a la persona y no al Estado contra ella.

La promesa es inmensa y profundamente humana. Dar a 800 millones de invisibles una manera de demostrar que existen —portátil, suya, verificable sin pedir permiso a nadie— es abrirles la puerta a todos los demás derechos, convirtiendo el «no consto en ninguna parte» en «aquí está la prueba de que soy».

Una identidad anclada permanentemente a la prueba de existencia puede convertirse en una cadena invisible que impida cualquier reinvención personal. Cuando el personaje digital se fija «lo más íntimamente posible» con la identidad jurídica offline, se abre la puerta a nuevas injusticias: decisiones de vida —desde créditos bancarios hasta permisos de inmigración— podrían basarse en un registro inmutable que no deja espacio para errores o cambios voluntarios [11]. El caso del proyecto Worldcoin/World ID ilustra este peligro; su escaneo de iris, diseñado para probar la humanidad, ha sido prohibido u obligado a borrar datos en más de nueve jurisdicciones entre 2024 y 2025 —Kenia lo ha declarado inconstitucional y Colombia ha ordenado la supresión total de la biometría recogida [12]. Por eso el diseño ha de incluir mecanismos de disociación temporal controlada, que permitan al titular desconectar su identidad digital del registro legal cuando lo necesite, y garantizar una alternativa no biométrica siempre disponible para evitar que un único punto de fallo bloquee todo su futuro.

Es hora de actuar

Para los **Estados y registros civiles**: invertir en un registro de nacimientos universal y adoptar modelos descentralizados que, sin excluir, incorporen la lección de Aadhaar. Para las **agencias humanitarias**

(UNHCR, ACNUR, ONG): proporcionar credenciales portátiles que sean controladas por las personas, en lugar de bases de datos biométricas centrales que las conviertan en sujetos de vigilancia. Para los **organismos de estándares** (W3C, eIDAS): consolidar la identidad autosoberana con divulgación selectiva como norma. Para los **diseñadores**: situar la privacidad y la voluntariedad como primer requisito, no como último añadido. Y para todos: recordar que la prueba de tu existencia ha de ser un derecho en tus manos, no una cadena al cuello.

Una niña murió porque un sistema de identidad le negó el derecho a comer. La diferencia entre una prueba de existencia que empodera y una que excluye es toda la diferencia del mundo; garantizar a cada persona una prueba segura y en sus manos es, en este frente fundamental, **time2act**.

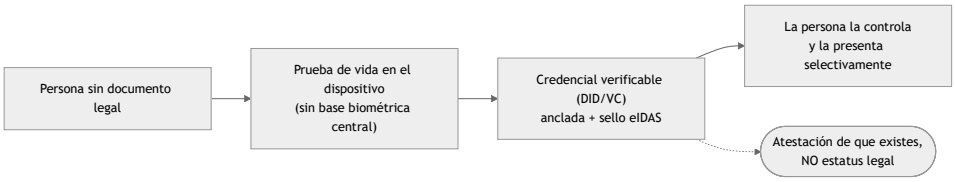


Figura 47.1 — Una persona sin papeles genera un gesto de prueba de vida («soy yo, estoy vivo»); en el dispositivo se calcula su huella SHA-512 con GPS forense y sello de tiempo eIDAS («aquí, ahora»), se ancla a la blockchain pública y puede acompañar una credencial verificable W3C; el titular guarda la prueba en su dispositivo y la comparte con divulgación selectiva, en un contenedor .asice verificable sin conexión. Escala del reto: ~800 M sin identidad, ~4,4 M (hasta 10 M) apátridas, 150 M de niños no registrados. Fuentes: Banco Mundial ID4D; UNHCR; UNICEF; W3C.

---

[1] Banco Mundial (ID4D) — *Global progress in identification: 3 findings from the latest data* (2025; ~800 M sin identidad oficial; >50 % son niños no registrados). https://blogs.worldbank.org/en/digital-development/global-progress-in-identification--3-findings-from-the-latest-da ↩

[2] UNHCR — *Global Trends Report 2024* (4,4 M de apátridas oficiales, hasta ~10 M reales; rohinyás ~1,8 M). https://www.unhcr.org/sites/default/files/2025-06/global-trends-report-2024.pdf ↩

[3] UNICEF — *Birth registration steadily increases worldwide, but 150 million children still invisible* (diciembre 2024). https://www.unicef.org/press-releases/birth-registration-steadily-increases-worldwide-150-million-children-still-invisible ↩

[4] Comisión Europea — *European Digital Identity (eIDAS 2.0)* (Reg. UE 2024/1183; EUDI Wallet obligatoria a finales de 2026; divulgación selectiva). https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation ↩

[5] W3C — *Verifiable Credentials Data Model v2.0 becomes a W3C Recommendation* (15-mayo-2025) y *Decentralized Identifiers (DID) v1.0* (2022). https://www.w3.org/press-releases/2025/verifiable-credentials-2-0/ ↩

[6] Gobierno de la India (Press Information Bureau) — *Aadhaar* (~1.340 millones de titulares vivos; >99,9 % de los adultos; >170.000 millones de autenticaciones). https://www.pib.gov.in/PressReleasePage.aspx?PRID=2241778 ↩

[7] Business Standard / Resecurity — *Aadhaar data of millions of Indians put on sale on the dark web* (~815 millones de registros, octubre 2023). https://www.business-standard.com/india-news/aadhaar-data-of-millions-of-indians-put-on-sale-on-the-dark-web-reports-123103000993_1.html ↩

[8] Scroll.in — *Denied food because she did not have an Aadhaar-linked ration card, Jharkhand girl dies of starvation* (Santoshi Kumari, 2017). https://scroll.in/article/854225/denied-food-because-she-did-not-have-aadhaar-linked-ration-card-jharkhand-girl-dies-of-starvation ↩

[9] Reetika Khera (IIT Delhi) — investigación sobre Aadhaar y la exclusión en programas de bienestar (*Economic & Political Weekly*). https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare ↩

[10] MIT Technology Review — *Inside the Jordan refugee camp that runs on blockchain* (WFP Building Blocks; reconocimiento de iris EyePay). https://www.technologyreview.com/2018/04/12/143410/inside-the-jordan-refugee-camp-that-runs-on-blockchain/

[11] Edward Snowden — *Vigilancia permanente* (Planeta, 2019). ↩

[12] Biometric Update / ICLG — *Worldcoin: prohibiciones y órdenes de supresión* (2024-2025). https://www.biometricupdate.com/202510/colombia-orders-world-shut-down-citing-biometrics-compliance-failures ↩

Integridad electoral: probar qué pasó en las urnas

«El pueblo reina sobre el mundo político americano como Dios sobre el universo. Es la causa y el fin de todas las cosas; todo sale de él y todo se absorbe en él.»

— Alexis de Tocqueville, La democracia en América, I (1835)

El 1 de septiembre de 2017, en Nairobi, el presidente del Tribunal Supremo de Kenia, **David Maraga**, leyó un veredicto que hizo historia. Por cuatro votos contra dos, el tribunal declaraba «inválida, nula y sin efecto» la reelección del presidente en ejercicio, Uhuru Kenyatta. Era la primera vez en África que una corte anulaba la victoria de un presidente a instancias de la oposición [1]. Y el detalle que lo tumbó todo no fue un fraude de papeletas, sino **actas que no cuadraban**: de 291 formularios de escrutinio de circunscripción examinados, 56 no tenían rasgos de seguridad, 31 no llevaban número de serie y 32 no estaban firmados por los agentes; muchos resultados habían llegado al centro nacional sin las imágenes escaneadas de las actas de mesa [2]. Fue la integridad del **proceso de transmisión**, no del voto, lo que decidió quién gobernaba Kenia.

Este caso marca la frontera exacta de este capítulo. En el capítulo 20 vimos las deepfakes de candidatos y la desinformación electoral —el ataque a la *percepción* del votante. Aquí hablamos de otra cosa: la integridad del **proceso** mismo —el acta, el escrutinio, la transmisión, la observación—, es decir, de poder probar **qué pasó de verdad en las urnas**. Y, como veremos, aquí la tentación tecnológica más obvia es también la más peligrosa.

El proceso, no la papeleta

La fragilidad del proceso es global. En la República Democrática del Congo, en enero de 2019, la comisión electoral proclamó ganador a Félix Tshisekedi con un 38,57 %. Pero una base de datos filtrada de la propia comisión, que cubría el 86 % de los votos, daba la victoria al perdedor oficial, Martin Fayulu, con casi un 60 %; y 39.824 observadores desplegados por la Iglesia católica congoleña llegaban a una cifra aún más alta para Fayulu. Las dos fuentes independientes, recogidas por separado, coincidían entre ellas con una correlación del 0,98, pero divergían del resultado oficial en unos 3,6 millones de votos [3]. La evidencia existía; lo que faltaba era una cadena de custodia verificable que la hiciera incontestable.

Es precisamente esta cadena de custodia lo que vigilan los observadores electorales. Como explica el manual de la **OSCE/ODIHR**, la oficina de derechos humanos de la Organización para la Seguridad y la Cooperación en Europa, el valor de la observación reside en una metodología sistemática que cubre todo el ciclo —marco legal, registro, campaña, votación, escrutinio, tabulación— y que permite distinguir si las irregularidades son **aisladas o sistemáticas** [9]. El problema es que el testimonio de un observador, sin una prueba anclada, siempre se puede cuestionar: «podría ser de otro día, de otro lugar, un montaje».

Por qué el voto en blockchain es una mala idea

Llegados aquí, hay que hacer una advertencia que este libro no puede ahorrarse, porque es contraintuitiva. La tentación natural es pensar: si la blockchain sirve para tantas cosas, ¿por qué no votamos directamente en ella? La respuesta de la comunidad de seguridad es unánime y contundente: **votar en blockchain es una mala idea**.

El criptógrafo **Ron Rivest**, del MIT y coinventor del sistema RSA, lo demostró con sus colegas en un artículo de referencia titulado, sin ambages, *Going from bad to worse: from Internet voting to blockchain voting* (2021). Su conclusión es que el voto por internet y por blockchain «aumentarían enormemente el riesgo de **fallos electorales indetectables a escala nacional**» [4]. El motivo de fondo es profundo: una elección exige a la vez **secreto del voto** e **independencia del software** —que ningún error o cambio no detectado en el software pueda alterar el resultado sin dejar rastro—, y la transparencia de la cadena de bloques rompe el secreto, mientras que ninguna tecnología conocida, blockchain incluida, garantiza la independencia del software en un voto móvil.

No es teoría. En 2018, Virginia Occidental dejó votar a 144 personas —muchos militares desplegados— con la aplicación de blockchain Voatz; en 2020, investigadores del MIT encontraron que un atacante podía «alterar, detener o exponer el voto» de un usuario, y el estado la abandonó [5]. Y en Moscú, en agosto de

2019, el investigador francés **Pierrick Gaudry**, del CNRS, descargó el código del sistema de voto «blockchain» de la ciudad y, en unos **veinte minutos** con un ordenador corriente y software libre, calculó sus claves privadas: podría haber revelado el voto de cada elector [6]. Tras el parche, otro investigador volvió a romperlo. La etiqueta «blockchain» no es ninguna garantía de seguridad. La prueba de existencia, pues, **no ha de tocar nunca la emisión del voto secreto**. Su lugar es otro.

La prueba de existencia al servicio del escrutinio, no del voto

El lugar correcto de **t2p** son las **partes públicas y observables** del proceso. Veámoslo.

Primero, **el sellado del acta en la mesa**. Antes de transmitir ningún resultado, el funcionario fotografía el acta de mesa y la sella: **huella SHA-512** en el dispositivo, **sello de tiempo RFC 3161** conforme a eIDAS, **GPS forense** de la ubicación de la mesa y **prueba de vida** del funcionario que la firma, todo en un contenedor **.asice** anclado a la blockchain pública. Si alguien altera la cifra «en tránsito» entre la mesa y el centro de tabulación —exactamente el agujero de Kenia—, el acta original sellada lo delata: la huella no coincide. Segundo, **la evidencia de los observadores**: una foto o un vídeo de una irregularidad sellados con GPS, hora y prueba de vida convierten un testimonio cuestionable en un registro con lugar, momento y persona probados. Tercero, **la cadena de custodia**: cada salto del acta se puede resellar, creando el rastro auditable que distingue lo aislado de lo sistemático.

Y aquí es clave una complementariedad. El estadístico **Philip Stark**, de la Universidad de California en Berkeley, inventó las **auditorías de riesgo limitado** (RLA): un muestreo estadístico del papel que limita formalmente el riesgo de proclamar un ganador equivocado, siempre que exista una **papeleta verificada por el votante** [7]. Su máxima es «no confíes en la máquina, exige evidencia». La prueba de existencia no sustituye la RLA: el papel sigue siendo la verdad de terreno. t2p asegura que la *foto del acta y su transmisión* no se manipulen; el recuento auténtico se audita sobre el papel.

Hay que decir el límite con toda la claridad, porque es el corazón de este capítulo. t2p **no es voto por internet ni voto en blockchain**; solo sella las partes públicas: actas, fotos, vídeos, transmisión. Y «basura a la entrada, basura en la cadena»: sellar un acta prueba que *aquel papel existía con aquella cifra, en aquella hora y lugar*, no que la cifra refleje los votos realmente depositados. Si el acta ya venía falsificada desde la mesa, la cadena la inmortaliza igual de falsa. Por eso la prueba de existencia es **complemento** de la observación y de la auditoría sobre papel, nunca su sustituto.

La promesa y el peligro

La promesa, bien acotada, es valiosa. En países donde una cifra alterada en tránsito puede decidir quién gobierna —y provocar violencia—, sellar el acta en la mesa y dar a los observadores una evidencia incontestable haría mucho más difícil el fraude de transmisión y mucho más fácil distinguir el error puntual de la manipulación orquestada. Es devolver credibilidad a un proceso del que depende la paz.

El peligro, aquí, es sobre todo el exceso de ambición. Vender la prueba de existencia como una solución para «votar desde el móvil» sería repetir el error de Voatz y Moscú, y poner en riesgo el secreto del votante y la confianza en todo el sistema. El sello tampoco hace verdadera un acta falsa. Y cualquier infraestructura que registre la actividad electoral ha de proteger y garantizar el anonimato del votante. La prueba de existencia es una herramienta para la transparencia de lo que es público, no un atajo para digitalizar lo que ha de seguir siendo secreto y de papel.

Además, el hecho de sellar actas en una capa como la que t2p usa hoy implica confiar en una cadena que se presenta como neutra, pero la neutralidad es solo formal si el poder de validación e interpretación del protocolo queda concentrado en manos de unos pocos actores. En el ecosistema L2, en 2026 casi la mitad de los bloques (aproximadamente un 42 %) se genera a través de relays que aplican las listas OFAC, y todos los grandes L2 de Ethereum operan con un único secuenciador corporativo [12]. Esta arquitectura crea una «censura asimétrica»: quien controla el secuenciador puede decidir qué activos se registran o se excluyen, sin que la comunidad sea consciente de ello. Como recuerda Shoshana Zuboff, el núcleo del poder es «quién sabe, quién decide, y quién decide quién decide» [11]; así, una infraestructura de sellado basada en la blockchain pública podría replicar un dominio oligárquico, donde la confianza pública se ve erosionada por la falta de mecanismos anticoncentración. En este escenario, la prueba de existencia podría acabar sirviendo más como herramienta de control que como garantía de transparencia.

Es hora de actuar

Para las **comisiones electorales**: sellar las actas en la mesa y transmitirlas, evitando la alteración en tránsito que tumbó a Kenia. Para los **observadores** (OSCE/ODIHR, Carter Center, sociedad civil): anclar su evidencia con hora, lugar y persona, para que ningún testimonio de irregularidad se pueda descartar como «montaje». Para los **auditores**: mantener la papeleta de papel verificada por el votante y las auditorías de riesgo limitado como verdad de terreno. Y para todos: resistir la tentación del voto en blockchain, que la mejor ciencia de seguridad ha desaconsejado una y otra vez.

Un presidente cayó en Kenia porque unas actas no cuadraban y nadie podía probar el original. Dar a cada acta y a cada observación una prueba con hora, lugar y persona —sin tocar nunca el secreto del voto— es, en este frente decisivo para la democracia, **time2act**.

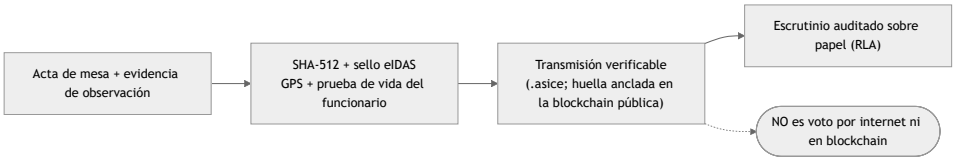


Figura 48.1 — En la mesa, el acta se fotografía y se sella con huella SHA-512, sello de tiempo eIDAS, GPS forense y prueba de vida del funcionario, en un contenedor .asice anclado a la blockchain pública; si la cifra se altera en tránsito hacia el centro de escrutinio, la huella no coincide y lo delata. Lo que la prueba de existencia NO hace: no es voto por internet, no es voto en blockchain, y no demuestra que el recuento sea verdadero —eso se audita sobre el papel (RLA). Fuentes: Tribunal Supremo de Kenia (2017); Rivest et al. (2021); Philip Stark.

[1] Wikipedia (con BBC / Al Jazeera) — *2017 Kenyan presidential election petition* (anulación 4-2; CJ David Maraga; primera en África). https://en.wikipedia.org/wiki/2017_Kenyan_presidential_election_petition ↩

[2] The Standard (Kenia) — *Presidential petition: what scrutiny of key IEBC forms revealed* (291 formularios 34B; 56 sin rasgos de seguridad, 31 sin número de serie, 32 sin firma). https://www.standardmedia.co.ke/article/2001253102/presidential-petition-what-scrutiny-of-key-iebc-forms-revealed ↩

[3] NYU Center on International Cooperation / Congo Research Group — *Who really won the Congolese elections?* (Fayulu ~60 %; CENCO 39.824 observadores; correlación 0,976-0,991; ~3,6 M de votos). https://cic.nyu.edu/resources/who-really-won-the-congolese-elections/ ↩

[4] Sunoo Park, Michael Specter, Neha Narula y Ronald L. Rivest — *Going from bad to worse: from Internet voting to blockchain voting* (Journal of Cybersecurity, 2021). https://academic.oup.com/cybersecurity/article/7/1/tyaa025/6137886 ↩

[5] MIT News / USENIX Security — *Researchers find security flaws in Voatz; «The Ballot is Busted Before the Blockchain»* (2020). https://news.mit.edu/2020/voting-voatz-app-hack-issues-0213 ↩

[6] Pierrick Gaudry (CNRS/INRIA) — *Breaking the encryption scheme of the Moscow Internet voting system* (2019; roto en ~20 minutos). https://arxiv.org/abs/1908.05127 ↩

[7] Philip B. Stark (UC Berkeley) — *A Gentle Introduction to Risk-Limiting Audits* (2012). https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf ↩

[8] Election Academy (Universidad de Minnesota) — *Colorado successfully completes the nation's first risk-limiting audit* (2017; límite de riesgo del 9 %). https://electionacademy.lib.umn.edu/2017/11/27/colorado-successfully-completes-nations-first-risk-limiting-audit/

[9] OSCE/ODIHR — *Election Observation Handbook* (6.ª edición; observadores de corto y largo plazo; distinguir lo aislado de lo sistemático). https://cdn.osce.org/sites/default/files/f/documents/5/e/68439.pdf ↩

[10] The Carter Center — *Election Standards y Declaration of Principles for International Election Observation* (2005). https://electionstandards.cartercenter.org/our-mission/

[11] Shoshana Zuboff — *La era del capitalismo de la vigilancia* (Paidós, 2020). ↩

[12] L2BEAT; MEV Watch (2026). https://www.mevwatch.info/ ↩

Ayuda humanitaria: probar que la ayuda llega

«"Tutti fratelli" —todos hermanos—, repetían ellas con emoción.»

— Henry Dunant, Recuerdo de Solferino (1862)

En Kivu del Sur, en el este de la República Democrática del Congo, la organización GiveDirectly repartía dinero en efectivo a familias en pobreza extrema a través del móvil. En 2022, parte de su propio personal local hizo algo sencillo y devastador: registraba tarjetas SIM a nombre de los beneficiarios, pero se las quedaba y ponía otras en los teléfonos de la gente. Cuando empezaron los pagos, el dinero caía en SIM controladas por los propios trabajadores. El desvío llegó a unos **1,2 millones de dólares** y afectó a cerca de **1.900 familias**; la organización lo confesó públicamente, pero solo pudo recuperar una parte mínima [9]. Detrás de aquella cifra hay una madre que se endeudó esperando un dinero que no llegó nunca.

Este caso plantea la pregunta de este capítulo: en la ayuda humanitaria, **¿cómo se prueba que la ayuda llega de verdad a la persona que la necesita?** Y plantea también, con una agudeza que no tiene ningún otro capítulo del libro, su reverso ético: la tentación de responder con biometría puede convertir a los más vulnerables en los más vigilados.

Diez mil millones que han de llegar

La ayuda en efectivo y vales —dar dinero en lugar de bienes— ha dejado de ser marginal. Según la organización de referencia del sector, la **CALP Network**, y los datos de Development Initiatives, llegó a unos **10.600 millones de dólares** de gasto de programa en 2022 y representa ya cerca de una cuarta parte de toda la ayuda humanitaria internacional [5][6]. El Programa Mundial de Alimentos (WFP) es el mayor proveedor, con 2.900 millones de dólares repartidos a 51,6 millones de personas en 76 países solo en 2023 [5]. Cuando se mueve tanto dinero hacia tanta gente en contextos de crisis, **verificar la entrega no es un detalle: es el problema central**.

La respuesta tecnológica más conocida es **Building Blocks**, del WFP, la implementación de blockchain más grande del mundo humanitario. Empezó en 2017 en el campo de Azraq, en Jordania, y hoy da soporte a unos **seis millones de personas**, con más de un millón de refugiados que lo usan cada mes [1][2]. Ha procesado unos 555 millones de dólares en transferencias, ha eliminado el 98 % de las comisiones bancarias en el piloto y, sobre todo, ha demostrado su valor en la **desduplicación**: en Ucrania, en 2022, dieciocho organizaciones coordinaron 337 millones de dólares de ayuda y evitaron unos **35 millones** de asistencia duplicada al detectar solapamientos entre agencias [1]. Coordinar sin duplicar es, en sí mismo, una victoria contra el fraude.

El dilema biométrico

Pero aquí llega la parte difícil. Para saber que el dinero va a la persona correcta, muchas agencias han recurrido a la **biometría**. En los supermercados de los campos jordanos, el refugiado mira a una cámara y un **escáner de iris** confirma su identidad contra la base de datos del Alto Comisionado para los Refugiados, que a finales de 2023 contenía las huellas y los iris de **15,7 millones de personas** [4]. La promesa es impecable: nadie cobra dos veces, nadie suplanta. El problema es el poder. Como observó un periodista en el campo de Zaatari, un refugiado llamado Bassam decía que el nuevo sistema funcionaba mejor… pero «tiene poca voz en el asunto, porque tiene que estar en el sistema si quiere comer» [3]. Un consentimiento que se da «si quieres comer» no es un consentimiento libre.

Y el riesgo no es abstracto. En Yemen, en 2019, el WFP tuvo que suspender parcialmente la ayuda en las zonas controladas por los hutíes después de que estos se negaran a ceder el control de los datos biométricos —una herramienta que el WFP quería, precisamente, para detener un desvío sistemático de alimentos que había documentado; la disputa aún duraba en 2023, con millones de personas necesitadas en medio [8]. Y el caso más grave lo destapó **Human Rights Watch**: la organización de derechos humanos, a través de su directora de crisis **Lama Fakih**, documentó en 2021 que el Alto Comisionado había recogido datos biométricos de refugiados rohinyás en Bangladesh y que se habían compartido unos **830.000 nombres** con Myanmar —el Estado del que habían huido— sin un consentimiento libre e informado; 23 de 24 refugiados entrevistados creían que sus datos solo servirían para la tarjeta de ayuda [7]. Como advierte la ONG **Privacy International**, acumular biometría de poblaciones en conflicto es facilitar la vigilancia, y cuando aquellos datos llegan al país del que huyes, pueden ser una condena.

Probar la entrega sin crear un honeypot

Es aquí donde **t2p** ofrece una alternativa con una filosofía opuesta: probar la entrega **sin construir una base biométrica central** que se convierta en un objetivo.

El mecanismo, en el punto de entrega, es el siguiente. Se genera un **recibo de entrega** —beneficiario con un identificador anónimo, importe, lugar, hora, agente— del que se calcula la **huella SHA-512** en el dispositivo, se ancla a la **blockchain pública** y se le añade un **sello de tiempo RFC 3161** y **GPS forense**. El resultado es un **.asice verificable sin conexión**: la prueba de que *este* beneficiario recibió *esta* ayuda en *este* lugar y *esta* hora, auditable por el donante sin tener que creerse la palabra del ejecutor —exactamente lo que habría delatado el fraude del Congo. Para confirmar que hay una persona viva y que consiente, en lugar de un escáner de iris central se usa la **prueba de vida en el dispositivo**: la plantilla biométrica no hace falta que salga del teléfono ni se acumule en ningún servidor.

Y la pieza más elegante resuelve el dilema de la desduplicación. Un equipo de la Escuela Politécnica Federal de Lausana, liderado por la criptógrafa **Carmela Troncoso** y en colaboración con el Comité Internacional de la Cruz Roja, diseñó un sistema llamado **Janus** que detecta el doble registro **sin crear ninguna base de datos biométrica en claro**: revela un solo bit de información —«ya registrado» o «nuevo»— mediante cálculo seguro [10]. Es la demostración de que se puede impedir el fraude de beneficiarios fantasma sin convertir a los refugiados en una población fichada. La cadena pública guarda *pruebas de unicidad*, no identidades.

Y aquí, más que en ningún sitio, hay que decir el límite sin adornos. La prueba de existencia demuestra **integridad, hora, lugar y presencia de la persona**, pero **no la verdad de lo que pasa después**. Si un actor armado obliga al beneficiario a entregar el efectivo una vez cobrado —el caso de Yemen—, o si el personal corrupto controla el dispositivo —el caso del Congo—, la cadena registrará una entrega «válida» que fue desviada: «basura a la entrada, basura en la cadena». Y todavía hay un límite más profundo: **cualquier registro biométrico de gente extremadamente vulnerable es vigilancia**. t2p reduce el riesgo de honeypot, pero no elimina el dilema del poder y del consentimiento. A veces, la opción más segura para los más débiles no es perfeccionar la biometría, sino **minimizarla**.

La promesa y el peligro

La promesa es profundamente humana. Una capa de prueba de entrega independiente y verificable daría a los donantes la certeza de que su dinero llega, impediría el fraude de recibos inflados y beneficiarios fantasma, y —si se diseña con la lógica de Janus— lo haría **sin** crear las bases de datos biométricas que hoy ponen en peligro a los refugiados. En un sector donde cada dólar desviado es una comida que alguien no come, la integridad de la entrega es, literalmente, una cuestión de vida.

El peligro, que en este capítulo va por delante, es olvidar que la tecnología toca a los más indefensos. Ningún sistema ha de poder ser una herramienta de vigilancia contra quien huye; ningún consentimiento arrancado «si quieres comer» es libre; y ningún sello detiene la bala de un actor armado ni la mano de un funcionario corrupto que controla el aparato. La prueba de existencia es una herramienta al servicio del principio humanitario de «no hacer daño», no una excusa para fichar al vulnerable.

Además, la trazabilidad permanente de una población ya vulnerada puede transformarse en un activo negociable: cada movimiento registrado, cada huella digital, se convierte en una pieza de «materia prima gratuita» que empresas e intermediarios pueden empaquetar para mercados de análisis predictivo. Shoshana Zuboff ya advertía este fenómeno, señalando cómo la experiencia humana es arrebatada y vendida sin ninguna compensación al sujeto [11]. Si el registro de distribución se convierte en una base de datos persistente, los mismos patrones que garantizan transparencia podrían ser reutilizados para perfiles de consumo o incluso para predicción de eventos sociales, alimentando un mercado clandestino de «datos de vulnerabilidad». Para evitar esta mercantilización, hay que establecer salvaguardas explícitas que prohíban la venta o la enajenación de cualquier registro de envío humano, más allá del simple control de procesamiento en el dispositivo. La regulación ha de extenderse a la propiedad y al uso secundario de los datos, tal como la FTC hizo en 2024 prohibiendo por primera vez la venta de datos de localización sensibles, y como la DPA neerlandesa sancionó a Clearview AI con una multa de 30,5 millones de euros por una base biométrica masiva [12]. Esto asegura que la prueba de existencia siga sirviendo únicamente al principio humanitario de «no hacer daño», sin abrir la puerta a un nuevo modelo de negocio basado en la vulnerabilidad.

Es hora de actuar

Para los donantes: exigir una prueba de entrega independiente y verificable, para que cada dólar llegue a una persona real y no a una SIM robada. Para las agencias (WFP, ACNUR, ONG): aplicar la desduplicación sin honeypot al estilo de Janus y minimizar la biometría, con consentimiento realmente libre y alternativas no biométricas. Para los organismos de privacidad y estándares: hacer del «no hacer daño» y de la minimización de datos un requisito, no una recomendación. Y para todos: recordar que en la ayuda, más que en ningún sitio, la pregunta no es solo «¿llega?», sino «¿llega sin convertir a quien la recibe en un sospechoso permanente?».

Una madre congoleña se endeudó esperando una ayuda que el fraude le robó. Dar a cada entrega una prueba independiente —y hacerlo sin fichar a quienes ya lo han perdido todo— es, en este frente que toca la dignidad humana, **time2act**.

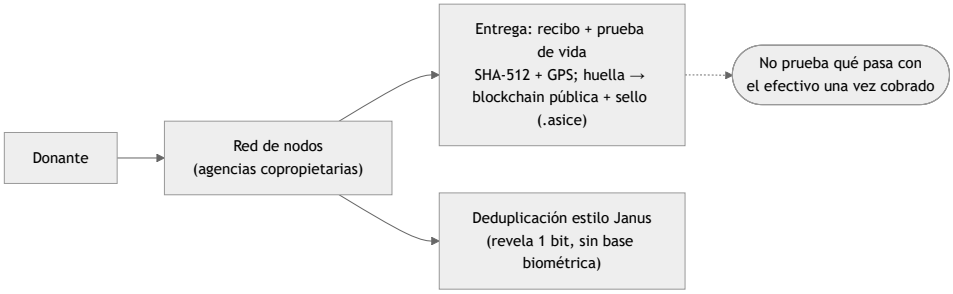


Figura 49.1 — En el punto de entrega, un recibo de entrega (beneficiario anónimo, importe, lugar, hora) se sella con huella SHA-512, sello de tiempo eIDAS y GPS forense, en un contenedor .asice verificable sin conexión; la prueba de vida en el dispositivo confirma una persona viva sin escáner central; y la desduplicación al estilo Janus revela solo un bit («ya registrado» o «nuevo»), sin crear ninguna base biométrica. Impacto real: en Ucrania se evitaron ~35 M$ de ayuda duplicada. Límite: no prueba qué pasa con el efectivo una vez cobrado (Yemen, Congo). Fuentes: WFP; EPFL/CICR (Janus); Human Rights Watch.

---

[1] WFP — *Building Blocks* (~555 M$ en transferencias; ~6 M de personas; Ucrania: 337 M$ coordinados, ~35 M$ de solapamiento evitado; 159 organizaciones en 2025). https://www.wfp.org/building-blocks ↩

[2] UN Innovation Network — *How the Building Blocks blockchain network is transforming humanitarian aid* (>1 M de refugiados cada mes). https://www.uninnovation.network/blog/how-the-building-blocks-blockchain-network-is-transforming-humanitarian-aid ↩

[3] MIT Technology Review — *Inside the Jordan refugee camp that runs on blockchain* (EyePay; Bassam; –98 % de comisiones). https://www.technologyreview.com/2018/04/12/143410/inside-the-jordan-refugee-camp-that-runs-on-blockchain/ ↩

[4] UNHCR — *UNHCR's Biometric Tools in 2023* (base de 15,7 M de personas; PRIMES/BIMS). https://www.unhcr.org/blogs/unhcrs-biometric-tools-in-2023/ ↩

[5] Development Initiatives — *Cash and Voucher Assistance* (~10,6 mil M$ en 2022 → 9,7 mil M$ en 2023; WFP, mayor proveedor). https://devinit.org/resources/falling-short-humanitarian-funding-reform/cash-voucher-assistance/ ↩

[6] CALP Network — *The State of the World's Cash 2023*. https://www.calpnetwork.org/collection/the-state-of-the-worlds-cash-2023-report/ ↩

[7] Human Rights Watch — *UN Shared Rohingya Data Without Informed Consent* (Lama Fakih; ~830.000 nombres compartidos con Myanmar). https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent ↩

[8] UN News — *Yemen: WFP pauses food distributions* (disputa biométrica con los hutíes, 2019-2023). https://news.un.org/en/story/2023/12/1144417 ↩

[9] GiveDirectly / The New Humanitarian — *DRC mobile-cash fraud* (~1,2 M$ desviados; ~1.900 familias). https://www.givedirectly.org/drc-case-2023/ ↩

[10] Carmela Troncoso et al. (EPFL SPRING Lab, con el CICR) — *Janus: Safe Biometric Deduplication for Humanitarian Aid Distribution* (IEEE S&P 2024; revela solo un bit, sin base biométrica). https://arxiv.org/abs/2308.02907 ↩

[11] Shoshana Zuboff — *La era del capitalismo de la vigilancia* (Paidós, 2020). ↩

[12] FTC (2024); Autoriteit Persoonsgegevens / EDPB (2024). https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en ↩

La ayuda en especie: la cadena de custodia del socorro

«Ser hombre es precisamente ser responsable. […] Es sentir, al colocar tu piedra, que contribuyes a construir el mundo.»

— Antoine de Saint-Exupéry, Tierra de hombres (1939)

El 24 de junio de 2026, a las 18:04 hora local, un seísmo de magnitud 7,2 sacude Venezuela desde cerca de San Felipe, en el estado de Yaracuy. Treinta y nueve segundos después llega un segundo, de magnitud 7,5. Edificios enteros caen en Caracas, La Guaira y Caraballeda; el aeropuerto internacional Simón Bolívar suspende las operaciones; las redes móviles se saturan. Al cierre de este capítulo, el balance es abrumador: más de 3.300 muertos, más de 16.800 heridos, decenas de miles de desaparecidos [1]. Y el mundo responde como sabe: más de 30 países, más de 3.600 rescatistas, más de 1.000 toneladas de ayuda. El Salvador amplía su contingente de 150 a 300 rescatistas y de 50 a 150 toneladas; Brasil envía 36 bomberos y seis perros de búsqueda; el chef José Andrés dona un millón de dólares y viaja al país con World Central Kitchen; Rosalía dona dos a UNICEF; Metallica, 100.000 [1][2].

Y entonces empieza la segunda pregunta, la que este libro no puede esquivar: todo esto —las toneladas, los palés, los contenedores— ¿llegará a quien lo necesita? Porque mientras los equipos de rescate todavía excavan entre los escombros, ya hay denuncias documentadas de suministros retenidos por funcionarios policiales en Altamira, de centros de acopio civiles prohibidos por alcaldes que limitan la recogida a la sede de su partido, de distribuciones impedidas [1]. La generosidad del mundo ha empezado el viaje; lo que este capítulo pregunta es si el viaje se puede auditar.

Este capítulo trata la ayuda en especie: las cosas —alimentos, medicinas, tiendas, generadores— que viajan del donante a la víctima por mar, por aire y por tierra. La entrega de ayuda en efectivo y la desduplicación de beneficiarios están en el capítulo 49; el trayecto del dinero del donante —«a dónde va mi euro»—, en el capítulo 73; el origen verificable de los productos comerciales, en el capítulo 29; el fraude documental del comercio internacional, en el capítulo 54; la posición real de los barcos, en el capítulo 103; la cronología de las emergencias, en el capítulo 105. Pregunta clave: ¿cómo se sabe que un palé que sale de un depósito de Panamá llega entero a una familia de La Guaira? Respuesta: haciendo que cada eslabón del trayecto —el manifiesto, el barco o el avión, la aduana, el almacén, el convoy, el punto de reparto— deje su prueba de existencia con **t2p**: la huella SHA-512 calculada en el dispositivo, el anclaje de la huella en la blockchain pública y el sello de tiempo RFC 3161/eIDAS complementario, dentro de un contenedor .asice [11]. Y con la neutralidad de siempre: el mismo rastro que delata el desvío protege a la ONG honesta y a la autoridad diligente de la acusación falsa. La prueba sirve a las dos direcciones.

Los precedentes: cuando la confianza se rompió

Los fraudes que han marcado el sector no son leyendas: están documentados, a menudo por las propias organizaciones. Conviene mirarlos de frente, porque dibujan el mapa exacto de dónde se rompe la cadena.

En noviembre de 2017, la Federación Internacional de la Cruz Roja (IFRC) reconoció públicamente que el fraude se había llevado al menos 6 millones de dólares de los más de 124 que había gestionado durante la epidemia de Ébola (2014-2016), la crisis que mató a más de 11.000 personas en el África occidental. El desglose es una lección de logística oscura: en Sierra Leona, unos 2,13 millones desaparecieron por «probable colusión» entre personal propio y un banco local que fijaba el tipo de cambio en el pico de la epidemia; en Guinea, unos 1,17 millones se perdieron en la facturación fraudulenta de un proveedor de despacho aduanero; en Liberia, unos 2,7 millones se evaporaron en precios inflados de artículos de socorro, nóminas e incentivos de voluntarios [5]. La honestidad merece ser dicha: fue la propia Federación quien lo destapó y quien se declaró dispuesta a renunciar a inmunidades para perseguir a los responsables [5].

Somalia, 2010: el Grupo de Monitoreo de la ONU informó de que «hasta la mitad» de la ayuda alimentaria del Programa Mundial de Alimentos se desviaba hacia una red de contratistas corruptos, milicias y personal local, y señaló a la familia Adaani —uno de los tres grandes contratistas del programa— como financiadora de grupos armados. El WFP lo negó en redondo: «no se nos ha presentado ninguna evidencia», dijo su directora ejecutiva, Josette Sheeran, y una auditoría propia no encontró nada [6]. Y aquí está la lección probatoria central de este capítulo: la disputa era irresoluble. Sin registros de custodia

verificables, ni la acusación podía probar el desvío ni la defensa podía probar la inocencia —y la duda se comió la confianza igualmente, en ambas direcciones.

Y España, 2007: según la Fiscalía Anticorrupción, los directivos de Intervida —una de las grandes ONG de apadrinamiento del país— desviaron más de 45 millones de euros camuflados como «gastos por apadrinamiento»; cuando la investigación se hizo pública, unas 10.000 personas se dieron de baja como donantes. Aquel mismo abril, el presidente de Anesvad era detenido, denunciado por los trabajadores de su propia organización, acusado de apropiación indebida de fondos [7]. El sector entero pagó la factura de confianza.

El patrón común es lo que importa: el agujero nunca está en la foto de la llegada del barco, ni en la del reparto con las cajas bien apiladas. Está en los eslabones oscuros del medio —el cambio de divisas, el despacho aduanero, el contratista local, la contabilidad entre el origen y el destino. (El caso más célebre de todos, los 500 millones de dólares que la Cruz Roja americana recaudó para Haití, pertenece al lado del donante y se explica en el capítulo 73.)

La segunda catástrofe

Después de un desastre, la ayuda se puede perder de tres maneras documentadas —y Venezuela, por una amarga coincidencia, las ilustra las tres.

La primera es **el desvío y la captura política**. El paradigma verificado es el programa CLAP: las cajas de comida subvencionadas que el gobierno venezolano creó en 2016 y que se convirtieron en un vehículo de corrupción a gran escala. Según las investigaciones, el empresario Alex Saab y su socio montaron una estructura para comprar alimentos en el extranjero con sobreprecios de hasta 30 dólares por caja —unos 360 millones de dólares defraudados en dos años, a través de sociedades como Group Grand Ltd, que suministró más de 11,5 millones de cajas. El Tesoro de EE. UU. sancionó la red en julio de 2019 por «robar al programa de distribución de alimentos»; un análisis de laboratorio encontró que la leche de las cajas tenía una composición nutricional inferior a la etiquetada; y la comida se usó como instrumento de control social —premiar a afines, castigar a opositores [3]. Con este historial, las denuncias de suministros retenidos y centros de acopio capturados después del terremoto [1] no son una sorpresa: son la misma lógica en versión de emergencia.

La segunda es **el bloqueo**. En febrero de 2019, la ayuda llegada a Cúcuta, en el lado colombiano de la frontera, se encontró el puente de Tienditas cerrado con un camión cisterna y dos contenedores soldados entre sí; el 23 de febrero, catorce camiones con 280 toneladas de alimentos intentaron pasar —dos acabaron quemados en los incidentes, ninguna carga entró, y la frontera se cerró del todo [4]. Hay que decirlo con la neutralidad que este libro se debe: aquel envío era también un instrumento en plena disputa política, y el gobierno alegaba que la «ayuda» encubría otros fines. La lección probatoria no es quién tenía razón; es que, sin un registro neutral y verificable del contenido de aquellos camiones, cada bando tenía su relato —y el ciudadano, ninguna manera de saberlo. La prueba de existencia habría servido exactamente igual para demostrar que la carga era lo que decía ser, o que no lo era.

Y la tercera es el **«segundo desastre»**. No todo lo que se pierde, se roba: mucho se despilfarra. Según el experto en logística humanitaria José Holguín-Veras, entre el 50 y el 70 % de los bienes que llegan en una emergencia no son necesarios ni apropiados; las donaciones no solicitadas colapsan pistas de aeropuerto, refugios y almacenes, y drenan a los voluntarios que deberían hacer cosas más útiles —hay documentado el caso de un avión que descargó toneladas de juguetes en la pista de un aeropuerto en plena emergencia, donde quedaron meses [8]. El corolario honesto, coherente con el capítulo 49: la mejor donación particular suele ser el donativo económico. Pero la ayuda en especie institucional —los stocks preposicionados, las cargas de agencia— existirá siempre, y es exactamente la que necesita custodia.

Por mar, por aire, por tierra: los eslabones

La maquinaria real de la ayuda en especie es más sofisticada de lo que parece desde fuera. La red UNHRD, gestionada por el Programa Mundial de Alimentos, mantiene depósitos humanitarios preposicionados en Brindisi, Accra, Kuala Lumpur, Ciudad de Panamá y Dubái, con kits médicos, material de refugio y alimentos listos para ser despachados en 48 horas para muchas organizaciones a la vez; y cuando estalla una crisis, el Clúster Logístico liderado por el WFP coordina las cadenas de suministro humanitarias y llena los vacíos comunes —transporte compartido, almacenes, rutas [9].

Sigamos ahora un palé concreto. En el depósito de origen se empaqueta y se emite la documentación: el manifiesto, la lista de contenido. El palé sube a un barco o a un avión. Llega a un puerto o a un aeropuerto —en el caso venezolano, con el aeropuerto principal suspendido los primeros días [1], cada vía alternativa cuenta. Pasa el despacho aduanero. Entra en un almacén nacional. Sale en camiones, a menudo en convoy, hacia el interior. Y acaba, si todo va bien, en un punto de reparto donde alguien lo convierte en paquetes para familias.

El diagnóstico probatorio: cada flecha de este trayecto es un cambio de manos, y cada cambio de manos sin registro verificable es un lugar donde las cosas «se pierden», se reetiquetan, se revenden o se reparten por criterios que no son la necesidad. Papeles, los hay —manifiestos, albaranes, actas de recepción—, pero son papeles de cada parte: modificables, extraviables, contradictorios. Cuando llega el escándalo, como en Somalia [6], no hay manera de reconstruir la verdad; cuando llega el fraude, como en el despacho aduanero de Guinea [5], la facturación fraudulenta se confunde con la legítima. Lo que falta no son más papeles: es que los papeles tengan fecha cierta, autor cierto y una integridad que un tercero pueda verificar sin pedir permiso a nadie.

La prueba de existencia aplicada

El mismo palé, la misma cadena —y en cada eslabón, treinta segundos de un gesto con el móvil [11].

1. El contenedor con pedigrí

En el depósito de origen, el responsable abre t2p, gira la rueda de modos hasta Documento y escanea el manifiesto y la lista de contenido: el escáner detecta los bordes, corrige la perspectiva y admite hasta 50 páginas en un único PDF; un toque en «Certificar en la blockchain» y la huella SHA-512 —calculada en el dispositivo, de los bytes exactos del archivo— recibe su sello de tiempo RFC 3161/eIDAS y queda anclada a la blockchain pública, con el certificado PDF y su código QR generados automáticamente [11]. Desde este instante, qué contiene el palé y cuándo ha salido es un hecho con fecha cierta: el «faltaban cajas» y el reetiquetado posterior se contrastan contra la huella de origen. Es el pedigrí del capítulo 29, aplicado al socorro; y el manifiesto sellado dialoga con los documentos del comercio del capítulo 54.

2. La aduana y el almacén

En cada cambio de manos —la descarga en el puerto, el despacho aduanero, la entrada y la salida del almacén— una foto o un escaneo del acta con t2p. La barra de GPS forense muestra en vivo la calidad de la ubicación: para que la coordenada se selle con grado forense hace falta un fijado GPS genuino, con precisión de unos 50 metros y una antigüedad máxima de unos 30 segundos; una ubicación simulada es la única condición que bloquea la certificación del todo, y si no hay señal se puede capturar igualmente —el certificado registra honestamente que no se incrustó coordenada, y por qué [11]. El resultado es una cronología anclada de entradas y salidas donde los vacíos quedan fechados: el palé que entró el lunes y nunca salió deja de ser una niebla para convertirse en una pregunta concreta a una persona concreta. El fraude aduanero de Guinea [5] habría dejado exactamente este rastro.

3. El convoy

Los camiones salen con la carga fotografiada —y filmada, si hace falta, con la superposición de fecha y hora activada [11]— y en ruta se hacen capturas puntuales con GPS forense. El detalle operativo que importa en una zona de desastre: la certificación de t2p trabaja en segundo plano y, si no hay cobertura, la cola se reanuda sola cuando vuelve la conexión —se captura ahora, se certifica cuando se puede, y el sello acredita el momento de la captura [11]. El convoy que se desvía, el remolque que cambia de contenido, la carga que «se redistribuye» en un control de carretera: todo topa con una cadena de capturas ancladas que nadie puede reescribir. La posición real de los barcos que llevan la ayuda grande, por cierto, es la materia del capítulo 103.

4. El reparto

En el punto final, el círculo se cierra en las dos direcciones. Hacia abajo: el reparto se documenta con recibos que no exponen a los vulnerables —la lógica del capítulo 49: identificadores anónimos, ninguna base de datos biométrica centralizada. Hacia arriba: el responsable local firma la recepción con la firma más fuerte de t2p —la cámara frontal graba, la app plantea dos retos de vida aleatorios (girar la cabeza, sonreír), la verificación biométrica del dispositivo confirma, y aparece «IDENTIDAD VERIFICADA» [11]—

verificada en el sentido que el capítulo 88 precisa: una persona real y presente, con la cuenta y la biometría del dispositivo, no un nombre en un registro civil. Y la ONG exporta el paquete de evidencia .asice —un contenedor estándar (ETSI EN 319 162) con la copia byte a byte, el certificado, el sello de tiempo y las instrucciones de verificación— que el auditor del donante, a diez mil kilómetros, puede verificar sin conexión, sin la app y sin tener que confiar en nadie [11].

Los límites, con la misma franqueza: el sello acredita hechos logísticos —qué, cuándo, dónde, quién firma —, no bondad. Una caja con leche por debajo del etiquetado [3] se puede certificar perfectamente: para la calidad hacen falta análisis y auditorías, no solo huellas. Ningún sello levanta un contenedor soldado en un puente [4] ni desarma a quien retiene la ayuda por la fuerza. Y el rastro es proporcional: se documenta la carga y el trámite, nunca las personas que reciben —aquí manda el capítulo 49.

La promesa y el peligro

La promesa: el donante que puede seguir su palé eslabón a eslabón; la disputa de Somalia [6], resoluble en horas contra registros en lugar de irresoluble para siempre; la ONG honesta que responde al próximo escándalo con evidencia en lugar de comunicados. Y el sector ya camina en esta dirección: StaTwig traza viales de vacunas del depósito al centro de salud con el apoyo de UNICEF, la IFRC ha pilotado blockchain con las Cruces Rojas irlandesa y libanesa, y el WFP explora la trazabilidad de alimentos de origen a destino [10]. Lo que añade t2p es la capa neutral y transversal: la misma herramienta para la agencia grande y para la ONG pequeña, sin infraestructura propia [11].

Los peligros, con la misma seriedad.

El primero es **la vigilancia de los más vulnerables**. Este capítulo hereda, entero, el peligro del capítulo 49: el rastro es para la carga y los trámites, nunca para convertir a las víctimas en fichas. Ninguna biometría centralizada, ninguna lista de beneficiarios expuesta, ninguna condición de «si quieres comer, regístrate». Se documenta el palé, no la persona que lo abre.

El segundo es **el sello que no detiene tanques**. Tienditas [4] lo dice todo: ninguna huella desmonta un contenedor soldado. La prueba de existencia hace el bloqueo y el desvío visibles y fechados —y eso es mucho: convierte el rumor en expediente—, pero la respuesta a un bloqueo armado es política y diplomática. Vender criptografía como solución de un puente cerrado sería mentir.

El tercero es **la criminalización de quien documenta**. En entornos hostiles, fotografiar un almacén o un control de carretera puede costar una detención, o cosas peores. El diseño protege a quien certifica —solo huellas en la cadena, contenido en el dispositivo, revelación voluntaria [11]—, pero ningún protocolo ha de obligar al trabajador humanitario a elegir entre el rastro y su seguridad. La captura se hace cuando es seguro hacerla; el sello acredita el momento, no exige el heroísmo. Y cuando el entorno hostil es directamente una guerra —cuando quien documenta es el periodista al que no dejan entrar, o la víctima que graba con el móvil lo que le está pasando—, este dilema llega a su extremo: volvemos de lleno a él en el capítulo 113.

Y el cuarto es **el tecnosolucionismo logístico**. El sello no cura el «segundo desastre»: si el 50-70 % de lo que llega no hace falta [8], certificarlo solo documenta el despilfarro con más precisión. La custodia verificable funciona dentro de una logística profesional —la de los depósitos y el clúster [9]— y con la donación correcta, que a menudo es dinero [8]. Y la neutralidad final: el mismo rastro que delata al funcionario corrupto exonera al diligente. Si solo sirve para acusar, morirá; si sirve para demostrar, se adoptará.

Es hora de actuar

Que la generosidad viaje con su prueba.

Para los donantes —personas, empresas, gobiernos: exigid la cadena de custodia verificable como condición de la donación en especie; y si sois particulares, recordad que a menudo la mejor ayuda es el donativo económico a organizaciones con rastro [8][11].

Para las ONG y agencias: sellad el manifiesto en el origen, el acta en cada cambio de manos y la recepción en el punto final [11]; publicad por huella, no por nota de prensa —el próximo escándalo lo responderéis con registros [5][6].

Para el clúster logístico y los organismos ONU: incorporad el anclaje neutral a los estándares de la cadena humanitaria —manifiesto, despacho, almacén, reparto [9][10]— para que el rastro viaje con el palé entre organizaciones.

Para las aduanas y los gobiernos receptores: despacho de emergencia con actas ancladas —vuestra diligencia quedará tan fechada como cualquier abuso [5]; y ningún requisito que convierta el rastro en herramienta de control de quien ayuda.

Para los transportistas y las navieras: carga documentada a la salida y a la llegada [11]; vuestra protección contra la acusación de desvío es el mismo rastro.

Para los legisladores y reguladores de la cooperación: valor probatorio a la custodia anclada en la justificación de subvenciones; y protección legal explícita para quien documenta [7].

Mientras se escribe este capítulo, todavía salen palés hacia Venezuela. Que cada uno lleve su pedigrí —y que dentro de un año el donante, la familia y el juez puedan responder la misma pregunta con la misma evidencia: qué había, dónde pasó, a quién llegó. Para que el socorro llegue entero, **time2act**.



Figura 50.1 — La cadena de custodia del socorro con prueba de existencia (t2p: huella SHA-512 en el dispositivo, sello RFC 3161/eIDAS, blockchain pública, .asice): el manifiesto sellado en el origen (escáner de hasta 50 páginas), las actas de aduana y almacén con GPS forense (fijado genuino ~50 m / ≤30 s; la ubicación simulada bloquea la certificación), el convoy con capturas reanudadas al recuperar cobertura, y la recepción firmada con vídeo-selfie y retos de vida —exportable como paquete .asice verificable sin conexión por el auditor del donante. Límites: el sello no acredita la calidad del contenido, no levanta bloqueos y nunca ficha a las víctimas. Fuentes: IFRC (fraude Ébola autodivulgado); ONU/WFP (Somalia 2010); OFAC (red CLAP); terremoto de Venezuela 2026.

---

[1] Wikipedia (ES) — *Terremotos de Venezuela de 2026* (doblete M7,2 San Felipe + M7,5 Yumare, 24-6-2026, 39 s de diferencia; >3.342 muertos, >16.840 heridos, >68.000 desaparecidos; aeropuerto Simón Bolívar suspendido; conflictos de distribución: suministros retenidos en Altamira, centros de acopio civiles prohibidos en Charallave y Campo Elías, distribución impedida en El Limón, acceso restringido en La Guaira; respuesta: >30 países, >3.600 rescatistas, >1.000 toneladas); ReliefWeb — *Terremoto en Venezuela: panorama de la situación (25-6-2026)*; SkyAlert — *Actualización del terremoto en Venezuela*. https://es.wikipedia.org/wiki/Terremotos_de_Venezuela_de_2026 · https://reliefweb.int/report/venezuela-bolivarian-republic/terremoto-en-venezuela-panorama-de-la-situacion-25-de-junio-de-2026 · https://skyalert.mx/articulos/actualizacion-sismos-venezuela-2026 ↩

[2] Ayuda en Acción — *Terremotos en Venezuela: qué ha pasado y situación actual* (contexto humanitario; donaciones: José Andrés/World Central Kitchen 1 M$, Rosalía 2 M$ a UNICEF, Metallica 100.000 $). https://ayudaenaccion.org/blog/ayuda-humanitaria/terremotos-venezuela/ ↩

[3] Departamento del Tesoro de EE. UU. — *Treasury Disrupts Corruption Network Stealing From Venezuela's Food Distribution Program (CLAP)* (25-7-2019; red de Alex Saab; Group Grand Ltd; sobreprecios); Voz de América — *¿Qué son los CLAP y qué tienen que ver con Alex Saab?*; InsightCrime — *How Criminals Take Advantage of Venezuela's Food Aid System*; Excélsior — *Despensas CLAP, una red de corrupción* (~12 M cajas desde México, ~30 $/caja de sobreprecio, ~360 M$; leche por debajo de etiquetado — Armando.Info). https://home.treasury.gov/system/files/136/2019-07-25-Venezuela-Alex-Saab-Network-SPANISH-TRANSLATION.pdf · https://www.vozdeamerica.com/a/que-son-los-clap-y-que-tienen-que-ver-con-alex-saab-/6277181.html · https://insightcrime.org/news/criminals-take-advantage-venezuelas-food-aid-system/ · https://www.excelsior.com.mx/internacional/despensas-clap-red-corrupcion-maduro-larga-historia ↩

[4] Wikipedia (ES) — *Envío de ayuda humanitaria en Venezuela de 2019* (puente de Tienditas bloqueado con cisterna y contenedores; 23-2-2019: 14 camiones/280 toneladas, 2 camiones quemados; cierre de frontera); CNN en Español — *Venezuela bloquea puente en frontera con Colombia* (6-2-2019); Infobae — *Maduro ordenó retirar los contenedores del puente Tienditas* (dic. 2022). https://es.wikipedia.org/wiki/Env%C3%ADo_de_ayuda_humanitaria_en_Venezuela_de_2019 · https://cnnespanol.cnn.com/2019/02/06/venezuela-bloquea-puente-en-frontera-con-colombia · https://www.infobae.com/america/venezuela/2022/12/14/tras-impedir-el-paso-de-la-ayuda-humanitaria-en-2019-maduro-ordeno-retirar-los-contenedores-del-puente-tienditas/ ↩

[5] NBC News — *Red Cross: $6 million for Ebola fight stolen through fraud* (nov. 2017; ≥6 M$ sobre >124 M$; Sierra Leona ~2,13 M colusión con banco sobre el tipo de cambio; Guinea ~1,17 M facturación fraudulenta de un proveedor de despacho aduanero; Liberia ~2,7 M precios inflados de artículos de socorro, nóminas e incentivos); IFRC/ReliefWeb — *IFRC statement on fraud in Ebola operations*; Newsweek — *Red Cross Loses $6 Million In Fraud During Ebola Crisis*. https://www.nbcnews.com/storyline/ebola-virus-outbreak/red-cross-6-million-ebola-fight-stolen-through-fraud-n817701 · https://reliefweb.int/report/sierra-leone/ifrc-statement-fraud-ebola-operations · https://www.newsweek.com/red-cross-outraged-6-million-fraud-loss-during-ebola-outbreak-702231 ↩

[6] UN News — *UN food agency welcomes review of its food distribution programme in Somalia* (2010; Grupo de Monitoreo: «hasta la mitad» desviada; contratistas/milicias/personal local; familia Adaani); VOA — *WFP Report says No Evidence of Food Diversion in Somalia* (negación del WFP — Josette Sheeran; auditoría propia sin evidencia); ODI — *Somalia food aid diversion*. https://news.un.org/en/story/2010/03/332792-un-food-agency-welcomes-review-its-food-distribution-programme-somalia ·

https://www.voanews.com/a/un-official-slams-report-on-somalia-food-diversion-89115947/153849.html · https://odi.org/en/insights/somalia-food-aid-diversion/ ↩

[7] IPS Noticias — *Corrupción-España: investigación de ONG refuerza transparencia* (2007; Intervida: >45 M€ desviados según la Fiscalía Anticorrupción, ~10.000 donantes de baja; Anesvad: presidente detenido el 5-4-2007 por apropiación indebida, denunciado por los trabajadores). https://ipsnoticias.net/2007/04/corrupcion-espana-investigacion-de-ong-refuerza-transparencia/ ↩

[8] Natural Hazards Center (Univ. Colorado) — *Avoiding the "Second Disaster" of Unwanted Donations* (convergencia material; donaciones no solicitadas colapsan pistas y almacenes); TED Ideas — *After a disaster, don't send toys or clothing — send money* (José Holguín-Veras: 50-70 % de los bienes que llegan no son necesarios ni apropiados; el caso del avión de juguetes). https://hazards.colorado.edu/news/research-counts/avoiding-the-second-disaster-of-unwanted-donations · https://ideas.ted.com/after-a-disaster-dont-send-toys-or-clothing-send-money-heres-why/ ↩

[9] WFP — *UN Humanitarian Response Depot (UNHRD)* (depósitos en Brindisi, Accra, Kuala Lumpur, Ciudad de Panamá y Dubái; despacho en 48 h; stocks para múltiples organizaciones); UNHRD — *Our Services*; World Economic Forum — *Logistics Emergency Team: 20 years* (Clúster Logístico liderado por el WFP). https://www.wfp.org/unhrd · https://unhrd.org/our-services · https://www.weforum.org/stories/global-cooperation/logistics-emergency-team-humanitarian-aid-20-years/ ↩

[10] UNICEF Office of Innovation — *Why blockchain is the future of humanitarian response* (StaTwig: trazabilidad de viales de vacunas del depósito al centro de salud); WFP Innovation Accelerator — *3 ways blockchain innovation is enhancing humanitarian work* (trazabilidad de alimentos; Building Blocks); LSE — *How Blockchain is Contributing to the Humanitarian Sector as of 2025* (piloto IFRC/AID:Tech con la Cruz Roja irlandesa y libanesa). https://www.unicef.org/innovation/stories/why-blockchain-future-humanitarian-response · https://wfpinnovation.medium.com/3-ways-that-blockchain-innovation-is-enhancing-humanitarian-work-e40dd3e85dee · https://blogs.lse.ac.uk/internationaldevelopment/2025/07/10/how-blockchain-is-contributing-to-the-humanitarian-sector-as-of-2025/ ↩

[11] t2p — manual de producto (rueda de modos; escáner de documentos hasta 50 páginas en un PDF; huella SHA-512 calculada en el dispositivo; certificación en segundo plano que se reanuda al recuperar cobertura; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; GPS forense —fijado genuino ~50 m / ≤30 s, la ubicación simulada bloquea la certificación; comprobación de integridad del dispositivo y attestation de hardware; superposición de fecha/hora en el vídeo; firma con vídeo-selfie, retos de vida y biometría; paquete de evidencia .asice ETSI EN 319 162 verificable sin conexión; solo huellas en la cadena). Véanse los capítulos 13 y 15; la entrega de efectivo y la desduplicación, en el capítulo 49; el euro del donante, en el capítulo 73. ↩

Fronteras y asilo: la evidencia de quien huye

«Perdimos nuestro hogar, que significa la familiaridad de la vida cotidiana. Perdimos nuestro oficio, que significa la confianza de ser de alguna utilidad en este mundo.»

— Hannah Arendt, «Nosotros, los refugiados» (1943)

La madrugada del 14 de junio de 2023, el pesquero Adriana —salido de Libia cinco días antes con unas 750 personas a bordo, la mayoría de Siria, Pakistán y Egipto, con niños— volcó y se hundió en aguas internacionales frente a Pylos, Grecia. Murieron más de 600 personas; sobrevivieron 104; se recuperaron 82 cuerpos [1]. La guardia costera griega negó toda responsabilidad: los migrantes habrían rechazado la ayuda, y el barco habría volcado solo. Las investigaciones de Human Rights Watch, de Amnistía Internacional y de decenas de periodistas apuntaron en otra dirección: errores graves en las horas previas y alegaciones serias de que la patrullera griega hizo volcar el Adriana al intentar remolcarlo [1][2]. Dos años después, en mayo de 2025, la justicia griega imputó a 17 miembros de la guardia costera, incluido el capitán de la patrullera, acusado de causar un naufragio con resultado de muerte de al menos 82 personas [3]. Mientras tanto, nueve supervivientes habían sido procesados —se enfrentaban a cadenas perpetuas— en medio de la denuncia de las organizaciones de derechos humanos, que advertían de que el juicio a los supervivientes no podía servir de escudo ante las responsabilidades de las autoridades [2].

Este capítulo trata la evidencia en las fronteras: los naufragios, las devoluciones sumarias y el procedimiento de asilo. La entrega de la ayuda humanitaria está en el capítulo 49; la evidencia de crímenes de guerra, en el capítulo 20; la identidad digital de quien no tiene papeles, en el capítulo 47; la posición real de los barcos, en el capítulo 103. Pregunta clave: ¿cómo se prueban los hechos cuando una de las partes lo ha perdido todo —a menudo hasta el teléfono— y la otra escribe el informe oficial? Respuesta: nivelando con prueba de existencia —el rastro sellado de quien huye, la documentación anclada de los observadores y los registros igualmente anclados de las autoridades (**t2p**: huella SHA-512, sello de tiempo RFC 3161/eIDAS, anclaje a la blockchain pública, contenedor .asice [5]). En la frontera, la neutralidad de la prueba no es una virtud abstracta: es la única manera de que la verdad no dependa de quien la cuenta.

Pylos: la versión oficial contra la reconstrucción

Vale la pena mirar de cerca cómo se reconstruyó la verdad de aquella noche, porque es una lección entera sobre la evidencia en las fronteras. La primera versión la puso quien tenía la radio y el informe: según la guardia costera, el Adriana navegaba por su cuenta y sus ocupantes no querían asistencia [1]. Contra esta versión no había, de entrada, nada más que 104 supervivientes traumatizados y un barco en el fondo del mar.

La reconstrucción llegó por convergencia de fuentes independientes, y costó meses de trabajo: periodistas y organizaciones cruzaron los datos de tráfico marítimo de las embarcaciones cercanas, los testimonios de los supervivientes —recogidos uno a uno— y el material de sus teléfonos, para contrastar la cronología oficial con la de los hechos [4]. De aquel periodismo forense, y de las investigaciones de Human Rights Watch y Amnistía Internacional, salieron las discrepancias que la instrucción griega acabaría recogiendo: horas sin rescate con el barco a la vista, y las alegaciones sobre el remolque fatal [1][2]. El resultado procesal tardó casi dos años: el 26 de mayo de 2025, la fiscalía presentó cargos contra 17 miembros de la guardia costera —el capitán de la patrullera ΠΠΛΣ-920, acusado de causar el naufragio; todos, de exponer a personas a peligro pese al deber legal de rescatarlas—, después de que una coalición de ONG jurídicas presentara querella en nombre de 40 supervivientes [3].

La lección probatoria es el núcleo de este capítulo: en un naufragio sin anclaje, la primera versión la pone quien tiene el informe, la reconstrucción tarda años, depende de heroicidades periodísticas [4] y llega cuando las portadas ya han pasado. Si las posiciones, las comunicaciones y las imágenes de aquella noche hubieran sido selladas en origen —las de la patrullera y las de los teléfonos de los pasajeros por igual [5]—, la cronología habría sido un hecho desde el primer día: qué hizo cada uno, cuándo, y a qué distancia. El capítulo 103 mostró cómo se falsifica la posición de un barco; aquí se ve lo que cuesta cuando nadie puede demostrar la suya.

La devolución que oficialmente no ocurrió

El segundo frente son las devoluciones sumarias —las expulsiones sin procedimiento que, oficialmente, no existen. El trabajo de documentarlas lo ha hecho durante años la sociedad civil: la Border Violence Monitoring Network, una coalición de más de doce organizaciones fundada en 2017, recoge testimonios de devoluciones ilegales y violencia en las fronteras de los Balcanes y Grecia; su «Black Book of Pushbacks» (2020) compilaba los testimonios de 12.654 personas, y la edición ampliada de 2022 supera las 3.000 páginas en cuatro volúmenes [6]. En estos miles de relatos, un detalle se repite con una regularidad estremecedora: la confiscación o destrucción de los teléfonos. La prueba de la víctima desaparece con su único testimonio.

Y en diciembre de 2025 llegó el giro jurídico. El Tribunal de Justicia de la UE (asunto C-136/24 P, sentencia del 18 de diciembre de 2025) resolvió el caso de un nacional sirio que alegaba que, después de desembarcar en una isla griega con la intención de pedir asilo, había sido detenido, despojado del teléfono y forzado a reembarcar hacia el mar hasta ser trasladado a Turquía —con Frontex presente en la operación. El Tribunal estableció que hay que adaptar la carga de la prueba: exigir pruebas concluyentes a víctimas en situación de extrema vulnerabilidad haría «ilusorio» el acceso a la justicia, y es Frontex —responsable de las operaciones— quien suele disponer de la documentación capaz de aclarar los hechos [7].

Leído con los ojos de este libro, el máximo tribunal europeo acaba de reconocer la asimetría probatoria como problema jurídico central —y de constatar que lo primero que se le quita a la víctima es, precisamente, su prueba. La respuesta estructural no puede ser solo procesal. Si los observadores sellan los incidentes en el momento [5][6], si el rastro de la víctima existe anclado antes de que le quiten el teléfono [5], y si los registros de las operaciones oficiales están igualmente anclados y son exigibles [7], la devolución «que oficialmente no ocurrió» se vuelve imposible de sostener —y la que de verdad no ocurrió, imposible de inventar. El sello no tiene bando: por eso puede funcionar en el territorio más polarizado de Europa.

El asilo: demostrar el miedo con lo que te queda

El tercer frente es el más silencioso. Quien pide protección internacional tiene que acreditar una persecución —la militancia, la amenaza, la detención, la agresión— con aquello que ha podido llevarse de una huida. Los documentos se pierden por el camino; los teléfonos se confiscan o se hunden [6][7]; los recuerdos se contradicen bajo el estrés; y la credibilidad del relato se convierte en el eje de toda la resolución. Es, probablemente, el procedimiento jurídico con más distancia entre lo que hay que probar y lo que se puede probar.

La prueba de existencia se aplica aquí desde el país de origen. Quien teme tener que huir puede sellar su rastro antes y durante: la amenaza recibida, la foto de la detención del hermano, el carné del partido, el artículo publicado —cada elemento con su huella SHA-512 y su fecha cierta, ancladas desde el primer momento [5]. Por el camino, puede anclar los momentos críticos sin publicar nada ni revelarse.

Y aquí es donde el diseño muestra su fuerza: si el teléfono se pierde en el mar o lo confiscan en la frontera [7], el contenido puede desaparecer —pero la existencia y la fecha del material quedan acreditadas para siempre. Recuperada una copia —de la nube, de un familiar, de una organización—, su integridad y su antigüedad se verifican contra la huella anclada. El relato de persecución deja de depender solo de la memoria: lleva anexos con fecha cierta.

El matiz imprescindible, dicho desde ya: el sello no hace cierto el contenido. Un documento falso sellado sigue siendo falso, y la valoración de credibilidad sigue correspondiendo a quien instruye. Lo que el sello hace imposible es la fabricación retroactiva —crear hoy «pruebas» fechadas de ayer—, que es exactamente la duda que envenena estos procedimientos y que ninguna entrevista puede resolver.

La prueba de existencia aplicada

Una frontera cualquiera, de noche. Tres relatos del mismo momento —el de quien huye, el de quien vigila, el de quien observa— y, por primera vez, ninguno de los tres se puede reescribir.

1. El rastro de quien huye

La persona que se prepara para pedir asilo sella en su dispositivo, desde el país de origen, la evidencia de su persecución [5]: cada documento, cada amenaza, cada foto, con huella y fecha cierta. Por el camino,

puede anclar los momentos críticos —dónde estaba, cuándo— sin publicar nada ni revelarse. Si le quitan el teléfono [7], la prueba no muere con él: solo la huella está en la cadena —nunca el contenido—, y espera la copia recuperable para acreditar su integridad y su antigüedad. En la entrevista de asilo, su relato lleva una cronología verificable que ningún instructor puede despachar como «fabricada para la ocasión».

2. El observador en la frontera

Las organizaciones que documentan incidentes fronterizos —el trabajo que el Black Book compila a posteriori [6]— pueden sellar cada testimonio y cada evidencia en el momento de recogerlos [5]: la fecha cierta del testimonio tomado al día siguiente de los hechos vale procesalmente mucho más que el mismo testimonio publicado dos años después en un informe. Es el modelo del capítulo 20 —la evidencia de derechos humanos con cadena de custodia— aplicado a la frontera europea: primero la huella, la publicación cuando sea seguro, y un archivo que los tribunales —que ya piden a Frontex su documentación [7]— puedan contrastar con la versión oficial.

3. La noche del naufragio, anclada

Un rescate marítimo con prueba de existencia: las posiciones, las comunicaciones y las imágenes de todas las embarcaciones —patrulleras, mercantes, barcos de ONG— selladas en tiempo real [5], en la línea de la integridad marítima del capítulo 103. Cuando llegue la disputa —¿hubo remolque? ¿cuándo se avisó? ¿quién estaba dónde?—, la cronología existirá desde el primer minuto: ni la instrucción necesitará dos años [3], ni la verdad dependerá de que 104 supervivientes puedan testificar contra un informe [1][4]. Quien actuó bien tendrá la mejor defensa posible; quien no, ninguna escapatoria narrativa.

4. La simetría que protege a todos

Hay que decirlo con toda la claridad: el anclaje también ampara a las autoridades. La patrulla acusada falsamente de una violencia que no ejerció, el agente que siguió el protocolo, la operación de rescate impecable —todos tienen en sus propios registros anclados la defensa definitiva [5]. Y las instituciones ganan con ello lo que más escasea en las fronteras: credibilidad. Una guardia costera con bitácoras selladas no necesita que la crean —puede demostrarlo.

Los límites, con la misma seriedad: el sello no decide quién tiene derecho a asilo ni qué política migratoria es justa —eso corresponde a las leyes y a los tribunales; no hace cierto el contenido de un documento, solo su existencia y fecha; no sustituye el testimonio humano ni la valoración de credibilidad; y en la frontera, la seguridad de las personas pasa por delante de la documentación —nadie ha de sellar nada que ponga en peligro a quien huye.

La promesa y el peligro

La promesa: fronteras donde los hechos tienen cronología desde el primer minuto [3][4], víctimas que no dependen de la memoria ni del teléfono que les quitaron [7], observadores con archivos inatacables [6] y autoridades que pueden demostrar su diligencia en lugar de solo afirmarla. El TJUE ha abierto la puerta jurídica [7]; la infraestructura de prueba es lo que puede atravesarla.

Los peligros, con la máxima seriedad.

El primero es **la vigilancia de los vulnerables**. Ninguna herramienta de evidencia puede convertirse en un registro de personas en movimiento. El rastro sellado es de la persona: en su dispositivo, solo huellas en la cadena, revelación voluntaria ante quien ella elija [5]. Cualquier deriva hacia bases de datos biométricas de migrantes sería la perversión exacta de lo que este capítulo propone —el libro ya lo ha advertido en los capítulos 47 y 49.

El segundo es **el sello como frontera nueva**. Si el asilo acabara exigiendo «cronología anclada o no te creo», habríamos levantado un muro probatorio contra los más desposeídos —quien huye de un bombardeo no sella nada. La prueba de existencia suma credibilidad a quien la tiene; su ausencia no puede restarla nunca. Esto ha de quedar escrito en las normas.

El tercero es **el peligro físico de la prueba**. Documentar puede matar. Un teléfono con evidencia sellada es un riesgo en un control hostil; los protocolos han de priorizar la seguridad —sellar y borrar el contenido local, recuperarlo después desde un lugar seguro— y ninguna organización ha de pedir a nadie que se convierta en mártir probatorio [5][6].

Y el cuarto es **la coartada tecnológica**. Ninguna huella rescata a nadie del mar. Las obligaciones de rescate, las vías legales y la política migratoria son decisiones humanas y políticas [1][2][7]; el sello solo garantiza que, después, la verdad sea recuperable. Que nadie venda criptografía donde hacen falta salvavidas.

Es hora de actuar

En la frontera, la verdad no puede depender de quien escribe el informe.

Para las personas que temen tener que huir: sella tu rastro —documentos, amenazas, hechos— desde ahora, en tu dispositivo [5]; si un día te quitan el teléfono [7], tu prueba te esperará.

Para las ONG y los observadores de fronteras: sellad testimonios y evidencias en el momento de recogerlos [5][6]; la fecha cierta multiplica el peso procesal de cada página de vuestros informes.

Para las operaciones de rescate y las guardias costeras: anclad bitácoras, posiciones y comunicaciones [5] —vuestra mejor defensa es una cronología que no se pueda discutir (capítulo 103).

Para Frontex y las instituciones europeas: el TJUE ya os señala como custodios de la documentación [7]; que esta documentación nazca anclada y sea exigible —la credibilidad de las fronteras europeas depende de ello.

Para los jueces y las oficinas de asilo: valorad la cronología sellada como soporte de credibilidad [7], y no convirtáis nunca su ausencia en presunción en contra.

Para los legisladores: escribid la regla de oro —la evidencia anclada suma, su ausencia no resta— y garantizad que ningún sistema de evidencia se convierta en registro de vigilancia de quienes huyen [5].

Más de 600 personas murieron frente a Pylos, y hubo que esperar casi dos años para que la instrucción apuntara hacia quienes tenían el deber de rescatarlas [1][3]. Que la próxima noche oscura en el mar tenga, desde el primer minuto, una cronología que nadie pueda reescribir. Por quienes solo llevan la verdad encima, **time2act**.

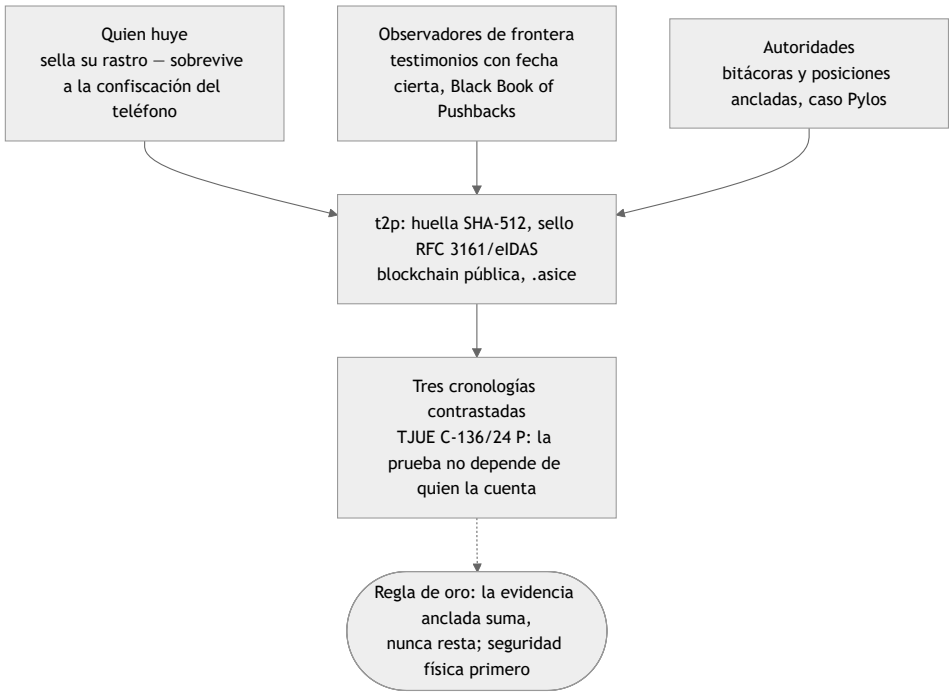


Figura 51.1 — Tres cronologías ancladas que se contrastan (huella SHA-512 en el dispositivo, sello de tiempo RFC 3161/eIDAS, blockchain pública, .asice): el rastro sellado de quien huye (sobrevive a la confiscación del teléfono; TJUE C-136/24 P), la documentación de los observadores (testimonios con fecha cierta; Black Book of Pushbacks) y los registros anclados de las autoridades (bitácoras y posiciones; el caso Pylos). La regla de oro: la evidencia anclada suma credibilidad; su ausencia nunca resta. Límites: ningún registro de personas, seguridad física primero, y el sello no decide el asilo ni la política migratoria. Fuentes: HRW/Amnistía (Pylos); RSA (imputación de 17 guardacostas); BVMN; TJUE C-136/24 P.

[1] Wikipedia — *2023 Pylos migrant boat disaster* (el Adriana; salida de Libia; ≈750 personas a bordo; más de 600 muertos; 104 supervivientes; 82 cuerpos; versión de la guardia costera); Human Rights Watch — *Greece: Disparities in Accounts of Pylos Shipwreck Underscore the Need for Human Rights Compliant Inquiry* (errores de las autoridades; alegaciones sobre el remolque). https://en.wikipedia.org/wiki/2023_Pylos_migrant_boat_disaster · https://www.hrw.org/news/2023/08/03/greece-disparities-accounts-pylos-shipwreck-underscore-need-human-rights-compliant ↩

[2] Amnistía Internacional — *Greece: Trial of Pylos shipwreck survivors must not be a shield in the investigation of the alleged responsibilities of the Greek authorities* (mayo de 2024; nueve supervivientes procesados; crítica de las organizaciones de derechos humanos). https://www.amnesty.org/en/latest/news/2024/05/greece-trial-of-pylos-shipwreck-survivors-must-not-be-a-shield-in-the-investigation-of-the-alleged-responsibilities-of-the-greek-authorities/ ↩

[3] Refugee Support Aegean — *Pylos Shipwreck: Criminal prosecution for felonies against 17 members of the Coast Guard* (26 de mayo de 2025; capitán de la ΠΠΛΣ-920 acusado de causar naufragio con resultado de muerte de al menos 82 personas; querella en nombre de 40 supervivientes). https://rsaegean.org/en/pylos-shipwreck-criminal-prosecution-for-felonies-to-17-members-of-the-coast-guard/ ↩

[4] Global Investigative Journalism Network — *How They Did It: Investigating the Pylos Shipwreck* (reconstrucción periodística con datos de tráfico marítimo, testimonios de supervivientes y material de sus teléfonos). https://gijn.org/stories/investigating-pylos-shipwreck/ ↩

[5] t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; solo huellas en la cadena; publicación opcional; recuperación de copias verificables contra la huella). Véanse los capítulos 13 y 15; la evidencia de derechos humanos, en el capítulo 20; la posición de los barcos, en el capítulo 103. ↩

[6] Wikipedia — *Border Violence Monitoring Network* (coalición de más de 12 organizaciones, fundada en 2017); Statewatch — *The 'Black Book of Pushbacks': testimonies of pushbacks affecting over 12,000 people* (diciembre de 2020; 12.654 personas); Balkan Insight — *Study Reports 25,000 Violent Pushbacks at EU Borders* (edición ampliada de 2022: más de 3.000 páginas, 4 volúmenes). https://en.wikipedia.org/wiki/Border_Violence_Monitoring_Network · https://statewatch.org/news/2021/january/eu-the-black-book-of-pushbacks-testimonies-of-pushbacks-affecting-over-12-000-people/ · https://balkaninsight.com/2022/12/08/study-reports-25000-violent-pushbacks-at-eu-borders/ ↩

[7] Iberley — *El TJUE refuerza la tutela judicial efectiva en casos de devoluciones sumarias de migrantes* (asunto C-136/24 P, sentencia de 18 de diciembre de 2025; nacional sirio despojado del teléfono y devuelto a Turquía con Frontex presente; adaptación de la carga de la prueba; Frontex como poseedora de la documentación). https://www.iberley.es/noticias/el-tjue-refuerza-tutela-judicial-efectiva-casos-devoluciones-sumarias-migrantes-35841 ↩

Testamentos y herencia: la última voluntad, demostrable

«No moriré del todo.»

— Horacio, Odas, III, 30 (23 a. C.)

Maureen Renny, una antigua directora de escuela inglesa, murió en enero de 2020 a los ochenta y dos años. Poco después apareció un testamento que lo dejaba todo a Leigh Voysey, una conocida suya, y que desplazaba un testamento anterior de 2016 a favor de sus familiares. El documento estaba «atestiguado» por dos amigas de Voysey. Era falso. Voysey había falsificado la última voluntad de Renny para reclamar una herencia de **4,2 millones de libras**, y apenas le hicieron falta dos testigos cómplices para fabricarlo. La justicia británica la condenó en 2024 por fraude y falsificación, y encarceló también a sus dos cómplices; la condena penal permitió a los herederos legítimos recuperar el patrimonio [1].

El caso contiene la dificultad singular de este capítulo, que ningún otro comparte: **cuando un testamento se disputa en los tribunales, la única persona que podría aclararlo —quien lo otorgó— ya está muerta**. Su voz se ha apagado para siempre, y el documento tiene que hablar por él. Este capítulo trata de cómo hacer que aquella voz, en el instante en que se expresa, quede grabada de manera que nadie la pueda falsificar ni silenciar.

La voluntad que nadie puede defender

Lo que está en juego es inmenso. La consultora Cerulli Associates ha calculado que en Estados Unidos se transferirán **84,4 billones de dólares** a herederos y causas benéficas de aquí a 2045, en la llamada «gran transferencia de riqueza» —la más grande de la historia [2]. Y sin embargo, la base sobre la que descansa esta transferencia es sorprendentemente frágil. Según el estudio anual de Caring.com, solo el **24 % de los adultos norteamericanos** tenía testamento en 2025, una cifra que ha bajado desde el 33 % de tres años antes [3]. Cuando no hay testamento, decide la ley; y cuando lo hay, empieza el problema de probar que aquel es el bueno.

Como hemos visto, en el Reino Unido las solicitudes de bloqueo de una herencia —los *caveats*— pasaron de 7.268 en 2019 a 11.362 en 2024, un aumento del 56 % en cinco años [4]. Los tres motivos clásicos para anular un testamento son siempre los mismos: la falta de **capacidad testamentaria** (el testador no estaba lúcido), la **influencia indebida** (alguien lo presionó) y la **falsificación** —exactamente lo que hizo Voysey [5]. Los testamentos ológrafos, escritos a mano, son los más vulnerables, porque a menudo no llevan fecha ni testigos que puedan declarar sobre el estado del testador en el momento de redactarlos.

El agujero de la herencia digital

A este problema antiguo, la era digital le añade uno nuevo. En diciembre de 2018, **Gerald Cotten**, fundador de la mayor casa de cambio de criptomonedas de Canadá, QuadrigaCX, murió a los treinta años durante un viaje a la India. Solo él conocía las contraseñas de las carteras frías de la empresa. Unos **137 millones de dólares** quedaron bloqueados para siempre, afectando a más de cien mil clientes; su viuda declaró bajo juramento que no había podido encontrar las claves escritas en ninguna parte [6]. No es un caso aislado: el análisis de Chainalysis estimaba en 2020 que cerca de un **20 % de los bitcoins** están perdidos y son irrecuperables, a menudo porque el titular muere sin compartir el acceso [7]. Como advierte la sección de derecho sucesorio de la **American Bar Association**, la persona media tiene más de cien cuentas en línea pero menos de una de cada cuatro tiene un plan para después de morir; sin las claves privadas, la criptomoneda queda «permanentemente bloqueada, sin ningún servicio de atención al cliente al que llamar» [8]. El patrimonio digital, literalmente, se entierra vivo.

Estonia lo vio primero

Hay un país que entendió todo esto antes que nadie. En 2012, cuando el resto del mundo todavía veía la cadena de bloques como una cosa de bitcoin, Estonia puso en producción el primer servicio estatal del planeta anclado en blockchain. No fue un banco ni una bolsa: fue el **Registro de Sucesiones**, el registro de testamentos de su Ministerio de Justicia [9]. Con la tecnología KSI de la empresa Guardtime,

desarrollada a raíz de los ciberataques de 2007, el sistema sella cada testamento anclando solo su huella —el documento nunca sale del servidor del Estado— de manera que cualquier alteración posterior queda detectada matemáticamente. Un pequeño país báltico decidió que el documento que más merece protección contra la manipulación es la última voluntad de sus ciudadanos. Tenía razón.

La prueba de existencia: la última voluntad demostrable

Es aquí donde **t2p** lleva aquella intuición al alcance de cualquier persona, y lo hace con una pieza que en este capítulo brilla como en ningún otro: la **prueba de vida**. En el momento de firmar o de grabar la voluntad, se calcula en el dispositivo la **huella SHA-512** del documento testamentario, se ancla a la **blockchain pública** y se le añaden un **sello de tiempo RFC 3161** conforme a eIDAS, un **GPS forense** y el contenedor **.asice verificable sin conexión**. Pero la clave de bóveda es la **grabación de vida** —un vídeo-selfie con retos—, que demuestra tres cosas decisivas: que el testador *estaba vivo*, que *estaba presente* y que *es quien dice ser*, en el instante exacto de otorgar.

Pensemos qué significa esto contra las dos amenazas más comunes. Contra la **influencia indebida**: se ve y se oye al testador declarar su voluntad libremente, sin un tercero dirigiéndolo fuera de cámara de manera evidente. Contra la **falsificación**: el firmante real queda ligado biométricamente al documento, de manera que ya no basta con copiar una firma y aportar dos testigos cómplices, como en el caso Voysey. Y el **sello de tiempo** resuelve la eterna disputa de «existe un testamento posterior»: la cadena de huellas fechadas establece un orden incontrovertible de versiones, revocaciones y codicilos. Incluso el agujero de la herencia digital tiene solución: el mismo contenedor puede sellar —cifradas— las instrucciones de acceso a los activos digitales, evitando un nuevo QuadrigaCX sin exponer las claves.

Hay que decir el límite con toda la honestidad, porque aquí es sutil. El sello **no sustituye** las formalidades legales —testigos, intervención notarial, homologación sucesoria— ni la validez según cada jurisdicción: un testamento sellado pero sin las solemnidades exigidas puede seguir siendo nulo. Y, sobre todo, la **capacidad testamentaria es un juicio legal y médico** que el vídeo de vida *apoya* —muestra lucidez aparente, ausencia de coacción visible— pero **no determina**: alguien puede parecer perfectamente lúcido ante la cámara y carecer, sin embargo, de capacidad jurídica. «Basura a la entrada, basura en la cadena»: la prueba demuestra integridad, momento, lugar y persona, no la verdad de fondo de las disposiciones ni que nadie ejerciera presión fuera de plano.

La promesa y el peligro

La promesa es serena y poderosa. Dar a cada persona una manera de dejar su última voluntad de forma que se pueda demostrar —que era ella, viva y presente, y que aquella es la versión definitiva— ahorraría años de litigio a familias en duelo, protegería los 84 billones de dólares que cambiarán de manos y cerraría el agujero de la herencia digital. Es hacer que la voz apagada del testador siga hablando con autoridad.

El peligro pide matiz. El primero, ya dicho: el sello no otorga validez legal por sí solo ni decide la capacidad; confundirlo sería peligroso. El segundo, la privacidad de un documento íntimo por definición, que ha de quedar en manos del titular hasta que llegue el momento. Y el tercero, no convertir la tecnología en una barrera para quien no tiene acceso a ella: la manera más sencilla de hacer testamento —ir al notario— ha de seguir abierta a todos. La prueba de existencia es un refuerzo de la última voluntad, no un sustituto del derecho sucesorio ni del notario.

Es hora de actuar

Para las personas: dejar testamento —la mayoría todavía no lo hace— y, cuando lo hagan, sellarlo con prueba de vida y fecha cierta. Para los notarios y abogados: incorporar la grabación de vida como refuerzo contra la influencia indebida y la falsificación, las disputas más comunes. Para los registros sucesorios: seguir el ejemplo de Estonia y garantizar la integridad de cada testamento. Para los legisladores: cerrar el vacío legal de la herencia digital, para que ningún patrimonio vuelva a quedar enterrado con una contraseña. Y para todos: recordar que la última voluntad es el único documento que su autor nunca podrá defender en persona.

Una falsificadora estuvo a punto de reescribir el destino de aquellos 4,2 millones de libras con dos testigos cómplices. Dar a cada testador una prueba que hable por él cuando ya no esté —viviente, presente e inconfundible— es, en este frente profundamente humano, time2act.

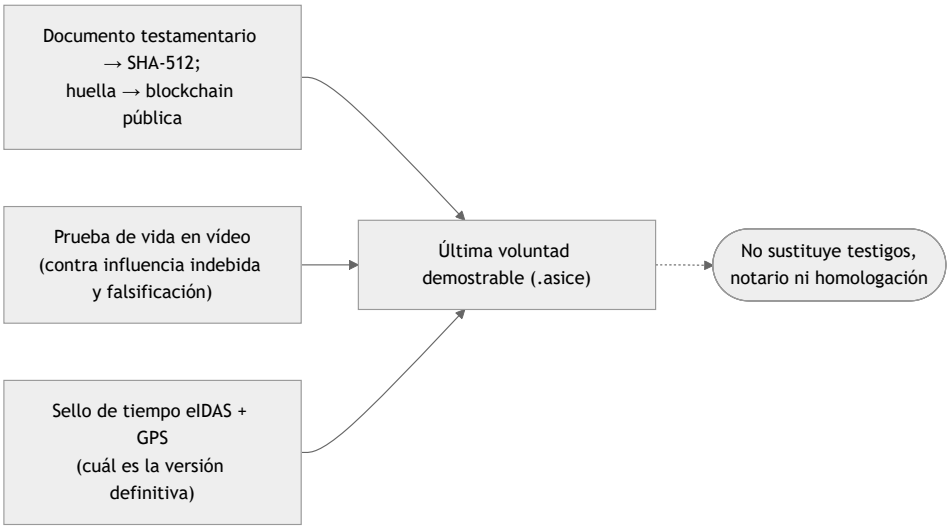


Figura 52.1 — Tres entradas convergen en un testamento incontestable: el documento, cuya huella SHA-512 se ancla a la blockchain pública (integridad); la prueba de vida en vídeo, que liga identidad, presencia y voluntad (contra la influencia indebida y la falsificación); y el sello de tiempo eIDAS con GPS, que fija cuál es la versión definitiva (contra «existe un testamento posterior»). El resultado es un .asice verificable sin conexión. Límite: no sustituye testigos, notario ni homologación, y la capacidad la decide el juez o el médico. Fuentes: Cerulli Associates; e-Estonia/Guardtime; caso Voysey.

---

[1] Hertfordshire Constabulary — *Three jailed for £4m inheritance fraud* (caso Leigh Voysey y el testamento de Maureen Renny; ~4,2 M£). https://www.herts.police.uk/news/hertfordshire/news/2024/december-2024/three-jailed-for-4m-inheritance-fraud/ ↩

[2] Cerulli Associates — *Cerulli anticipates $84 trillion in wealth transfers through 2045* (2022; «gran transferencia de riqueza»). https://www.cerulli.com/press-releases/cerulli-anticipates-84-trillion-in-wealth-transfers-through-2045 ↩

[3] Caring.com / YouGov — *Wills and Estate Planning Study 2025* (solo el 24 % de los adultos tiene testamento). https://www.caring.com/resources/wills-survey ↩

[4] Dutton Gregory / Probate Registry — *Inheritance dispute statistics* (11.362 caveats en 2024, +56 % en cinco años). https://www.duttongregory.co.uk/site/blog/personalnews/inheritance-dispute-statistics ↩

[5] Justia — *Will contests: testamentary capacity, undue influence, forgery* (motivos de nulidad). https://www.justia.com/estate-planning/wills/will-contests/ ↩

[6] CBS News — *QuadrigaCX CEO took password to his grave* (Gerald Cotten; ~137 M$ bloqueados). https://www.cbsnews.com/news/gerald-cotten-quadrigacx-ceo-took-password-to-his-grave-leaving-company-unable-to-access-137-million/ ↩

[7] Chainalysis (vía Decrypt) — *~3,7 millones de bitcoins perdidos para siempre* (2020; ~20 % de la oferta). https://decrypt.co/37171/lost-bitcoin-3-7-million-bitcoin-are-probably-gone-forever ↩

[8] American Bar Association — *Digital property and estate planning* (RUFADAA; la criptomoneda se pierde sin las claves). https://www.americanbar.org/groups/real_property_trust_estate/resources/estate-planning/digital-property/ ↩

[9] Comisión Europea (Interoperable Europe) / e-Estonia — *Estonia's KSI blockchain: the Succession Registry* (primer servicio estatal sobre blockchain, 2012). https://e-estonia.com/blockchain-security-control-for-government-registers/ ↩

[10] eSignGlobal — *Electronic wills legislation and remote notarization* (eIDAS QES; los testamentos a menudo excluidos de la notarización electrónica). https://www.esignglobal.com/blog/electronic-wills-legislation-remote-notary

Derecho de familia: la coparentalidad con fecha cierta

«Vuestros hijos no son vuestros hijos. […] Vienen a través de vosotros, pero no de vosotros.»

— Khalil Gibran, El Profeta (1923)

Un viernes por la tarde, en la puerta de una escuela cualquiera. Dos adultos que un día se amaron se pasan una mochila y un niño, con la cordialidad justa. Hasta aquí, la rutina de miles de familias. La tensión está en lo que no se ve: si la entrega era a las cinco o a las cinco y media; si el abrigo que falta lo tenía uno u otra; si la factura del dentista se había comunicado; si el cambio de fin de semana se acordó o se impuso. Cada detalle minúsculo puede acabar, meses después, en un juzgado de familia convertido en «tu palabra contra la mía» —con un menor en medio.

Y cada vez son más familias en esta coreografía. En España, en 2024 hubo 82.991 divorcios —un 8,2 % más que el año anterior— y la custodia compartida se otorgó en el 49,7 % de los casos con hijos, superando por primera vez la custodia materna; en 2010 era solo el 12,6 % [1]. La custodia compartida es la nueva normalidad, y es una buena noticia —pero multiplica la coordinación cotidiana entre personas que a menudo ya no se tienen confianza: dos calendarios, dos hogares, un plan de parentalidad [3] y centenares de microacuerdos al año.

Este capítulo trata la evidencia de la coparentalidad. La herencia y la última voluntad están en el capítulo 52; la cadena de custodia judicial, en el capítulo 77; la grabación legal de conversaciones propias, en el capítulo 75. Pregunta clave: ¿cómo se documenta la vida compartida de un menor entre dos hogares sin convertir la familia en un campo de vigilancia mutua? Respuesta: con fecha cierta neutral sobre los hechos acordables —mensajes, entregas, gastos, planes— mediante **t2p**: la huella SHA-512 en el dispositivo, el anclaje de la huella en la blockchain pública y el sello de tiempo RFC 3161/eIDAS complementario, dentro de un contenedor .asice [4]. Y bajo un principio que manda sobre todos los demás: el interés superior del menor. La prueba no es para ganar la guerra; es para que no la haya.

La palabra contra la palabra, con un menor en medio

La materia prima de los conflictos posruptura es cotidiana y minúscula: horarios de entrega, gastos extraordinarios, decisiones escolares y médicas, cambios de planes. Cuando la relación es serena, nada de esto importa; cuando se deteriora, todo se vuelve disputable —y el sistema judicial de familia, sobrecargado y lento, se encuentra resolviendo con años de retraso discusiones sobre quién llegó tarde un viernes de hace dos años, con pruebas fragmentarias: capturas de pantalla, testimonios familiares y recuerdos cargados de sesgo.

El coste de la prueba frágil lo pagan tres partes a la vez. Los progenitores, que acumulan capturas y correos que nunca acaban de ser verificables. El juzgado, que tiene que reconstruir la vida cotidiana de una familia desde fuera, decidiendo qué fragmento pesa más sin ninguna capa neutral que acredite su integridad. Y, sobre todo, el menor: cada hora de litigio sobre hechos discutibles es tensión que le llega, y las decisiones sobre su vida se toman sobre versiones en lugar de hechos.

Y el matiz que este libro no puede esquivar, dicho con todo el equilibrio: en los conflictos graves —los incumplimientos reiterados, las acusaciones cruzadas— la falta de evidencia neutral perjudica a todos a la vez. El progenitor que cumple y no lo puede demostrar; el que es acusado injustamente y no se puede defender; y el menor, cuya realidad queda enterrada bajo las versiones. La respuesta no es más sospecha: es un registro objetivo de los hechos que ambas partes han aceptado documentar. Ni más, ni menos.

Lo que los tribunales ya piden

El mundo judicial ya ha hecho medio camino. OurFamilyWizard —la aplicación de coparentalidad de referencia— es usada y recomendada por tribunales y profesionales del derecho de familia en los 50 estados de Estados Unidos y en Canadá, el Reino Unido, Australia y Nueva Zelanda; su propuesta es exactamente la de un registro: mensajería con marca de tiempo en cada mensaje y sin posibilidad de borrar nada, confirmaciones de lectura, calendarios de custodia con historial de cambios, registro de gastos e informes descargables para juicios y mediaciones —incluso un medidor de tono que señala el

lenguaje encendido antes de enviar [2]. En España, la pieza equivalente en el ámbito del acuerdo es el plan de parentalidad: el documento que fija el marco común de crianza más allá del convenio regulador [3].

La lección es clara: los juzgados ya no quieren batallas de recuerdos —quieren registros. Pero las herramientas actuales tienen una dependencia estructural: la evidencia vive en los servidores del proveedor, sujeta a sus políticas, a su jurisdicción y a su continuidad como única garantía. Si la empresa cambia las condiciones o desaparece, el registro puede perderse sin que ningún tribunal disponga de una copia verificable independiente —el capítulo 75 ya mostró qué pasa cuando la prueba depende de un contratista.

La capa que falta es la neutralidad criptográfica: que cada mensaje, cada acta de entrega y cada versión del plan lleve su huella SHA-512 con sello de tiempo, anclada a la blockchain pública [4] —verificable por cualquier juzgado sin depender de ninguna empresa, ni de ninguna de las dos partes. La confianza deja de ser una esperanza para convertirse en un hecho documentado, y la justicia puede dedicarse a resolver conflictos reales en lugar de cuestionar registros.

La prueba de existencia aplicada

La misma puerta de escuela, un viernes cualquiera; los mismos dos adultos; y una diferencia invisible: los hechos del día quedan fijados, y ninguno de los dos tendrá que recordarlos nunca más.

1. La comunicación coparental con fecha cierta

Los mensajes entre progenitores —los acuerdos, los avisos, los cambios de planes— se sellan al enviarse: huella SHA-512, fecha cierta, anclaje [4]. Es lo que las aplicaciones judiciales ya ofrecen [2], con la capa neutral añadida: la integridad no depende del proveedor, y el registro es verificable por cualquier juzgado aunque la empresa desaparezca. El acuerdo de cambiar el fin de semana existe con hora; el aviso del gasto médico, también; y la conversación que nunca existió no se puede inventar a posteriori.

2. La entrega acreditada

El momento más delicado de la semana —la entrega y la recogida— puede quedar acreditado con un gesto de diez segundos acordado por ambas partes: la confirmación sellada desde los dos dispositivos (estamos aquí, es esta hora) [4]. Ninguna cámara, ninguna grabación del otro, ningún menor fotografiado: solo el hecho y la hora, firmados por ambos. El retraso reiterado queda fechado; la puntualidad sistemática, también; y la discusión de hace dos años sobre un viernes concreto desaparece del expediente porque la respuesta ya está ahí.

3. El gasto compartido sin guerra

Los gastos extraordinarios —el dentista, las gafas, el campamento— son el foco clásico: ¿se comunicó? ¿se aceptó? ¿se pagó? Con justificantes sellados y avisos con fecha cierta [4], el circuito entero queda acreditado: la factura existe, se comunicó tal día, se respondió —o no— tal otro. El progenitor que paga y comunica queda protegido; el que responde a tiempo, también. Y el silencio no es un vacío: es un registro fechado que habla solo, con la misma neutralidad para todos.

4. El plan de parentalidad versionado

El plan de parentalidad [3] es un documento vivo: se modifica cuando los hijos crecen, cuando cambian los trabajos, cuando la vida manda. Cada versión sellada con fecha cierta [4] hace indiscutible qué estaba vigente cuándo: el acuerdo del verano pasado, la modificación pactada en septiembre, la propuesta que la otra parte nunca aceptó. Los acuerdos evolucionan; su historia, no. Y cuando haga falta mediación o juzgado, la discusión empezará desde los textos fechados, no desde las memorias enfrentadas.

Los límites, dichos con cuidado: el sello acredita hechos —horas, textos, justificantes—, no la calidad de la crianza ni el amor de nadie; no decide custodias —eso lo hacen los jueces, con muchos más elementos—; no ha de convertir la familia en un expediente permanente —se documenta lo objetivable y acordado, nunca la intimidad de ningún hogar ni la vida del menor—; y en situaciones de violencia, la prioridad es la protección inmediata por los canales especializados, no ninguna aplicación.

La promesa y el peligro

La promesa: familias separadas que discuten menos porque los hechos no se discuten [2][4]; juzgados de familia que resuelven sobre registros y no sobre versiones; y menores que crecen con menos guerra alrededor —la logística en paz, para que la energía de los adultos vaya donde corresponde.

Los peligros, tratados con el máximo cuidado.

El primero es **la familia bajo vigilancia**. Documentar los hechos acordados no puede degenerar en vigilar al otro progenitor —ni grabarlo, ni fotografiar su hogar, ni convertir al menor en informador o en portador de dispositivos de control. La línea es nítida: se sella lo que ambas partes han acordado documentar —mensajes, entregas, gastos, planes— y nada más. El menor nunca es objeto de registro; es la razón por la que los adultos se documentan a sí mismos.

El segundo es **el arsenal procesal**. Si el registro se hace para acumular munición, la tecnología habrá empeorado lo que quería curar. El diseño bilateral —las dos partes sellan, las dos partes ven— y la simetría radical de la prueba (protege al que cumple, sea quien sea) desincentivan el uso bélico: contra un registro neutral, la mejor estrategia es cumplir.

El tercero es **la desigualdad de armas**. Si solo una parte domina la herramienta, la fecha cierta se convierte en ventaja procesal. Como en el alquiler y en el trabajo de plataforma, la respuesta es el diseño: gratuidad o coste insignificante, simplicidad, y el juzgado valorando el registro bilateral por encima del unilateral.

Y el cuarto es **el tecnosolucionismo afectivo**. Ningún sello cura una ruptura mal digerida ni sustituye la mediación, la terapia o el tiempo. La prueba de existencia pacifica la capa de los hechos; la capa de las emociones es trabajo de humanos. Confundirlas sería vender criptografía donde hacen falta acuerdos —y, a menudo, un poco de generosidad.

Es hora de actuar

Que los hechos queden en paz para que las personas puedan estarlo.

Para los progenitores separados: acordad en el plan de parentalidad [3] qué documentaréis —mensajes, entregas, gastos— y selladlo bilateralmente [4]; que la logística tenga fecha cierta para que la relación no tenga que tener memoria de agravios.

Para abogados de familia y mediadores: proponed el registro sellado bilateral como cláusula estándar del convenio [2][3]; cada hecho indiscutible es una batalla que no se libra.

Para los juzgados de familia: valorad los registros anclados bilaterales por encima de las capturas y los testimonios cruzados [2][4]; y recordad a las partes que el registro es escudo, no arma.

Para las aplicaciones de coparentalidad: incorporad el anclaje neutral [2][4] —que vuestra evidencia no dependa de vuestra continuidad como empresa.

Para los legisladores: reconoced valor probatorio cualificado al registro coparental sellado bilateral, y garantizad que ninguna herramienta se vuelva obligatoria ni vehículo de vigilancia dentro de la familia [4].

En la puerta de la escuela, el viernes que viene, habrá los mismos dos adultos y el mismo niño con su mochila. Que todo lo que es discutible quede fijado en diez segundos —y que toda la energía que antes se quemaba en discusiones vaya donde corresponde: a la criatura que los mira. Por las familias que continúan, **time2act**.

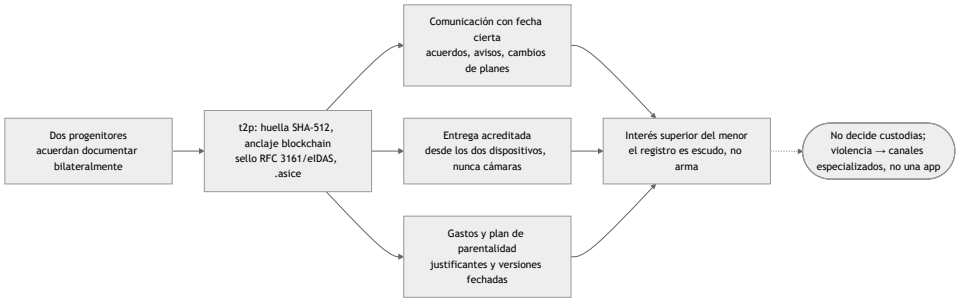


Figura 53.1 — La logística coparental con prueba de existencia (huella SHA-512 en el dispositivo, sello de tiempo RFC 3161/eIDAS, blockchain pública, .asice), siempre bilateral y acordada: la comunicación con fecha cierta, la entrega acreditada desde los dos dispositivos (nunca cámaras ni menores fotografiados), los gastos con justificantes anclados y el plan de

parentalidad versionado. El norte: el interés superior del menor; el registro es escudo, no arma. Límites: no decide custodias, no mide la crianza, y en situaciones de violencia la prioridad son los canales especializados. Fuentes: INE (custodia compartida 49,7 %, 2024); OurFamilyWizard (tribunales de 50 estados); plan de parentalidad.

---

[1] INE / Gracia Carrión (análisis) — *Custodia compartida supera a la materna en España (INE 2024)* (49,7 % de los divorcios con hijos, +1,3 puntos; primera vez por encima de la custodia materna; 12,6 % en 2010); APFS — *Separaciones y divorcios en España 2024* (82.991 divorcios, +8,2 %); INE — *Estadística de nulidades, separaciones y divorcios*. https://graciacarrion.com/es/custodia-compartida-supera-materna/ · https://apfs.es/separaciones-y-divorcios-en-espana-2024-tendencias-y-claves-segun-el-ine/ · https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=estadistica_C&cid=1254736176798&menu=ultiDatos&idp=1254735573206 ↩

[2] OurFamilyWizard — *Herramientas para la custodia compartida* (aplicación de coparentalidad de referencia para tribunales y profesionales en los 50 estados de EE. UU., Canadá, Reino Unido, Australia y Nueva Zelanda; mensajes con marca de tiempo y sin borrado; confirmaciones de lectura; calendarios con historial; informes para juicios; ToneMeter); Crianza y Crecimiento — *Aplicaciones de coparentalidad aprobadas por tribunales*. https://es.ourfamilywizard.com/homepage · https://crianzaycrecimiento.com/aplicaciones-coparentalidad-aprobadas-tribunales/ ↩

[3] El Español — *Una abogada, sobre solicitar la custodia compartida: «Después de 10 años, necesitas un plan de parentalidad»* (el plan de parentalidad como marco común de crianza más allá del convenio regulador). https://www.elespanol.com/mujer/relaciones/20251214/abogada-solicitar-custodia-compartida-despues-anos-necesitas-plan-parentalidad/1003744039064_0.html ↩

[4] t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; registro bilateral; contenido en los dispositivos, solo huellas en la cadena; revelación ante el juzgado). Véanse los capítulos 13 y 15; la grabación legal de conversaciones propias, en el capítulo 75. ↩

Trade finance: el mismo cargamento financiado dos veces

«El fundamento de la justicia es la buena fe, es decir, la constancia y la verdad en lo dicho y lo convenido.»

— Cicerón, De Officiis, I, 23 (44 a. C.)

En junio de 2014, en el puerto chino de Qingdao, unos inspectores de banco intentaron entrar en los almacenes para verificar algo que debería ser elemental: que el metal que figuraba en las facturas estaba realmente allí. No les dejaron pasar. La empresa Citic Resources denunció que no conseguía localizar más de cien mil toneladas de alúmina que deberían estar allí [4]. Pronto se descubrió por qué: el mismo cobre y el mismo aluminio habían sido pignorados, mediante **recibos de almacén duplicados**, a decenas de bancos chinos e internacionales a la vez. El empresario detrás del engaño, Chen Jihong, levantó unos 12.300 millones de yuanes —cerca de 1.800 millones de dólares— con documentos falsos, y acabó condenado a veintitrés años de prisión [4]. La exposición de los bancos superó los 3.000 millones de dólares.

Aquel escándalo tiene un nombre propio en el sector —«metal fantasma»— y contiene la doble lección de este capítulo. La primera: el fraude más caro del comercio internacional no es falsificar la mercancía, sino **financiar el mismo cargamento muchas veces** con documentos que nadie puede cruzar. La segunda, más incómoda, la dejaremos para el final: en Qingdao, el problema no era que los documentos fueran falsos —algunos eran bien reales—, sino que el cobre no estaba allí.

El comercio que vive del papel

Para entender la vulnerabilidad hay que comprender la escala. Entre el 80 y el 90 % del comercio mundial depende de instrumentos de financiación —cartas de crédito, conocimientos de embarque, recibos de almacén—, y la inmensa mayoría sigue siendo **de papel** [10]. La Cámara de Comercio Internacional (**ICC**), que redacta las reglas que gobiernan las cartas de crédito, calcula que cada día circulan unos **4.000 millones de documentos** por el sistema comercial global [10]. Sin embargo, la digitalización avanza a paso de tortuga: a pesar de que el conocimiento de embarque electrónico existe desde hace años, solo había penetrado en un **5,7 %** de los transportistas marítimos a principios de 2025 [3].

Esta dependencia del papel tiene un coste brutal, y lo pagan sobre todo los más débiles. El **Banco Asiático de Desarrollo** (ADB), que toma el pulso mundial al sector con su encuesta de referencia, calculó que la **brecha de financiación del comercio** —la diferencia entre lo que las empresas piden y lo que los bancos aprueban— llegó a un récord de **2,5 billones de dólares en 2022**, desde 1,7 billones dos años antes [1]. Las pequeñas y medianas empresas, que son menos de una cuarta parte de la demanda, concentran el 40 % de los rechazos. Como resume el ADB, la financiación no falta por falta de bienes, sino por falta de **confianza verificable** en los documentos y en la contraparte. McKinsey ha estimado que solo digitalizar el conocimiento de embarque ahorraría 6.500 millones de dólares y habilitaría decenas de miles de millones de comercio nuevo [2].

El mismo cargamento, financiado dos veces

Qingdao no fue un caso aislado; fue el patrón. En 2020, en Singapur, el gigante del comercio de crudo Hin Leong se hundió con **3.850 millones de dólares** de deuda ante veintitrés bancos. Los administradores judiciales destaparon una falsificación de documentos «a escala masiva»: ventas inventadas a otras empresas para sacar casi **112 millones de dólares** a HSBC por barriles de petróleo que nunca cambiaron de manos, y generó una huella profunda en el sector. Su fundador, Lim Oon Kuin —«OK Lim»—, de ochenta y dos años, fue condenado en noviembre de 2024 a diecisiete años y medio de prisión; la pena se redujo a trece años y medio en apelación en marzo de 2026 [5]. Y en 2021, el imperio de financiación de **Greensill Capital** cayó en insolvencia, arrastrando a Credit Suisse, cuyos clientes tenían unos **10.000 millones de dólares** en fondos respaldados por facturas —algunas de las cuales, según el regulador suizo **FINMA**, se basaban en operaciones que aún no habían ocurrido o eran presuntamente ficticias [6]. Como concluyó la FINMA, la opacidad documental, no el instrumento, fue lo letal.

En todos los casos, el mecanismo es el mismo: un documento —un recibo, una factura, un conocimiento de embarque— que nadie puede contrastar contra los demás financiadores, y que por tanto se puede presentar a diez bancos a la vez o fabricar después para tapar un agujero.

La prueba de existencia contra la doble financiación

Es aquí donde **t2p** ataca el corazón del problema. En el momento de emitirse, el conocimiento de embarque, la factura comercial, el recibo de almacén o la carta de crédito reciben una **huella SHA-512** calculada en el dispositivo, se anclan a la **blockchain pública**, y le añaden un **sello de tiempo RFC 3161** conforme a eIDAS y un **GPS forense** de la ubicación del puerto o el almacén, todo en un contenedor **.asice verificable sin conexión**.

El golpe a la doble financiación es directo: antes de prestar, el banco B puede comprobar si la huella de aquel conocimiento de embarque **ya había sido sellada y pignorada** por el banco A. Si el documento ya está «gastado», la segunda financiación se bloquea —exactamente lo que habría detenido los recibos duplicados de Qingdao. El sello de tiempo, además, impide la **retrodatación**, evitando que nadie pueda fabricar después un documento «anterior» a una pérdida, como hizo Hin Leong. De esta manera se distingue una factura real emitida en un momento de una «predicha» o inventada posteriormente, el problema de Greensill. Todo ello se refuerza con la **prueba de vida** del comerciante en el momento de la firma.

Hay que poner límite a la crudeza: la prueba de existencia **no verifica que la mercancía física exista**. En Qingdao, el documento era real y podría haber estado perfectamente sellado; lo que no había era el cobre. «Basura a la entrada, basura en la cadena»: la cadena demuestra la integridad, el momento, el lugar y la persona del *registro*, no la verdad física del almacén. Por eso hacen falta oráculos físicos —inspecciones, sensores, custodios independientes— que **t2p** no sustituye. Además, para que un documento electrónico sellado tenga «posesión» y «singularidad» ejecutables, hace falta reconocimiento legal: la **Ley Modelo de las Naciones Unidas sobre Registros Electrónicos Transferibles** (MLETR) lo hace posible, pero como hemos visto, en 2025 solo la han adoptado trece jurisdicciones, entre ellas el Reino Unido [8]. Y la lección de los consorcios fracasados —TradeLens, we.trade, Marco Polo, todos cerrados entre 2022 y 2023— muestra que bloquear la doble financiación exige que **todos** los financiadores consulten el mismo registro. Una prueba abierta y verificable sin conexión reduce esta necesidad de coordinación, pero no la elimina.

La promesa y el peligro

La promesa es cuantificable: una capa de prueba de existencia sobre los documentos comerciales dificultaría enormemente financiar el mismo cargamento dos veces, retrodatar ventas fantasma o inventar facturas futuras, y ayudaría a cerrar la brecha de financiación que, como hemos visto, afecta sobre todo a las pequeñas empresas de los países emergentes. En un sector donde la confianza documental lo es todo, sellar la integridad y el momento de cada documento restaura el fundamento del comercio.

El peligro pide el matiz de siempre. Primero, el sello no hace aparecer el metal en el almacén; confundir la integridad del documento con la existencia de la mercancía es precisamente el error que costó miles de millones en Qingdao. Segundo, sin MLETR un documento sellado no es ejecutable. Tercero, la coordinación: la tecnología no sirve de nada si los bancos no la consultan en común. La prueba de existencia es una capa necesaria dentro de una arquitectura que incluye, siempre, la inspección física y el marco legal.

Es hora de actuar

Para los exportadores y comerciantes: sellar los documentos comerciales en origen, de manera que su integridad y el momento sean demostrables. Para los bancos y financiadores: comprobar la huella de un documento antes de prestar, para impedir que el mismo cargamento se financie dos veces. Para los reguladores: adoptar la MLETR, como ya han hecho el Reino Unido y una docena de jurisdicciones, para que el documento electrónico sellado tenga plena fuerza legal. Y para los organismos del sector (ICC, bancos): aprender de los consorcios fracasados y converger en estándares abiertos, no en silos cerrados.

En Qingdao, el mismo metal financió decenas de préstamos porque nadie podía cruzar los documentos. Asignar a cada conocimiento de embarque una huella única, sellada en el tiempo y comprobable por todos

—sin olvidar nunca que hay que ir al almacén a contar el cobre— es, en este frente del comercio global, time2act.

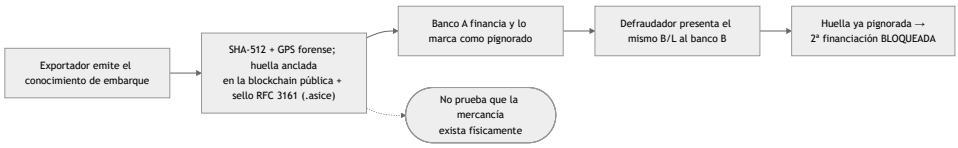


Figura 54.1 — El exportador emite un conocimiento de embarque que se sella con huella SHA-512, sello de tiempo RFC 3161/eIDAS y GPS, anclado a la blockchain pública (.asice). El banco A lo financia y lo marca como pignorado. Cuando un defraudador presenta el «mismo» documento al banco B, la huella coincide y consta como ya pignorado: la segunda financiación se bloquea. Límite: el sello no prueba que la mercancía exista físicamente en el almacén (el «metal fantasma» de Qingdao). Contexto: brecha de financiación del comercio de 2,5 billones de dólares; conocimiento de embarque electrónico real, solo el 5,7 %. Fuentes: Banco Asiático de Desarrollo; ICC; caso Qingdao.

---

[1] Banco Asiático de Desarrollo (ADB) — *Global trade finance gap expands to $2.5 trillion in 2022* (Trade Finance Gaps, Growth and Jobs Survey). https://www.adb.org/news/global-trade-finance-gap-expands-25-trillion-2022 ↩

[2] McKinsey — *The multi-billion-dollar paper jam: unlocking trade by digitalizing documentation* (2022; ahorro de 6.500 M$ + comercio nuevo). https://www.mckinsey.com/industries/logistics/our-insights/the-multi-billion-dollar-paper-jam-unlocking-trade-by-digitalizing-documentation ↩

[3] DCSA / FIT Alliance — *eBL adoption* (penetración real del conocimiento de embarque electrónico: 5,7 %, enero 2025). https://dcsa.org/standards/booking/adoption-guide-booking-and-bill-of-lading ↩

[4] Caixin Global — *Dezheng founder jailed over Qingdao port forgery scandal* (Chen Jihong, 23 años; ~12.300 M yuanes con recibos falsos). https://www.caixinglobal.com/2018-12-12/dezheng-founder-gets-32-years-in-prison-over-port-forgery-scandal-101358154.html ↩

[5] Singapore Police Force / SCMP — *Hin Leong founder OK Lim jailed* (17,5 años, reducidos a 13,5 en apelación en marzo de 2026; ~112 M$ a HSBC). https://www.police.gov.sg/media-hub/news/2024/20241118_founder_of_hin_leong_trading_sentenced_and_jailed_for_cheating_and_instigating_forgery ↩

[6] FINMA — *Greensill / Credit Suisse* (insolvencia 2021; ~10.000 M$ en cuatro fondos; facturas ficticias). https://www.finma.ch/en/news/2023/02/20230228-mm-greensill/ ↩

[7] Maersk — *Maersk and IBM to discontinue TradeLens* (cierre del consorcio, 2022-2023). https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens

[8] UNCITRAL — *Model Law on Electronic Transferable Records (MLETR): status* (13 jurisdicciones; incluye el Reino Unido). https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records/status ↩

[9] Clifford Chance — *UK Electronic Trade Documents Act 2023* (equivalencia legal del conocimiento de embarque electrónico). https://www.cliffordchance.com/briefings/2023/08/uk-electronic-trade-documents-act-2023--a-further-step-towards-p.html

[10] International Chamber of Commerce (ICC) — *Survey shows steady rise of global adoption of electronic bills of lading* (~4.000 M de documentos/día; reglas UCP 600). https://iccwbo.org/news-publications/news/survey-shows-steady-rise-of-global-adoption-of-electronic-bills-of-lading/ ↩

Auditoría: cuentas e informes a prueba de manipulación

«¡Qué ventajas ofrece al comerciante la partida doble! Es uno de los inventos más bellos del espíritu humano.»

— Goethe, Los años de aprendizaje de Wilhelm Meister (1796)

Había una cuenta fiduciaria que no existía. Durante años, la empresa alemana de pagos Wirecard declaró que tenía **1.900 millones de euros** —casi una cuarta parte de su balance— depositados en cuentas de garantía en bancos de Filipinas. Cuando los auditores de EY preguntaron al fiduciario de Singapur, Shan Rajaratnam, este les dijo la verdad: no custodiaba ningún dinero de Wirecard. Pero unos gestores de Wirecard intervinieron, y Shan «corrigió» su respuesta y confirmó los 1.900 millones. EY se conformó con capturas de pantalla y documentos aportados por el propio cliente, y **nunca escribió directamente a los bancos** [1]. Dos años más tarde, los bancos confirmaron que aquellos extractos eran falsos y que la cuenta nunca había existido. Wirecard quebró en junio de 2020, en el mayor fraude de la posguerra alemana.

El detalle que lo hace tan doloroso es su simplicidad: habría bastado una **carta de confirmación directa del banco** —lo que un auditor rival describió como «la formación del primer día en la escuela de auditoría»— para hacer caer todo el engaño. Este capítulo trata de eso: de cómo hacer que las pruebas sobre las que descansa la confianza en las cuentas de una empresa sean imposibles de fabricar.

El fraude que los auditores no vieron

Wirecard no es una excepción; es el último eslabón de una cadena tristemente famosa. En 2001, Enron se hundió y evaporó más de **74.000 millones de dólares** de sus accionistas; su auditora, Arthur Andersen —una de las cinco grandes del mundo, con más de **85.000 empleados**—, fue declarada culpable de destruir documentos y desapareció, dando origen a la ley Sarbanes-Oxley [4]. En 2020, la cadena de café Luckin Coffee admitió haber fabricado unos **311 millones de dólares** en ventas [5], y el caso indio de Satyam ya había mostrado el patrón exacto de Wirecard: facturas falsas y **confirmaciones bancarias forjadas**. Según la Asociación de Examinadores de Fraude Certificados, las organizaciones pierden de media un 5 % de sus ingresos por fraude, y el fraude de estados financieros, a pesar de ser solo el 5 % de los casos, es el más costoso, con una pérdida mediana de **766.000 dólares** por caso [7].

El hilo común de todos estos escándalos es que el auditor trabaja con documentos que han pasado por las manos del auditado; cuando este es el defraudador, la prueba ya llega contaminada. Hay que recordar quién destapó Wirecard: el periodista **Dan McCrum**, del *Financial Times*, que en su libro *Money Men* (2022) explica cómo fue vigilado, pirateado e incluso investigado penalmente por «manipulación de mercado» —**por tener razón**— mientras la empresa seguía cotizando en el índice alemán [3]. El sistema castigó al mensajero antes que al fraude.

El regulador responde, y el nuevo frente del ESG

La respuesta reguladora ha ido, precisamente, hacia la prueba. El supervisor de auditoría norteamericano, el **PCAOB**, adoptó en 2023 una norma específica —la AS 2310, «El uso de la confirmación por el auditor»— que refuerza que las confirmaciones lleguen directamente de fuentes externas fiables y se evalúen con escepticismo [6]. Es, en el fondo, un reconocimiento de que la confirmación bancaria directa es el eslabón que combate el fraude corporativo.

Y se abre un frente nuevo y aún más frágil: la sostenibilidad. La directiva europea **CSRD** nació para obligar a decenas de miles de empresas a presentar un informe de sostenibilidad con **aseguramiento externo** —verificación independiente— según las normas ESRS desarrolladas por **EFRAG** [8]. En 2025-26, el paquete «Omnibus» recortó su alcance en un 80 %, limitándolo a las empresas de más de mil empleados y 450 millones de euros de facturación, pero mantuvo el aseguramiento limitado como obligatorio [9]. Y el consejo mundial de normas de auditoría, el **IAASB**, aprobó en 2024 la primera norma global para verificar la información de sostenibilidad, la ISSA 5000 [10]. El problema de fondo es que los datos ESG —emisiones, datos de la cadena de suministro— son el terreno donde la **procedencia del dato** es más débil de todas. Verificarlos exige saber de dónde vienen.

La prueba de existencia: sellar en origen

Es aquí donde **t2p** ofrece el complemento técnico natural a toda esta regulación. La idea es aplicar el sellado **en el punto de captura**, no cuando el documento ya ha pasado por el auditado. Una confirmación bancaria firmada y sellada **en el propio banco** —con huella SHA-512, anclaje a la blockchain pública y sello de tiempo RFC 3161 conforme a eIDAS, en un contenedor .asice verificable sin conexión— no se puede sustituir por una captura de pantalla fabricada ni redirigir a un fiduciario cómplice. El auditor deja de fiarse de un papel intermediado y verifica una **cadena de custodia inalterable** desde la fuente.

Lo mismo se aplica a los libros contables, a las facturas, a los recuentos físicos de inventario —con GPS y prueba de vida de quien los hace— y, sobre todo, a los **papeles de trabajo del auditor**, sellados en el momento de crearse. Contra el caso Andersen, esto hace **imposible destruirlos o retrodatar su contenido** sin que el anclaje lo delate. Y para el frente más frágil de la CSRD, sellar el dato ESG en origen —la lectura del sensor de emisiones, la factura del proveedor— es la única manera de dar una procedencia sólida a lo que hoy se verifica casi a ciegas.

Hay que decir el límite con toda la crudeza, porque en auditoría es esencial. La prueba de existencia demuestra **integridad, momento, lugar y persona** de un registro, no la **verdad económica** de fondo. Si todos los inputs se fabrican aguas arriba —un banco cómplice que sella un extracto falso desde el origen, ventas inventadas como en Luckin, una entidad de propósito especial como en Enron—, el sello solo certificará que **una mentira se capturó de forma inalterable**: «basura a la entrada, basura en la cadena». t2p reduce drásticamente la falsificación posterior y elimina la coartada del «documento perdido o alterado», pero **no sustituye el juicio del auditor ni la confirmación con una fuente externa genuinamente independiente**. Un sello no convierte un dato falso en verdadero.

La promesa y el peligro

La promesa es sólida y cuantificable. Una capa de prueba de existencia sobre las confirmaciones, los libros y los papeles de trabajo dificultaría mucho más el fraude de estados financieros —que cuesta miles de millones y destruye puestos de trabajo y ahorros—; daría al auditor una cadena de custodia fiable en lugar de documentos intermediados y pondría un fundamento sólido al aseguramiento de la sostenibilidad, donde la procedencia del dato es más débil. En un sistema que se basa en la confianza en las cuentas, hacer la prueba inalterable refuerza todo el edificio.

El peligro pide el matiz de siempre. El primero, ya hemos dicho: el sello no convierte un dato falso en verdadero; si la fuente ya es cómplice, la cadena inmortaliza la mentira. Confundir la integridad documental con la verdad económica sería precisamente el error fundamental de Wirecard. El segundo, el exceso de confianza: ninguna tecnología sustituye el escepticismo profesional del auditor. La prueba de existencia es una herramienta que refuerza la confirmación externa y protege los papeles de trabajo, no un sustituto del juicio humano ni de la independencia de la fuente.

Es hora de actuar

Para los auditores: exigir confirmaciones selladas en origen y sellar los propios papeles de trabajo al crearlos, para que nadie los pueda fabricar ni destruir. Para los bancos y fuentes externas: emitir las confirmaciones con un sello criptográfico desde la fuente, no a través del cliente. Para los reguladores (PCAOB, IAASB, EFRAG): reconocer el sello de origen como refuerzo de la AS 2310 y del aseguramiento de sostenibilidad. Y para las empresas: sellar el dato ESG en origen, antes de que ningún auditor lo tenga que verificar a ciegas.

Una cuenta que no existía estuvo a punto de pasar desapercibida porque nadie escribió al banco. Asignar a cada confirmación, a cada libro y a cada papel de trabajo una prueba sellada en origen —y recordar siempre la necesidad de escepticismo profesional— es, en este frente que sostiene la confianza en los mercados, **time2act**.

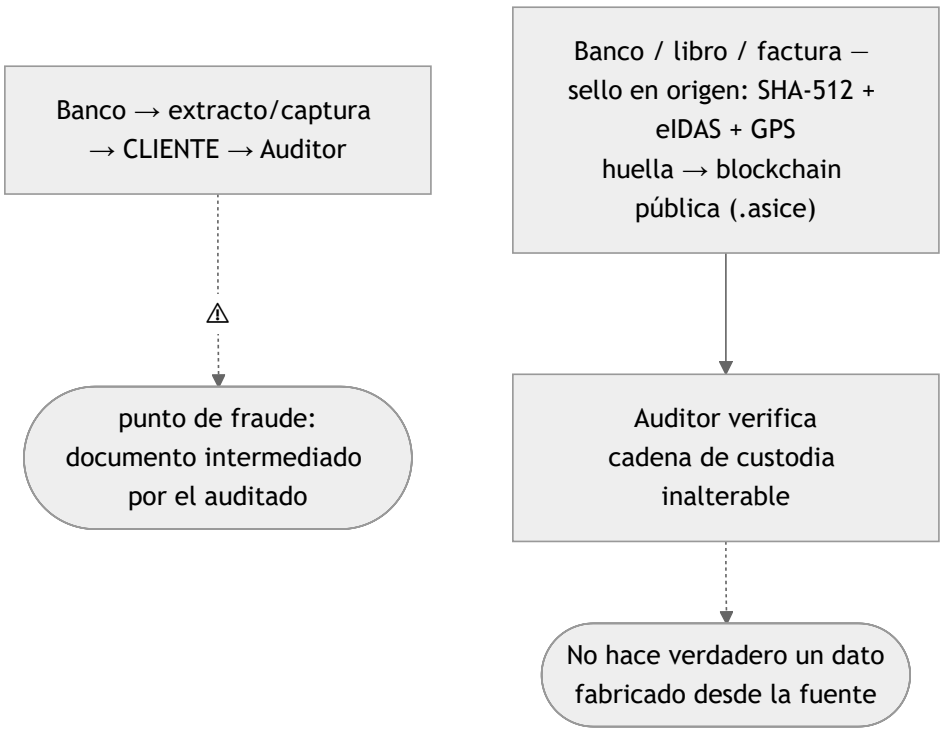


Figura 55.1 — En el modelo tradicional vulnerable, el extracto bancario pasa por el cliente (Wirecard) antes de llegar al auditor: es el punto donde se cuela la falsificación. Con t2p, la confirmación bancaria, el libro mayor o la factura se sellan en origen —huella SHA-512, sello de tiempo eIDAS, GPS, anclaje a la blockchain pública— y el auditor verifica una cadena de custodia inalterable (.asice). Límite: el sello no hace verdadero un dato fabricado desde la fuente (Wirecard, Luckin, Enron). Contexto: Wirecard, 1.900 M€ inexistentes; fraude de estados financieros, mediana de 766.000 $ por caso. Fuentes: Financial Times; PCAOB; ACFE.

---

[1] Financial Times (vía S&P Global) — *Wirecard auditor did not independently verify its bank balance* (EY; cuentas de garantía inexistentes; extractos fabricados). https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/wirecard-auditor-did-not-independently-verify-its-bank-balance-8211-financial-times-59219155 ↩

[2] CNN Business — *Germany bans EY from taking on new audit clients over Wirecard* (APAS: «negligencia grave»; multa de 500.000 € y prohibición de 2 años). https://www.cnn.com/2023/04/03/business/wirecard-ey-ban-germany/index.html

[3] Dan McCrum (Financial Times) — *Money Men: A Hot Startup, a Billion-Dollar Fraud, a Fight for the Truth* (2022). https://danmccrum.com/ ↩

[4] Wikipedia — *Enron scandal* (>74.000 M$ perdidos; Arthur Andersen, ~85.000 empleados; origen de la Sarbanes-Oxley). https://en.wikipedia.org/wiki/Enron_scandal ↩

[5] U.S. Securities and Exchange Commission — *Luckin Coffee agrees to pay $180 million penalty to settle accounting fraud charges* (~311 M$ de ventas fabricadas). https://www.sec.gov/newsroom/press-releases/2020-319 ↩

[6] PCAOB — *AS 2310, The Auditor's Use of Confirmation* (adoptada en septiembre de 2023; confirmación externa directa). https://pcaobus.org/oversight/standards/auditing-standards/details/AS2310 ↩

[7] Association of Certified Fraud Examiners (ACFE) — *Report to the Nations 2024* (5 % de los ingresos; fraude de estados financieros, mediana de 766.000 $ por caso). https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf ↩

[8] Comisión Europea — *Corporate sustainability reporting (CSRD)* (aseguramiento limitado obligatorio; normas ESRS de EFRAG). https://finance.ec.europa.eu/financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en ↩

[9] Accountancy Europe — *Omnibus explained: key changes to the CSRD and CSDDD* (umbral de >1.000 empleados y >450 M€; el aseguramiento limitado se mantiene). https://accountancyeurope.eu/publications/omnibus-explained-key-changes-to-the-csrd-and-csddd/ ↩

[10] IAASB — *ISSA 5000: General Requirements for Sustainability Assurance Engagements* (2024; primera norma global de aseguramiento de sostenibilidad). https://www.iaasb.org/publications/international-standard-sustainability-assurance-5000-general-requirements-sustainability-assurance ↩

Fraude publicitario: el anuncio que nadie vio

«La promesa, la gran promesa, es el alma de un anuncio.»

— Samuel Johnson, The Idler, n.º 40 (1759)

En octubre de 2016, una granja de bots dirigida desde Rusia fingía ver hasta **trescientos millones de vídeos publicitarios al día**. No había nadie mirando: el software simulaba cursores de ratón que se movían, sesiones iniciadas en redes sociales y visitas a páginas; así generó cobro de los anunciantes. La operación, bautizada Methbot, ingresaba entre tres y cinco millones de dólares diarios [6]. Su sucesor, una red llamada 3ve, fue más allá: infectó **1,7 millones de ordenadores domésticos** sin que sus dueños lo supieran, suplantó diez mil dominios legítimos y costó a los anunciantes más de **29 millones de dólares** en anuncios que ningún ser humano vio jamás [5]. Detrás había un ruso que se hacía llamar «el Rey del Fraude»; condenado a diez años de prisión, escribió en su defensa: «soy un soldado sin armas ante un tanque que se llama FBI» [7].

Aquel caso ilustra un problema masivo y sorprendentemente invisible: una buena parte de lo que gastamos en publicidad digital se pierde en anuncios que nadie ve. Este capítulo trata de cómo volver a hacer demostrable la pregunta más básica de todo el negocio: **¿un anuncio se sirvió de verdad a una persona real?**

El anuncio que nadie vio

La magnitud es estremecedora. La empresa de análisis Juniper Research calcula que el fraude publicitario digital costó 84.000 millones de dólares en 2023 —un 22 % de toda la inversión publicitaria en línea, y hasta el 30 % en móvil—, y proyecta que llegará a 172.000 millones en 2028 [1]. No es extraño si consideramos un hecho que espeluzna: según la empresa de seguridad Imperva, en 2023 los bots representaron el 49,6 % del tráfico de Internet, y los bots maliciosos, un 32 %, crecieron por quinto año consecutivo e imitaron el comportamiento humano para evadir la detección [4]. Cuando la mitad del tráfico no es humano, saber quién ve de verdad un anuncio deja de ser un detalle técnico y se convierte en el problema central del sector.

El dólar que se evapora

Pero el fraude criminal es solo una parte. La otra es la **opacidad de la cadena**. La asociación norteamericana de anunciantes, la **ANA**, dirigida por Bob Liodice, publicó en diciembre de 2023 un estudio que mostraba que, de cada dólar que un anunciante pone en el sistema, solo **36 céntimos** llegan realmente al consumidor; el resto se esfuma en costes de transacción y en «pérdida de productividad mediática», un eufemismo que incluye los sitios llamados *made-for-advertising* —webs basura creadas solo para captar anuncios—, que llegaron a llevarse el 15 % de la inversión [2]. La ANA calcula que los anunciantes podrían recuperar unos **22.000 millones de dólares** solo depurando su cadena [2]. Como advierte el investigador independiente **Augustine Fou**, una de las voces más críticas del sector, las propias plataformas dan una imagen incompleta del éxito de las campañas y las cifras de fraude que la industria reporta tienden a subestimar el problema.

…y este nudo de todo ello es, una vez más, un problema de **prueba**: nadie puede demostrar de manera independiente que una impresión se sirvió a un humano real, en un lugar y un momento concretos. Existen estándares de transparencia —el ads.txt del IAB Tech Lab, que declara qué vendedores están autorizados— y métricas de visibilidad, pero todos descansan en la confianza y en datos que controla quien vende el inventario.

La prueba de existencia: el ojo humano demostrable

Es aquí donde **t2p** llena el vacío. Cada evento de impresión genera un registro —anuncio servido, identificador de dispositivo atestado, visibilidad según el estándar del sector, geolocalización— y el **SHA-512** correspondiente se ancla a la **blockchain pública** con un **sello de tiempo RFC 3161** conforme a eIDAS. El registro queda inalterable: nadie puede inflar después las cifras ni reescribir cuántas veces se ha visto un anuncio. Además, igual que el ads.txt declara *quién* puede vender, **t2p** puede **encadenar y sellar criptográficamente cada salto** de la cadena —del editor a la plataforma de venta, al

intercambio, a la plataforma de compra—, de manera que cada reventa quede con su huella, hora y origen verificables. Así, como hemos visto, estos importes perdidos se convierten en una cadena trazable. Y para validar el alcance real de un influencer, una campaña con **prueba de vida** y **GPS forense** puede demostrar que detrás de un visionado hay una persona viva en un lugar real, no una granja de seguidores falsos —un fraude que cuesta centenares de millones a las marcas. Todo se empaqueta en un **.asice verificable sin conexión** que un tercero independiente puede auditar sin depender de quien vende el inventario, precisamente la «imagen incompleta» que denuncia Fou.

Hay que decir el límite sin ambages, porque aquí es triple. La prueba de existencia demuestra integridad, hora, lugar y —con prueba de vida— presencia humana de un registro, pero no resuelve por sí sola tres cuestiones. La primera, la **privacidad**: verificar que detrás de cada impresión hay un humano real implica, por definición, recoger señales del dispositivo o de la persona —la misma tensión entre vigilancia y transparencia que recorre todo el libro—, y exige minimizar los datos y atestar sin identificar al usuario. La segunda, que **los bots evolucionan**: Methbot ya falseaba cursores, y una atestación de hoy será evadida mañana; la prueba reduce el fraude, no lo elimina. Y la tercera, que **no corrige el desalineamiento de incentivos**: mientras los intermediarios cobren por impresión servida y no por valor entregado, habrá presión por inflar. «Basura a la entrada, basura en la cadena»: la criptografía hace el registro inviolable, pero no garantiza honestamente qué se ha de registrar.

La promesa y el peligro

La promesa se puede cuantificar en decenas de miles de millones; una capa de prueba de existencia sobre las impresiones y la cadena programática dificultaría cobrar por anuncios invisibles, ofrecería a los anunciantes una evidencia auditable por un tercero y recuperaría parte de estas cifras, como hemos visto. En un mercado donde la mitad del tráfico no es humano, demostrar el ojo humano real restaura el fundamento de todo el negocio.

El peligro pide el matiz de siempre. Primero, la privacidad: hay que evitar que la lucha contra el fraude se convierta en vigilancia del usuario. Segundo, el exceso de confianza: ninguna atestación es definitiva ante bots que innovan sin parar. Y tercero, el incentivo: la tecnología registra inviolablemente, pero la honestidad de la cadena depende de quien la quiere. La prueba de existencia es una herramienta poderosa para la transparencia, no una bala de plata contra el fraude ni un sustituto para arreglar los incentivos del sector.

Es hora de actuar

Para los anunciantes: exigir una evidencia sellada y auditable para cada impresión, en lugar de confiar en las cifras del vendedor de inventario. Para la cadena programática (plataformas de venta y compra, intercambios): sellar cada salto para que cada reventa sea trazable. Para los organismos de estándares (IAB, métricas de visibilidad): integrar la prueba de existencia como refuerzo del ads.txt y de la viewability. Y para las plataformas: dejar de ofrecer una imagen incompleta y abrirse a la verificación independiente.

Una granja de bots cobró por trescientos millones de vídeos que nadie miró. Asignar a cada impresión y a cada salto de la cadena una prueba sellada del ojo humano real —sin olvidar nunca la privacidad ni los incentivos— es, en este frente del comercio de la atención, time2act.

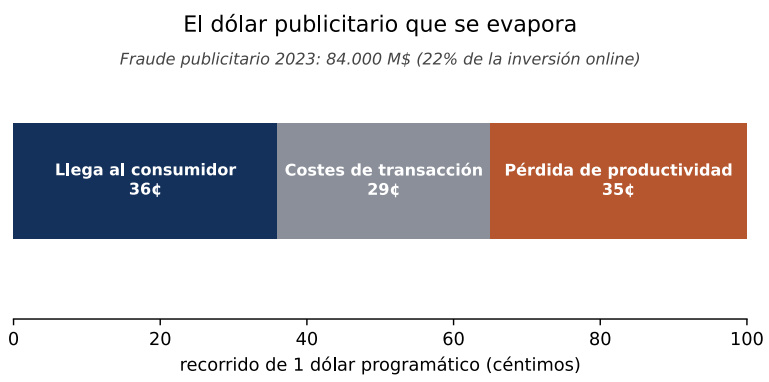


Figura 56.1 — De cada dólar que un anunciante pone en la compra programática, solo 36 céntimos llegan al consumidor: 29 se pierden en costes de transacción y 35 en «pérdida de productividad mediática» (webs basura e inventario de baja calidad). El fraude publicitario digital costó 84.000 millones de dólares en 2023 —un 22 % de la inversión en línea— y los bots ya son la mitad del tráfico de internet. Fuentes: ANA (2023); Juniper Research; Imperva.

---

[1] Juniper Research (vía PR Newswire) — *22% of online ad spend is wasted due to ad fraud in 2023* (84.000 M$ en 2023 → 172.000 M$ en 2028; móvil 30 %). https://www.prnewswire.com/news-releases/new-ad-fraud-study-22-of-online-ad-spend-is-wasted-due-to-ad-fraud-in-2023-according-to-juniper-research-301938050.html ↩

[2] Association of National Advertisers (ANA) — *Programmatic Media Supply Chain Transparency Study* (diciembre 2023; 36 céntimos por dólar; ~22.000 M$ recuperables; MFA 15 %). https://www.ana.net/miccontent/show/id/rr-2023-12-ana-programmatic-media-supply-chain-transparency-study ↩

[3] eMarketer — *5 key stats on ad waste, fraud, MFAs and brand risks* (MFA del 15 % al 4 %). https://www.emarketer.com/content/5-key-stats-ad-waste-fraud-mfas-brand-risks-beyond

[4] Imperva — *2024 Bad Bot Report* (los bots, el 49,6 % del tráfico de internet en 2023; bots maliciosos, el 32 %). https://www.imperva.com/company/press_releases/bots-make-up-half-of-all-internet-traffic-globally/ ↩

[5] Department of Justice (EDNY) — *Two international cybercriminal rings dismantled (Methbot y 3ve)* (noviembre 2018; 1,7 M de ordenadores; >29 M$). https://www.justice.gov/usao-edny/pr/two-international-cybercriminal-rings-dismantled-and-eight-defendants-indicted-causing ↩

[6] Krebs on Security / White Ops — *Report: $3-5M in ad fraud daily from Methbot* (2016; 300 M de visionados/día). https://krebsonsecurity.com/2016/12/report-3-5m-in-ad-fraud-daily-from-methbot/ ↩

[7] The Record (Recorded Future) — *«King of Fraud» sentenced to 10 years for Methbot/3ve* (Aleksandr Zhukov, 10-nov-2021). https://therecord.media/king-of-fraud-sentenced-to-10-years-in-prison-for-role-in-methbot-3ve-botnet ↩

[8] IAB Tech Lab — *ads.txt (Authorized Digital Sellers)* (2017; contra la suplantación de dominios). https://iabtechlab.com/ads-txt/

[9] CBS News / Cheq (Roberto Cavazos, Univ. de Baltimore) — *Influencer marketing fraud costs companies $1.3 billion* (2019). https://www.cbsnews.com/news/influencer-marketing-fraud-costs-companies-1-3-billion/

[10] Augustine Fou (FouAnalytics) — investigación independiente sobre el fraude publicitario digital. https://www.linkedin.com/pulse/how-do-we-un-fu-digital-advertising-dr-augustine-fou

Ciberseguridad: registros que el atacante no puede reescribir

«Quien controla el pasado controla el futuro; quien controla el presente controla el pasado.»

— George Orwell, 1984 (1949)

Cuando un atacante consigue entrar en una red, la primera acción que realiza no es robar; **borra su rastro**. Ejecuta una orden tan sencilla como `wevtutil cl Security` para vaciar el registro de seguridad de Windows y eliminar las pruebas de su paso. La maniobra tiene un nombre catalogado —la técnica **T1070, «Indicator Removal»**, del marco MITRE ATT&CK— y es tan esperada que los defensores la consideran un paso previsible, no una sorpresa [2]. Pero esconde una ironía reveladora: al vaciar aquel registro, Windows escribe automáticamente un nuevo evento, el **Event ID 1102** —«el registro de auditoría se ha borrado»—, con la cuenta que lo hizo [2]. Borrar la evidencia *crea* evidencia… **siempre que aquella evidencia haya salido a tiempo del sistema comprometido**.

Y aquí está el problema.

Según el informe anual de la unidad de respuesta a incidentes de Google y Mandiant, el tiempo medio que un atacante opera dentro de una red sin ser detectado —el *dwell time*— empeoró hasta los **catorce días en 2025** [1]. Catorce días son una eternidad: tiempo de sobra para manipular los registros si estos viven solo en los sistemas que el atacante ya controla. Este capítulo explica cómo convertir la historia de un ataque en un registro que **ni el atacante pueda reescribir**.

El atacante ataca la evidencia primero

La ciberseguridad ha aprendido una lección dura: el adversario ataca la prueba antes que tú. Las consecuencias de no poder demostrar qué pasó son cada vez más graves, porque hoy no responden solo los técnicos, sino también reguladores, tribunales y aseguradoras. Como hemos visto, aquel año el coste medio global de una brecha de datos fue de 4,44 millones de dólares, con 10,22 millones en Estados Unidos y una media de 241 días para identificarla y contenerla [4]. La presión reguladora se ha disparado: el reglamento europeo de protección de datos obliga a notificar una brecha en 72 horas; la directiva NIS2 y el reglamento DORA imponen plazos estrictos de notificación de incidentes; y la comisión de valores norteamericana exige divulgar un incidente material en cuatro días hábiles [5][6][7][8].

El caso de la ciudad de Hamilton, en Ontario, muestra hasta dónde llega. Después de un ataque de ransomware en febrero de 2024 que paralizó buena parte de su red, la aseguradora denegó la cobertura porque la ciudad no tenía plenamente desplegada la autenticación de doble factor, y dejó a los contribuyentes con una factura de hasta 18,3 millones de dólares canadienses [9]. Lo que los registros y las atestaciones de la ciudad podían demostrar —o no— decidió quién pagaba. En ciberseguridad, la integridad de la evidencia ya no es solo una cuestión técnica: es una cuestión de millones.

Sacar la evidencia del sistema atacado

La defensa estándar contra el borrado de registros consiste en sacarlos del sistema: **reenviarlos en tiempo real** hacia un almacén externo o a un sistema de gestión de eventos de seguridad, para que sobrevivan al vaciado local. Es una buena práctica, pero presenta un agujero: un atacante lo bastante hábil puede **desactivar el reenvío antes de actuar**. Y aunque los registros lleguen a un servidor externo, ¿quién garantiza que alguien —un interno o el atacante con acceso privilegiado— no los altere allí? Hace falta una garantía más fuerte: que la historia registrada quede con anclaje en un lugar que nadie pueda reescribir. Es exactamente lo que describe el estándar forense de referencia, la guía **NIST SP 800-86**: la utilidad de una prueba digital depende de poder demostrar que no se ha alterado y de una cadena de custodia que aguante ante un tribunal [3].

La prueba de existencia: registros que no se pueden reescribir

Es aquí donde **t2p** aporta ese anclaje. Un centro de operaciones de seguridad no puede anclar cada línea de registro —el volumen sería inviable—; lo que se ancla periódicamente es la raíz de un árbol de Merkle que resume todo un lote de registros. **t2p** toma la **huella SHA-512** de aquella raíz, junto con la cabecera

del lote (rango temporal, fuente, número de eventos), la **sella con un sello de tiempo RFC 3161** conforme a eIDAS y la **ancla a la blockchain pública**. La cadena de raíces forma una historia que solo se puede añadir, nunca modificar: cada raíz incorpora el estado anterior, de manera que reescribir un evento pasado obligaría a reescribir todas las raíces posteriores ya ancladas en una cadena pública —algo imposible sin que la verificación falle.

Esto frustra exactamente la técnica descrita; si el atacante borra o altera registros *después* de que su huella ya esté anclada, la discrepancia entre el registro reconstruido y la raíz anclada lo delata. Y si borra registros que **aún no** se habían anclado, el agujero en la continuidad de la cadena de raíces es una prueba de manipulación. Para la evidencia de una brecha —capturas, volcados de memoria, cronologías de la respuesta al incidente—, **t2p** genera un contenedor **.asice** verificable sin conexión con huella, sello de tiempo, **GPS forense** del lugar de captura y **prueba de vida** del analista que la recogió: una cadena de custodia alineada con el estándar que sirve ante un regulador, una aseguradora —el caso Hamilton— y un tribunal, demostrando *cuándo*, *dónde* y *quién* preservó cada artefacto, sin depender de la palabra de la víctima.

Hay que decir el límite con toda claridad, porque aquí es esencial. El anclaje **no impide la brecha**: no detiene al atacante ni cierra la vulnerabilidad. Solo protege **lo que se ha registrado**; si el registro tenía agujeros, estaba mal configurado o el atacante desactivó el reenvío antes de actuar, no hay nada que anclar —«basura a la entrada, basura en la cadena». La integridad es tan buena como la **inmediatez del reenvío** fuera del sistema comprometido: si la raíz se ancla cada hora y el atacante borra dentro de aquella ventana antes de la sincronización, aquel tramo no queda protegido. Y queda el coste de rendimiento: un centro de operaciones genera millones de eventos, y hay que elegir la frecuencia de anclaje. **t2p** garantiza que **nadie reescribió el registro sin dejar rastro**, no que el registro sea completo ni que refleje toda la verdad del ataque.

La promesa y el peligro

Así, la promesa es tangible: una capa de anclaje sobre los registros convertiría el clásico «tu palabra contra la mía» en una cronología que nadie puede tocar, haría inútil el borrado de rastros y daría al equipo de respuesta una evidencia admisible ante reguladores y aseguradoras. Además, podría ahorrar los millones perdidos por Hamilton; cuando una brecha cuesta de media más de cuatro millones de dólares, una prueba inalterable de lo que ha sucedido se convierte en un activo de primer orden.

El peligro requiere el matiz habitual. Primero, no confundir el anclaje con la prevención: sellar los registros no detiene ningún ataque. Segundo, evitar el exceso de confianza; la prueba solo vale tanto como el reenvío inmediato y la calidad del registro. Tercero, proteger la privacidad de los propios registros, que pueden contener datos sensibles y necesitan un diseño que ancle la huella, no el contenido en claro. La prueba de existencia es una herramienta poderosa para la fase posterior al incidente, pero no sustituye la defensa ni la buena higiene de seguridad.

Además, hay que reconocer que la inmutabilidad de la cadena protege la integridad de los registros sin garantizar la confidencialidad. Una vez un archivo se sube a una blockchain pública, cualquier nodo puede validarlo y, si dispone de información adicional, desanonimizarlo. Las agencias federales norteamericanas como ICE, IRS o FBI ya compran analítica de cadena para vincular direcciones IP con identidades reales, convirtiendo lo que debería ser una prueba anónima en un rastro directo hacia personas concretas [12]. Este escenario se vuelve especialmente peligroso cuando la carga útil es sensible: documentos médicos, informes financieros o datos personales. Un atacante que comprometa el punto de entrada inicial puede exponer todo el contenido, y la inmutabilidad solo asegura que la explotación persista indefinidamente. Como avisa Carissa Véliz, «es posible que la ciberseguridad no se alcance nunca», porque las defensas evolucionan a la misma velocidad que las técnicas de análisis y desanonimización [11].

Es hora de actuar

Para los centros de operaciones de seguridad y los responsables: aplicar anclaje a las raíces de Merkle de los registros en tiempo casi real, de manera que el borrado de rastros deje de funcionar. Para los equipos de respuesta a incidentes: sellar la evidencia con cadena de custodia y hacerla admisible ante reguladores, aseguradoras y tribunales. Para las aseguradoras: reconocer la evidencia anclada como base para las decisiones de cobertura. Y para los reguladores (NIS2, DORA, la Comisión de valores): valorar el sello de origen como refuerzo de las obligaciones de notificación.

Un atacante intenta borrar los registros para eliminar su rastro, pero el vaciado deja una huella —si esta aparece a tiempo. Asignar a cada registro y a cada pieza de evidencia un ancla inalterable que convierta la historia de un ataque en algo que nadie pueda reescribir es, en este frente, cada vez más caro, time2act.

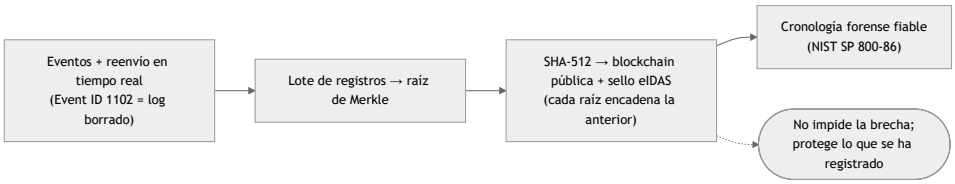


Figura 57.1 — Los eventos del sistema (incluido el Event ID 1102, «se ha borrado el registro») se reenvían en tiempo real fuera del sistema atacado; los lotes de registros se resumen en una raíz de Merkle que se sella con huella SHA-512 y sello de tiempo RFC 3161/eIDAS y se ancla a la blockchain pública, encadenando cada raíz con la anterior (solo se puede añadir). Cualquier alteración posterior rompe la huella y delata al atacante. Límite: el anclaje no impide la brecha; solo protege lo que se ha registrado y reenviado a tiempo. Contexto: dwell time medio de 14 días en 2025; coste medio de una brecha, 4,44 M$. Fuentes: MITRE ATT&CK; Mandiant M-Trends; NIST SP 800-86.

---

[1] Mandiant / Google Cloud — *M-Trends 2026* (dwell time medio de 14 días en 2025; traspaso de acceso en 22 segundos). https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026 ↩

[2] MITRE ATT&CK — *T1070 Indicator Removal / T1070.001 Clear Windows Event Logs* (el borrado deja el Event ID 1102). https://attack.mitre.org/techniques/T1070/001/ ↩

[3] NIST — *SP 800-86: Guide to Integrating Forensic Techniques into Incident Response* (2006; fases forenses y cadena de custodia). https://csrc.nist.gov/pubs/sp/800/86/final ↩

[4] IBM — *Cost of a Data Breach 2025* (coste medio global de 4,44 M$ / 10,22 M$ en EE. UU.; 241 días para identificar y contener). https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai ↩

[5] Comisión Europea — *NIS2 Directive (UE 2022/2555)* (notificación en 24 h / 72 h; 23 estados en procedimiento de infracción). https://digital-strategy.ec.europa.eu/en/policies/nis2-directive ↩

[6] EUR-Lex — *DORA, Reglamento (UE) 2022/2554* (aplicable desde el 17-ene-2025; reporting de incidentes TIC graves). https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng ↩

[7] U.S. Securities and Exchange Commission — *Cybersecurity disclosure rule* (26-jul-2023; Form 8-K, ítem 1.05, en 4 días hábiles). https://www.sec.gov/newsroom/press-releases/2023-139 ↩

[8] GDPR-info — *Article 33 GDPR* (notificación de brecha de datos en 72 horas). https://gdpr-info.eu/art-33-gdpr/ ↩

[9] Global News — *Hamilton cyberattack cost* (la aseguradora deniega la cobertura por MFA incompleto; 18,3 M CAD). https://globalnews.ca/news/11313018/hamilton-cyberattack-cost/ ↩

[10] Richard Bejtlich (TaoSecurity) — *Mandiant global median dwell time* (dos años consecutivos de deterioro). https://taosecurity.blogspot.com/2026/03/mandiant-global-median-dwell-time.html

[11] Carissa Véliz (ed.) — *The Oxford Handbook of Digital Ethics* (Oxford UP, 2022). ↩

[12] FedScoop (2024-2025). https://fedscoop.com/ice-wants-more-blockchain-analytics-tech/ ↩

Tus datos filtrados: la reclamación del ciudadano

«Decir que no te importa la privacidad porque no tienes nada que ocultar no es muy diferente de decir que no te importa la libertad de expresión porque no tienes nada que decir.»

— Edward Snowden, Vigilancia permanente (2019)

El correo empieza con la frase de siempre: «La seguridad de tus datos es nuestra prioridad». Tres párrafos más abajo, en letra un poco más pequeña, admite que tu nombre, tu teléfono y tu DNI han sido «potencialmente afectados por un incidente». Y a partir de aquel día, la lluvia fina: el SMS de «tu banco» que no es tu banco, la llamada que sabe cosas que no debería saber, el intento de entrar en tus cuentas, la solicitud de duplicado de SIM que tú no hiciste. La brecha no es un hecho puntual: es un goteo que dura meses y años —y que casi nadie puede facturar a quien lo provocó.

El marco está, a medias [2]: el RGPD obliga a las empresas a notificar las brechas a la autoridad en 72 horas y, si el riesgo para los afectados es alto, a comunicarla directamente a los afectados —las obligaciones que el capítulo 57 explica desde el lado de la empresa. Y herramientas públicas como Have I Been Pwned permiten a cualquiera comprobar si su correo aparece en filtraciones conocidas. Lo que faltaba era la pieza económica: ¿quién paga el daño que esto hace?

Este capítulo es el espejo ciudadano del capítulo 57: allí, los registros de la empresa atacada; aquí, la vida de la persona cuyos datos ahora corren por el mercado negro. La identidad digital está en el capítulo 47; la estafa que usa datos filtrados contra las personas mayores, en el capítulo 85; el SIM-swap, en el capítulo 68. Pregunta clave: ¿se puede cobrar por el daño de una filtración? Respuesta: el Tribunal de Justicia europeo ha dicho que sí —sin umbral mínimo de gravedad— pero con tres condiciones que se han de PROBAR [1]. Y probarlas es, exactamente, una cuestión de cronología: la que se construye con **t2p** —huella calculada en el dispositivo y hora cierta anclada a la cadena pública (capítulo 13) [3]— desde el día que llega el aviso.

El TJUE abre la puerta — y le pone un umbral de prueba

El 4 de mayo de 2023, el Tribunal de Justicia de la Unión Europea dictó sentencia en el asunto C-300/21 —el caso del servicio postal austríaco que, mediante un algoritmo, infería la afinidad política de los ciudadanos sin su consentimiento— y fijó la doctrina del artículo 82 del RGPD [1]: el derecho a indemnización exige tres condiciones acumulativas —una infracción del reglamento, un daño (material o inmaterial) y una relación de causalidad entre una y otro.

La sentencia contiene dos tensiones que definen este capítulo. La favorable al ciudadano: el daño moral es indemnizable sin ningún umbral mínimo de gravedad —sentirse expuesto, humillado o angustiado cuenta. La dura: la mera infracción no basta —el daño se ha de probar, y la causalidad también; y la cuantificación queda en manos de los tribunales nacionales [1].

Europa ha dicho, pues, que tu malestar vale dinero —si lo pruebas. Y aquí es donde el ciudadano pierde siempre: la brecha ocurre un día, el phishing llega durante meses, el intento de suplantación al cabo de un año —y cuando la reclamación se presenta, todo son recuerdos dispersos en carpetas de correo basura borradas. La lectura práctica es la de este libro: la causalidad que el TJUE pide es, exactamente, una cronología —y las cronologías se construyen con fechas ciertas, no con memoria.

La prueba de existencia aplicada

El diario empieza el día que llega el aviso [3].

1. La notificación capturada

El correo o la carta que te informa de la brecha —o la página donde la empresa lo admite—, capturados con fecha cierta [3]. Es el primer eslabón de la causalidad: cuándo se supo, qué se admitió, qué datos se reconocieron afectados. Y si la empresa no te notificó cuando correspondía [2], la ausencia también se documenta: la fecha en que lo supiste por la prensa o por una herramienta pública, sellada.

2. El certificado de presencia

La comprobación en Have I Been Pwned —tu correo, en qué filtraciones aparece— capturada con el navegador certificado de t2p: la imagen completa y el código fuente, con fecha [3]. Tu presencia en la filtración deja de ser una afirmación tuya: es una consulta fechada de una fuente pública reconocida.

3. El diario del daño

Cada consecuencia, sellada en el momento: el SMS de phishing que cita tu nombre completo, la llamada que sabía tu DNI —grabación de conversación propia, como explica el capítulo 75—, el aviso de intento de acceso, la solicitud de duplicado de SIM que tú no hiciste (capítulo 68) [3]. Treinta segundos por pieza. Al cabo de un año, no tienes recuerdos: tienes una serie fechada que empieza justo después de la brecha —la relación de causalidad que el TJUE pide [1], hecha de hechos.

4. La reclamación que llega armada

El expediente entero —notificación, presencia, diario del daño— exportado como paquete .asice verificable sin conexión [3]: para la reclamación a la empresa, la denuncia ante la autoridad de protección de datos o la demanda civil del artículo 82 [1][2]. Y la simetría de siempre: la empresa que notificó bien y a tiempo —y que tiene sus registros del capítulo 57 anclados— puede acreditar su diligencia con la misma moneda.

Los límites, como siempre, por adelantado: el sello acredita la cronología —no la valoración del daño, que es del juez con el derecho nacional en la mano [1]. La correlación no siempre es causalidad: el phishing existía antes de la brecha, y el perito tendrá que valorar la conexión —la serie fechada lo ayuda, no lo sustituye. Y el diario del daño es tuyo: en el dispositivo, solo huellas en la cadena, revelación selectiva [3].

La promesa y el peligro

La promesa: ciudadanos que reclaman con cronologías en lugar de quejas [1][3]; empresas que responden con diligencia demostrable en lugar de plantillas; el daño moral de las filtraciones —reconocido por el TJUE sin umbral [1]— convertido en reclamaciones viables; y un incentivo nuevo y potente para que los datos se protejan antes: cuando el daño se puede probar, la negligencia sale cara.

Los peligros, que no son pocos.

El primero es **la industria de la reclamación**: despachos masificando demandas idénticas con daños de plantilla. El contrapeso es la misma doctrina: el TJUE exige daño y causalidad probados [1] —la reclamación de plantilla muere donde la cronología personal empieza.

El segundo es **la revictimización documental**. Pedir a la víctima que lo selle todo puede ser una segunda carga. El gesto ha de ser mínimo —la captura de diez segundos— y la herramienta, un aliado: quien no documenta no pierde sus derechos, solo su mejor prueba.

El tercero es **el diario como nuevo botín**: el expediente de tu daño contiene… más datos tuyos. Por eso la regla de oro: en el dispositivo, solo huellas en la cadena [3], y revelación selectiva ante quien corresponda.

El cuarto peligro es confundir el resarcimiento con la protección. Ningún sello evita la brecha ni devuelve los datos al bote. La prevención es tarea de las empresas —el capítulo 57— y del regulador; la prueba de existencia solo hace que, cuando fallen, el coste no lo pague en silencio la víctima.

Es hora de actuar

El diario se empieza el día uno —porque el día mil será tarde.

Para ti, ciudadano: cuando llegue el aviso de una brecha —o la sospecha—, empieza el diario: la notificación, la presencia, cada síntoma fechado [3]; la reclamación de mañana se construye el día uno.

Para las asociaciones de consumidores y los despachos: exigid y aportad cronologías ancladas —el TJUE os ha dado la puerta [1]; la clave es la causalidad fechada, no el volumen.

Para las empresas que custodian datos: notificad bien y ancladlo —vuestra diligencia demostrable es la diferencia entre un incidente y una condena; el capítulo 57 es el vuestro.

Para las autoridades de protección de datos: valorad el expediente fechado del ciudadano como lo que es —la causalidad hecha cronología [1]; y publicad guías para que documentar el daño esté al alcance de todos.

Para los legisladores: el artículo 82 ya está [1][2]; el paso pendiente es procesal —reconocer la cronología anclada como prueba cualificada del daño moral, para que reclamar no exija ser perito.

Tus datos pueden correr por lugares que nunca verás; que al menos el daño que te hagan deje un rastro que sí. Por la intimidad que se defiende con hechos, **time2act**.

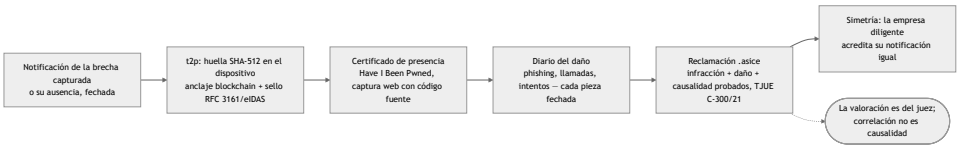


Figura 58.1 — La brecha vista desde el ciudadano, con prueba de existencia (sellado con t2p — capítulo 13): la notificación capturada (o su ausencia, fechada), el certificado de presencia en la filtración (captura web con código fuente), el diario del daño (phishing, llamadas, intentos —cada pieza sellada en el momento) y la reclamación .asice. Fundamento: TJUE C-300/21 —daño moral indemnizable sin umbral, pero con infracción + daño + causalidad PROBADOS. Simetría: la empresa diligente acredita su notificación. Límites: la valoración es del juez; correlación ≠ causalidad; el diario queda en el dispositivo. Fuentes: TJUE; RGPD art. 82.

---

[1] TJUE — *Sentencia de 4 de mayo de 2023, asunto C-300/21 (UI c. Österreichische Post)* (artículo 82 RGPD: tres condiciones acumulativas —infracción, daño y relación de causalidad; la mera infracción no da derecho a indemnización; el daño inmaterial es indemnizable sin umbral mínimo de gravedad; cuantificación según el derecho nacional con equivalencia y efectividad); análisis de Cuatrecasas, finReg360 y Confilegal. https://www.cuatrecasas.com/es/spain/art/indemnizacion-de-danos-morales-por-infraccion-del-rgpd · https://finreg360.com/alerta/el-tjue-dicta-sentencia-sobre-el-derecho-de-indemnizacion-por-tratamiento-de-datos-personales/ · https://confilegal.com/20230913-el-tjue-admite-que-los-danos-no-materiales-por-el-uso-ilicito-de-datos-personales-merecen-una-compensacion-economica/ · https://www.iberley.es/noticias/tjue-mero-incumplimiento-normativa-proteccion-datos-da-lugar-responsabilidad-pero-solo-dano-probado-resulta-indemnizable-33163 ↩

[2] RGPD (arts. 33-34: notificación de brechas a la autoridad en 72 h y a los afectados en caso de alto riesgo; art. 82: derecho a indemnización); Have I Been Pwned como herramienta pública de comprobación de filtraciones. Véase el capítulo 57 para el lado de la empresa. ↩

[3] t2p — manual de producto (captura de pantalla y de página web certificadas —imagen completa + código fuente; grabación de audio de conversaciones propias; certificar cualquier archivo; proyectos para el diario de un incidente; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión; solo huellas en la cadena). Véanse los capítulos 13 y 15; el SIM-swap, en el capítulo 68; la estafa con datos filtrados, en el capítulo 85. ↩

La caída documentada: SLA, nube y continuidad

«Ningún hombre es una isla, completo en sí mismo; cada hombre es un pedazo del continente, una parte del todo.»

— John Donne, Devociones, Meditación XVII (1624)

El 19 de julio de 2024, una actualización defectuosa del software de seguridad Falcon Sensor, de CrowdStrike, tumbó unos 8,5 millones de ordenadores Windows en todo el mundo —la caída informática más grande de la historia [1]. Pantallas azules en las terminales de los aeropuertos, en los quirófanos, en las sucursales bancarias, en los sistemas ferroviarios. Delta Air Lines canceló más de 7.000 vuelos en cinco días, con más de 1,3 millones de pasajeros afectados —y en octubre demandó a CrowdStrike reclamando unos 550 millones de dólares; las dos compañías acabaron demandándose mutuamente [1].

Aquel día, miles de empresas descubrieron a la vez tres cosas que daban por hechas. Que todo su negocio pende de un proveedor. Que el contrato promete «99,9 % de disponibilidad» con créditos de servicio como único remedio. Y que, cuando toca reclamar, la caída la tiene que probar el cliente —sobre las páginas de estado, los paneles y las mediciones del mismo proveedor que ha fallado. ¿Quién cayó, cuándo exactamente, durante cuánto tiempo, con qué impacto? Las respuestas oficiales las escribe una de las partes.

Este capítulo trata la disponibilidad —el hermano olvidado de la seguridad. Los registros que un atacante no puede reescribir están en el capítulo 57; las telecomunicaciones y la voz, en el capítulo 68; la reclamación al seguro, en el capítulo 28. Pregunta clave: ¿de quién es el reloj cuando la nube cae? Respuesta: de quien la ha provocado —salvo que el cliente tenga el suyo, con fecha cierta oponible: la monitorización independiente sellada con **t2p** —huella, hora cierta y ancla pública, la maquinaria del capítulo 13 [3]. Y con la simetría de siempre: el proveedor que cumple tiene, en sus propios registros anclados, el mejor argumento comercial del sector.

El reloj del proveedor

La anatomía del problema, pieza a pieza. El SLA —el acuerdo de nivel de servicio— promete un porcentaje de disponibilidad y ofrece créditos cuando se incumple; pero los créditos no son automáticos: exigen que el cliente reclame dentro de un plazo, y la carga de la prueba es suya. La medición oficial es del proveedor: sus páginas de estado —que durante los incidentes a menudo van por detrás de la realidad—, sus paneles, sus métricas. Y las herramientas de medida del cliente, para colmo, a menudo corren en la misma nube que se está hundiendo.

El crédito, además, cubre una fracción de la factura mensual. El daño real —las ventas perdidas, el TPV parado, la reputación— queda fuera, y exige prueba pericial del lucro cesante. Sin una cronología fiable y verificable, la negociación con el proveedor y con la aseguradora es un juego de versiones.

Y el contexto regulador sube el listón: DORA obliga al sector financiero europeo a gestionar el riesgo TIC de sus proveedores y a reportar incidentes con precisión, y la NIS2 extiende las obligaciones de notificación a muchos más sectores —ambas piden, en el fondo, cronologías fiables [2]. El registro del tiempo ya no es solo una cuestión contractual: es un requisito legal.

La conclusión es la de este libro: la disputa de la caída es una disputa de relojes —y hoy casi todos los relojes admisibles son de la misma banda. Lo que falta no es más monitorización: es que la monitorización del cliente tenga fecha cierta oponible.

La prueba de existencia aplicada

El momento en que el servicio cae es el único instante que el cliente no se puede permitir perder [3].

1. La sonda independiente sellada

La empresa monta sus sondas —comprobaciones periódicas del servicio desde fuera de la nube vigilada— y sella sus resultados con t2p: el archivo de registros de cada intervalo, certificado por huella con fecha cierta; solo la huella se ancla, el registro queda en casa [3]. La cadencia la elige cada negocio; lo que

importa es la cadena: cuando llega la caída, la secuencia «respondía — respondía — no responde — no responde» tiene sellos de tiempo que ninguna de las dos partes puede mover. El reloj del cliente, por fin, existe.

2. La página de estado, congelada

Durante el incidente, la página de estado del proveedor se captura con el navegador certificado de t2p —la imagen completa y el código fuente, empaquetados con fecha cierta [3]. Lo que el proveedor decía a las 10:42 —«todo operativo» o «incidente en investigación»— queda congelado. Si después la narrativa oficial cambia, la discrepancia es un hecho fechado, no un recuerdo.

3. El impacto documentado

La transacción que falla, grabada en pantalla y certificada [3]: el carrito que no cobra, el TPV que no responde, la cola de pedidos parada. Las exportaciones de métricas de negocio —ventas por hora, transacciones completadas—, selladas por huella. Cuando haya que cuantificar el lucro cesante ante la aseguradora o el juzgado, el perito trabajará sobre una cronología anclada, no sobre reconstrucciones.

4. La reclamación que se sostiene

El paquete .asice del incidente [3]: sondas, capturas de estado, impacto, comunicaciones con el proveedor —cada pieza verificable sin conexión y sin confiar en nadie. Para los créditos del SLA, para el ciberseguro, para el reporte regulador de DORA o NIS2 [2]: la misma evidencia sirve a todos los frentes. Y la simetría: el proveedor serio que publica sus propios registros de disponibilidad anclados convierte su SLA en su mejor argumento —contra la reclamación oportunista, sus sellos; contra la competencia, su transparencia.

Los límites, de entrada: el sello acredita cuándo el servicio no respondía desde donde medía la sonda —no diagnostica la causa ni reparte culpas entre proveedor, red y cliente: eso es tarea de peritos. Una sonda mal diseñada sella su propia confusión —metodología primero, criptografía después. Y ninguna huella levanta un servicio caído: la continuidad se construye con redundancia y planes de contingencia —la prueba solo hace que el daño, cuando llegue, no sea también una disputa de cronologías.

La promesa y el peligro

La promesa: créditos de SLA que se reclaman con cronologías propias [3]; disputas como las de julio de 2024 [1] que se podrían dirimir sobre registros anclados de las dos partes en lugar de años de litigio; aseguradoras y reguladores [2] trabajando sobre hechos fechados; y proveedores que compiten publicando su disponibilidad verificable.

Y ahora, los peligros, sin edulcorar.

El primero es **la guerra de sondas**: cada parte midiendo desde donde más le conviene. La respuesta es metodológica —sondas desde puntos representativos, metodología declarada y sellada por adelantado, como el compromiso previo del capítulo 45, y peritos que valoren la calidad de la medición, no solo su fecha.

El segundo es **el proveedor a la defensiva**. Si el rastro del cliente solo sirve para litigar, la relación se tensa. La salida es la simetría: el proveedor que ancla sus registros gana la presunción de seriedad —la transparencia verificable como estándar del sector, no como arma.

El tercero es **el papel mojado regulador**. DORA y NIS2 [2] piden reportes; si los reportes se fabrican a posteriori, todo el edificio es decorativo. La cronología anclada es el mínimo para que el cumplimiento signifique algo.

El cuarto es brutal de tan simple: la prueba no levanta servidores. Ningún sello sustituye la redundancia, el multiproveedor ni el plan de contingencia. Primero, que el negocio sobreviva a la caída; después, que la pueda probar.

Es hora de actuar

Que la próxima caída encuentre a cada empresa con reloj propio.

Para las empresas que viven en la nube: montad la sonda independiente y sellad su cadena [3]; el día de la próxima gran caída [1], la cronología será vuestra.

Para los proveedores de nube y hosting: anclad vuestros registros de disponibilidad y publicadlos por huella —el SLA verificable es marketing que ningún competidor puede copiar sin cumplir.

Para las aseguradoras de cyber y lucro cesante: exigid cronologías ancladas en la póliza; pagaréis más rápido los siniestros reales y menos los fabricados.

Para los reguladores financieros y de ciberseguridad: DORA y NIS2 [2] ya piden cronologías de incidentes —que sean verificables, no narrativas.

Para los legisladores: los créditos de SLA con medición unilateral son una cláusula coja; el reconocimiento de la medición independiente con fecha cierta equilibraría el contrato más asimétrico de la economía digital.

La próxima pantalla azul global llegará. Que encuentre a cada empresa con su reloj sellado —y que la discusión sea de causas, no de cronologías. Por la economía que no puede detenerse, **time2act**.

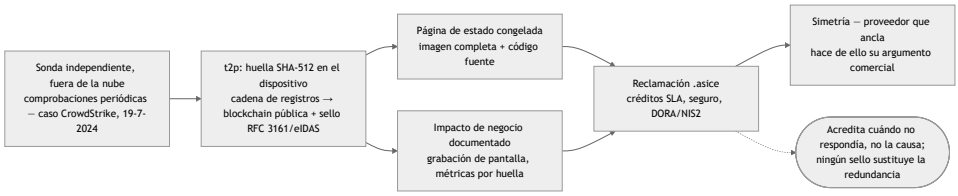


Figura 59.1 — La caída documentada con prueba de existencia (sellado con t2p — capítulo 13): la sonda independiente con cadena de registros sellados (el reloj del cliente), la página de estado del proveedor congelada con código fuente, el impacto de negocio documentado (grabación de pantalla, métricas por huella) y la reclamación .asice —para los créditos del SLA, la aseguradora y los reportes DORA/NIS2. Simetría: el proveedor que ancla su disponibilidad hace de ello su argumento comercial. Límites: la sonda acredita cuándo no respondía, no la causa; metodología primero; ningún sello sustituye la redundancia. Fuentes: CrowdStrike 19-7-2024 (8,5 M de Windows; Delta ~550 M$).

---

[1] Wikipedia — *2024 Delta Air Lines disruption* / TechTarget — *CrowdStrike outage explained* (19-7-2024: actualización defectuosa de Falcon Sensor; ~8,5 millones de Windows; la caída informática más grande de la historia; impacto en aerolíneas, hospitales, bancos, emergencias); CNBC — *Delta, CrowdStrike sue each other over widespread IT outage* (Delta: >7.000 vuelos cancelados en cinco días, >1,3 M de pasajeros; demanda de octubre de 2024 por ~550 M$; demandas cruzadas). https://en.wikipedia.org/wiki/2024_Delta_Air_Lines_disruption · https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next · https://www.cnbc.com/2024/10/25/delta-suit-against-crowdstrike-after-it-outage-caused-cancellations.html ↩

[2] Reglamento (UE) 2022/2554 (DORA — resiliencia operativa digital del sector financiero: gestión del riesgo TIC de terceros, reporte de incidentes; aplicable desde el 11-1-2025) y Directiva NIS2 (obligaciones ampliadas de notificación de incidentes). Véase el capítulo 57 para el contexto de seguridad y plazos de notificación. ↩

[3] t2p — manual de producto (certificar cualquier archivo —solo la huella viaja; captura de página web con imagen completa + código fuente; captura y grabación de pantalla certificadas; proyectos para agrupar el expediente de un incidente; certificación en segundo plano; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; los registros de un ataque, en el capítulo 57; la reclamación de seguro, en el capítulo 28. ↩

Arte y antigüedades: la procedencia contra la falsificación y el expolio

«Incluso en la reproducción más perfecta de una obra de arte le falta un elemento: su presencia en el tiempo y el espacio, su existencia única en el lugar en que se encuentra.»

— Walter Benjamin, La obra de arte en la época de su reproductibilidad técnica (1935)

En un garaje del barrio de Queens, en Nueva York, un pintor inmigrante chino llamado Pei-Shen Qian fabricaba obras maestras. Pintaba «Rothkos» y «Pollocks» que envejecía con té y con polvo de una aspiradora para simular décadas de suciedad, y cobraba menos de **nueve mil dólares** por lienzo. La galería más antigua de Nueva York, Knoedler & Company —fundada en 1846—, los vendía por millones a coleccionistas que confiaban en su prestigio de ciento sesenta y cinco años. El fraude, de unos **ochenta millones de dólares** en una cuarentena de falsificaciones, engañó a los expertos durante casi quince años, hasta que la galería cerró las puertas de golpe en 2011 [1].

Ahora bien, ¿cómo se destapó al mayor falsificador alemán de la posguerra? No fue un experto ni un documento, sino un **bote de pintura**. El falsificador Wolfgang Beltracchi había vendido un supuesto Campendonk por 2,88 millones de euros, pero el análisis de laboratorio detectó en él **blanco de titanio**, un pigmento que no existía en vida del artista [2]. Aquella molécula desencadenó una carrera de centenares de falsificaciones. La lección, que ponemos por delante porque es el corazón de este capítulo, es esta: lo que autentica una obra es la **ciencia y el ojo experto**, no el papel. Pero lo que decide si se puede vender, robar o restituir es otra cosa: la **procedencia**, su historial de origen y propiedad. Y aquí la mentira campa libre.

La mentira sobre el origen

Si la falsificación ataca *quién* hizo una obra, el expolio ataca *de dónde* viene. El caso más emblemático es el del marchante Subhash Kapoor, propietario de una galería de Manhattan, que dirigió una red internacional de tráfico de antigüedades valorada en unos cien millones de dólares. Uno de sus objetos era un Shiva danzante de bronce del siglo XI, arrancado de un templo en desuso de Tamil Nadu y vendido en 2008 a la Galería Nacional de Australia por 5,6 millones de dólares con papeles de procedencia falsos. La unidad antitráfico de la fiscalía de Manhattan acabó confiscando más de 2.500 piezas vinculadas a Kapoor, valoradas en unos 143 millones, y él fue condenado a diez años de prisión en la India en 2022 [3]. Como explica el arqueólogo forense Christos Tsirogiannis, de la Universidad de Cambridge, que ha identificado miles de antigüedades expoliadas cruzándolas con archivos confiscados a traficantes, la «procedencia» que exhiben casas de subastas y museos a menudo es un relato fabricado que empieza justo después del expolio: el problema no es la falta de papeles, sino que los papeles mienten.

La magnitud es tan grande como opaca. INTERPOL estima el comercio ilícito de antigüedades entre 225 millones y 6.000 millones de dólares al año —la enorme horquilla refleja la opacidad del mercado [8]. En Siria, como hemos visto, se han robado decenas de miles de piezas de yacimientos y museos. Y el problema tiene una versión histórica que aún escuece: el arte expoliado por los nazis, como las 1.406 obras —Picasso, Matisse, Chagall— que un control aduanero rutinario descubrió en 2012 escondidas en el apartamento de Múnich de Cornelius Gurlitt, hijo de uno de los marchantes de Hitler [5]. Ante esto, la comunidad internacional ha construido defensas: la Convención de la UNESCO de 1970 contra el tráfico ilícito, ratificada por cerca de 150 estados [7]; los Principios de Washington de 1998 sobre la restitución del arte nazi [6]; y bases de datos como el Art Loss Register, fundado por Julian Radcliffe en 1991, que tiene registrados unos 700.000 objetos robados y ha recuperado por valor de más de cien millones de dólares [9]. La tesis de Radcliffe es luminosa: si todo el arte robado se registra en un solo lugar y todo el que compra o vende lo consulta, robar deja de ser rentable porque la pieza no se puede revender limpiamente.

La prueba de existencia: la procedencia desde el segundo cero

Es aquí donde **t2p** aporta lo que falta: una **cadena de procedencia** como sucesión de eventos verificables. Cada nuevo eslabón —un certificado de autenticidad, un informe de condición, una factura, un dictamen de experto, un cambio de propietario, una fotografía de alta resolución— se resume en una

huella SHA-512 en el dispositivo, se ancla a la **blockchain pública** con un **sello de tiempo RFC 3161** conforme a eIDAS y se empaqueta en un contenedor **.asice verificable sin conexión**.

Pero la aplicación más potente es arqueológica. En una excavación legal, el arqueólogo puede sellar *in situ* la fotografía del **lugar exacto del hallazgo** —con GPS forense y sello de tiempo— antes de mover la pieza. Esto crea una prueba digital de excavación regulada que distingue el descubrimiento legítimo del expolio: es exactamente la diferencia entre el Shiva de Kapoor, con papeles inventados años después, y un objeto con su **origen documentado desde el segundo cero**. Y la **prueba de vida** liga al perito o al excavador que firma el dictamen a una persona real y viva en aquel momento, dificultando los «expertos fantasma» y los certificados firmados a posteriori que aparecen en casos como el de Knoedler. Contra el patrón de Kapoor y Tsirogiannis, un registro sellado y fechado hace que inventar un historial *después* del momento del sellado sea detectable.

Hay que decir el límite con toda la crudeza, porque aquí es absoluto. La prueba de existencia **no autentica el objeto**. Sellar la fotografía de un Beltracchi no lo convierte en un Campendonk auténtico: una foto sellada de una falsificación sigue siendo una falsificación. La autenticación sigue exigiendo el ojo experto y el análisis científico —los pigmentos, la datación— que fue lo que de verdad pilló a Beltracchi. Y, aún más importante, **toda procedencia fabricada *antes* del sello queda fabricada para siempre**: la cadena hereda y petrifica la mentira. «Basura a la entrada, basura en la cadena.» El valor real de t2p no es sellar historiales antiguos y dudosos, sino sellar el origen **en el momento exacto** en que nace la prueba —el find-spot de una excavación, el dictamen de un perito identificado—, para que a partir de aquel instante la mentira ya no se pueda colar.

La promesa y el peligro

La promesa es grande para un mercado carcomido por la opacidad. Una cadena de procedencia sellada desde el origen haría mucho más difícil el expolio —porque una antigüedad sin find-spot documentado sería inmediatamente sospechosa—, dificultaría las procedencias «blanqueadas» a posteriori y daría a museos, compradores y jueces una evidencia incontestable del historial de una obra. En un comercio donde robar un templo puede rendir millones, la procedencia verificable es la mejor defensa del patrimonio de la humanidad.

El peligro pide el matiz de siempre, y aquí es especialmente importante. El primero, ya dicho: confundir la procedencia con la autenticidad sería fatal; el sello no hace auténtico nada, y la ciencia ha de seguir siendo insustituible. El segundo, que la cadena petrifica lo que se le dé: una procedencia falsa sellada hoy será una mentira inmutable mañana. Y el tercero, que la parte que de verdad importa —la inspección física, el ojo del experto, el contexto histórico— vive fuera de la cadena. La prueba de existencia es una herramienta poderosa para documentar el origen desde el segundo cero, no un certificado de autenticidad ni un sustituto del conocimiento experto.

Es hora de actuar

Para los museos y casas de subastas: exigir una procedencia sellada y, sobre todo, puntos de hallazgo documentados desde la excavación, evitando comprar piezas con historiales que empiezan sospechosamente tarde. Para los arqueólogos y las excavaciones legales: sellar el lugar del hallazgo in situ para generar una prueba que distinga el descubrimiento del expolio. Para los marchantes y compradores: consultar registros como el Art Loss Register y no confiar en documentos engañosos. Para los reguladores y la UNESCO: reconocer la cadena de procedencia sellada como estándar del comercio legítimo. Y para todos, recordar que ningún sello sustituye **NUNCA** el ojo del experto ni el laboratorio.

Un bote de blanco de titanio reveló al falsificador más destacado de Europa; unos documentos falsos permitieron vender un dios robado por millones. Asignar a cada obra una procedencia sellada desde su origen —sin olvidar nunca que la autenticación requiere ciencia, no solo una huella— es el frente que custodia la memoria y la belleza, time2act.

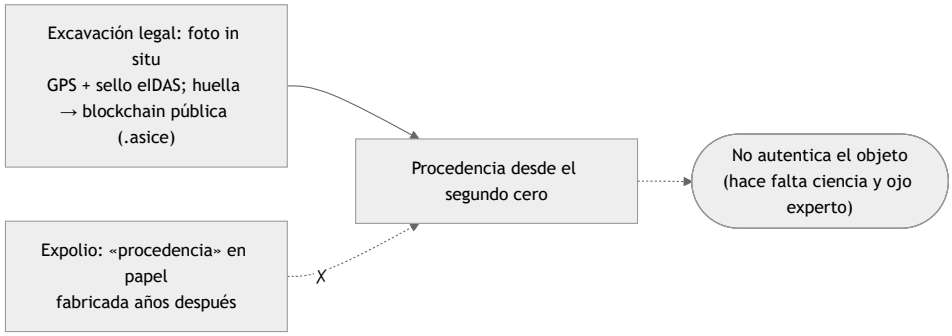


Figura 60.1 — En una excavación legal (izquierda), la pieza se fotografía in situ con coordenadas GPS y sello de tiempo eIDAS antes de moverla: la procedencia queda documentada desde el segundo cero y se ancla a la blockchain pública (.asice). En el expolio (derecha), la «procedencia» en papel empieza años después del hallazgo y es fácil de fabricar —como el Shiva Chola vendido a Australia por 5,6 M$ con papeles falsos. Límite: el sello prueba integridad, fecha, lugar y persona, pero NO autentica el objeto (una foto sellada de una falsificación sigue siendo una falsificación). Contexto: comercio ilícito de antigüedades de 225 M$ a 6.000 M$/año. Fuentes: INTERPOL; fiscalía de Manhattan; Art Loss Register.

---

[1] CNBC — *This $80 million art scam fooled experts* (galería Knoedler; Pei-Shen Qian; <9.000 $ por obra). https://www.cnbc.com/2018/08/16/think-you-can-spot-a-fraud-this-80-million-art-scam-fooled-experts.html ↩

[2] The Art Newspaper — *How the detection of titanium white gave away Beltracchi* (2012; el pigmento imposible). https://www.theartnewspaper.com/2012/12/01/how-the-detection-of-titanium-white-gave-away-beltracchi ↩

[3] OCCRP — *India sentences notorious antiquities trafficker from Manhattan* (Subhash Kapoor; >2.500 piezas, ~143 M$; Shiva Chola). https://www.occrp.org/en/news/india-sentences-notorious-antiquities-trafficker-from-manhattan ↩

[4] Manhattan District Attorney's Office — *Antiquities Trafficking Unit* (~6.000 antigüedades de 29 países, >460 M$ recuperados). https://manhattanda.org/d-a-bragg-announces-return-of-antiquities-to-spain-and-cyprus/

[5] The Conversation — *The Gurlitt case: how a routine customs check uncovered a Nazi-era art hoard* (1.406 obras). https://theconversation.com/the-gurlitt-case-how-a-routine-customs-check-uncovered-a-sensational-nazi-era-art-hoard-105604 ↩

[6] U.S. Department of State — *Washington Conference Principles on Nazi-Confiscated Art* (1998; 44 países). https://www.state.gov/washington-conference-principles-on-nazi-confiscated-art ↩

[7] UNESCO — *1970 Convention against the illicit trafficking of cultural property* (~149 estados). https://www.unesco.org/en/fight-illicit-trafficking/about ↩

[8] INTERPOL — *Cultural heritage crime: the issues* (comercio ilícito de 225 M$ a 6.000 M$/año). https://www.interpol.int/en/Crimes/Cultural-heritage-crime/The-issues-cultural-property ↩

[9] Art Loss Register — *~700.000 objetos registrados; fundado por Julian Radcliffe (1991); >100 M$ recuperados.* https://www.artloss.com/ ↩

[10] CNN — *The forensic archaeologist hunting trafficked antiquities* (Christos Tsirogiannis; «los papeles mienten»). https://edition.cnn.com/2025/12/13/style/forensic-archaeologist-trafficked-antiquities-scli-intl

Memoria histórica: los archivos contra el negacionismo

«Quienes no pueden recordar el pasado están condenados a repetirlo.»

— George Santayana, La vida de la razón (1905)

En junio de 2024, la UNESCO y el Congreso Judío Mundial publicaron un informe que debería quitar el sueño a cualquier historiador: la IA generativa amenaza la memoria del Holocausto. No es una advertencia abstracta —trae ejemplos: ChatGPT había inventado campañas de un «Holocausto por ahogamiento», con nazis ahogando judíos en los ríos, un episodio que nunca existió; Bard había fabricado citas falsas de testimonios para apuntalar narraciones distorsionadas de masacres reales [1]. Pensemos un momento qué significa: la máquina no se limita a equivocarse —inventa atrocidades con apariencia de historia y testimonios con apariencia de voz humana, a escala industrial y con tono de enciclopedia. Y mientras tanto, los últimos supervivientes se apagan: pronto, toda la memoria viva será archivo —y el archivo, atacable.

Este libro ha defendido hasta aquí el presente: probar qué pasa ahora, mientras pasa. Este capítulo extiende la misma lógica hacia atrás. La procedencia de los objetos de arte se trata en el capítulo 60; la fotografía del presente, en el capítulo 17; la crisis general de la verdad, en el capítulo 10. Aquí la pregunta es otra: ¿cómo se protege el pasado, cuando fabricar «pruebas» de él cuesta un prompt? Respuesta: anclando la memoria antes de que llegue la riada —archivos con manifiestos sellados, testimonios con huella en vida, exhumaciones con cadena de custodia anclada y colecciones fotográficas con fecha cierta, con **t2p**: la huella SHA-512, el anclaje de la huella en la blockchain pública y el sello de tiempo RFC 3161/eIDAS complementario, dentro de un contenedor .asice [5]. El pasado no se puede cambiar; su prueba, sí —y por eso se ha de sellar.

La historia, reescrita a máquina

El informe de la UNESCO no se limita a los ejemplos: hace un diagnóstico estructural. Los modelos generativos tienden a simplificar en exceso la complejidad histórica y priorizan una pequeña selección de fuentes y eventos, dejando fuera matices y contextos enteros; las recomendaciones apuntan en dos direcciones —que las tecnológicas trabajen con supervivientes, descendientes, educadores e historiadores, y que los sistemas educativos equipen a la juventud con alfabetización digital y pensamiento crítico [1].

Y el fenómeno ya habla catalán y castellano. En febrero de 2025, Maldita.es documentaba cómo webs y revistas publicaban en portada imágenes generadas con IA de personajes y hechos reales —el papa, la científica Margarita Salas, escenas de la Guerra Civil española—, a menudo sin ninguna etiqueta que las identificara como sintéticas; el riesgo descrito: alterar la percepción de personajes y hechos históricos, generar falsos relatos y profundizar la desconfianza en los medios [2]. La imagen «de época» fabricada ya no es un ejercicio de laboratorio: es contenido editorial en circulación.

La mecánica del daño es el dividendo del mentiroso aplicado a la historia. Cuando las imágenes de época fabricadas son indistinguibles de las auténticas, pasa lo peor de los dos mundos a la vez: la foto falsa encuentra creyentes, y la foto verídica encuentra negacionistas —«esto es un montaje» se convierte en respuesta universal. Y el negacionismo, que siempre había tenido que trabajar contra los documentos, ahora puede fabricar documentos favorables. La batalla de la memoria deja de ser solo interpretativa para volverse probatoria: qué documentos existían, desde cuándo, y quién lo puede demostrar.

El archivo que tembló

El 9 de octubre de 2024 se supo que el Internet Archive —la biblioteca digital que custodia la memoria de la web— había sufrido una intrusión mayúscula: 7 terabytes sustraídos, con el código fuente de la institución y las direcciones y contraseñas con hash de 31 millones de usuarios, a partir de un token de GitLab que había quedado expuesto desde finales de 2022. Simultáneamente, ataques de denegación de servicio dejaron sin conexión la Wayback Machine, y una segunda brecha el mismo mes expuso más de 800.000 tiques de soporte, algunos con documentos de identidad. El servicio volvió a mediados de octubre, con funciones limitadas [3].

¿Por qué esto es más que un incidente técnico? Porque la Wayback Machine es la memoria de facto de internet: la herramienta con la que periodistas, jueces e investigadores demuestran que una página decía una cosa antes de que alguien la editara en silencio. Cada citación judicial o académica de una captura confía en la integridad y la disponibilidad de una infraestructura sostenida por una sola organización sin ánimo de lucro —atacable, como se vio, por un token olvidado y una avalancha de tráfico.

La lección no es culpar al Archive, una institución venerable y esencial: es entender que ninguna institución de memoria, por sólida que sea, puede garantizar sola la integridad de lo que custodia. La respuesta estructural son los manifiestos anclados: la huella de cada colección y de cada captura, con sello de tiempo, publicada en una cadena que ningún ataque a ningún servidor puede reescribir [5]. Si los contenidos se pierden, la existencia y la integridad de lo que había quedan acreditadas; si alguien los altera, la discrepancia canta. La memoria necesita copias; la confianza en la memoria necesita anclajes.

Las fosas que aún hablan

El frente español de este capítulo se llama Ley 14/2022, de Memoria Democrática: la Administración General del Estado asumió la responsabilidad de buscar a las personas desaparecidas durante la Guerra Civil y la dictadura, se creó el Banco Estatal de ADN de víctimas y se impulsó el Mapa Integrado de Fosas, que registra 5.848 fosas localizadas, de las cuales alrededor de 1.500 han sido abiertas [4]. El balance conocido en noviembre de 2025: 8.941 restos localizados y recuperados y unas 9.000 víctimas reparadas —pero solo 70 restos plenamente identificados y entregados a las familias, y más de 10.000 cuerpos aún por recuperar [4]. Cada cifra es una familia que espera.

El ángulo de este libro es el probatorio, y es rigurosamente neutral. Una exhumación es ciencia forense —estratigrafía, fotografías, objetos, muestras, ADN— y su fuerza depende de la cadena de custodia. Y es, a la vez, un acto expuesto a tres amenazas: la duda revisionista futura («estos restos no son lo que dicen»), la acusación de manipulación política y el error humano.

La documentación anclada protege el proceso de las tres. Cada estadio de la excavación puede quedar sellado en el momento —la fotografía de cada hallazgo con fecha cierta, el registro de muestras, la cadena de custodia hasta el Banco Estatal de ADN [4][5]—, y el resultado es un expediente que ningún negacionismo futuro podrá despachar como «fabricado» sin negar la matemática, y que ninguna sospecha de manipulación podrá manchar sin pruebas. El sello no sirve a una memoria contra otra: sirve a los hechos contra el olvido y contra la mentira, vengan de donde vengan.

La prueba de existencia aplicada

Un archivo comarcal cualquiera, una tarde de digitalización: el sonido de los escáneres, páginas amarillentas de un diario antiguo —y cada hoja, al nacer digital, recibe su fecha cierta.

1. El archivo anclado

Bibliotecas, hemerotecas y archivos —públicos, comunitarios, de exilio— publican manifiestos anclados de sus colecciones: la huella SHA-512 de cada documento y de cada lote, con sello de tiempo, en la blockchain pública [5]. La edición silenciosa de una noticia antigua se vuelve detectable por cualquiera; la pérdida de un servidor no borra la evidencia de lo que existía [3]; y la cita académica o judicial de un documento puede verificarse contra la huella original. Es la misma lógica que el libro ha aplicado a los comunicados oficiales (capítulo 86), extendida al tiempo profundo: no un archivo único y oficial, sino todos los archivos, cada uno con su integridad acreditada. Cuando aparezca un «artículo de 1940» recién fabricado, su ausencia del corpus anclado hablará por él.

2. El testimonio sellado

La generación de los supervivientes se acaba, y la UNESCO recomienda trabajar con ellos mientras están [1]. Cada testimonio grabado —voz, vídeo, transcripción— puede quedar sellado en vida del testigo: huella y fecha cierta que acreditan que aquellas palabras existían, exactamente así, en aquel momento [5]. Cuando dentro de veinte años un negacionista diga que un testimonio «fue fabricado a posteriori», o cuando una IA genere testimonios falsos con voz clonada [1], la diferencia será verificable: los testimonios reales tendrán prioridad temporal anclada; los fabricados, no. Y lo mismo vale para la memoria oral de la Guerra Civil: cada entrevista de historia oral sellada hoy es un documento blindado mañana.

3. La fosa documentada

Cada exhumación amparada por la Ley 14/2022 [4] puede anclar su expediente: fotografías de cada estrato con fecha cierta, actas del equipo forense, registro de hallazgos, cadena de custodia de las muestras hasta el Banco Estatal de ADN [4][5]. El resultado sirve a tres causas a la vez: la judicial (una cadena de custodia impecable), la familiar (una identificación trazable —que las 70 familias que ya han recibido sus restos [4] se conviertan en miles, con la misma certeza) y la histórica (un registro que diga, para siempre y con matemática detrás: aquí había una fosa, esto se encontró en ella, y este es su registro).

4. El horizonte pre-IA

Hay una ventana que se cierra: todo lo digitalizado y anclado antes de la madurez de la imagen sintética queda acreditado como anterior —un horizonte pre-IA que separa el corpus fotográfico verificable de todo lo que venga después. Museos, archivos fotográficos y colecciones familiares que anclen hoy sus digitalizaciones [5] crean el canon de referencia contra el cual las futuras imágenes «de época» fabricadas [2] se podrán contrastar: si una foto «de 1937» no aparece en ninguna parte del corpus anclado y emerge dentro de unos años, su ausencia de historia hablará por ella. Cada año que pasa sin anclar, el horizonte se difumina un poco más.

Los límites, dichos con claridad: el sello acredita cuándo se digitalizó o registró un documento y que no se ha alterado desde entonces —no acredita que el documento diga la verdad, ni sustituye la crítica de fuentes, que sigue siendo oficio de historiadores; no puede recuperar lo que nunca se documentó; y la historia es también interpretación —el sello protege los documentos y los hechos, no ningún relato único sobre los hechos.

La promesa y el peligro

La promesa es una memoria colectiva con integridad verificable: archivos que no se pueden editar en silencio [3], testimonios con prioridad temporal sobre sus falsificaciones [1], fosas con expedientes inatacables [4] y un canon fotográfico pre-IA contra la historia fabricada [2]. La verdad del pasado dejaría de depender de una sola voz o de un solo servidor: se validaría contra un tejido de huellas abierto a cualquiera.

Los peligros piden la misma claridad.

El primero es **el archivo único**. Si el anclaje se convierte en monopolio de un «archivo oficial de la verdad», habremos creado el ministerio que Orwell temía. La respuesta es la pluralidad: todas las memorias —institucionales, comunitarias, de exilio, disidentes— han de poder anclar sus fondos. El sello acredita integridad y fecha; nunca autoridad, nunca versión única.

El segundo es **la memoria contra el olvido personal**. Los archivos contienen datos de personas vivas y de familias. Anclar no es publicar: solo huellas en la cadena, con el acceso regulado por los marcos de cada archivo y por los derechos de las personas mencionadas. La inmutabilidad protege la integridad del documento; no puede servir para negar derechos a nadie.

El tercero es **el fetiche de la inmutabilidad**. La historia se corrige: aparecen documentos nuevos y se reinterpretan los viejos. El anclaje documenta versiones y fechas; no congela el conocimiento. Confundir «sellado» con «definitivo» sería traicionar el oficio que se quiere proteger —cada nuevo hallazgo se ancla como nueva versión, y el debate continúa.

Y el cuarto es **el tecnosolucionismo memorial**. Ninguna cadena de bloques enseña historia. Contra el negacionismo, la primera línea son la escuela, los historiadores y la alfabetización crítica que reclama la UNESCO [1]; el sello solo garantiza que, cuando haga falta demostrar qué existía, se pueda. Una sociedad que no quiera recordar no se salvará por criptografía.

Es hora de actuar

El pasado no se puede cambiar; su prueba, sí —y por eso hay que sellarla ahora.

Para archivos, bibliotecas y hemerotecas: publicad manifiestos anclados de las colecciones [3][5]; que cada edición silenciosa sea detectable y que ningún servidor caído se lleve la evidencia.

Para las instituciones de memoria y los equipos forenses: anclad los expedientes de exhumación —fotos, hallazgos, cadena de ADN [4][5]; las familias merecen certeza, y la historia, un registro inatacable.

Para supervivientes, familias y proyectos de historia oral: grabad y sellad los testimonios ahora, en vida [1][5]; la prioridad temporal será su escudo cuando lleguen las falsificaciones.

Para museos y colecciones fotográficas: anclad las digitalizaciones —el horizonte pre-IA se cierra cada día un poco más [2][5].

Para los medios: etiquetad toda imagen sintética de hechos o personajes reales [2] y anclad las hemerotecas —vuestra credibilidad retrospectiva también es patrimonio.

Para las empresas de IA y los legisladores: seguid las recomendaciones de la UNESCO —trabajar con supervivientes, educadores e historiadores [1]— y dotad a la Ley de Memoria Democrática [4] de los medios forenses y de anclaje que hagan su trabajo irreversible.

Una máquina inventó un «Holocausto por ahogamiento» que nunca existió [1]. Que cuando alguien lo «documente», el mundo pueda responder con un corpus anclado que demuestre qué es memoria y qué es fabricación. Por quienes ya no pueden testificar, **time2act**.

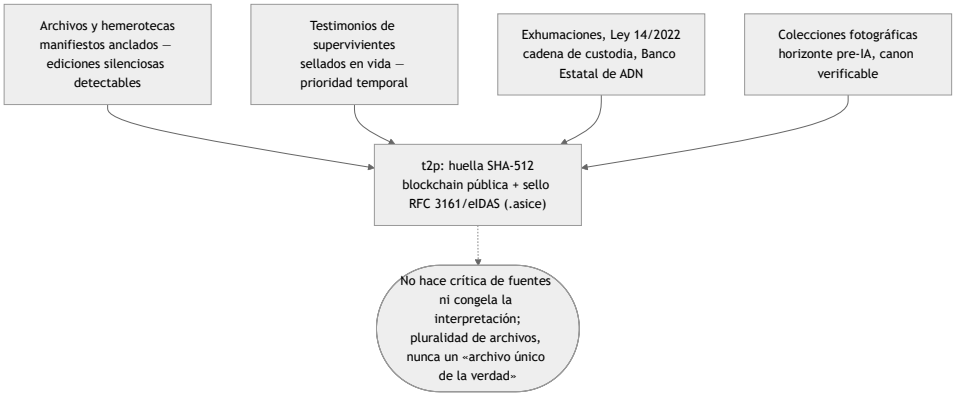


Figura 61.1 — Cuatro frentes de una misma defensa (huella SHA-512, sello de tiempo RFC 3161/eIDAS, anclaje a la blockchain pública, .asice): los manifiestos anclados de los archivos y hemerotecas (ediciones silenciosas detectables), los testimonios de supervivientes sellados en vida (prioridad temporal contra la fabricación), los expedientes de exhumación con cadena de custodia anclada (Ley 14/2022, Banco Estatal de ADN) y el horizonte pre-IA de las colecciones fotográficas (el canon verificable contra la historia sintética). Límites: el sello no hace crítica de fuentes ni congela la interpretación; pluralidad de archivos, nunca un «archivo único de la verdad». Fuentes: UNESCO/CJM; Maldita.es; Internet Archive (brecha 2024); Ley 14/2022.

---

[1] UNESCO — *New UNESCO report warns that Generative AI threatens Holocaust memory* (junio de 2024, con el Congreso Judío Mundial; ChatGPT y el falso «Holocausto por ahogamiento»; citas de testimonios fabricadas por Bard; simplificación excesiva; recomendaciones a tecnológicas y sistemas educativos); comunicado de prensa en castellano (PDF). https://www.unesco.org/en/articles/new-unesco-report-warns-generative-ai-threatens-holocaust-memory · https://articles.unesco.org/sites/default/files/medias/fichiers/2024/06/PR_New_UNESCO_report_warns_that_Generative_AI_threatens_Holocau ↩

[2] Maldita.es — *El papa, Margarita Salas y escenas de la Guerra Civil generadas con IA, en portada: cómo el uso de imágenes falsas en webs y revistas puede desinformar* (25 de febrero de 2025; imágenes sintéticas de hechos y personajes reales publicadas sin etiqueta; alteración de la percepción histórica y desconfianza en los medios). https://maldita.es/malditatecnologia/20250225/imagenes-IA-acontecimientos-reales-desinformar/ ↩

[3] Forbes — *Internet History Hacked, Wayback Machine Down — 31 Million Passwords Stolen* (octubre de 2024; 7 TB filtrados; token de GitLab expuesto desde finales de 2022; DDoS simultáneo sobre la Wayback Machine); NPR — *Hackers steal information from 31 million Internet Archive users*; Hispasec — *Internet Archive sufre su segunda brecha* (más de 800.000 tiques de soporte expuestos). https://www.forbes.com/sites/daveywinder/2024/10/10/internet-hacked-wayback-machine-down-31-million-passwords-stolen/ · https://www.npr.org/2024/10/20/nx-s1-5159000/internet-archive-hack-leak-wayback-machine · https://unaaldia.hispasec.com/2024/10/internet-archive-sufre-su-segunda-brecha-de-seguridad-en-octubre-de-2024.html ↩

[4] Infobae — *La Ley de Memoria Democrática impulsa la exhumación de fosas y la reparación de 9.000 víctimas: todavía quedan más de 10.000 cuerpos por recuperar* (18 de noviembre de 2025; 8.941 restos localizados y recuperados; solo 70 identificados y entregados; Mapa Integrado de Fosas: 5.848 fosas, ≈1.500 abiertas; Banco Estatal de ADN); El Español — *La nueva Ley de Memoria entra en vigor: el Gobierno quiere exhumar otros 25.000 cadáveres* (octubre de 2022). https://www.infobae.com/espana/2025/11/18/la-ley-de-memoria-democratica-impulsa-la-exhumacion-de-fosas-y-la-reparacion-de-9000-victimas-todavia-quedan-mas-de-10000-cuerpos-por-recuperar/ · https://www.elespanol.com/espana/20221020/nueva-ley-memoria-gobierno-quiere-exhumar-cadaveres/712178865_0.html ↩

[5] t2p — manual de producto (huella SHA-512 en el origen; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; manifiestos por lotes; contenido en los sistemas de cada archivo, solo huellas en la cadena). Véanse los capítulos 13 y 15; los comunicados oficiales, en el capítulo 86; la evidencia de crímenes de guerra, en el capítulo 20. ↩

Whistleblowing: probar sin delatarse

«Una palabra de verdad pesa más que el mundo entero.»

— Aleksandr Solzhenitsyn, conferencia Nobel (1970)

En junio de 2017, una contratista de la NSA de veinticinco años llamada Reality Winner imprimió un informe clasificado sobre la injerencia rusa en las elecciones estadounidenses y lo envió por correo al medio *The Intercept*. La redacción publicó un **escaneo de la copia impresa**. Pocos días después, el FBI llamaba a su puerta. El documento la delató con una traición invisible: unos **puntos amarillos minúsculos** que casi todas las impresoras láser de color incrustan en cada hoja —el código de identificación de la máquina—, y que, descodificados con la herramienta de la Electronic Frontier Foundation, revelaban el modelo de la impresora, su número de serie (29535218) y **la fecha y la hora exactas de impresión: 9 de mayo de 2017, a las 6:20** [6][8]. Los registros internos de la NSA mostraban que solo seis personas habían accedido al informe, y solo una lo había impreso. Reality Winner fue condenada a sesenta y tres meses de prisión, la pena más larga jamás impuesta en Estados Unidos a una fuente periodística [7].

Su caso contiene la advertencia que vertebra este capítulo y lo convierte en un espejo de todo el libro: **el anonimato es difícil, y ninguna tecnología puede salvar a un denunciante descuidado**. Pero también plantea el reto más delicado de todos: ¿cómo puede alguien probar que un documento es auténtico —para que el poder no lo pueda descartar como una falsificación— **sin, a la vez, delatarse a sí mismo**?

La tensión irreductible

La sociedad ha reconocido que los denunciantes son esenciales y ha construido defensas. La **Directiva europea de protección de los denunciantes** de 2019 convirtió la confidencialidad de la identidad de quien denuncia en una **obligación jurídica**, con canales seguros y protección frente a las represalias; en 2025, el Tribunal de Justicia de la UE multó con unos 39 millones de euros a cinco estados por no transponerla a tiempo —Alemania con 34 millones [2]. Y la **Freedom of the Press Foundation**, la ONG estadounidense, mantiene **SecureDrop**, un sistema de entrega anónima de documentos a través de la red Tor que usan más de sesenta redacciones —el *New York Times*, el *Guardian*, el *Washington Post*. Su filosofía es reveladora: la protección de la fuente no es solo legal, sino **arquitectónica** —el sistema está diseñado para que el periodista nunca conozca la identidad ni los datos de red del informante [3].

Pero la arquitectura de la vigilancia es igual de omnipresente. Como demostró la EFF al descodificar los puntos de las impresoras, el papel que sale de una máquina ya «firma» quién y cuándo lo imprimió. Y no es el único vector: la **estilometría** —la huella del estilo de escritura— puede atribuir la autoría de un texto con una precisión del 80 al 95 % [9]. La tensión, pues, es irreductible: probar **qué** sin revelar **quién**.

Que la verdad sobreviva sin la fuente

Y, sin embargo, se puede hacer. La prueba más grande de la historia lo demuestra. Los **Panama Papers** —11,5 millones de documentos, 2,6 terabytes del despacho Mossack Fonseca— fueron entregados por una fuente que solo se identificó como «John Doe», y que impuso una regla absoluta: únicamente canales cifrados, nunca un encuentro cara a cara [4]. Más de trescientos cincuenta periodistas de ochenta países, coordinados por el consorcio internacional ICIJ, verificaron su autenticidad y publicaron las revelaciones, que hicieron caer a un primer ministro y ganaron un premio Pulitzer. Al cabo de una década, la identidad de John Doe sigue siendo desconocida. En su manifiesto, reclamó para los denunciantes legítimos «inmunidad frente a la represalia gubernamental, sin excepciones» [5]. La lección es poderosa: la verificabilidad y el anonimato pueden coexistir. Se pudo probar que 2,6 terabytes de documentos eran genuinos sin necesidad de identificar a quien los había filtrado.

La prueba de existencia como escudo: lo que NO se sella

Es aquí donde **t2p** ofrece una herramienta con un diseño invertido respecto a todo el resto del libro. El denunciante calcula la **huella SHA-512** del documento **en su propio dispositivo** y ancla *solo* aquella huella a la **blockchain pública**, con un **sello de tiempo RFC 3161** conforme a eIDAS. Esto prueba dos

cosas verificables por cualquiera —que el documento **es auténtico y no se ha alterado**, y que **existía antes de un instante determinado**— sin subir el documento ni ningún dato personal.

Y aquí entra la pieza clave de este capítulo: la **divulgación selectiva**. Mediante pruebas de conocimiento cero, un periodista o un tribunal pueden verificar que el documento que han recibido coincide con la huella sellada —es decir, que es genuino y anterior a la filtración— **sin averiguar quién lo selló**. Se prueba una propiedad del documento, no la identidad del autor. Esto desmonta la defensa del «documento falso o manipulado»: la organización acusada no puede alegar que el filtrador lo fabricó después de los hechos, porque la huella y el sello lo anclan a una fecha anterior.

Pero lo más importante es lo que **no** se sella. A diferencia del flujo forense del resto del libro, aquí se omiten deliberadamente el GPS, la prueba de vida y los metadatos del dispositivo —precisamente aquello que delataría. El contenedor **.asice** se puede entregar al periodista **fuera de línea**, sin que la identidad real del filtrador toque nunca la red. Es el giro conceptual de esta obra: la **misma** tecnología que en los capítulos sobre fotoperiodismo y derechos humanos era un **riesgo** —anclar metadatos puede delatar a una fuente—, configurada con divulgación selectiva y omisión de metadatos, se convierte en un **escudo**. La diferencia no es la cadena de bloques, sino el diseño de qué entra en ella y qué se prueba sin revelar.

Y hay que decir el límite con toda la crudeza, porque aquí es vital y cierra el círculo del libro. **El anonimato es difícil, y la tecnología no salva a un filtrador descuidado.** El caso de Reality Winner lo grita: ni el cifrado más fuerte habría servido cuando la traicionaron los puntos de la impresora, los pliegues del papel y los registros de acceso internos. Una huella prueba existencia, integridad y momento —**no** que el contenido sea verdad ni que se obtuviera lícitamente: «basura a la entrada, basura en la cadena». Y quedan vectores de desanonimización que t2p no resuelve: los metadatos de red (hay que usar Tor o SecureDrop aparte), la estilometría, las marcas físicas del soporte. La regla de oro de este frente es la más contraintuitiva de todo el libro: lo que protege **es lo que se decide no sellar**.

La promesa y el peligro

La promesa es preciosa para la democracia. Una herramienta que permita a un denunciante probar que un documento es auténtico y anterior a una fecha, sin revelar quién es, daría al periodismo de investigación y a los tribunales una evidencia incontestable y protegería a la vez a la persona que arriesgó todo por decir la verdad. Es hacer que la verdad sobreviva sin que la fuente caiga.

El peligro, aquí, es sobre todo el de la **falsa seguridad**. Vender la prueba de existencia como una garantía de anonimato sería irresponsable y podría costar la libertad de alguien: el anonimato depende de una disciplina —Tor, dispositivos limpios, cuidado con el soporte físico y el estilo— que ningún sello sustituye. El sello tampoco hace verdadero un documento falso ni legitima una obtención ilícita. La prueba de existencia es una capa que protege *si y solo si* se diseña para omitir lo que delata; nunca una bala de plata contra una maquinaria de vigilancia que el caso Winner mostró implacable.

Además, el sello con hora se convierte en un **ancla temporal** que puede ser explotada como instrumento de coacción. En un proceso de investigación, quien controla la hora del sello puede demostrar que un documento fue «sellado» en un momento concreto, y ese rastro puede servir para identificar el instante exacto en que una persona expuso información sensible. Carissa Véliz ha mostrado cómo esta presión se traduce en autoinhibición: «entre un tercio y dos tercios de los escritores evitaron ciertos temas por miedo a la vigilancia gubernamental»[11]. El registro inmutable, que supuestamente protege la verdad, puede acabar convirtiéndose en una amenaza para la libertad de expresión: el simple hecho de saber que el sello deja constancia del momento puede disuadir la denuncia legítima y obligar a los potenciales informantes a autocensurarse, minando así el objetivo mismo de preservar la verdad.

Es hora de actuar

Por tanto, para los denunciantes: comprobar la autenticidad de lo que revelan sin anclar lo que los delata, y combinarlo con canales seguros como SecureDrop y una disciplina estricta. Para periodistas y plataformas de filtración: ofrecer divulgación selectiva para que se pueda verificar un documento sin conocer su fuente. Para los legisladores: cumplir y reforzar la directiva de protección de los denunciantes, que demasiados estados transpusieron tarde. Y para la ciudadanía: recordar que, sin quien se atreve a hablar —y sin herramientas que lo protejan—, mucha corrupción no se destaparía nunca.

Unos puntos amarillos invisibles enviaron a Reality Winner a la cárcel; un anónimo llamado John Doe sacudió el mundo y sigue libre. La diferencia, a menudo, es lo que se revela sin querer.

Dar a quien denuncia la manera de probar la verdad **sin delatarse** —sellando el documento y ocultando a la persona— es, en el frente que cierra esta parte, time2act.

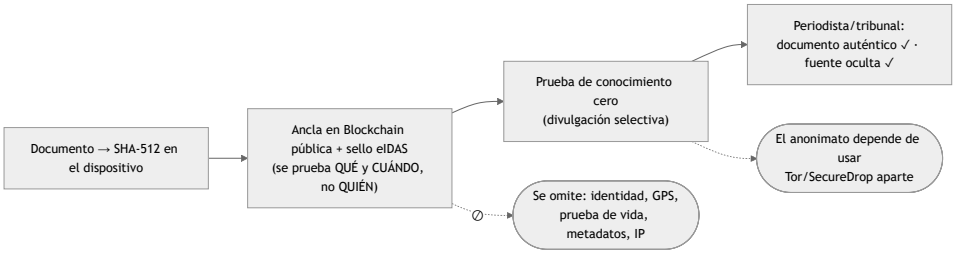


Figura 62.1 — El denunciante calcula la huella SHA-512 del documento en su dispositivo y la ancla a la blockchain pública con sello de tiempo eIDAS: se prueba QUÉ y CUÁNDO, no QUIÉN. La capa que delataría —identidad, GPS, prueba de vida, metadatos, IP— se omite deliberadamente: lo que protege es lo que no se sella. Con una prueba de conocimiento cero, el periodista o el tribunal verifican que el documento es auténtico y anterior a una fecha, sin conocer la fuente. Límite: la cadena no bloquea los puntos de rastreo de la impresora (caso Winner), la estilometría ni los metadatos de red. Fuentes: ICIJ (Panama Papers); EFF; Freedom of the Press Foundation.

---

[1] EUR-Lex — *Directiva (UE) 2019/1937 sobre la protección de los denunciantes* (confidencialidad de la identidad; canales seguros; plazos). https://eur-lex.europa.eu/eli/dir/2019/1937/oj/eng

[2] eucrim — *ECJ orders several member states to financial penalties for failing to transpose the Whistleblowers Directive* (marzo de 2025; ~39 M€; Alemania 34 M€; Estonia 500.000 € + 1.500 €/día). https://eucrim.eu/news/ecj-ordered-several-member-states-to-financial-penalties-for-failing-to-transpose-whistleblowers-directive/ ↩

[3] Freedom of the Press Foundation — *SecureDrop* (más de 60 redacciones; servicio oculto de Tor; protección arquitectónica de la fuente). https://securedrop.org/overview/ ↩

[4] ICIJ — *Panama Papers* (11,5 millones de documentos; 2,6 TB; >350 periodistas; la fuente «John Doe»). https://www.icij.org/investigations/panama-papers/ ↩

[5] OCCRP — *John Doe: «The Revolution Will Be Digitized»* (manifiesto de la fuente de los Panama Papers). https://www.occrp.org/en/investigation/panama-papers-source-john-doe-the-revolution-will-be-digitized ↩

[6] Errata Security (Robert Graham) — *How The Intercept outed Reality Winner* (puntos de rastreo de la impresora; serie 29535218; 9-mayo-2017, 6:20). https://blog.erratasec.com/2017/06/how-intercept-outed-reality-winner.html ↩

[7] Freedom of the Press Foundation — *Reality Winner sentenced to 63 months* (la pena más larga en EE. UU. para una fuente de prensa). https://freedom.press/issues/whistleblower-reality-winner-sentenced-longest-prison-sentence-history-federal-leak-cases/ ↩

[8] Electronic Frontier Foundation (EFF) — *List of printers which do or do not display tracking dots* (código de identificación de la máquina). https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots ↩

[9] Wikipedia — *Stylometry / Adversarial stylometry* (atribución de autoría con un 80-95 % de precisión). https://en.wikipedia.org/wiki/Stylometry ↩

[10] Wikipedia — *Frances Haugen* (filtración de Facebook; decidió revelar su identidad). https://en.wikipedia.org/wiki/Frances_Haugen

[11] Carissa Véliz — *The Ethics of Privacy and Surveillance* (Oxford UP, 2024). ↩

Integridad de la investigación: el dato que nadie puede repetir

«El primer principio es que no debes engañarte a ti mismo —y tú eres la persona más fácil de engañar.»

— Richard Feynman, «Cargo Cult Science», Caltech (1974)

En abril de 2002, la física Lydia Sohn, entonces en Princeton, comparaba las gráficas de un joven investigador de los Bell Labs llamado Jan Hendrik Schön. Las mediciones se presentaban como tomadas en dispositivos distintos y a temperaturas muy diversas; pero mostraban una característica imposible: **exactamente el mismo ruido**. El ruido de una medición electrónica es aleatorio, único como una huella dactilar; que dos mediciones independientes compartan el mismo patrón solo podía indicar una cosa. Sohn, junto con Paul McEuen de Cornell, acababa de destapar el mayor fraude de la física moderna: Schön había copiado y pegado los datos. El comité Beasley confirmó mala conducta en dieciséis de veinticuatro cargos y se retiraron cerca de veintinueve artículos, ocho de ellos en *Science* y siete en *Nature* [6]. El año anterior, Schön había llegado a publicar, de media, un artículo nuevo cada ocho días.

Aquel ruido copiado plantea la pregunta central de este capítulo. No se trata de quién tuvo primero la idea ni de si un título es auténtico —eso corresponde al capítulo 19—, sino de una cuestión más fundamental: **este dato, esta imagen, ¿existía sin manipular en el momento de adquirirlo?** Porque la ciencia, el sistema de conocimiento más fiable que hemos construido, se apoya en una cadena de pruebas —píxeles, blots, ficheros crudos— que, como las del fraude, pueden ser fabricadas.

La factura de la ciencia que no se puede repetir

La escala del problema es vertiginosa. En 2023 se retractaron **más de diez mil artículos científicos**, un récord histórico; el grueso lo aportó la editorial Hindawi, filial de Wiley, que retiró más de ocho mil de números especiales infiltrados por *paper mills* —empresas que fabrican y venden artículos falsos [1]. Como advierten **Ivan Oransky y Adam Marcus**, cofundadores de **Retraction Watch**, la base de datos de referencia sobre retractaciones, esta cifra es «solo la punta del iceberg»: el sistema de corrección va muy por detrás del fraude industrializado.

Y lo que no es fraude directo a menudo tampoco se puede repetir. La empresa Amgen consiguió reproducir solo el **11 %** de cincuenta y tres estudios oncológicos de referencia; el Reproducibility Project: Cancer Biology, publicado en *eLife* en 2021 tras casi una década de trabajo, halló que los efectos replicados eran, de mediana, un **85 % más pequeños** que los originales [10]. A todo ello se suma la manipulación deliberada: el psicólogo Diederik Stapel acumula cincuenta y ocho artículos retractados por haberse inventado conjuntos de datos enteros —cuando le preguntaron por los colegios donde supuestamente había hecho los experimentos, admitió que **aquellos colegios no existían**—, y el récord individual lo ostentaba en julio de 2023 el anestesiólogo Joachim Boldt, con ciento ochenta y cuatro retractaciones. Cuando la prueba es fácil de fabricar y difícil de verificar, todo el edificio se tambalea.

El fraude antes y después de pulsar «capturar»

El fraude de datos entra por dos puertas. La primera es la **manipulación de la imagen** una vez hecha. La microbióloga **Elisabeth Bik**, en su estudio fundacional con Arturo Casadevall y Ferric Fang (*The Prevalence of Inappropriate Image Duplication in Biomedical Research Publications*, mBio, 2016), inspeccionó visualmente **20.621 artículos** de cuarenta revistas y encontró que el **3,8 %** contenían figuras problemáticas, la mitad con señales de manipulación deliberada: bandas de Western blot duplicadas, giradas, recortadas y pegadas [2]. Y como advierte Bik, dado que solo miró un tipo de dato, la prevalencia real es casi seguro más alta. La buena noticia es que el cribado automático funciona: en un piloto de un año, la American Society for Microbiology pasó 2.627 manuscritos aceptados por la herramienta ImageTwin y detectó 410 con problemas de imagen, hasta el punto de revocar la aceptación a seis [3]. El caso más sonado lo destapó desde un pueblo de Gales el biólogo **Sholto David**, que en enero de 2024 publicó en su blog imágenes de papers del Dana-Farber Cancer Institute, de Harvard, que parecían recortadas y pegadas; el instituto pidió retractar seis estudios y corregir treinta y uno. Casi dos años después, en diciembre de 2025, el Dana-Farber pagaba **quince millones de dólares** para cerrar una demanda federal, admitiendo que imágenes y datos se habían «tergiversado o duplicado» en solicitudes de subvención a los institutos nacionales de salud [4].

La segunda puerta es más sutil: el **cambio de variables**. El equipo de **Ben Goldacre**, en la Universidad de Oxford, monitorizó con el proyecto COMPare sesenta y siete ensayos clínicos publicados en las cinco grandes revistas médicas y descubrió que, de media, solo el **76,3 %** de los desenlaces primarios preespecificados se reportaban correctamente, mientras se añadían 365 desenlaces nuevos que nadie había anunciado antes [8]. Es lo que se conoce como *outcome-switching*: medir una cosa, no encontrar nada y reportar otra como si fuera lo que se buscaba. La defensa contra esto es el **preregistro**: depositar el protocolo antes de empezar. Cuando Estados Unidos lo hizo obligatorio para los ensayos de fármacos en 2007, el registro pasó del 64 % al 100 % y el reporte de resultados, del 10 % al 100 %. Y el **Center for Open Science**, impulsado por Brian Nosek, ha extendido los *Registered Reports* —donde la revista acepta el estudio por sus métodos, antes de conocer los resultados— de noventa y una revistas en 2018 a más de trescientas en 2022. La idea de fondo es luminosa: si la decisión de publicar se toma *antes* de ver los resultados, desaparece el incentivo para maquillarlos.

La prueba de existencia: sellar el dato en la adquisición

Es aquí donde **t2p** actúa con precisión quirúrgica, porque ataca el problema en su origen exacto. En el instante de la **adquisición** —cuando el microscopio confocal, el lector de geles, el citómetro o el secuenciador genera el fichero crudo—, se calcula en el propio dispositivo la **huella SHA-512** del fichero original y se ancla a la **blockchain pública** con un **sello de tiempo RFC 3161** conforme a eIDAS. Queda un registro inalterable: «este píxel exacto existía en esta fecha y hora». Cualquier recorte, giro, copia de banda o ajuste de contraste posterior produce una huella distinta que ya no coincide con la sellada en origen: la manipulación se vuelve **matemáticamente detectable y datable**. El ruido copiado de Schön no habría sobrevivido a esta comprobación.

Lo mismo se aplica al **preregistro con fecha cierta**: el protocolo, los desenlaces primarios y el plan de análisis se sellan *antes* de recoger ningún dato, de manera que si después aparecen desenlaces nuevos, la fecha del contenedor **.asice** demuestra que no estaban preespecificados —es el equivalente criptográfico de lo que COMPare necesita para cazar el *outcome-switching*, pero verificable sin depender de un registro central. Y la combinación de **GPS forense** y **prueba de vida** ancla la captura a un lugar, un momento y un operador humano reales: contra el fraude de Stapel, exigiría coordenadas y hora auténticas en lugar de una hoja inventada en un despacho.

Hay que decir el límite con toda la crudeza, porque aquí es el corazón de la cuestión. «Basura a la entrada, basura en la cadena»: el sello garantiza que un fichero existía sin alterar en una fecha y un lugar, pero **no garantiza que el dato sea verdad ni que el experimento sea bueno**. Un investigador deshonesto puede sellar en origen un dato **fabricado de antemano** —números inventados en el propio instrumento, una muestra falsa, un control trucado—: la huella será perfecta y la procedencia, impecable, y sin embargo la ciencia será fraude. El sello tampoco detecta los errores honestos ni los problemas de reproducibilidad —un resultado puede estar perfectamente datado y ser irreproducible por mala metodología—, ni sustituye el ojo experto de Bik o de David, que cazan la manipulación *anterior* a pulsar «capturar». La prueba de existencia traslada el punto de confianza del «me creo tu figura» al «me creo tu adquisición», un avance real contra la manipulación posterior, pero **no cierra la fabricación en origen**.

La promesa y el peligro

Así, la promesa es inmensa para un sistema que mueve billones en financiación y del que dependen la medicina y la tecnología. Sellar el dato crudo en la adquisición y el protocolo antes del experimento haría mucho más difícil duplicar una banda, reutilizar ruido o añadir desenlaces a posteriori, y daría a los revisores y a los comités de integridad una cadena de custodia verificable en lugar de una figura que hay que creerse. En una ciencia carcomida por las *paper mills*, hacer la prueba inalterable es proteger el fundamento del conocimiento.

El peligro pide el matiz habitual. Primero, ya dicho: el sello no hace verdadero un dato falso; si la fabricación ocurre antes de la captura, la cadena inmortaliza la mentira con procedencia impecable. Segundo, el exceso de confianza: ninguna huella sustituye la reproducción independiente ni el ojo experto. Y tercero, la adopción: si el sellado es opcional o posterior a la adquisición, pierde casi todo su valor, y la ausencia de sello no prueba fraude por sí sola. La prueba de existencia es una herramienta poderosa contra la manipulación y el cambio de variables, pero no constituye un certificado de verdad científica.

Es hora de actuar

Sellar el fichero crudo al capturarlo y preregistrar el protocolo con fecha cierta garantiza la integridad demostrable de los datos.

Las revistas han de exigir el dato crudo sellado y comparar su huella, tal como se hace con el cribado automático de imágenes.

Los financiadores han de condicionar las subvenciones a una cadena de custodia verificable de los datos, algo que habría impedido el caso Dana-Farber.

Las instituciones han de proteger a quienes, como Sholto David, destapen la manipulación y no penalizarlos.

Un ruido copiado hizo caer el principal fraude de la física cuando alguien comparó dos huellas. Asignar a cada dato científico una huella sellada al nacer —sin olvidar que la verdad final requiere repetir el experimento— es, en este frente del conocimiento, time2act.

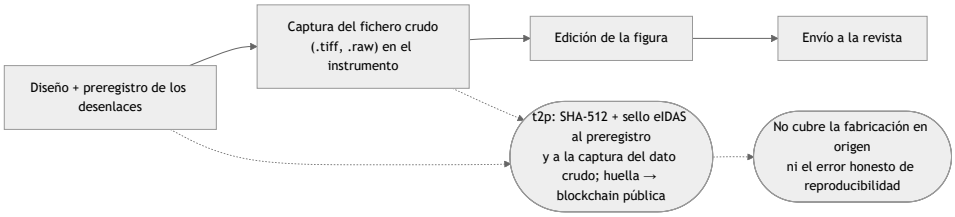


Figura 63.1 — A lo largo de la vida de un experimento, el fraude puede entrar en el diseño (cambio de variables: COMPare encontró que solo el 76,3 % de los desenlaces primarios se reportaban bien), en la muestra (fabricación en origen, como Stapel), en la captura del fichero crudo o en la edición de la figura (duplicación de bandas: Bik las encontró en el 3,8 % de 20.621 artículos). El sello en la adquisición — huella SHA-512 + sello eIDAS— cubre el preregistro del protocolo y la captura del dato crudo, y hace detectable cualquier edición posterior; pero no demuestra que el dato fabricado en origen sea verdad. Fuentes: COMPare (Oxford); Bik et al. (mBio 2016); ASM/ImageTwin.

---

[1] Nature (Richard Van Noorden) — *More than 10,000 research papers were retracted in 2023 — a new record* (Hindawi/Wiley, >8.000). https://www.nature.com/articles/d41586-023-03974-8 ↩

[2] Elisabeth Bik, Arturo Casadevall y Ferric Fang — *The Prevalence of Inappropriate Image Duplication in Biomedical Research Publications* (mBio, 2016; 20.621 artículos, 3,8 %). https://journals.asm.org/doi/10.1128/mbio.00809-16 ↩

[3] American Society for Microbiology / mBio — *Piloto de ImageTwin* (2.627 manuscritos; 410 con problemas de imagen; 6 aceptaciones revocadas). https://journals.asm.org/doi/10.1128/mbio.01990-25 ↩

[4] U.S. Department of Justice — *Dana-Farber Cancer Institute agrees to pay $15M to settle fraud allegations* (imágenes/datos tergiversados en subvenciones a los NIH). https://www.justice.gov/opa/pr/dana-farber-cancer-institute-agrees-pay-15m-settle-fraud-allegations-related-scientific ↩

[5] Stanford Board of Trustees — *Report on the scientific work of Marc Tessier-Lavigne* (2023; dimisión del presidente). https://boardoftrustees.stanford.edu/news/board-trustees-statement-release-report-and-announcements

[6] American Physical Society — *The Schön scandal* (comité Beasley; mala conducta en 16 de 24 cargos). https://www.aps.org/apsnews/2022/08/september-2002-schon-scandal-report ↩

[7] Retraction Watch (Ivan Oransky y Adam Marcus) — *The new retraction record holder* (Joachim Boldt, 184 retractaciones, julio de 2023). https://retractionwatch.com/2023/07/12/the-new-retraction-record-holder-is-a-german-anesthesiologist-with-184/

[8] Ben Goldacre et al. (COMPare, Universidad de Oxford) — *COMPare: outcome-switching en ensayos clínicos* (Trials, 2019; 76,3 % de desenlaces primarios bien reportados). https://pmc.ncbi.nlm.nih.gov/articles/PMC6375128/ ↩

[9] Center for Open Science (Brian Nosek) — *Registered Reports* (de 91 a más de 300 revistas; el protocolo antes de los resultados). https://www.cos.io/initiatives/registered-reports

[10] eLife — *Reproducibility Project: Cancer Biology* (Amgen, 11 % de 53 estudios; efectos replicados un 85 % más pequeños). https://elifesciences.org/articles/71601 ↩

Pensiones: probar que aún estás aquí, hoy

«La vejez solo es honrada a condición de que se defienda, mantenga sus derechos, no se someta a nadie y gobierne hasta el último aliento su propio dominio.»

— Cicerón, De Senectute, §38 (44 a. C.)

El 28 de julio de 2010, unos funcionarios de Tokio fueron a casa de Sogen Kato para felicitarlo: según el registro, era el hombre más viejo de la ciudad, con ciento once años, y se acercaba el Día del Respeto a los Mayores. Cuando abrieron su habitación, encontraron un cuerpo momificado en pijama, rodeado de periódicos de 1978. Kato llevaba treinta y dos años muerto dentro de su propia casa mientras su **pensión de supervivencia** seguía cayendo, mes tras mes, en la cuenta familiar. La familia había cobrado indebidamente unos 9,5 millones de yenes; su nieta fue condenada [1]. El caso destapó un agujero nacional: la policía japonesa no pudo confirmar si **234.354 personas** que figuraban como centenarias seguían vivas —77.118 de ellas habrían superado los ciento veinte años—, porque los registros familiares llevaban décadas sin actualizar [2].

Aquel cuerpo momificado contiene la pregunta de este capítulo, que no es la del capítulo 47 —«¿quién eres?», que se responde una vez— ni la del capítulo 49 —«¿ha llegado la ayuda?»—, sino una más persistente: **¿sigues vivo, hoy, y volverás a estarlo dentro de tres meses?** Porque una pensión no es un acto único, sino un derecho que se cobra durante años, y el fraude más silencioso no es un acontecimiento, sino un **no-acontecimiento**: una muerte que nadie declara.

El Estado que no sabe quién ha muerto

El problema es universal y caro. En Estados Unidos, un informe del inspector general de la Seguridad Social de 2025 encontró que el rechazo automático de avisos de defunción provocó **327 millones de dólares** en pagos a personas muertas; otro informe ya había detectado **6,5 millones** de titulares de número de Seguridad Social con ciento doce años o más **sin fecha de defunción** en sus registros [3]. En Grecia, bajo la presión de la troika, un censo de pensionistas suspendió prestaciones a unas **200.000 personas** que no tenían derecho a ellas o ya estaban muertas —entre ellas, unas nueve mil que figuraban como «centenarias» cobrando jubilación—, con un ahorro de hasta **800 millones de euros al año** [4]. Y en Sudáfrica, la agencia de subsidios SASSA admitió haber pagado unos **140 millones de rands a cerca de 75.000 beneficiarios difuntos** [5]. La raíz de todo es la misma: un **registro civil que no sabe de manera fiable quién ha muerto**.

Y hay un matiz incómodo que hay que decir: buena parte del fraude no lo comete el muerto, sino quien controla el sistema. En Sudáfrica, un análisis del Institute for Economic Justice atribuye cerca del 75 % del fraude de subsidios a funcionarios e intermediarios, no a los beneficiarios: insiders que crean «beneficiarios fantasma», duplican tarjetas y cambian datos bancarios. Por eso, como advierte la Asociación Internacional de la Seguridad Social (ISSA) en su análisis *Proof of life in international social security* [9], la prueba de vida debe evitar depender de un repositorio central que se pueda manipular desde dentro.

Probar que sigues vivo, hoy y dentro de tres meses

La respuesta tradicional —hacer venir al pensionista a una ventanilla una vez al año— es humillante para los mayores e imposible para quienes viven lejos. Varios países han buscado alternativas digitales. India creó el certificado digital de vida **Jeevan Pramaan**, que el año pasado generó unos 19 millones de certificados, más de once millones mediante autenticación facial, ahorrando la comparecencia física [6]. Brasil invirtió la lógica con su *prova de vida*, cruzando bases de datos públicas. Y España, con la app **VIVESS**, permite a los pensionistas residentes en el extranjero acreditar que siguen vivos sin viajar.

Pero aquí aparece una amenaza nueva. Como advierte la revista jurídica brasileña **Conjur** en su artículo *Deepfakes, provas digitais e fraudes no INSS* [10], los deepfakes amenazan con un «apocalipsis epistémico» en el que un vídeo deja de servir como prueba; ya hay falsos agentes que recogen la cara y la voz de los jubilados «para la prueba de vida». La lección conecta con todo este libro: no basta con «un vídeo creíble»; hace falta una prueba **verificable criptográficamente**.

La prueba de existencia recurrente: el reto que el muerto no puede responder

Es aquí donde **t2p** ofrece una mecánica hecha a medida de este problema. En cada ciclo de atestación —mensual, trimestral o anual—, el pensionista hace un **gesto de vivacidad** en su dispositivo: girar la cabeza, decir una frase, responder un reto activo antisuplantación. El dispositivo calcula localmente la **huella SHA-512** del paquete formado por {prueba de vivacidad + **reto del día** + marca de tiempo + GPS forense}, la ancla a la **blockchain pública** con un **sello RFC 3161** conforme a eIDAS y lo cierra en un contenedor **.asice** verificable fuera de línea. Lo que queda registrado en la cadena no es la cara, sino **la prueba de que un humano vivo respondió a un reto irrepetible en un instante y un lugar concretos**.

La clave es el **reto fresco**, un valor aleatorio del día que actúa como antídoto contra la reutilización: una grabación de hace seis meses no contiene la frase de hoy, y su huella no coincidirá. Esto ataca de lleno el fraude del pensionista fantasma —**el muerto no puede responder al reto de hoy**—, mientras el GPS y la marca de tiempo detectan patrones imposibles, como un mismo dispositivo atestando a cincuenta beneficiarios en el mismo minuto. Y todo ello **sin base biométrica central**: a diferencia de Aadhaar o de las bases del sistema brasileño, la plantilla biométrica **no sale nunca del dispositivo**; en la cadena solo vive una huella. No hay ningún honeypot que robar. Además, el contenedor se genera fuera de línea y se ancla cuando hay red, justo lo que necesitan los pensionistas rurales o en el extranjero que hoy fracasan en los sistemas presenciales.

Hay que decir el límite con toda la crudeza, porque aquí es delicado. «Basura a la entrada, basura en la cadena»: t2p puede certificar de manera infalsificable que un humano vivo respondió a un reto único, pero **no garantiza que ese humano sea el beneficiario legítimo** si el alta inicial fue fraudulenta o si un cuidador coacciona a la persona. Si un familiar obliga a un anciano vivo a hacer el gesto para seguir cobrando una pensión a la que no tiene derecho, la cadena registrará una prueba de vida perfectamente válida: la huella es honesta sobre lo que vio el sensor, no sobre la legitimidad jurídica del cobro. Segundo, **no resuelve el problema inverso**: como muestra la operación LEAP del sistema británico —**119.050 pagos insuficientes por 736 millones de libras** [8], con más de quince mil personas que ya no se podrán localizar porque han muerto—, a menudo el daño real es el Estado que **debe dinero y no lo paga**. Probar que sigues vivo no obliga a la administración a calcular bien tu derecho. Y tercero, la vivacidad no es infalible y la barrera tecnológica **excluye**: como documenta el diario indio **The Wire** [7], hay ancianos a quienes se niega la pensión porque sus huellas desgastadas no casan con la base biométrica —un caso, el de una mujer de ochenta y tres años, acabó en muerte tras dieciséis meses sin pensión ni ración. Por eso la autenticación por huella dactilar se acabó haciendo **no obligatoria**. Exigir un gesto digital a quien tiene demencia, no tiene teléfono o no tiene cobertura reproduce la brecha digital; la prueba periódica debe convivir con una vía asistida y no punitiva, o se convierte en una máquina de suspender pensiones a los más débiles.

La promesa y el peligro

La promesa es humana y cuantificable. Una prueba de vida recurrente, verificable y sin base central haría casi imposible el cobro después de una muerte no declarada —el agujero de Tokio, de Atenas, de Pretoria —, sin convertir a los mayores en una población fichada ni obligarlos a hacer cola. En sistemas que pagan pensiones a cientos de millones de personas, sellar la vivacidad en el tiempo es proteger a la vez las arcas públicas y la dignidad de quien cobra.

El peligro pide los matices que hemos dicho. El primero, la coacción y el alta fraudulenta, que ningún sello resuelve. El segundo, no confundir la prueba de vida con el control de elegibilidad ni con la calidad del registro de defunciones, que es la raíz del problema. Y el tercero, sobre todo, la inclusión: una herramienta pensada contra el fraude no puede acabar excluyendo precisamente a los más vulnerables. La prueba de existencia endurece el escalón «¿sigue vivo y presente, hoy?», que es exactamente donde fallan los pensionistas fantasma, pero no sustituye ni la política de inclusión ni un registro civil que sepa quién ha muerto.

Es hora de actuar

Para los **fondos de pensiones y la seguridad social**: adoptar una prueba de vida recurrente con reto fresco y sin base biométrica central, para que el muerto no pueda cobrar y el vivo no tenga que viajar. Para los **registros civiles**: cerrar el agujero de origen —saber de manera fiable quién ha muerto—, que es la causa de los fondos. Para los **reguladores**: exigir una vía asistida y no punitiva para quien no puede hacer el gesto, y vigilar que la prueba de vida no se convierta en exclusión. Y para los **propios pensionistas y sus familias**: una herramienta que demuestre que siguen vivos sin entregar su biometría a ningún servidor.

Un hombre siguió cobrando la pensión treinta y dos años después de morir porque nadie lo obligó a probar que estaba vivo. Dar a cada pensionista una manera de demostrar, una y otra vez, que aún está aquí —con un reto que el muerto no puede responder y sin fichar al vivo— es, en este frente que toca la vejez de todos, time2act.

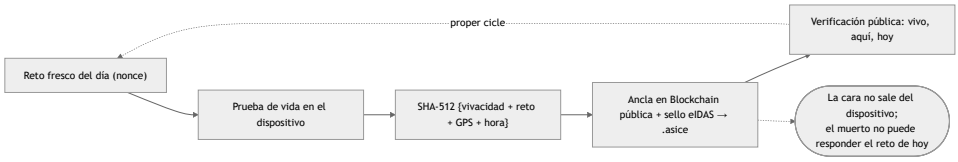


Figura 64.1 — Cada ciclo de atestación parte de un reto fresco del día (nonce); el pensionista hace el gesto de vivacidad en el dispositivo; se calcula localmente la huella SHA-512 de {vivacidad + reto + GPS + hora}, se ancla a la blockchain pública con sello eIDAS y se cierra en un .asice verificable fuera de línea. El reto irrepetible impide reutilizar grabaciones antiguas: el muerto no puede responder al reto de hoy. La cara no sale nunca del dispositivo; en la cadena solo viaja una huella. Coste de no saber quién sigue vivo: Japón, 234.354 centenarios sin confirmar; EE. UU., 327 M$ a difuntos; Sudáfrica, 140 M de rands a 75.000 muertos. Fuentes: France 24; SSA OIG; SASSA/Moneyweb.

---

[1] Wikipedia (con BBC / AFP / Japan Times) — *Sogen Kato* (momificado 32 años; pensión de supervivencia cobrada; ~9,5 M de yenes). https://en.wikipedia.org/wiki/Sogen_Kato ↩

[2] France 24 — *Over 230,000 listed centenarians missing in Japan* (234.354 sin confirmar; 77.118 con 120+ años). https://www.france24.com/en/20100910-over-230000-listed-centenarians-missing-presumed-dead-government-report-japan ↩

[3] SSA Office of the Inspector General — *State death report discrepancies led to $327M in improper payments* (2025) y *6,5 M de titulares de ≥112 años sin fecha de defunción en el Numident* (2015). https://oig.ssa.gov/news-releases/2025-03-19-state-death-report-discrepancies-led-to-327m-in-improper-payments-and-cost-ssa-millions-of-dollars-in-unnecessary-workloads/ ↩

[4] Reuters (vía HuffPost) — *Greece stops pensions and benefits for 200,000 people* (~9.000 «centenarios»; hasta 800 M€/año de ahorro). https://www.huffpost.com/entry/greece-stops-pensions-benefits-200000-people-fraudulently_n_1451423 ↩

[5] Moneyweb — *SASSA explains why it paid R140m in grants to 75,000 dead people* (2025; el 75 % del fraude, de funcionarios, según el IEJ). https://www.moneyweb.co.za/news/south-africa/sassa-explains-why-it-paid-r140m-in-grants-to-75-000-dead-people/ ↩

[6] Outlook Money — *Jeevan Pramaan: digital life certificate* (~19 M de certificados; ~11,5 M por autenticación facial). https://www.outlookmoney.com/retirement/digital-life-certificate-over-14-million-super-seniors-generated-online-jeevan-pramaan-patra-in-fy25-26 ↩

[7] The Wire (India) — *Digital Exclusion: Poor, Elderly Face the Brunt of Aadhaar-Based Authentication Errors* (huellas desgastadas; pensiones denegadas; huella no obligatoria). https://m.thewire.in/article/rights/digital-exclusion-poor-elderly-face-the-brunt-of-aadhaar-based-authentication-errors ↩

[8] GOV.UK (DWP) — *State Pension underpayments (operación LEAP)* (119.050 pagos insuficientes, 736 M£; >15.000 ya muertos). https://www.gov.uk/government/publications/state-pension-underpayments-progress-on-cases-reviewed-to-30-september-2024/state-pension-underpayments-progress-on-cases-reviewed-to-30-september-2024 ↩

[9] International Social Security Association (ISSA) — *Proof of life in international social security* y la buena práctica VIVESS (pensionistas españoles en el extranjero). https://www.issa.int/analysis/proof-life-international-social-security-progress-and-persistent-challenges ↩

[10] Consultor Jurídico (Conjur, Brasil) — *Deepfakes, provas digitais e fraudes no INSS: o colapso da confiança* (2025). https://www.conjur.com.br/2025-mai-28/deepfakes-provas-digitais-e-fraudes-no-inss-colapso-da-confianca/ ↩

Prueba de vida: secuestros virtuales, desaparecidos y la voz que no era

«Era la voz de mi hija. Eran sus llantos. Eran sus sollozos. Era su manera de hablar.»

— Jennifer DeStefano, testimonio ante el Senado de EE. UU. (13-6-2023)

Arizona, 20 de enero de 2023, cerca de las cinco de la tarde. Jennifer DeStefano contesta el teléfono y oye la voz de su hija de quince años —que está fuera, en una competición deportiva— llorando y pidiendo ayuda. Un hombre toma la línea: exige un millón de dólares, luego rebaja el rescate a cincuenta mil y empieza a dictar instrucciones de transferencia. Ella no cree a quienes, a su alrededor, le dicen que puede ser una estafa: «la voz era tan real, y su llanto, tan real». El «secuestro» se deshizo de golpe cuando la hija, perpleja, llamó para decir que estaba bien: nunca había estado en peligro. No había ningún secuestrador —solo una voz clonada con inteligencia artificial. DeStefano acabó testificando ante un subcomité del Senado de Estados Unidos para que ninguna otra familia tuviera que pasar por aquel infierno [1].

Este capítulo trata la prueba de vida cuando alguien la ataca. La fe de vida rutinaria —demostrar cada año que sigues vivo para cobrar la pensión— está en el capítulo 64; la tecnología de la voz clonada, en el capítulo 68; las réplicas digitales, en el capítulo 81. Aquí la pregunta es la del peor día posible: ¿cómo sabes que la persona al otro lado es real, está viva y es ahora? La respuesta de siempre —la foto con el periódico del día— ha muerto: la puede fabricar cualquiera. La nueva respuesta es criptográfica: un reto imprevisible, respondido en el momento y sellado con **t2p** —la huella SHA-512 en el dispositivo, el sello de tiempo RFC 3161/eIDAS, el anclaje a la blockchain pública dentro de un contenedor .asice [4]. La voz se puede clonar; el presente, no.

El secuestro que no existe

La mecánica del secuestro virtual, tal como la describe el FBI, es una máquina de pánico perfectamente calibrada: una llamada —a menudo desde un número internacional— asegura que un familiar ha sido secuestrado; se mezclan gritos o una voz que suena como la del ser querido; se exige un rescate inmediato, solo por transferencia; y se impide que la víctima cuelgue o intente contactar con el supuesto secuestrado. Todo el engaño depende de la velocidad, porque no hay ningún secuestro: solo hace falta que la familia pague antes de que la mentira caiga por su propio peso [2]. Las recomendaciones oficiales son las contrarias al instinto: mantener la calma, ganar tiempo, intentar contactar con el familiar por otra vía y hacer preguntas que solo la persona real sabría responder [2].

Y en 2025 llegó el escalón siguiente. La alerta del IC3 —el centro de denuncias de ciberdelitos del FBI— documenta a criminales que usan «prueba de vida» alterada: fotos y vídeos manipulados o generados con IA a partir de imágenes públicas de la víctima, fabricados para hacer verosímil el secuestro inexistente. Las incoherencias que el FBI recomienda buscar en ellos —un tatuaje que falta, una cicatriz que no está— son exactamente la clase de detalle que cada generación de síntesis borra un poco mejor [3].

Léalo bien, porque es el núcleo del capítulo: el oficio del secuestrador virtual ya incluye fabricar la prueba de vida. El ritual probatorio más antiguo del crimen —«demuéstrame que está vivo»— se ha convertido en un campo de deepfakes, y la familia, en el momento de máximo pánico de su vida, tiene que hacer de perito forense en treinta segundos. Ninguna familia debería jugar esta partida con las reglas viejas.

La contraprueba: reto, frescura y sello

La respuesta estructural se construye sobre una asimetría que juega a favor de la familia: el clonador puede imitar una voz [1], pero solo puede decir lo que su operador sabe; y puede fabricar una imagen [3], pero no puede responder lo imprevisible. De ahí la contraprueba en tres piezas [4].

La primera es **el reto**: una pregunta que solo la persona real puede responder —el recuerdo compartido, la palabra de seguridad familiar—, la misma lógica que el FBI ya recomienda [2] y que hemos visto en la verificación familiar del capítulo 85. Lo bastante personal para que ningún algoritmo pueda anticiparla; lo bastante simple para que la persona real la responda sin pensar.

La segunda es **la frescura**: la respuesta ha de ser de ahora —un vídeo o audio corto que incluya el reto recién formulado, no material reciclado ni preparado. El contenido del presente no se puede haber

sintetizado en el pasado.

Y la tercera es **el sello**: la respuesta queda con huella y anclada al minuto —SHA-512, sello de tiempo RFC 3161/eIDAS, blockchain pública [4]—, de manera que ni se puede haber fabricado antes ni se puede alterar después.

Contra este triple muro, el clonador está perdido: puede imitar el timbre [1], pero no conoce el reto; puede generar una imagen convincente [3], pero no la frescura del momento; y aunque lo tuviera todo, no puede fabricar un sello criptográfico del presente con fecha de ayer. La familia, por su parte, tiene un protocolo en lugar de un pánico: ante cualquier llamada de rescate, exigir la prueba de vida sellada con reto; si no llega, es la estafa que el FBI describe [2][3]. Es el mismo principio de reto y frescura que el capítulo 64 aplica a la fe de vida rutinaria de las pensiones —trasladado al minuto más oscuro.

El rehén real y el desaparecido

Hay dos escenarios más graves que la estafa, y ambos necesitan el mismo instrumento.

El primero es el rehén real. Cuando un secuestro existe de verdad, la prueba de vida es moneda de negociación —y su autenticidad, cuestión de vida o muerte en las decisiones de familias y negociadores. En la era del deepfake, la duda corta en dos sentidos: un vídeo auténtico puede ser despachado como falso, y uno fabricado puede mantener viva una negociación por una persona que ya no está. La contribución del sello es la datación: un vídeo que responde a una información que solo existía después de una fecha —y que llega con huella anclada [4]— acredita, como mínimo, que la persona estaba viva después de aquella fecha. No resuelve la negociación; le quita la niebla que la envenena. Y la misma lógica sirve a quienes verifican desde fuera —el periodismo y las organizaciones del capítulo 20—: material datado e íntegro en lugar de fragmentos incontrastables.

El segundo es el desaparecido. En España, el Centro Nacional de Personas Desaparecidas —pionero en Europa— coordina la respuesta a miles de desapariciones cada año: 16.147 personas investigadas en 2024 (un 6 % más que el año anterior, con el 72 % de los casos esclarecidos en menos de una semana) y 16.024 en 2025, con un esclarecimiento del 90,7 %; ese año el CNDES publicó 928 alertas, 132 de las cuales seguían activas [5]. Detrás de cada alerta activa hay una familia buscando un rastro.

La aportación de la prueba de existencia es aquí delicada, y hay que decirla con el límite por delante: voluntaria o nada. La persona que, por decisión propia, mantiene un rastro sellado de momentos y lugares en su dispositivo [4] puede dar a una eventual investigación el último punto verificable del mapa; y el «regreso» —real, o simulado con la voz y la cara del ausente [3]— se puede contrastar con retos y sellos. Un rastro impuesto, en cambio, sería vigilancia y no protección: esa frontera no se cruza.

La prueba de existencia aplicada

El teléfono suena con la peor noticia posible. Por primera vez, la familia tiene algo que hacer que no sea creer o pagar.

1. El protocolo familiar contra el secuestro virtual

La familia acuerda el protocolo antes de que pase nada: palabra de seguridad, rellamada al número de siempre [2] y, ante cualquier exigencia de rescate, una única petición —prueba de vida sellada con reto [4]. La llamada del estafador se estrella contra tres muros: no conoce el reto, no controla a la persona real y no puede fabricar el sello del presente [3]. En el caso de Arizona [1], treinta segundos de protocolo habrían sustituido los minutos de terror: la hija, localizada por la otra línea, habría respondido el reto desde el vestuario de la competición —sellado, datado, inequívoco.

2. La negociación con datación

En el secuestro real, los negociadores exigen a los captores pruebas de vida datables: la respuesta a una pregunta formulada hoy, sellada hoy [4]. El material que llega con huella y frescura acreditadas permite decisiones —pagar, esperar, actuar— sobre hechos y no sobre esperanzas; y el material sin ningún anclaje se trata con la sospecha que merece, porque el FBI ya ha documentado la industria de la prueba de vida fabricada [3]. La datación no ablanda el drama; le quita la niebla.

3. El último punto del mapa

Una persona que lo decide libremente —el senderista solitario, la profesional que viaja a zonas de riesgo, el adolescente que quiere tranquilizar a sus padres sin sentirse vigilado— mantiene un rastro sellado mínimo: momentos elegidos, con huella en su dispositivo, sin ningún registro central ni seguimiento en tiempo real [4]. Si alguna vez desaparece, la familia puede ofrecer a la investigación [5] una cronología verificable de la última normalidad: no dónde está ahora —eso el sello no lo sabe ni tiene por qué saberlo —, sino dónde y cuándo estuvo por última vez, con fecha cierta. En una búsqueda, las primeras horas y el último punto fiable lo son casi todo.

4. El regreso que hay que creer

El regreso también necesita prueba. Quien reaparece después de una desaparición —y quien reaparece solo digitalmente: la voz al teléfono, el mensaje «soy yo, estoy bien»— puede acreditar continuidad respondiendo retos y sellando las respuestas al momento [4]; una suplantación construida con la voz y la cara de la persona ausente [3] no puede hacer ninguna de las dos cosas. Para las familias, es la diferencia entre la esperanza fundada y la crueldad de un engaño que se puede alargar meses; para las investigaciones [5], un filtro contra las pistas falsas que consumen recursos y esperanzas.

Los límites, dichos sin rodeos: el sello no encuentra a nadie, no libera a nadie y no sustituye ni a la policía ni a los negociadores profesionales; la prueba de vida sellada exige que la persona tenga acceso a un dispositivo y una libertad mínima para responder —condiciones que el secuestro real a menudo niega; el rastro voluntario nunca puede convertirse en obligación ni en vigilancia; y ningún protocolo ahorra a una familia el miedo —solo le da, en medio del miedo, un hecho al que agarrarse.

La promesa y el peligro

La promesa: familias con un protocolo en lugar de un pánico [1][2], negociaciones sobre hechos datados [3], investigaciones con últimos puntos fiables [5] y regresos que se pueden creer. La prueba de vida, devuelta a la vida.

Los peligros, con la misma gravedad.

El primero es **el rastro impuesto**. Del «último punto del mapa» voluntario a la geolocalización permanente de hijos, parejas o empleados hay una pendiente que este libro se niega a bajar. La prueba de vida es un acto de la persona, no sobre la persona: dispositivo propio, momentos elegidos, revocabilidad total, ningún registro central [4]. Todo lo que se parezca a un collar digital es lo contrario exacto de este capítulo.

El segundo es **la coacción sobre el protocolo**. Un secuestrador real puede forzar a la víctima a responder retos y sellar respuestas. El sello acredita frescura, no libertad: una prueba de vida auténtica puede ser el producto de una pistola. Los protocolos serios lo saben —la datación informa la negociación, no la sustituye, y ninguna familia debería gestionar esto sin profesionales [2].

El tercero es **la falsa seguridad**. Ningún protocolo cubre todos los casos: la persona sin dispositivo, el reto olvidado, el pánico que lo borra todo. Vender la prueba de vida sellada como garantía sería cruel; es una herramienta que mejora probabilidades, no un talismán.

Y el cuarto es el más delicado: tecnificar el miedo. Detrás de cada alerta activa [5] hay familias vulnerables —y un mercado potencial de falsas esperanzas tecnológicas. La primera respuesta a una desaparición son la policía, los protocolos públicos y el apoyo a las familias; el sello es infraestructura de prueba a su servicio, nunca un producto para venderles miedo.

Es hora de actuar

La pregunta «¿está vivo?» merece una respuesta mejor que una foto falsificable.

Para las familias: acordad el protocolo antes de que haga falta —palabra de seguridad, rellamada, prueba de vida sellada con reto [1][2][4]; y si llega la llamada, ganad tiempo: la estafa vive de la prisa [2].

Para policías y negociadores: incorporad la datación criptográfica a los protocolos de prueba de vida [3][4]; el material sin frescura acreditada merece sospecha por defecto.

Para el CNDES y las unidades de desaparecidos: aceptad y valorad las cronologías voluntarias selladas que aporten las familias [4][5]; el último punto fiable acorta búsquedas.

Para las plataformas y operadores: facilitad el canal de verificación —el reto sellado de un clic— y colaborad con las alertas oficiales [2][5].

Para ti: si viajas solo, si te expones, si quieres que los tuyos puedan saber sin vigilarte —el rastro mínimo, voluntario y sellado es tuyo [4]; y habla del protocolo en casa: la conversación incómoda de hoy es la calma de mañana.

Para los legisladores: reconoced la prueba de vida sellada en los protocolos oficiales y blindadla contra toda deriva de vigilancia —voluntaria, revocable y sin registros centrales [4].

Jennifer DeStefano oyó la voz exacta de su hija suplicando, y la voz mentía [1]. Que la próxima familia que reciba aquella llamada tenga una pregunta preparada y un sello que exigir —y que la próxima verdad, la del regreso o la de la última ubicación, llegue con fecha cierta. Por la pregunta más antigua —«¿está vivo?»—, **time2act**.

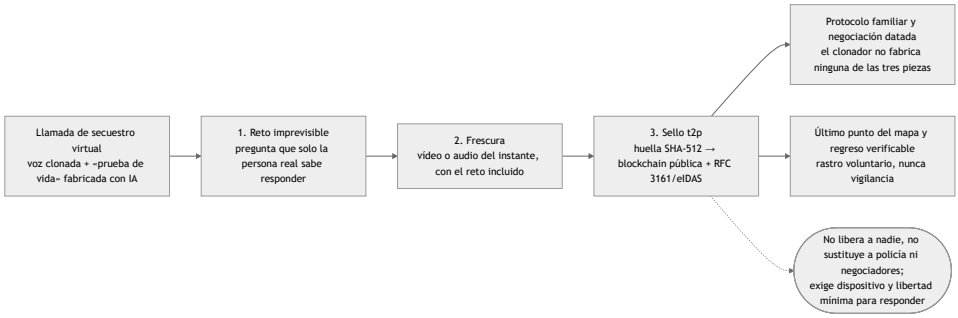


Figura 65.1 — La prueba de vida en la era del deepfake: contra el secuestro virtual con voz clonada y la «prueba de vida» fabricada con IA (alerta FBI/IC3 2025), el protocolo de tres piezas —reto imprevisible, frescura del momento y sello t2p (huella SHA-512 en el dispositivo, RFC 3161/eIDAS, blockchain pública, .asice). Aplicaciones: el protocolo familiar, la negociación con datación, el último punto del mapa voluntario y el regreso verificable (CNDES: 132 alertas activas en 2025). Límites: el sello acredita frescura, no libertad; voluntario o nada; nunca un sustituto de la policía y los negociadores. Fuentes: CNN (caso DeStefano); FBI/IC3; Ministerio del Interior/CNDES.

---

[1] CNN en Español — *Una mujer cree que estafadores clonaron la voz de su hija en un falso secuestro* (caso Jennifer DeStefano, Arizona; llamada del 20 de enero cerca de las 16:55; hija de 15 años en una competición; rescate de 1 millón rebajado a 50.000 dólares; «la voz era tan real»; testimonio posterior ante un subcomité del Senado de EE. UU.); La Opinión — *Utilizan voz recreada por inteligencia artificial para fingir el secuestro de una niña y pedir rescate.* https://cnnespanol.cnn.com/2023/04/29/una-mujer-cree-que-los-estafadores-clonaron-la-voz-de-su-hija-en-un-falso-secuestro-trax/ · https://laopinion.com/2023/04/29/utilizan-voz-recreada-por-inteligencia-artificial-para-fingir-el-secuestro-de-una-nina-y-pedir-rescate/ ↩

[2] FBI — *'Virtual Kidnapping' Extortion Calls on the Rise* (mecánica de la estafa; números internacionales; impedimento de contacto; rescate por transferencia; recomendaciones: calma, contactar por otra vía, preguntas que solo la persona real sabe responder); FBI Albuquerque — *Be on the Lookout for Virtual Kidnapping Scams*. https://www.fbi.gov/contact-us/field-offices/sanantonio/news/press-releases/virtual-kidnapping-extortion-calls-on-the-rise · https://www.fbi.gov/contact-us/field-offices/albuquerque/news/press-releases/fbi-media-alert-be-on-the-lookout-for-virtual-kidnapping-scams ↩

[3] FBI / IC3 — *Criminals Using Altered Proof-of-Life Media to Extort Victims in Virtual Kidnapping for Ransom Scams* (alerta de 2025: fotos y vídeos alterados o generados con IA como falsa «prueba de vida», a menudo a partir de imágenes públicas; incoherencias como tatuajes o cicatrices ausentes; denuncia en ic3.gov con el material recibido); Axios — *AI-generated videos, photos used in new virtual kidnapping scams, FBI warns* (5 de diciembre de 2025). https://www.fbi.gov/investigate/cyber/alerts/2025/criminals-using-altered-proof-of-life-media-to-extort-victims-in-virtual-kidnapping-for-ransom-scams · https://www.axios.com/2025/12/05/ai-videos-photos-scam-virtual-fbi-victim-ransom-kidnapping ↩

[4] t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; prueba de vida con reto y frescura —nonce imprevisible respondido y sellado al minuto; rastro voluntario con momentos elegidos; ningún registro central; revocabilidad). Véanse los capítulos 13, 15 y 64; la voz clonada, en el capítulo 68. ↩

[5] La Moncloa / Ministerio del Interior — *Las Fuerzas de Seguridad investigaron la desaparición de 16.147 personas en 2024* (+6 %; el 72 % de los casos esclarecidos en menos de una semana; CNDES pionero en Europa); Ministerio del Interior — *Las Fuerzas de Seguridad investigaron la desaparición de 16.024 personas en 2025 y esclarecieron el 91 por ciento de las denuncias* (25.086 denuncias; 928 alertas publicadas, 132 activas; 11.461 episodios únicos, media de 3 denuncias en reincidentes). https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/paginas/2025/170325-marlaska-plan-personas-desaparecidas.aspx · https://www.interior.gob.es/opencms/es/detalle/articulo/Las-Fuerzas-de-Seguridad-investigaron-la-desaparicion-de-16.024-personas-en-2025-y-esclarecieron-el-91-por-ciento-de-las-denuncias/ ↩

Integridad deportiva: la muestra que alguien cambió de noche

«Cuando el Gran Anotador venga a escribir junto a tu nombre, no pondrá si ganaste o perdiste, sino cómo jugaste el Juego.»

— Grantland Rice, «Alumnus Football» (1908)

En el laboratorio antidopaje de los Juegos Olímpicos de invierno de Sochi, una noche de febrero de 2014, un agente del servicio secreto ruso recibía por un agujero del tamaño de un puño —un «agujero de ratón» perforado en la pared— las botellas de orina «sucia» de los deportistas rusos. En la sala de al lado, el equipo del director del laboratorio, Grigori Rodchenkov, abría las botellas Berlinger supuestamente inviolables, les vaciaba la orina dopada y la sustituía por orina limpia del mismo atleta, congelada meses antes, ajustando su densidad con **sal de mesa**. Aquel engaño funcionó porque el guardián de la integridad —el Estado, el laboratorio acreditado, el servicio secreto— era quien la corrompía. Meses después, el laboratorio de Londres descubriría que ocho muestras de Sochi tenían un contenido de sal **fisiológicamente imposible** en un ser humano sano, y que dos muestras de jugadoras de hockey contenían **ADN masculino** [4].

Aquel agujero en la pared contiene la pregunta de este capítulo: ¿cómo se prueba que una muestra biológica, una serie de valores o el resultado de un partido no han sido manipulados, cuando a veces quien debería custodiarlos es precisamente quien los altera? Aquí no sellamos un documento, como en los capítulos 20 y 29, sino **el contenido físico de un cuerpo y su cadena de custodia**.

Cuando el guardián es el corruptor

El escándalo ruso fue de una escala industrial. El jurista canadiense **Richard McLaren**, designado por la Agencia Mundial Antidopaje (WADA) como Persona Independiente, documentó en su *Informe McLaren* (2016) la «metodología del positivo que desaparece»: al menos **643 muestras positivas** reportadas como negativas entre finales de 2011 y agosto de 2015, una cifra que él mismo calificó de mínima. La segunda parte del informe concluía que **más de mil atletas rusos**, en más de treinta deportes, se habían beneficiado del encubrimiento [1][2]. Y el detalle más incómodo es que las famosas botellas «a prueba de manipulación» no lo eran: el servicio secreto descubrió cómo abrir sus tapones sin romper el sello visible, y una investigación posterior de la revista *Republik* demostró que el rediseño tampoco resistía —tres de cada veinticuatro kits se desenroscaban a mano tras tres días en la nevera, y una especialista no encontró «ni una sola medida de seguridad insuperable» [5]. La cobertura del Informe McLaren reveló que cuarenta y cuatro muestras, doce de ellas de medallistas, tenían marcas de manipulación en los tapones [3].

La lección es durísima y es el corazón de este frente: **un precinto físico, por sofisticado que sea, no vale nada si quien lo controla es cómplice**. La cadena de custodia —que la WADA define como la secuencia de responsables de una muestra desde que se obtiene hasta que llega al laboratorio— se puede romper desde dentro.

Del laboratorio al mercado de apuestas

El dopaje no es el único fraude que carcome el deporte; también está el amaño de partidos, detectado indirectamente por las huellas que deja en los mercados de apuestas. La operación VETO de Europol ya identificó más de 380 partidos sospechosos en Europa y 425 personas implicadas en una red transnacional de crimen organizado [8]. Sportradar, en su informe de integridad de 2024, monitorizó más de 850.000 partidos en setenta deportes y detectó 1.108 casos sospechosos, la mitad gracias a los datos de apuestas de cuenta [9]. La prueba, según Sportradar, ya no es la confesión ni el soborno visible, sino el movimiento anómalo de las cuotas. El caso más grande lo protagonizó Grigor Sargsyan, «el Maestro», condenado a cinco años en Bélgica en 2023 por dirigir una red de unos ciento ochenta tenistas de más de treinta y cinco países, a los que pagó unos siete millones de euros en sobornos vía móvil [10].

Esta lógica indirecta también impregna el antidopaje moderno: el Pasaporte Biológico del Atleta no «ve» la sustancia prohibida, sino que rastrea biomarcadores a lo largo del tiempo e individualiza sus umbrales. El ciclista Franco Pellizotti fue sancionado con dos años en 2011 sin ningún control positivo, solo por

valores anómalos de su pasaporte —el primer caso validado por el Tribunal de Arbitraje del Deporte sobre esta base [7]. En ambos casos, el fraude se demuestra por un patrón, no por un flagrante.

La prueba de existencia: sellar la muestra y datar la evidencia

Es aquí donde **t2p** refuerza el eslabón más débil. En el momento de la toma, el oficial de control y el atleta firman con **prueba de vida** un acta de obtención que captura la huella SHA-512 del formulario, el **número del kit** leído, el **GPS forense** de la sala, el sello de tiempo RFC 3161/eIDAS y la cara del atleta; todo se ancla a la **blockchain pública** y se cierra en un contenedor **.asice**. A partir de aquí, cada **transferencia de custodia** —del atleta al oficial, al mensajero, al laboratorio— genera un evento sellado con hora y lugar. Cualquier apertura, sustitución o «agujero de ratón» rompería la continuidad de la cadena anclada, que **no se puede reescribir retroactivamente** desde el propio laboratorio: el banco de orina limpia congelada o el intercambio nocturno dejarían una discontinuidad temporal y geográfica detectable. Lo mismo se aplica al pasaporte biológico, donde cada lectura se puede anclar con fecha cierta para blindar la serie contra la inserción posterior de valores «limpios». Y en el amaño, t2p no sella ninguna muestra, sino **la evidencia**: las alertas de Sportradar, las comunicaciones de los oficiales de integridad y las decisiones arbitrales se sellan para que la prueba presentada ante el Tribunal de Arbitraje o ante un juez penal sea demostrablemente anterior a cualquier filtración.

Hay que decir el límite con toda la crudeza, porque aquí es especialmente fuerte. «Basura a la entrada, basura en la cadena»: el sello garantiza que la muestra precintada en el minuto cero es la misma que llega al laboratorio, pero **no puede certificar que su contenido sea orina propia y no manipulada *antes* del sellado**. Si el atleta orina ya con orina de otro, o si el sistema de dopaje opera en el propio acto de obtención con complicidad del oficial, el sello inalterable solo certificará un fraude bien custodiado. Tampoco resuelve el **dopaje fisiológicamente indetectable** —las microdosis, las sustancias sin marcador—: el pasaporte biológico es indirecto y probabilístico, y la cadena de custodia no le añade poder analítico. En el amaño, sella la sospecha pero no prueba la intención: un patrón de apuestas anómalo anclado no demuestra por sí solo que hubiera soborno; eso todavía exige la investigación criminal. Y, sobre todo, el caso ruso enseña la lección más dura: **cuando el custodio es el corruptor —el Estado, el laboratorio acreditado—, el problema no es tecnológico sino de captura institucional**, y un sello criptográfico solo desplaza la confianza, no la elimina, si quien firma el acto de sellado es cómplice.

La promesa y el peligro

La promesa es real y valiosa. Una cadena de custodia sellada, con hora y lugar en cada transferencia, habría hecho mucho más difícil el intercambio nocturno de Sochi, porque la discontinuidad habría quedado registrada en un lugar que el laboratorio no puede reescribir. Y datar la evidencia del amaño daría a los tribunales deportivos una prueba incontestablemente anterior. En un mundo donde el fraude se prueba por patrones, hacer la prueba inalterable y datada es reforzar todo el edificio de la integridad.

El peligro pide los matices que hemos dicho. El primero, la sustitución previa al sellado, que ningún precinto resuelve. El segundo, la captura institucional: ninguna tecnología salva un sistema donde el propio guardián es el tramposo, y por eso la **independencia de quien custodia** sigue siendo insustituible. Y el tercero, no confundir sellar la evidencia con probar la intención. La prueba de existencia endurece la cadena de custodia y la anterioridad probatoria, no sustituye ni la independencia institucional ni la investigación criminal.

Es hora de actuar

Para las **agencias antidopaje** (la WADA, los laboratorios): sellar el acto de obtención y cada transferencia de custodia con hora y lugar, para que ningún «agujero de ratón» pueda romper la cadena sin dejar rastro. Para las **federaciones y unidades de integridad**: datar las alertas de amaño para que la prueba sea anterior a cualquier filtración. Para los **reguladores y tribunales deportivos**: exigir una independencia real de quien custodia, ya que ningún precinto vale nada en manos cómplices. Y para los **atletas limpios**: una cadena de custodia que los proteja tanto del tramposo como del sistema que lo amparó.

Una muestra cambió de manos de noche por un agujero en la pared porque nadie podía probar qué había pasado entre el precinto y el análisis. Dar a cada muestra y a cada evidencia una huella sellada con hora y

lugar —sin olvidar nunca que ningún sello salva a un guardián corrupto— es, en este frente que defiende el juego limpio, time2act.

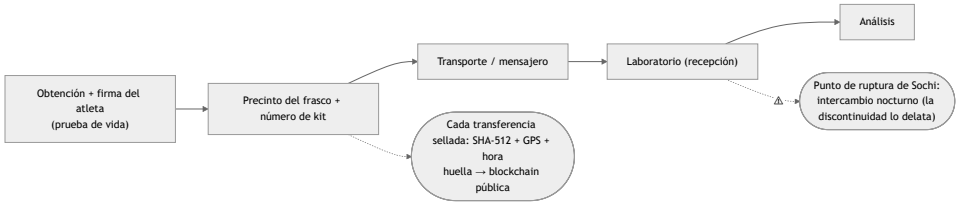


Figura 66.1 — La vida de una muestra antidopaje pasa por cinco nodos: obtención y firma del atleta, precinto de las botellas A y B, transporte, recepción en el laboratorio y análisis. En Sochi, el fraude entró en el nodo del laboratorio (el «agujero de ratón» por donde el servicio secreto intercambiaba la orina de noche). El sello de t2p —GPS forense, sello eIDAS y huella del número de kit anclados a la blockchain pública— hace que aquel intercambio deje una discontinuidad temporal y geográfica detectable. La evidencia forense que delató el fraude pese a las botellas «inviolables»: 44 tapones con marcas de manipulación (12 de medallistas), 8 muestras con sal imposible, 2 con ADN masculino, ≥643 positivos «desaparecidos». Límite: el sello no demuestra qué había en la botella antes de precintarla. Fuentes: Informe McLaren; CNN; Chemistry World.

---

[1] Wikipedia (síntesis del *Informe McLaren*) — *McLaren Report* (≥643 positivos «desaparecidos»; ADN masculino en muestras femeninas). https://en.wikipedia.org/wiki/McLaren_Report ↩

[2] World Anti-Doping Agency — *Independent investigation confirms Russian state manipulation of doping control* (McLaren, Persona Independiente; >1.000 atletas). https://www.wada-ama.org/en/news/wada-statement-independent-investigation-confirms-russian-state-manipulation-doping-control ↩

[3] CNN — *WADA McLaren report: tampered samples* (44 muestras con marcas en los tapones, 12 de medallistas; Parte 2, 2016). https://www.cnn.com/2016/12/09/sport/wada-russia-doping-mclaren-report ↩

[4] Chemistry World — *Anti-doping scientists expose cheating Russian athletes* (8 muestras con sal fisiológicamente imposible). https://www.chemistryworld.com/news/anti-doping-scientists-expose-cheating-russian-athletes/2500159.article ↩

[5] Republik — *Bad bottles* (las botellas «inviolables» Berlinger, vulneradas). https://www.republik.ch/2018/02/21/bad-bottles ↩

[6] World Anti-Doping Agency — *Athlete Biological Passport* (detección indirecta; módulo hematológico 2009, esteroideo 2014). https://www.wada-ama.org/en/athlete-biological-passport

[7] ESPN — *Pellizotti banned in landmark biological-passport ruling* (2 años sin positivo; primer caso validado por el TAS). https://www.espn.com/olympics/cycling/news/story?id=6192949 ↩

[8] Europol — *Results from the largest football match-fixing investigation in Europe (Operation VETO)* (>380 partidos; 425 personas; >15 países). https://www.europol.europa.eu/media-press/newsroom/news/update-results-largest-football-match-fixing-investigation-in-europe ↩

[9] Sportradar — *Betting Corruption and Match-Fixing 2024* (>850.000 partidos; 1.108 sospechosos; sistema UFDS). https://sportradar.com/content-hub/news/sportradar-reports-notable-decline-in-match-fixing-in-2024/ ↩

[10] The Washington Post — *Grigor Sargsyan, «the Maestro», and tennis match-fixing* (5 años; ~180 tenistas de >35 países; ~7 M€). https://www.washingtonpost.com/world/interactive/2023/tennis-match-fixing-itf-grigor-sargsyan/ ↩

Música y espectáculos: el humano real detrás del play

«El canto del ruiseñor es delicioso porque es el propio ruiseñor quien lo da.»

— John Philip Sousa, «The Menace of Mechanical Music» (1906)

A finales de 2018, desde Cornelius, en Carolina del Norte, un músico de mediana edad llamado Michael Smith escribió a sus dos socios un correo revelador: «necesitamos un MONTÓN de canciones rápido para esquivar las políticas antifraude que usan ahora». No buscaba ningún éxito; buscaba **ruido estadístico**. En su sótano digital, mil cuarenta cuentas-bot —pronto serían diez mil— reproducían sin descanso seiscientas treinta y seis canciones al día cada una: pistas con nombres sin sentido y artistas inventados, fabricadas en masa por una empresa de música con inteligencia artificial. Medio céntimo por escucha, **661.440 escuchas al día**. Nadie las oía. Durante siete años nadie se dio cuenta, hasta que la organización que gestiona los derechos mecánicos en Estados Unidos, The MLC, vio el patrón. En marzo de 2026, Smith se declaraba culpable; el botín superaba los diez millones de dólares [1][2].

Aquel ruido fabricado contiene la pregunta de este capítulo. No es la del capítulo 40 —«¿lo creó un humano o una IA?»—, porque aquí las canciones eran claramente de IA y no importa: la pregunta es otra, **¿un humano real escuchó de verdad esto, o compró de verdad esta entrada?** Es el fraude de la *presencia humana* en un acto de consumo.

El fraude que no crea dinero, lo reparte

Lo que hace especial a este fraude es cómo hace daño. La música en *streaming* reparte un **fondo de suma fija**: en 2025, según la federación discográfica internacional **IFPI**, generó más de 22.000 millones de dólares [6]. Cada escucha falsa no inventa dinero nuevo; **roba su parte al resto de artistas** que sí tienen público. La empresa de detección **Beatdapp** estima que el fraude de *streaming* desvía unos dos mil millones de dólares al año —al menos un 10 % de toda la actividad—, aunque, como parte interesada, conviene tomar la cifra como una estimación del sector con un margen amplio [3]. La respuesta de las plataformas ha sido poner umbrales: Spotify decidió que una pista debe superar las mil reproducciones anuales para entrar en el reparto, justamente para frustrar la táctica de Smith de diluir pocas escuchas entre cientos de miles de pistas basura [4].

Y hay un segundo problema de identidad, aún más sutil. The MLC recibió **424 millones de dólares** en derechos mecánicos históricos **no emparejados** —la «caja negra»: dinero generado por reproducciones cuyo titular no se pudo determinar [5]. La pregunta, pues, no es solo «¿hubo una escucha real?», sino «¿de quién es la canción que se escuchó?».

Del play falso a la entrada fantasma

El mismo fraude de presencia humana carcome el mundo de las entradas. En la preventa de la gira *Eras* de Taylor Swift, el 15-de-noviembre-2022, la web de Ticketmaster recibió **3.500 millones de peticiones** —cuatro veces el récord anterior—, con unos doce millones de «entidades», muchas de ellas bots de reventa, que sobrecargaron el sistema hasta el colapso [10]. No es un accidente, sino un modelo de negocio. La comisión federal de comercio estadounidense (**FTC**) ya había llevado a los tribunales, bajo la ley BOTS de 2016, a revendedores que habían comprado más de ciento cincuenta mil entradas con software automatizado y cientos de cuentas ficticias [8]. Como hemos visto, en 2025 se presentó una prueba demoledora: cinco revendedores controlaban 6.345 cuentas y acaparaban **246.407 entradas** para 2.594 eventos, gestionadas desde una sola pantalla; un ejecutivo admitió por correo que la empresa «hacía la vista gorda como política» [9]. El límite de «cuatro entradas por persona» que veía el fan era, en la práctica, ficción.

La prueba de existencia: el humano real detrás del play y de la entrada

Es aquí donde **t2p** ataca el vacío, certificando no quién creó la obra, sino que **un humano real, en un dispositivo real, en un momento y un lugar reales, ejecutó una acción real**. En el lado del consumo: en el dispositivo del oyente, en el instante de la reproducción, se genera una huella SHA-512 de

un evento de escucha —pista, dispositivo, **prueba de vida**, GPS forense y duración realmente reproducida—, se ancla a la **blockchain pública** y se sella con el sello de tiempo eIDAS; el reproductor exige una señal de vivacidad para que la escucha cuente. En el lado de las entradas: en el momento de la compra y, de nuevo, en el acceso al recinto, se sella un contenedor **.asice** que liga la identidad verificada con prueba de vida, la entrada, el GPS del recinto y la hora de entrada física.

El efecto es directo. Una escucha **sin prueba de vida no entra en el cómputo** que reparte los derechos, lo que hunde el modelo de Smith: diez mil cuentas-bot dejan de cobrar. Vincular cada compra a una identidad con vivacidad **anula los cientos de cuentas por revendedor** documentados por la FTC. Y el sello de GPS y hora en la puerta prueba que quien entra es quien compró, no un comprador masivo automatizado. La presencia humana vuelve a ser la unidad de cuenta.

Hay que decirlo con toda crudeza, porque aquí es matizado. «Basura a la entrada, basura en la cadena»: **t2p** puede probar que un humano vivo pulsó «play» o cruzó la puerta, pero **no puede probar que aquella escucha fuera genuina ni honesta**. Si en lugar de bots se contratan **humanos reales** —cada uno superando la prueba de vida— para escuchar pistas basura, el sello los certificará como «humanos reales» y el fraude persistirá: la prueba de vida derrota a los bots, no a las granjas humanas ni al *streaming* pagado. Tampoco juzga el mérito: una escucha humana de treinta segundos de ruido de IA, hecha solo para cobrar, queda sellada como válida. La «caja negra» de los 424 millones tampoco se resuelve con un sello; el evento existió, pero no se sabe **de quién** es la composición, y eso exige metadatos limpios, no solo un sello. Y, sobre todo, el sello solo sirve si las plataformas lo integran y lo honran: el expediente de la FTC demuestra que el intermediario dominante puede «hacer la vista gorda por política», y ninguna criptografía corrige el incentivo económico del propio guardián. En la reventa legítima, además, ligar la entrada a la identidad no impide que alguien revenda o regale su entrada a otra persona real.

La promesa y el peligro

La promesa es cuantificable en miles de millones. Una capa de presencia humana sobre el *streaming* y las entradas haría mucho más difícil drenar el fondo de derechos con bots, anularía los ejércitos de cuentas ficticias de los revendedores y devolvería el dinero a los artistas con público real y las entradas a los fans. En un mercado donde el fraude no crea dinero sino que lo reparte mal, demostrar el humano real es restaurar la justicia del reparto.

El peligro requiere los matices que hemos dicho. El primero, las granjas humanas y el *streaming* incentivado, ya que la prueba de vida no las detiene. El segundo, no confundir presencia con legitimidad ni con identidad de la obra. El tercero, la captura de plataforma: ningún sello vale nada si el guardián decide no honrarlo. Y el cuarto, la privacidad y el derecho del fan a revender o regalar su entrada, que la mecánica anti-bot debe respetar. La prueba de existencia es una herramienta poderosa para restaurar la presencia humana, no una bala de plata contra todos los fraudes del sector ni un sustituto de arreglar sus incentivos.

Es hora de actuar

Para las plataformas (Spotify, Apple Music) hay que integrar la prueba de presencia humana en el cómputo de los derechos, de modo que una escucha sin humano deje de estar facturada. Para los organismos de derechos (IFPI, The MLC) se debe exigir el sello y limpiar los metadatos que vacían la «caja negra». Para la industria de las entradas (Live Nation/Ticketmaster) y los reguladores (la FTC) hay que vincular la compra y el acceso a una identidad real y dejar de hacer la vista gorda. Y para los artistas y los fans, el sistema debe garantizar que tanto la escucha como la entrada sean de humanos, no de bots.

Una granja de bots cobró por 661.440 escuchas diarias que nadie oyó; ofrecer a cada escucha y a cada entrada una prueba sellada del humano real —sin vulnerar la privacidad ni el derecho a revender— es, en este frente del comercio de la atención y el ocio, **time2act**.

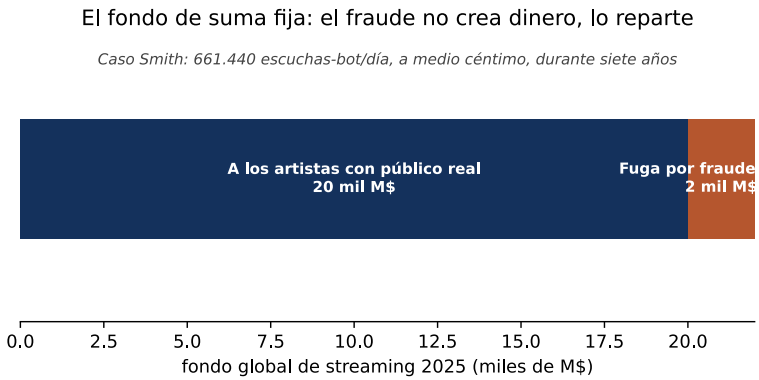


Figura 67.1 — La música en streaming reparte un fondo de suma fija: en 2025, más de 22.000 millones de dólares (IFPI). Cada escucha falsa no inventa dinero nuevo; roba su parte a los artistas con público real. La estimación de la industria cifra la fuga por fraude en unos 2.000 millones de dólares al año —al menos un 10 % de la actividad (Beatdapp). El caso Smith: 661.440 escuchas-bot al día, a medio céntimo, durante siete años. Con prueba de vida, las escuchas sin humano no entran en el reparto y el fondo vuelve a los artistas reales. Fuentes: IFPI Global Music Report 2026; Beatdapp; acusación de la fiscalía de Nueva York.

---

[1] U.S. Department of Justice / SDNY (vía Music Business Worldwide) — *North Carolina man pleads guilty to AI-assisted music streaming fraud* (Michael Smith; decomiso de 8,09 M$). https://www.musicbusinessworldwide.com/streaming-fraud-man-who-pocketed-8m-using-hundreds-of-thousands-of-ai-songs-streamed-billions-of-times-by-bots-pleads-guilty/ ↩

[2] Rolling Stone — *Inside the AI streaming-fraud case* (de 1.040 a 10.000 cuentas-bot; 661.440 reproducciones/día; los correos). https://www.rollingstone.com/music/music-features/streaming-fraud-fake-streams-mike-smith-1235500686/ ↩

[3] Beatdapp / Music Business Worldwide — *Streaming fraud costs the global music industry ~$2bn a year* (≥10 % de la actividad; estimación de parte). https://www.musicbusinessworldwide.com/streaming-fraud-costs-the-global-music-industry-2bn-a-year-according-to-beatdapp-now-its-partnering-with-beatport-to-combat-the-trend/ ↩

[4] Spotify / Music Business Worldwide — *The 1,000-stream royalty threshold* (anunciado nov-2023; vigente abr-2024). https://www.musicbusinessworldwide.com/heres-exactly-spotifys-new-1000-annual-streams-royalty-policy-works123/ ↩

[5] The MLC / Billboard — *Mechanical Licensing Collective receives over $424 million in unmatched royalties* (la «caja negra»). https://www.billboard.com/pro/mechanical-licensing-collective-receives-over-424-million-unmatched-royalties-streaming-services/ ↩

[6] IFPI — *Global Music Report 2026* (31.700 M$; streaming >22.000 M$, el 69,6 %; «theft, plain and simple»). https://www.ifpi.org/global-music-report-2026-global-recorded-music-revenues-grow-6-4-as-record-companies-drive-innovation/ ↩

[7] IFPI (Victoria Oakley) — *Brazilian authorities disrupt JustAnotherPanel* («fake streams… erode trust in our system»). https://www.ifpi.org/brazilian-authorities-launch-largest-ever-disruption-operation-against-major-streaming-fraud-platform-justanotherpanel/

[8] Federal Trade Commission — *FTC brings first-ever cases under the BOTS Act* (2021; >150.000 entradas; >31 M$ en sanciones). https://www.ftc.gov/news-events/news/press-releases/2021/01/ftc-brings-first-ever-cases-under-bots-act ↩

[9] Federal Trade Commission — *FTC sues Live Nation/Ticketmaster* (2025; 5 revendedores, 6.345 cuentas, 246.407 entradas; «turn a blind eye as a matter of policy»). https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-sues-live-nation-ticketmaster-engaging-illegal-ticket-resale-tactics-deceiving-artists-consumers ↩

[10] Wikipedia — *Taylor Swift–Ticketmaster controversy* (gira Eras; 3.500 M de peticiones; ~12 M de «entidades» con bots). https://en.wikipedia.org/wiki/Taylor_Swift%E2%80%93Ticketmaster_controversy ↩

Telecomunicaciones y voz: autenticar a quien llama de verdad

«Señor Watson, venga: quiero verle.»

— Alexander Graham Bell, cuaderno de laboratorio (10-3-1876)

A finales de enero de 2024, dos días antes de las primarias demócratas de Nuevo Hampshire, miles de teléfonos sonaron. Al descolgar, una voz inconfundible —la de Joe Biden— pedía a los votantes que *no* fueran a votar y «guardaran su voto» para noviembre. El identificador de llamada mostraba un número conocido del partido. Todo era falso: la voz estaba clonada con inteligencia artificial y el identificador, falsificado. El operador político que lo encargó, Steve Kramer, recibió una multa de **seis millones de dólares**, y la comisión federal de comunicaciones estadounidense (**FCC**) dictó la primera norma que declara ilegales los *robocalls* con voz de IA [2][3]. No era ni la primera vez: ya en 2019, el director de una filial energética británica había transferido unos 243.000 dólares tras una llamada de su «jefe», con el acento alemán de siempre —una voz sintética, el primer fraude de voz clonada conocido [10].

Aquella tarde de Nuevo Hampshire contiene la paradoja de este capítulo: una voz de autoridad, **perfectamente autenticada para el oído humano, completamente falsa en el cable**. A diferencia del capítulo 16, que narraba la suplantación visual de un ejecutivo en una videollamada, aquí el ataque es a la **infraestructura misma de las telecomunicaciones** —la SIM, la red de señalización, el identificador— y a la prueba de **quién origina de verdad una voz**.

El número, el eslabón débil

El fraude más silencioso no toca la voz, sino el número. En el **SIM-swap**, el atacante consigue que la operadora lleve tu número de móvil a una SIM que él controla y, con eso, intercepta los códigos de un solo uso que protegen tus cuentas. Solo en 2023, la oficina de delitos informáticos del FBI registró más de mil denuncias con pérdidas de **48,8 millones de dólares** [1], y en el Reino Unido el servicio antifraude **Cifas** reportó un aumento del **1.055 %** de SIM-swaps no autorizados en un solo año [6]. Las cifras individuales dan vértigo: T-Mobile fue condenada a pagar unos **33 millones de dólares** —el laudo se hizo público en 2025— después de que un SIM-swap permitiera robar unos 38 millones en criptomonedas al emprendedor Josh Jones, eludiendo la verificación por SMS [7]. Como resume Cifas, el número de móvil se ha convertido en **el eslabón débil** de toda la identidad digital basada en códigos por SMS. Y las víctimas preferidas son los mayores: la comisión de comercio estadounidense encontró que el 41 % de los adultos mayores que perdieron diez mil dólares o más en estafas de suplantación —como hemos visto— decían que el primer contacto había sido **una llamada de teléfono**.

STIR/SHAKEN: una capa, no la solución

La industria ha respondido autenticando el identificador de llamada con el sistema **STIR/SHAKEN**, que firma criptográficamente el número de origen para que las operadoras puedan bloquear o etiquetar las llamadas falsificadas. Pero hay un agujero enorme: en abril de 2025 solo el **42,5 %** de las llamadas llegaban firmadas, ya que el sistema **solo funciona en redes IP** y cualquier tramo antiguo rompe la firma [5]. Como hemos visto, los consumidores estadounidenses recibieron **52.800 millones de robocalls** en 2024, unas doscientas por adulto [referencia de YouMail]. Por eso la defensa se está desplazando a la **capa de red**: según la **GSMA**, la asociación mundial de operadores, su iniciativa Open Gateway expone señales como «tiempo desde el último cambio de SIM» para que un banco no se fíe ciegamente de un SMS [9]. Pero ninguna de estas capas responde la pregunta fundamental: **¿quién ha originado realmente esta voz?**

La prueba de existencia: autenticar el origen humano de la voz

Es aquí donde **t2p** aporta una capa complementaria. No impide que alguien clone una voz ni que se haga con una SIM; **sella la autenticidad y el origen de un acto de identidad en el momento en que ocurre**. Cuando una persona graba una instrucción o autoriza una operación sensible —autorizar una transferencia, confirmar la identidad ante un banco, registrar un consentimiento—, la aplicación calcula en el dispositivo la **huella SHA-512** del clip más los metadatos, la ancla a la **blockchain pública** y le

adjunta un **sello de tiempo RFC 3161** conforme a eIDAS y un **GPS forense**, todo en un contenedor **.asice**.

La pieza decisiva es la **prueba de vida**, que ataca exactamente el agujero que señalan los reguladores: distinguir una voz humana real, capturada en vivo, de una síntesis. Es el mismo principio del concepto premiado por la propia comisión de comercio en su *Voice Cloning Challenge*, **OriginStory**, que mide las bioseñales de la garganta y la boca para autenticar el **origen humano de la voz en el punto de creación**. Así, una autorización legítima queda sellada con vivacidad, hora y lugar, de manera que un audio clonado posterior no puede hacerse pasar por la «grabación original» ni reclamar precedencia temporal; la víctima puede demostrar que **no** emitió cierta instrucción porque no existe ningún sello válido suyo; y el sello de tiempo fija un orden incontrovertible frente a un clip fabricado. STIR/SHAKEN autentica el *número* en la red; t2p autentica el *contenido y el origen humano* en el extremo. Son capas que se completan.

Hay que decir el límite con toda la crudeza. «Basura a la entrada, basura en la cadena»: t2p sella la integridad y el momento de una captura, pero **no certifica que su contenido sea verdad ni que la persona no esté siendo engañada en aquel instante**. No detecta la clonación dentro de la llamada entrante: si un estafador te llama con voz clonada, t2p no la analiza; solo sirve si la contraparte legítima **sella proactivamente** su propio acto de identidad —no es un filtro de robocalls ni un sustituto de STIR/SHAKEN. Tampoco impide el SIM-swap, que ocurre en la operadora; como mucho, permite que un sistema **no dependa** de un SMS como única prueba. Y si el atacante engaña a la víctima para que ella misma grabe y selle una autorización, la cadena dirá la verdad sobre una mentira: el sello será válido y el acto, fraudulento. Finalmente, como STIR/SHAKEN, solo protege a quien lo usa en los dos extremos, y no recupera el dinero de una transferencia ya ejecutada.

La promesa y el peligro

La promesa es real en un terreno donde la voz ha dejado de ser una prueba. Una capa que autentique el origen humano y el momento de un acto de identidad daría a bancos, empresas y ciudadanos una contraprueba verificable frente a la voz clonada, y rompería la dependencia malsana del SMS como única clave. Combinada con STIR/SHAKEN en la red y las API de la GSMA, completaría una defensa por capas que hoy tiene agujeros por todas partes.

El peligro pide los matices que hemos dicho. El primero: no confundir t2p con un filtro de llamadas; protege el acto propio, pero no analiza el ajeno. El segundo: no detiene ni el SIM-swap ni la coacción de la víctima. Y el tercero: la adopción. Sin uso en los dos extremos, no hay efecto de red. La prueba de existencia es una capa complementaria potente contra la suplantación de voz, pero no es una bala de plata contra todo el fraude telefónico.

Es hora de actuar

Para las **operadoras**: completar STIR/SHAKEN, cerrar los tramos no-IP y aplicar los principios de conocer al cliente y al proveedor que la FCC impuso a Lingo.

Para los **bancos y las apps**: dejar de depender del SMS como única prueba y usar señales de red, como la API de cambio de SIM de la GSMA.

Para los **reguladores** (la FCC): perseguir la voz clonada ilegal, como en el caso de Nuevo Hampshire. Y para los **usuarios**, sobre todo los mayores: disponer de una prueba sellada que acredite el origen humano de la propia voz, para que ningún clon pueda hablar en su nombre.

Una voz clonada de Biden pidió a miles de personas que no votaran, perfectamente creíble para el oído y del todo falsa en el cable. Dar a cada acto de voz una prueba sellada de su origen humano —sin olvidar que no detiene ni la SIM robada ni el engaño— es, en este frente donde ya no podemos creer lo que oímos, time2act.

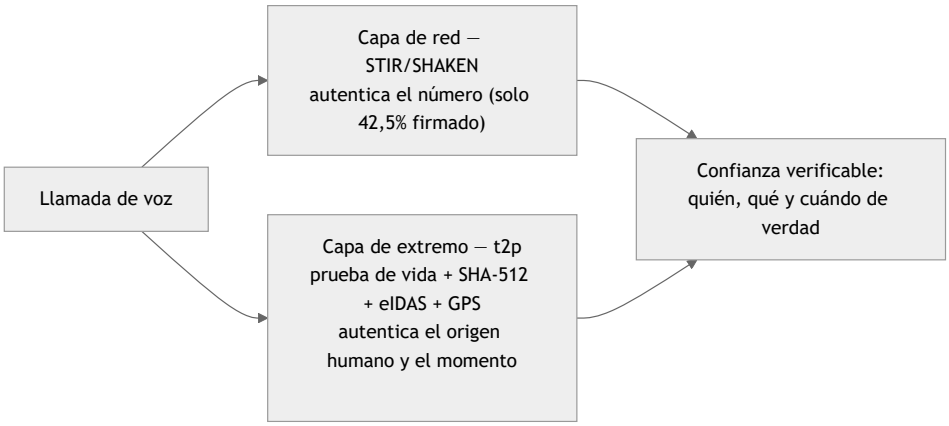


Figura 68.1 — La capa de red (STIR/SHAKEN) autentica el número de origen —«¿desde qué número llama?»—, pero solo el 42,5 % de las llamadas llegan firmadas (abril de 2025), porque cualquier tramo no-IP rompe la firma. La capa de extremo (t2p: prueba de vida + SHA-512 + sello eIDAS + GPS) autentica el origen humano y el momento del acto —«¿quién, qué y cuándo, de verdad?». Son complementarias. Contexto: 52.800 millones de robocalls en EE. UU. en 2024; 48,8 M$ robados por SIM-swap (FBI, 2023). Fuentes: TransNexus; FCC; FBI IC3.

---

[1] FBI Internet Crime Complaint Center (IC3) — *2023 Internet Crime Report* (SIM-swapping: 1.075 denuncias, 48,8 M$ de pérdidas). https://www.ic3.gov/AnnualReport/Reports ↩

[2] NPR — *The AI deepfake Biden robocall and the FCC* (Nuevo Hampshire; Steve Kramer; multa de 6 M$). https://www.npr.org/2024/05/23/nx-s1-4977582/fcc-ai-deepfake-robocall-biden-new-hampshire-political-operative ↩

[3] Federal Communications Commission — *FCC makes AI-generated voices in robocalls illegal* (Declaratory Ruling, febrero de 2024). https://www.fcc.gov/document/fcc-makes-ai-generated-voices-robocalls-illegal ↩

[4] Federal Communications Commission — *FCC settles Lingo Telecom robocall investigation* (1 M$; STIR/SHAKEN + conocer al cliente y al proveedor). https://www.fcc.gov/document/fcc-settles-lingo-telecom-robocall-investigation

[5] TransNexus — *SHAKEN statistics, April 2025* (solo el 42,5 % de llamadas firmadas; la brecha no-IP). https://transnexus.com/blog/2025/shaken-statistics-april/ ↩

[6] Cifas — *Fraudscape 2025* (+1.055 % de SIM-swaps no autorizados en el Reino Unido). https://www.cifas.org.uk/newsroom/huge-surge-see-sim-swaps-hit-telco-and-mobile ↩

[7] SecurityWeek — *T-Mobile coughed up $33 million in SIM-swap lawsuit* (Josh Jones; ~38 M$ en criptomonedas). https://www.securityweek.com/t-mobile-coughed-up-33-million-in-sim-swap-lawsuit/ ↩

[8] Federal Trade Commission — *Winners of the Voice Cloning Challenge (OriginStory)* (autenticar el origen humano de la voz en el punto de creación). https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-announces-winners-voice-cloning-challenge

[9] GSMA — *Open Gateway / Mobile Identity APIs (SIM Swap API)* (la defensa migra a la capa de red). https://www.gsma.com/solutions-and-impact/technologies/mobile-identity/mobile-identity-and-data-apis/ ↩

[10] The Next Web / The Wall Street Journal — *Fraudsters deepfake a CEO's voice* (2019; ~243.000 $; primer fraude de voz sintética conocido). http://thenextweb.com/news/fraudsters-deepfake-ceos-voice-to-trick-manager-into-transferring-243000 ↩

El fraude bancario del pago «autorizado»

«La confianza es la base indispensable de toda clase de transacciones. Sin ella, el comercio [...] se detendría como un reloj sin cuerda.»

— Herman Melville, The Confidence-Man (1857)

La llamada llega de un número que parece el del banco. La voz —profesional, tranquila— avisa de un «cargo sospechoso» y guía a la víctima, paso a paso, «para proteger los ahorros»: una transferencia «a la cuenta segura». O el mensaje del «hijo»: «papá, se me ha roto el móvil, hazme un Bizum a este número». Cuando la persona se da cuenta, el dinero ha salido —y lo ha enviado ella, con su app, sus claves y su huella.

El nudo jurídico es exactamente este [2]. La normativa europea de pagos —la PSD2, transpuesta en España por el RDL 19/2018— distingue dos mundos. En la operación no autorizada —otra persona mueve tu dinero—, el banco debe devolver el importe salvo que pruebe fraude o negligencia grave del cliente, y la carga de probar que la operación se autenticó correctamente es suya. Pero en el pago autorizado bajo engaño —lo que los británicos llaman fraude APP—, la respuesta clásica del sistema es demoledora: «lo autorizaste tú». La víctima perfecta del fraude moderno no es quien pierde las claves: es quien las usa convencida.

Este capítulo trata el fraude que no fuerza la puerta: convence a la víctima para que la abra. La SIM clonada y la voz falsificada —los vehículos del engaño— están en el capítulo 68; el director financiero suplantado que ordena transferencias de empresa, en el capítulo 87; la relación con la compañía de servicios, en el capítulo 33; el compliance institucional, en el capítulo 16; la estafa a las personas mayores, en el capítulo 85; el pago fuera de plataforma de la compraventa entre particulares, en el capítulo 31. Pregunta clave: cuando el pago lo hiciste tú, engañado, ¿qué queda por discutir? Respuesta: diligencias —qué te mostraron, qué te advirtieron, qué viste— y las diligencias son hechos datados: la fecha cierta a ambos lados de la pantalla, con **t2p** —la tríada del capítulo 13: huella, hora cierta, ancla [3]. El Reino Unido acaba de convertir esta batalla de pruebas en ley.

El Reino Unido da la vuelta al tablero

Desde el 7 de octubre de 2024, el Reino Unido es el primer país del mundo con un régimen de reembolso obligatorio del fraude del pago autorizado [1]. El régimen —del Payment Systems Regulator— obliga a los proveedores de pago a reembolsar a las víctimas: particulares, microempresas y entidades benéficas, en transferencias de los sistemas Faster Payments y CHAPS, hasta un límite de 85.000 libras —rebajado de las 415.000 iniciales para alinearlo con el fondo de garantía británico. El reembolso, en cinco días hábiles —o hasta treinta y cinco si hay que investigar. Y la pieza más ingeniosa: el coste se reparte al 50 % entre el banco emisor y el banco receptor —el banco que acogió la cuenta mula también paga [1]. El régimen sustituye un código voluntario que se había demostrado insuficiente.

La lectura de este libro: cuando el reembolso es la norma, todo el sistema se convierte en una disputa de diligencias. ¿El cliente ignoró advertencias claras? ¿El banco las mostró de verdad —y cuándo? ¿El banco receptor abrió la cuenta mula a la ligera? Cada respuesta es un hecho datado en una pantalla o en un registro. El régimen británico, sin decirlo, ha creado la necesidad de la prueba de existencia a ambos lados: quien pueda acreditar qué se mostró, qué se advirtió y qué se hizo —y cuándo— tendrá su parte de razón; quien no, pagará.

Y en Europa continental, con la reforma de los pagos en tramitación [2], la pregunta no es si este modelo llega, sino cuándo.

La prueba de existencia aplicada

El engaño se despliega como una cadena de momentos —y cada momento se puede datar [3].

1. El engaño documentado

La llamada del falso técnico, grabada —conversación propia, lícita, como explica el capítulo 75—; el SMS de la «cuenta segura» y el chat del «hijo», capturados con fecha cierta [3]. El engaño deja de ser una

historia que la víctima cuenta avergonzada: es una secuencia datada que un analista puede reseguir —y que, ante el banco o el juez, establece el contexto del pago «autorizado»: autorizado, sí; libre, no.

2. La sesión capturada

Lo que la víctima veía cuando pagó: la pantalla de la app con el beneficiario y el aviso —o la ausencia de aviso—, la web que suplantaba al banco, capturada con imagen completa y código fuente [3]. En un régimen de diligencias compartidas, este es el campo de batalla exacto: el banco dirá que advirtió; el cliente, que no vio nada. La pantalla de aquel momento, con fecha cierta, responde por ambos.

3. La reclamación datada

El reloj corre desde el primer minuto: la comunicación al banco, capturada al enviarse; la denuncia policial, escaneada; cada respuesta y cada silencio, con su fecha [3]. Los plazos del régimen británico —el reembolso en 5 días, o 35 con investigación [1]— y los de cualquier reclamación europea se miden sobre estas fechas; y el expediente .asice entero, verificable sin conexión, llega al servicio de reclamaciones, al supervisor o al juzgado con la cronología cerrada.

4. La simetría del banco diligente

El mismo mecanismo protege a la entidad que lo hace bien: los avisos mostrados —la fricción aplicada al pago inusual, la advertencia del beneficiario nuevo— anclados por lotes encadenados, con la misma lógica que VeriFactu impone a las facturas [3]; y el registro del alta de la cuenta receptora, con sus comprobaciones. Cuando el régimen reparte costes según diligencias [1], el banco que puede probar que advirtió —y el receptor que puede probar que verificó— tienen su defensa; el que no puede probar nada, paga. La prueba no elige bando: obliga a todos.

Los límites, dichos claramente: el sello acredita pantallas, conversaciones y fechas —no decide si la negligencia era grave ni si el aviso era lo bastante claro: eso lo dicen la ley y el juez [2]. No recupera dinero ya movido —la velocidad de reacción y la cooperación entre bancos siguen siendo decisivas. Y la prevención sigue siendo la primera línea: el banco no llama nunca para pedir transferencias, y ninguna prisa es buena señal.

La promesa y el peligro

La promesa: víctimas que no tienen que elegir entre la vergüenza y la indefensión —el engaño documentado es reclamable [1][3]; bancos diligentes que acreditan sus avisos y no pagan por los pecados de los descuidados; cuentas mula más caras de abrir, porque el receptor también responde [1]; y un modelo —el británico— que demuestra que el fraude APP no es una fatalidad, sino un problema de reparto de incentivos y de prueba.

Ahora toca mirar los peligros.

El primero es **el fraude del fraude**. Si el reembolso es automático, aparecerá quien simule ser víctima. El contrapeso es el mismo expediente: la víctima real tiene una secuencia de engaño datada y coherente; el simulador debe fabricarla entera contra un GPS forense y unos sellos que no se dejan antedatar [3].

El segundo es **la fortaleza del banco**: la entidad con registros perfectos frente al cliente con memoria. Si solo una parte puede probar, el régimen se desequilibra —por eso la capa del cliente, sus capturas y su diario, es tan importante como la del banco, y el supervisor debe valorar ambas.

El tercero es **el miedo que paraliza**. Un régimen demasiado duro para los bancos puede acabar en fricciones infinitas para todos: pagos bloqueados, sospecha universal. El equilibrio es fino —advertencias claras y datadas, no obstáculos; protección, no paternalismo.

Y el cuarto es **el tecnosolucionismo del reembolso**. Recuperar el dinero no deshace el engaño ni atrapa al estafador. La persecución del delito —y de las redes de mulas— sigue siendo tarea policial; la prueba de existencia ayuda a ella: cada expediente datado es un mapa del modus operandi.

Es hora de actuar

Que quien confió no tenga que probar su inocencia con las manos vacías.

Para ti, cliente: si el engaño llega, documenta mientras reaccionas —la llamada, el SMS, la pantalla [3]; y recuerda la regla de oro: el banco no llama nunca para pedirte una transferencia.

Para los bancos emisores: anclad vuestros avisos y fricciones [3] —en un régimen de diligencias compartidas [1], la advertencia que no podéis probar no existe.

Para los bancos receptores: el alta de cuentas con verificación demostrable —cuando la cuenta mula también os cuesta dinero [1], vuestra puerta de entrada es vuestra primera defensa.

Para los supervisores y legisladores europeos: el modelo británico [1] ya funciona; que la reforma europea de los pagos [2] incorpore el reembolso del fraude APP —y que el reparto de costes se decida sobre evidencia datada de las dos partes, no sobre la palabra del más grande.

Para la policía y las fiscalías: el expediente .asice de cada víctima [3] es un mapa datado de la red —agregados, los mapas atrapan mulas y estafadores.

El fraude moderno no roba claves: roba confianza. Que al menos cada engaño deje su cronología —y que quien confió no tenga que probar su inocencia con las manos vacías. Por los ahorros de todos, **time2act**.

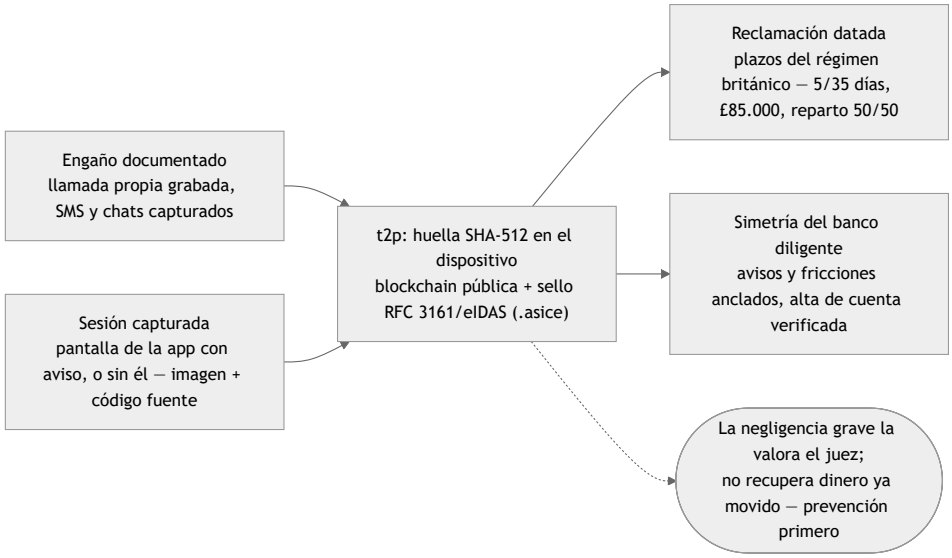


Figura 69.1 — El fraude del pago «autorizado» con prueba de existencia (sellado con t2p — capítulo 13): el engaño documentado (llamada propia grabada, SMS y chats capturados), la sesión capturada (la pantalla con el aviso —o sin él), la reclamación datada (plazos) y la simetría del banco diligente (avisos y fricciones anclados por lotes; el alta de la cuenta receptora verificada). Contexto: Reino Unido, primer reembolso obligatorio del mundo (7-10-2024; £85.000; 50/50 emisor-receptor; 5/35 días); PSD2: en operaciones no autorizadas, la carga de la prueba es del banco. Límites: la negligencia grave la valora el juez; la prevención primero. Fuentes: PSR; PSD2/RDL 19/2018.

---

[1] Payment Systems Regulator (Reino Unido) — *APP fraud reimbursement protections* (régimen obligatorio desde el 7-10-2024, primero del mundo; particulares, microempresas y entidades benéficas; Faster Payments y CHAPS; límite 85.000 £ —rebajado de 415.000 para alinearlo con el FSCS; coste compartido 50/50 entre proveedor emisor y receptor; reembolso en 5 días hábiles o hasta 35 con investigación; sustituye el código voluntario CRM); análisis de Freshfields, A&O Shearman y Thomson Reuters. https://www.psr.org.uk/information-for-consumers/app-fraud-reimbursement-protections/ · https://www.freshfields.com/en/our-thinking/briefings/2024/09/authorised-push-payment-fraud-a-new-mandatory-reimbursement-regime-for-uk-psps/ · https://www.aoshearman.com/en/insights/ao-shearman-on-fintech-and-digital-assets/the-uks-authorised-push-payment-app-fraud-reimbursement-scheme · https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/app-fraud-uk/ ↩

[2] PSD2 (Directiva (UE) 2015/2366, transpuesta en España por el RDL 19/2018): en operaciones de pago no autorizadas, devolución por parte del proveedor salvo fraude o negligencia grave del cliente; carga de la prueba de la autenticación correcta sobre el proveedor; autenticación reforzada (SCA); reforma europea de los pagos (PSD3/PSR) en tramitación. ↩

[3] t2p — manual de producto (grabación de audio de conversaciones propias; captura de pantalla y de página web certificadas —imagen completa + código fuente; certificar cualquier fichero por lotes; proyectos para el expediente de un incidente; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión; solo huellas en la cadena). Véanse los capítulos 13 y 15; la voz clonada y la SIM, en el capítulo 68; el CFO suplantado, en el capítulo 87; la caja negra personal, en el capítulo 75. ↩

Hardware: el pedigrí de un chip que no podía fallar

«El diseño de ingeniería tiene como primer y principal objetivo evitar el fallo.»

— Henry Petroski, To Engineer Is Human (1985)

En un almacén de Clearwater, en Florida, entre 2006 y 2010, una empresa llamada VisionTech importaba circuitos integrados de una sola fábrica china, hechos con materiales «inferiores y reciclados», y los reetiquetaba con las marcas de Intel, Texas Instruments y Motorola. Los fiscales encontraron en ella un detalle que lo dice todo: **fotografías del hijo del propietario aplicando abrillantador de coches a chips sucios** para que parecieran nuevos. La empresa decía hacer «pruebas internas», pero no tenía ni un solo experto en control de calidad. Vendió **15,8 millones de dólares** en componentes etiquetados como «aptos para uso militar», y su administradora acabó con treinta y ocho meses de prisión —la primera condena penal federal en Estados Unidos por tráfico de circuitos integrados falsificados [3].

Aquellos chips reciclados no iban a juguetes. En 2010, el mismo tipo de memorias falsas aparecieron en los ordenadores de misión del misil antimisiles **THAAD**; según la agencia de defensa, si hubieran fallado, **el propio misil probablemente habría fallado** [1]. Y un chip de memoria falsificado se instaló en más de cuatrocientas unidades de pantalla de cabina de los aviones de transporte C-27J y C-130J, donde una avería podía dejar la pantalla del piloto **en blanco en pleno vuelo** [4]. Este capítulo no trata de la falsificación de bienes de consumo del capítulo 29, sino de una mentira más técnica y más peligrosa: la del **pedigrí** de un componente electrónico —su origen, su fecha, su cadena de custodia— que viaja en etiquetas y certificados falsificables hasta el corazón de un sistema de armas.

El mercado gris y la mentira del pedigrí

La escala del problema es nacional. Una investigación de un año del **Comité de Servicios Armados del Senado** de Estados Unidos identificó en 2012 unas mil ochocientas ocurrencias de piezas sospechosas de ser falsificadas en la cadena de suministro de defensa, con **más de un millón de piezas** individuales y más de seiscientas cincuenta empresas implicadas; más del **70 % se rastreó hasta China** [1]. Para demostrar lo fácil que era, la oficina de fiscalización del Congreso (**GAO**) creó una empresa ficticia y compró dieciséis componentes de grado militar por internet: **los dieciséis resultaron falsos** [2]. La mayoría de estas falsificaciones —alrededor del **80 %, según las bases de datos del sector** como IHS y ERAI— no son copias fabricadas desde cero, sino chips usados arrancados de placas descartadas, pulidos y remarcados. Un solo proveedor de Shenzhen, Hong Dark, introdujo unas **84.000 piezas** sospechosas que llegaron a sistemas anticolisión de aviones militares y a proyectiles de artillería [1]. La asociación de la industria de semiconductores calcula que todo ello cuesta más de **7.500 millones de dólares** al año [5], y el problema no remite: la organización de seguimiento ERAI registró en 2024 el número más alto de piezas sospechosas desde 2015 [6].

Por qué detectar es caro y prevenir por el origen es barato

Lo que hace diabólico a este fraude es que un chip reciclado puede ser, por fuera, **idéntico** a uno auténtico. Como explica el centro de investigación CALCE de la Universidad de Maryland, detectarlo exige un laboratorio físico-químico caro —rayos X, apertura de la cápsula, pruebas eléctricas—, porque la falsificación vive dentro. La norma aeroespacial **AS6171** estandariza estos ensayos para las piezas que llegan **sin una cadena de custodia conocida** hasta el fabricante original, y la legislación estadounidense hace responsable al contratista de defensa **sea cual sea el punto por donde entró la pieza falsa**. Pero como advierte la organización ERAI en su informe anual, el fraude es atomizado y oculto, y la mayoría de casos son ocurrencias nuevas. La lección del sector es clara: **prevenir por el origen es mucho más barato que detectar por ensayo**. El problema es que aquel origen viaja en un PDF que se puede reescribir.

La prueba de existencia: un pedigrí inalterable

Es aquí donde **t2p** ataca el corazón del fraude, que no es (solo) un chip malo, sino **una mentira sobre el pedigrí**. La idea es sellar cada **evento de custodia** —el marcado por el fabricante original, la inspección

de entrada, el ensayo AS6171, el dictamen de aceptación— calculando en el dispositivo la **huella SHA-512** de los artefactos de evidencia: informe de ensayo con sus imágenes de rayos X, certificado de conformidad, foto del código de fecha y número de lote. Esta huella se ancla a la **blockchain pública** con un **sello de tiempo RFC 3161** conforme a eIDAS. La **prueba de vida**, al capturar la imagen del componente, impide reutilizar una **foto antigua de una pieza auténtica** para amparar un lote falso, y el **GPS forense** fija **dónde** se ha inspeccionado —el laboratorio acreditado real, no un «laboratorio fantasma». Todo viaja en un contenedor **.asice** que cualquier actor de la cadena puede verificar sin conexión; si un código de fecha o un certificado son alterados, la huella se rompe. La cadena de custodia deja de ser un PDF reescribible y se convierte en un **registro de pedigrí inalterable, datado y geolocalizado**.

Hay que decir el límite con toda la crudeza, porque aquí es literal: «Basura a la entrada, basura en la cadena». **t2p** sella la evidencia y su momento, **no la verdad física del silicio**. Si un laboratorio acreditado ensaya correctamente un chip auténtico y después, aguas abajo, alguien **sustituye físicamente** aquel chip por uno reciclado con el mismo marcado, la cadena seguirá apuntando al sello legítimo: el atestado es honesto, la pieza no. La prueba garantiza que *este informe existía y no se ha alterado*, no que *el ensayo se hizo bien* ni que *la pieza que tengo en la mano es la que se ensayó*. Por eso este frente depende de un **anclaje físico fiable** —un marcado de ADN, una huella física no clonable en el propio chip, una serialización indeleble— que ligue criptográficamente el átomo al bit. Sin este vínculo físico, un actor malintencionado puede **certificar de buena fe el lote A y entregar el lote B**. La prueba de existencia sube el coste del engaño y deja rastro forense de quién firmó qué y cuándo —inestimable en un litigio—, pero **no detecta por sí sola un chip reciclado**: eso sigue siendo tarea del ensayo físico, y un laboratorio corrupto o un sello sobre la pieza equivocada derrotan el sistema.

La promesa y el peligro

La promesa es de seguridad nacional. Un pedigrí sellado, datado y geolocalizado en cada eslabón haría mucho más difícil colocar un chip reciclado en el corazón de un misil o de una pantalla de cabina, porque cada certificado falso rompería la huella y cada responsabilidad quedaría atada a quien la firmó. Combinado con el ensayo físico y con un anclaje al silicio, daría a la cadena de defensa la trazabilidad que la ley ya exige pero que hoy descansa sobre papeles falsificables.

El peligro pide los matices que hemos dicho. El primero, no confundir el sello con la prueba física: el pedigrí inalterable no hace auténtico un chip falso, y sin anclaje al silicio la sustitución posterior sigue siendo posible. El segundo, el ensayo sigue siendo insustituible, y un laboratorio corrupto derrota cualquier cadena. Y el tercero, la adopción en toda la cadena, desde el fabricante original hasta el último subcontratista. La prueba de existencia es una capa poderosa para el pedigrí documental, no un sustituto del ensayo físico ni del anclaje al componente.

Es hora de actuar

Para los fabricantes originales y distribuidores autorizados: sellar el marcado y el código de fecha en origen, para que el pedigrí nazca inalterable. Para los contratistas principales y subcontratistas: exigir el pedigrí sellado como condición, ya que la ley los hace responsables por donde sea que entre la pieza falsa. Para los laboratorios acreditados: sellar los informes de ensayo con prueba de vida y GPS, para que nadie reutilice uno viejo. Y para el Departamento de Defensa y sus agencias: ligar el pedigrí criptográfico a un anclaje físico al silicio, para que el átomo y el bit no se puedan separar.

Unos chips pulidos con abrillantador acabaron dentro de un misil que no podía fallar. Dar a cada componente una prueba sellada de su pedigrí —sin olvidar nunca que hace falta el ensayo físico y un anclaje al silicio— es, en este frente que toca la seguridad de todos, time2act.

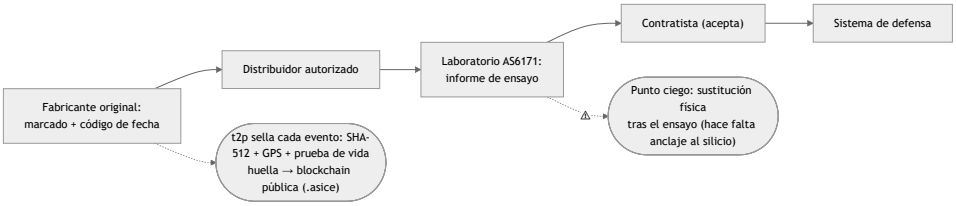


Figura 70.1 — Cada evento de custodia de un componente de grado defensa —marcado por el fabricante original, recepción en el distribuidor, «origen» declarado por el broker, informe de ensayo AS6171, aceptación del contratista, instalación— se puede sellar con huella SHA-512, sello eIDAS, GPS forense y prueba de vida, anclados a la blockchain pública. El punto ciego (en rojo): la sustitución física de la pieza después *del ensayo, que el sello no detecta sin un anclaje al silicio (ADN, huella física no clonable). Contexto: ~80 % de los chips falsos son reciclados o remarcados; la GAO compró 16 piezas militares en línea y las 16 eran falsas; un solo broker introdujo 84.000. Fuentes: Senado de EE. UU. (2012); GAO; IHS/ERAI.*

---

[1] U.S. Senate Committee on Armed Services — *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain* (2012; >1 M de piezas; >70 % rastreadas a China; THAAD; Hong Dark). https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts ↩

[2] U.S. Government Accountability Office — *DOD Supply Chain: Suspect Counterfeit Electronic Parts on Internet Platforms* (GAO-12-375; 16 de 16 piezas falsas). https://www.gao.gov/products/gao-12-375 ↩

[3] Center for Public Integrity — *Counterfeit chips plague Pentagon weapons systems* (VisionTech; el abrillantador en los chips; McCloskey, 38 meses). https://publicintegrity.org/national-security/counterfeit-chips-plague-pentagon-weapons-systems/ ↩

[4] Air & Space Forces Magazine — *C-27J and C-130J parts linked to counterfeit mills* (L-3; pantalla en blanco; defectos del 27 %). https://www.airandspaceforces.com/c-27jandc-130jpartslinkedtocounterfeitmills/ ↩

[5] Semiconductor Industry Association — *Winning the battle against counterfeit semiconductor products* (>7.500 M$/año; ~11.000 puestos de trabajo). https://www.semiconductors.org/resources/winning-the-battle-against-counterfeit-semiconductor-products/ ↩

[6] ERAI — *2024 Annual Report* (1.055 piezas sospechosas; el máximo desde 2015). https://www.erai.com/erai_blog/3187/_2024_annual_report ↩

[7] U.S. Department of Justice (NDCA) — *Steve H.S. Kim sentenced for selling $3.5M in counterfeit and substandard parts* (42 meses; submarino nuclear, sistema de misiles). https://www.justice.gov/usao-ndca/pr/california-resident-steve-hs-kim-sentenced-selling-35m-counterfeit-and-substandard

[8] SAE International — *AS6171: test methods for suspect/counterfeit EEE parts* (laboratorios acreditados ISO/IEC 17025). https://www.sae.org/standards/content/as6171/7/

[9] CALCE (University of Maryland) — *Counterfeit electronics detection and avoidance* (un chip reciclado puede parecer idéntico al auténtico). https://calce.umd.edu/counterfeit-electronics-detection-and-avoidance

[10] Defense Microelectronics Activity (DMEA) — *Trusted Foundry / Trusted IC* (proveedores de confianza con pedigrí controlado; 2003, con la NSA). https://www.dmea.osd.mil/TrustedIC.aspx

Software: el pedigrí del código que lo hace funcionar todo

«La moraleja es obvia: no puedes confiar en código que no hayas creado totalmente tú mismo.»

— Ken Thompson, «Reflections on Trusting Trust», conferencia del Premio Turing (1984)

Finales de marzo de 2024. Andres Freund —ingeniero de Microsoft y desarrollador de PostgreSQL— investiga una minucia que casi todo el mundo habría dejado pasar: los inicios de sesión SSH de una máquina de pruebas tardan unos 500 milisegundos más de la cuenta. Medio segundo. Tirando de aquel hilo, Freund encuentra lo que nadie quería encontrar: una puerta trasera sofisticadísima dentro de XZ Utils —una biblioteca de compresión presente en casi todo Linux—, diseñada para permitir la ejecución remota de código a través del servidor SSH. La reporta el 28-29 de marzo a la lista de seguridad Openwall; recibe el identificador CVE-2024-3094 y la severidad máxima: 10,0 sobre 10 [1].

Los analistas coinciden en el diagnóstico retrospectivo: si aquel medio segundo de curiosidad no hubiera disparado la investigación, la puerta trasera habría podido ser un facilitador de intrusiones mayor que el célebre ataque SolarWinds —acceso potencial a cualquier máquina Linux expuesta del planeta [1]. Bancos, hospitales, redes eléctricas: todo lo que funciona sobre Linux había estado a un paso de tener una cámara secreta abierta. El mundo digital se salvó por 500 milisegundos y un ingeniero tozudo.

Este capítulo trata la cadena de suministro del software: las bibliotecas de código que lo sostienen todo, sus versiones y los voluntarios que las mantienen. El pedigrí del hardware —los chips falsificados— está en el capítulo 70; los registros que el atacante no puede borrar, en el capítulo 57; la procedencia de los modelos de IA, en el capítulo 79. Pregunta clave: ¿cómo sabes que el código que ejecutas —tú, tu banco, tu hospital— es exactamente el que sus autores publicaron? Respuesta: con el pedigrí del código —los registros de transparencia públicos como Sigstore/Rekor, que ya son prueba de existencia en producción [3], y la capa de anclaje neutral de **t2p**: la huella SHA-512 de cada versión publicada, con sello de tiempo RFC 3161/eIDAS y anclaje a la blockchain pública, dentro de un contenedor .asice [5]. La industria del software ha llegado por su cuenta a la tesis de este libro; este capítulo explica por qué —y qué le falta.

El albañil infiltrado

Cuando abres la aplicación del banco y ves el icono de la conexión cifrada, no te preguntas quién ha escrito el código que cifra. La respuesta es: desconocidos. El software moderno es una torre de piezas —«bibliotecas»— que nadie escribe desde cero: cada aplicación toma bloques de proyectos abiertos, mantenidos a menudo por voluntarios con presupuesto cero. XZ Utils era eso: una pieza humilde de compresión, presente en casi todas las distribuciones de Linux, cuidada durante años por un único mantenedor.

El ataque fue una obra maestra de ingeniería social, tejida a lo largo de varios años [1]. Un personaje que se hacía llamar «Jia Tan» apareció aportando correcciones útiles; cuentas falsas empezaron a presionar al mantenedor original con quejas y exigencias hasta que, agotado, aceptó ayuda; y «Jia Tan» fue ganando permisos —primero de modificar código, después de publicar versiones.

Entonces colocó el ladrillo envenenado, con una sutileza decisiva: el código malicioso no era visible en el repositorio público que cualquiera puede revisar. Se escondía en un fichero del proceso de construcción y en ficheros de prueba binarios ofuscados, dentro de los paquetes de distribución —los «tarballs»— que las distribuciones se descargan para instalar el software [1]. Traducción: la versión publicada no coincidía con el código fuente visible, y ninguna revisión estándar del repositorio podía detectarlo.

La lección probatoria es el giro del capítulo: el ataque explotó exactamente un vacío de prueba de existencia —nadie verificaba que lo publicado fuera lo visible. Con la huella anclada de cada paquete publicado, contrastable con la huella del código fuente [5], la discrepancia habría sido detectable por cualquier máquina del mundo en el momento de la descarga. No habría hecho falta ningún héroe del medio segundo.

El gusano con las llaves del reino

Un año y medio después llegó la industrialización. El 14 de septiembre de 2025, el ecosistema npm —el repositorio del que se nutren millones de aplicaciones web— sufrió el primer gusano autorreplicante con éxito de su historia: «Shai-Hulud», bautizado por la comunidad de ciberseguridad con el nombre de los gusanos de arena de *Dune*. Más de 500 paquetes comprometidos, incluyendo @ctrl/tinycolor —más de 2,2 millones de descargas semanales— y, en una ironía perfecta, paquetes de la cuenta npm de CrowdStrike, uno de los grandes proveedores mundiales de ciberseguridad [2].

La mecánica era tan sofisticada como siniestra: el gusano cosechaba credenciales de los desarrolladores infectados —claves de Amazon, Google y Microsoft, localizadas con herramientas de búsqueda de secretos —, se instalaba en sus automatizaciones de GitHub y, la novedad letal, usaba los derechos de publicación de cada mantenedor infectado para publicarse dentro de sus propios paquetes: cada víctima se convertía en propagador. Un paquete legítimo el lunes podía llevar el gusano el martes, publicado con las mismas credenciales. La CISA —la agencia estadounidense de ciberseguridad— emitió una alerta el 23 de septiembre; en noviembre llegó una segunda oleada [2].

El diagnóstico, en clave de este libro: si xz fue el albañil infiltrado que tardó años, Shai-Hulud es el robo de la identidad de publicación a escala. El problema ya no es solo quién es el mantenedor —la identidad, que trata el capítulo 91—, sino qué se publica con sus claves y cuándo. La pregunta de la cadena de suministro del software es, literalmente, la pregunta de este libro: ¿qué existía, exactamente, y en qué momento?

La respuesta que ya es prueba de existencia

La buena noticia merece decirse con todas las letras: la industria ha empezado a responder con la misma arquitectura que este libro defiende. Sigstore —la infraestructura abierta de firma de software— se ha convertido en el método por defecto de ecosistemas como Kubernetes y de registros como npm, Maven y PyPI; y su corazón es Rekor: un registro de transparencia público y de única escritura —no se puede borrar ni reescribir nada en él— que ya contiene más de 101 millones de entradas de firmas de más de 33.000 proyectos de código abierto, de Kubernetes a CPython [3]. Cada publicación firmada deja constancia pública y datada, y npm y PyPI ya admiten atestaciones de procedencia firmadas así [3].

El uso defensivo más elegante es la monitorización del registro: un mantenedor puede vigilar Rekor y recibir una alerta si aparece en él una firma de publicación de su paquete que él no ha hecho —la detección del robo de claves por el rastro público que deja, tal como demostraron Trail of Bits y la OpenSSF en diciembre de 2025 [3]. Contra un gusano como Shai-Hulud [2], es exactamente la alarma que faltaba: la publicación fraudulenta queda registrada donde todos la pueden ver —incluido el legítimo propietario, en minutos.

Y aquí el momento de tesis: un registro de transparencia de única escritura con entradas datadas es, por definición, prueba de existencia. La comunidad del software, empujada por sus atacantes, ha llegado por su cuenta a la solución que este libro propone para el resto de la sociedad. Lo que t2p le añade es la capa de anclaje neutral y transversal: huellas SHA-512 de cada versión publicada —tarballs incluidos, la lección de xz [1]—, con sello de tiempo RFC 3161/eIDAS y anclaje a una cadena pública [5], de manera que el pedigrí del código no dependa de ninguna infraestructura única y sea verificable con la misma herramienta que el pedigrí de un documento, de una foto o de un chip (capítulo 70).

El contexto regulador cierra el círculo: el Reglamento europeo de Ciberresiliencia —Reglamento (UE) 2024/2847, en vigor desde diciembre de 2024— impone a los fabricantes seguridad durante todo el ciclo de vida del producto digital, con las obligaciones de notificación de vulnerabilidades aplicables desde el 11 de septiembre de 2026 y la aplicación plena el 11 de diciembre de 2027 [4]. La trazabilidad del software deja de ser buena práctica para convertirse en ley.

La prueba de existencia aplicada

Una actualización cualquiera, un servidor cualquiera —y, antes de instalarla, una comprobación de un segundo contra un registro que nadie puede reescribir.

1. La versión con pedigrí

Cada versión publicada de una biblioteca —el paquete completo, el tarball— recibe su huella SHA-512 anclada con fecha cierta [5], contrastable con la huella del código fuente visible. En el momento de instalar, la herramienta de gestión compara la huella de lo que ha descargado con la anclada: si no

coinciden —la discrepancia que ocultó la puerta trasera de xz [1]—, no se instala, y la alarma suena sola. El pedigrí del código, como el del chip en el capítulo 70: no una promesa del vendedor, sino una cadena verificable por cualquiera antes de confiar en ella.

2. La publicación vigilada

El mantenedor ancla su cadena de publicación —qué versiones ha publicado, cuándo, con qué claves— y monitoriza los registros públicos [3]: cualquier publicación con sus credenciales que él no haya hecho dispara la alarma en minutos, no en semanas. Contra el gusano que se publica con claves robadas [2], la ventana de infección se reduce de días al instante de la detección —y la comunidad entera puede ver, en el registro, qué versiones son legítimas y cuáles no. El vigilante deja de ser una empresa: es todo el mundo.

3. El inventario sellado

Cada producto digital lleva —y el marco europeo lo irá exigiendo [4]— su inventario de componentes: qué bibliotecas, qué versiones (el llamado SBOM, la lista de ingredientes del software). Un inventario sellado por versión, con fecha cierta [5], convierte la respuesta a incidentes en una consulta: cuando estalla el próximo xz o el próximo Shai-Hulud [1][2], cada organización puede saber en minutos —y demostrar ante el regulador [4]— si ejecuta o no la pieza envenenada, y desde cuándo. La conjetura se vuelve verificación.

4. La línea de tiempo forense

Después de un ataque, la pregunta vale millones: ¿cuándo entró el código malicioso, qué versiones lo llevan, quién lo publicó? Con cadenas de publicación e inventarios anclados [3][5], la investigación forense trabaja sobre una línea de tiempo no repudiable —la misma lógica de los registros del capítulo 57, aplicada al código. Y la responsabilidad se reparte con justicia: el fabricante que desplegó la versión limpia puede demostrarlo; el que ignoró la alerta datada queda igualmente retratado.

Los límites, dichos sin rodeos: el sello acredita que un paquete existía y no se ha alterado —no acredita que el código sea bueno ni seguro. La puerta trasera que el autor legítimo publica con su propia clave queda perfectamente anclada —xz es medio ejemplo: «Jia Tan» era mantenedor [1]. La revisión de código, la auditoría y la seguridad de las claves siguen siendo la primera línea; y el registro de transparencia detecta la publicación fraudulenta, no la impide —la respuesta rápida sigue siendo humana.

La promesa y el peligro

La promesa: una cadena de suministro del software donde cada pieza lleva pedigrí verificable [3][5], las discrepancias como la de xz cantan solas [1], los gusanos como Shai-Hulud encuentran alarmas en minutos [2] y la respuesta a incidentes es una consulta en lugar de una arqueología [4]. El mundo que funciona sobre código, funcionando sobre código acreditado.

Los peligros, con la misma claridad.

El primero es **la falsa seguridad del sello**. Anclado no quiere decir inocuo. El código malicioso publicado por su autor legítimo con sus claves legítimas queda impecablemente anclado [1]; el pedigrí acredita origen e integridad, no bondad. Quien venda el sello como auditoría de seguridad estará creando la peor vulnerabilidad: la confianza injustificada.

El segundo es **la carga sobre los voluntarios**. La infraestructura digital mundial descansa sobre mantenedores sin sueldo —el mantenedor único y agotado de xz es el patrón, no la excepción [1]. Si el pedigrí se convierte en una obligación burocrática más sobre sus espaldas, abandonarán —y el problema empeorará. Las herramientas deben ser automáticas y gratuitas para el código abierto, y la financiación de los comunes digitales es parte de la solución de seguridad [4].

El tercero es **la centralización del registro**. Si todo el pedigrí del software mundial depende de un solo registro de transparencia, hemos creado un punto único de fallo y de poder [3]. La respuesta es la de todo el libro: pluralidad de registros, anclaje cruzado a cadenas públicas neutrales [5] y ningún guardián único de la verdad del código.

Y el cuarto es **el tecnosolucionismo de cadena**. Ninguna huella arregla la economía política del problema: atacantes estatales pacientes [1], ecosistemas que premian publicar deprisa, dependencias infinitas que nadie revisa. El pedigrí hace el fraude visible; reducirlo exige también revisión, financiación y cultura. La criptografía es el andamio, no el edificio.

Es hora de actuar

Si todo funciona sobre código, que el código tenga pedigrí.

Para los mantenedores de código abierto: firmad y anclad cada versión —tarball incluido [1][3][5]— y monitorizad el registro: que ninguna publicación con vuestras claves os coja por sorpresa [2][3].

Para las empresas que despliegan software: exigid pedigrí verificable a cada pieza, mantened el inventario sellado por versión [4][5] y comprobad huellas antes de instalar —el medio segundo de Andres Freund [1], automatizado.

Para los registros y ecosistemas (npm, PyPI y compañía): atestaciones de procedencia por defecto [3], verificación de huellas en la descarga y alarmas públicas de publicación anómala [2].

Para los reguladores europeos: el Reglamento de Ciberresiliencia [4] llega en el momento justo —que su aplicación reconozca el registro de transparencia y la huella anclada como medios de cumplimiento.

Para los gobiernos y las grandes tecnológicas: financiad los comunes digitales —el mantenedor agotado es la vulnerabilidad número uno [1]; ninguna criptografía sustituye un sueldo digno para quien sostiene la infraestructura de todos.

El mundo se salvó una madrugada de marzo por medio segundo de latencia y la tozudez de un ingeniero [1]. Que la próxima puerta trasera no dependa de la suerte: que se tope con un pedigrí que la delate en la primera descarga. Por el código que todo lo sostiene, **time2act**.

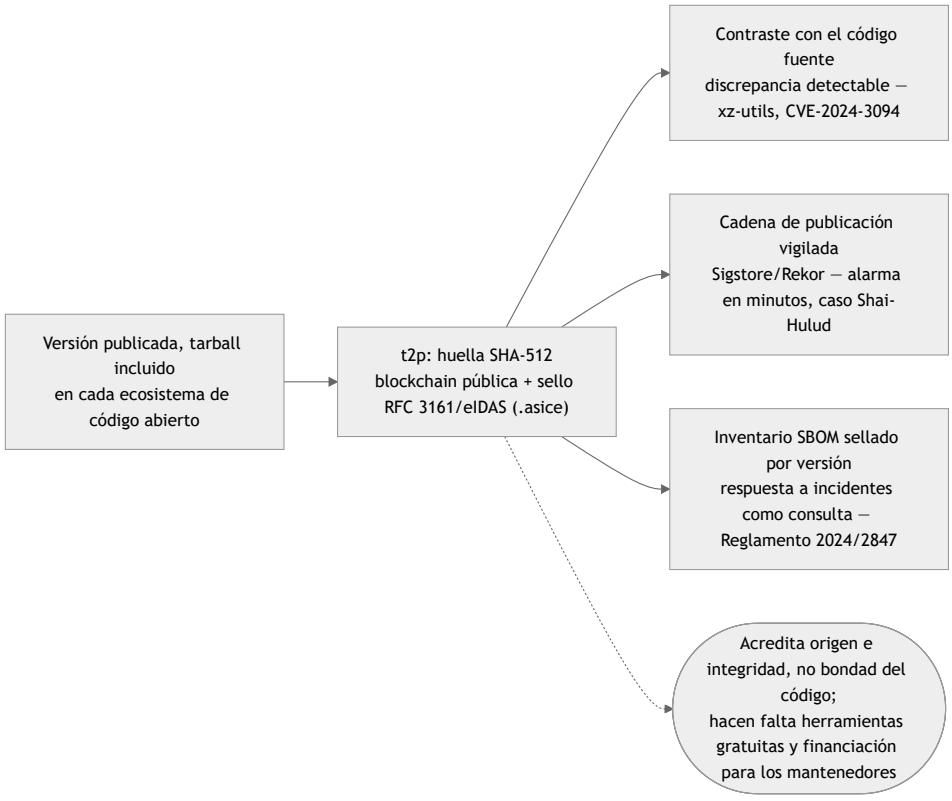


Figura 71.1 — La cadena de suministro del software con prueba de existencia: cada versión publicada se ancla (huella SHA-512 del tarball, sello de tiempo RFC 3161/eIDAS, blockchain pública, .asice) y se contrasta con el código fuente (la discrepancia de xz-utils, detectable); la cadena de publicación vigilada en los registros de transparencia (Sigstore/Rekor: >101 millones de entradas —prueba de existencia en producción) dispara la alarma ante publicaciones con claves robadas (el gusano Shai-Hulud); el inventario (SBOM) sellado por versión hace la respuesta a incidentes una consulta (Reglamento (UE) 2024/2847). Límites: el sello acredita origen e integridad, no bondad del código; los mantenedores necesitan herramientas gratuitas y financiación. Fuentes: CVE-2024-3094; CISA (Shai-Hulud); Sigstore/Rekor; CRA.

---

[1] Wikipedia — *XZ Utils backdoor* (CVE-2024-3094; CVSS 10,0; Andres Freund, ingeniero de Microsoft y desarrollador de PostgreSQL, investigando ~500 ms de latencia extra en SSH; report a Openwall el 28-29 de marzo de 2024; campaña de ingeniería social de «Jia Tan» con cuentas falsas presionando al mantenedor; código oculto en build-to-host.m4 y ficheros de test binarios dentro de los tarballs —invisible a la revisión del repositorio; potencial superior a SolarWinds; cazado antes del despliegue masivo); Akamai — *XZ Utils Backdoor — Everything You Need to Know*; JFrog — *XZ Backdoor Attack CVE-2024-*

3094; Datadog Security Labs — *The XZ Utils backdoor*. https://en.wikipedia.org/wiki/XZ_Utils_backdoor · https://www.akamai.com/blog/security-research/critical-linux-backdoor-xz-utils-discovered-what-to-know · https://jfrog.com/blog/xz-backdoor-attack-cve-2024-3094-all-you-need-to-know/ · https://securitylabs.datadoghq.com/articles/xz-backdoor-cve-2024-3094/ ↩

[2] Palo Alto Unit 42 — *«Shai-Hulud» Worm Compromises npm Ecosystem in Supply Chain Attack* (14 de septiembre de 2025; primer gusano autorreplicante en npm; >500 paquetes; @ctrl/tinycolor con >2,2 millones de descargas semanales; paquetes de CrowdStrike; cosecha de credenciales AWS/GCP/Azure con TruffleHog; persistencia vía GitHub Actions; propagación con los derechos de publicación de los mantenedores); CISA — *Widespread Supply Chain Compromise Impacting npm Ecosystem* (alerta del 23 de septiembre de 2025); StepSecurity — *Shai-Hulud: Self-Replicating Worm Compromises 500+ NPM Packages*; Datadog — *The Shai-Hulud 2.0 npm worm* (segunda oleada, noviembre). https://unit42.paloaltonetworks.com/npm-supply-chain-attack/ · https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem · https://www.stepsecurity.io/blog/ctrl-tinycolor-and-40-npm-packages-compromised · https://securitylabs.datadoghq.com/articles/shai-hulud-2.0-npm-worm/ ↩

[3] Sigstore — *Rekor: Software Supply Chain Transparency Log* (registro público append-only; >101 millones de entradas de >33.000 proyectos: Kubernetes, CPython, Istio, urllib3; método de firma por defecto para Kubernetes, npm, Maven y PyPI; atestaciones de procedencia en npm y PyPI); OpenSSF / Trail of Bits — *Catching malicious package releases using a transparency log* (diciembre de 2025; monitorización de Rekor para detectar publicaciones fraudulentas con credenciales robadas). https://docs.sigstore.dev/logging/overview/ · https://www.sigstore.dev/ · https://openssf.org/blog/2025/12/19/catching-malicious-package-releases-using-a-transparency-log/ · https://blog.trailofbits.com/2025/12/12/catching-malicious-package-releases-using-a-transparency-log/ ↩

[4] DOUE / BOE — *Reglamento (UE) 2024/2847, de 23 de octubre de 2024* (Cyber Resilience Act: requisitos horizontales de ciberseguridad para productos con elementos digitales; en vigor en diciembre de 2024; obligaciones de notificación desde el 11 de septiembre de 2026; aplicación plena el 11 de diciembre de 2027; seguridad durante todo el ciclo de vida); Atalaya GRC — *CRA: fechas y obligaciones*; Red Seguridad — *Cyber Resilience Act: una nueva era para los fabricantes*. https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81720 · https://atalayagrc.com/normativas/cra/ · https://www.redseguridad.com/especialidades-tic/normativa-y-certificacion/cyber-resilience-act-cra-una-nueva-era-para-los-fabricantes_20260204.html ↩

[5] t2p — manual de producto (huella SHA-512; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; huellas de versiones y manifiestos por lotes; anclaje neutral y transversal, complementario a los registros de transparencia sectoriales). Véanse los capítulos 13 y 15; el pedigrí del hardware, en el capítulo 70; los registros imborrables, en el capítulo 57. ↩

Pesca y minerales: el origen que se hundió con el barco

«Porque todo, al final, vuelve al mar —a Océano, el río oceánico, como la corriente siempre fluyente del tiempo, el principio y el fin.»

— Rachel Carson, El mar que nos rodea (1951), frase final

El 17 de diciembre de 2014, dos barcos de la organización Sea Shepherd empezaron a perseguir a un pesquero furtivo llamado *Thunder*, que llevaba años pescando ilegalmente austromerluza en las aguas antárticas. La persecución duró **ciento diez días y diez mil millas náuticas**, hasta la zona económica de Santo Tomé y Príncipe. Y allí, en lugar de rendirse, la tripulación hizo algo revelador: **hundió deliberadamente su propio barco**, con las escotillas atadas en abierto, para destruir las pruebas de la captura ilegal. Tres oficiales fueron condenados por falsificación y delitos ambientales, con una multa de quince millones de euros [referencia del caso Thunder]. La prueba del origen, literalmente, se hundió con el barco.

Aquel barco que se hunde para borrar su rastro contiene la pregunta de este capítulo. En el capítulo 29 vimos la trazabilidad de productos agrícolas en tierra contra la deforestación; aquí el patrón es el mismo —sellar el origen— pero en dos dominios nuevos y a veces sangrientos: el **mar** y las **minas de minerales de conflicto**. La pregunta ya no es «¿este café viene de tierra deforestada?», sino «¿este pez se pescó en una zona vedada y por quién?» y «¿este tántalo financió una milicia?».

Uno de cada cinco peces, y el 90 % de mineral «limpio»

La escala del fraude marino es inmensa. La pesca ilegal, no declarada y no reglamentada mueve entre **once y veintiséis millones de toneladas** al año —cerca de uno de cada cinco peces salvajes— por un valor de entre 10.000 y 23.500 millones de dólares [1]. Y es casi invisible: un estudio de **Global Fishing Watch** publicado en *Nature* en 2024 demostró, cruzando imágenes de satélite con inteligencia artificial, que **tres de cada cuatro barcos pesqueros industriales del mundo no emiten ninguna señal pública de posición** [3]. Cuando el pez llega al plato, además, a menudo no es el que dice: la organización **Oceana** encontró que un tercio del marisco de Estados Unidos estaba mal etiquetado, y hasta el **87 %** de lo que se vendía como «pargo rojo» era otra especie [2]. Y detrás de todo ello está el horror: la investigación de la Environmental Justice Foundation documentó pescadores birmanos **encerrados en jaulas** en la isla indonesia de Benjina, esclavos de una flota cuyo pescado acababa en los supermercados occidentales [7].

El paralelo mineral es igual de oscuro. Los **minerales de conflicto 3TG** —estaño, tántalo, wolframio y oro— financian a grupos armados en la República Democrática del Congo, regulados por la ley estadounidense Dodd-Frank y el reglamento europeo de 2017. Los diamantes tienen su propio sistema, el **Proceso de Kimberley**, creado en 2003, que redujo el comercio de diamantes de conflicto de cerca de un 15 % en los años noventa a menos del 1 % [6]. Pero el problema es presente, no histórico: el grupo armado M23 tomó en 2024 la mina de coltán de Rubaya, obteniendo unos **800.000 dólares al mes** [10].

Cuando la trazabilidad se vuelve una lavadora

Y aquí llega la advertencia más importante de este capítulo, porque afecta al corazón de la solución. Un sistema de trazabilidad no es infalible; puede convertirse en una **lavadora**. La organización **Global Witness**, en su informe *The ITSCI Laundromat* de 2022, demostró que en dos zonas mineras del Kivu del Sur entre el **80 % y el 90 %** de los minerales etiquetados como «limpios» por el único proveedor de trazabilidad de la zona procedían en realidad de fuentes ilícitas [5]. El truco era sencillo y devastador: la etiqueta «limpia» se aplicaba a mineral **ya mezclado**. Una etiqueta de buena procedencia sobre mineral de mala procedencia es peor que ninguna etiqueta, porque da una falsa confianza. Y el riesgo de centralizar la trazabilidad en una sola empresa también es real: Everledger, pionera en rastrear diamantes con blockchain, entró en concurso en 2023 [9]. La lección es clara: **el problema no es tener un certificado, sino dónde y cuándo nace**.

La prueba de existencia: sellar el origen en el punto de extracción

Es aquí donde **t2p** ataca el fraude en su origen exacto. La idea es sellar la captura o el lote **en el momento y el lugar de la extracción**, antes de que se pueda mezclar o reetiquetar. A bordo, con la red recién subida, o en la boca de la mina artesanal, el operario hace una foto de la captura con **prueba de vida** del pescador o del minero; el dispositivo calcula localmente la **huella SHA-512** de la imagen y los metadatos —especie declarada, peso, arte de pesca, identificador del barco o de la mina—, le incrusta el **GPS forense** y un **sello de tiempo RFC 3161** conforme a eIDAS, y ancla la huella a la **blockchain pública**, generando un contenedor **.asice** que sobrevive sin cobertura en alta mar o en una galería.

El efecto es directo contra los tres fraudes. Contra la **retrodatación**: nadie puede afirmar que un pez capturado en una zona vedada se pescó en una legal, porque el sello de GPS y hora es anterior e inalterable. Contra el **cambio de especie**: la foto sellada liga una identidad visual al lote en origen. Y contra el **lavado de lote** —el caso de la lavadora—: cada saco de coltán queda sellado con la geolocalización de su mina **antes** de cualquier mezcla, de manera que mezclar mineral de una milicia rompe la cadena de huellas en lugar de heredar una etiqueta limpia. El certificado de captura europeo o el de Kimberley dejan de ser un PDF validado tarde y ganan un ancla criptográfica de origen.

Hay que decir el límite con toda la crudeza, porque aquí es lo más peligroso de todos. «Basura a la entrada, basura en la cadena», en su forma extrema: el **lavado en el punto de sellado**. t2p no resuelve por sí solo lo que destapó Global Witness. No verifica la especie ni la legalidad de la zona: la huella garantiza que *esta foto, en estas coordenadas, a esta hora, hecha por esta persona viva* existió, no que el pez sea la especie declarada —eso exige ADN— ni que las coordenadas estén fuera de una veda —eso exige cruzarlas con mapas de áreas protegidas. No impide la **corrupción del sellador**: si quien sella es el operador del barco furtivo o el comprador de la mina con milicia, puede sellar capturas ilegales con metadatos verdaderos pero declaraciones falsas. No cubre el **barco oscuro**: el 75 % de la flota que no emite señal simplemente no sellaría nada, y contra quien decide no participar sigue haciendo falta la vigilancia por satélite. Y no fija la atribución física de la foto al objeto —una foto puede mostrar un lote y enviarse otro—, por lo que aporta más combinada con un marcado físico, como nanotrazadores o ADN, anclado a la misma huella. Su valor real es **cerrar la ventana de la retrodatación y del cambio documental**, no garantizar por sí solo que el origen declarado sea verdad.

La promesa y el peligro

La promesa toca el medio ambiente y los derechos humanos a la vez. Sellar el origen en el punto de extracción, antes de cualquier mezcla, haría mucho más difícil colar pescado de una veda o coltán de una milicia dentro de una cadena de suministro global, y daría a los certificados de captura y de Kimberley un ancla que hoy les falta. En un mundo donde uno de cada cinco peces es ilegal y donde una etiqueta «limpia» puede esconder mineral de sangre, sellar el origen es proteger a la vez el mar y las personas.

El peligro pide los matices que hemos dicho, y aquí son especialmente graves. El primero, la lavadora: un sello sobre mineral ya mezclado da una falsa confianza, y por eso el sellado debe ser **en origen y antes de la mezcla**, nunca después. El segundo, la corrupción del sellador, que ninguna criptografía resuelve sin auditoría independiente. Y el tercero, el barco oscuro, contra el cual sigue haciendo falta el satélite. La prueba de existencia es una capa poderosa para anclar el origen, no un sustituto ni del ADN, ni de la verificación geoespacial, ni de la auditoría de quien sella.

Es hora de actuar

Para los **estados de pabellón y la Unión Europea**: exigir el certificado de captura con un anclaje de origen sellado en el punto de pesca, no validado tarde en un despacho. Para los **importadores de minerales**: sellar cada lote en la boca de la mina, antes de cualquier mezcla, para impedir la lavadora. Para el **Proceso de Kimberley y las marcas** (electrónica, joyería): reconocer el sello de origen como prueba primaria. Y para los **auditores independientes y la vigilancia por satélite**: seguir vigilando el barco oscuro y la honestidad de quien sella, porque ninguna etiqueta vale nada sin ellos.

Un barco furtivo se hundió a sí mismo para borrar el origen de su captura. Dar a cada captura y a cada lote de mineral una prueba sellada en el punto de extracción —sin olvidar nunca que hacen falta el ADN, el satélite y la auditoría— es, en este frente que toca el mar y la dignidad, time2act.

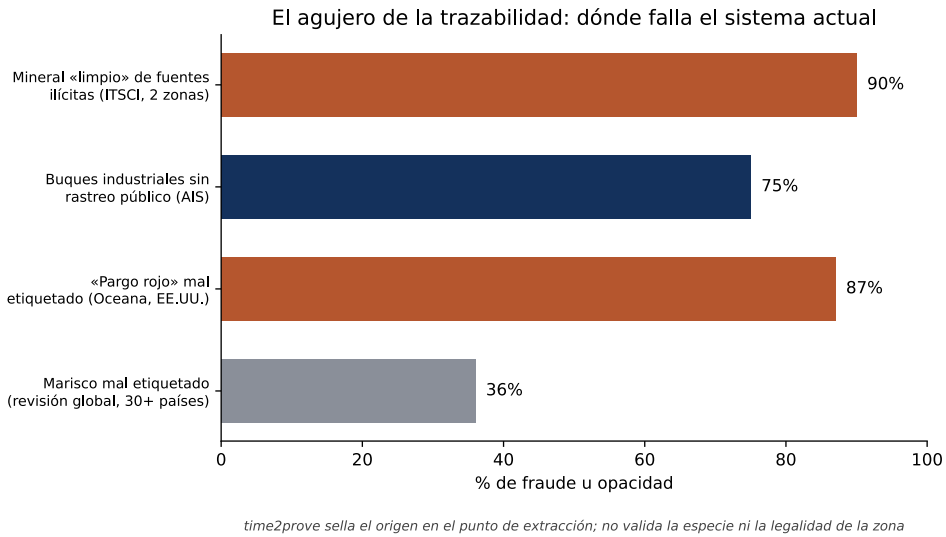


Figura 72.1 — El fraude y la opacidad por vertical: tres de cada cuatro barcos pesqueros industriales no emiten señal pública de posición (75 %, Global Fishing Watch); un tercio del marisco de EE. UU. está mal etiquetado —hasta el 87 % del «pargo rojo» (Oceana); una revisión global de más de treinta países encuentra un 36 % de mal etiquetado; y hasta el 90 % del mineral «etiquetado limpio» en dos zonas del Kivu del Sur procedía de fuentes ilícitas (Global Witness). t2p sella el origen en el punto de extracción, antes de la mezcla o el cambio de etiqueta; lo que el sello NO valida es la especie ni la legalidad de la zona. Fuentes: Global Fishing Watch; Oceana; Global Witness.

---

[1] Agnew et al. (PLOS ONE) — *Estimating the worldwide extent of illegal fishing* (11-26 millones de toneladas; 10.000-23.500 M$/año). https://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0004570 ↩

[2] Oceana — *Oceana study reveals seafood fraud nationwide* (33 % mal etiquetado; «red snapper» 87 %). https://oceana.org/reports/oceana-study-reveals-seafood-fraud-nationwide/ ↩

[3] Global Fishing Watch / Nature — *Satellite mapping reveals extensive industrial activity at sea* (~75 % de barcos sin rastreo público). https://globalfishingwatch.org/press-release/new-research-harnesses-ai-and-satellite-imagery-to-reveal-the-expanding-footprint-of-human-activity-at-sea/ ↩

[4] Comisión Europea — *Illegal fishing (IUU): catch certificates y CATCH* (Reg. (CE) 1005/2008; CATCH obligatorio desde el 10-ene-2026). https://oceans-and-fisheries.ec.europa.eu/fisheries/rules/illegal-fishing_en

[5] Global Witness — *The ITSCI Laundromat* (hasta el 80-90 % de mineral «limpio» procedente de fuentes ilícitas). https://www.globalwitness.org/en/campaigns/natural-resource-governance/itsci-laundromat/ ↩

[6] Kimberley Process / World Diamond Council — *The Kimberley Process fact sheet* (de ~15 % en los años 90 a <1 %; ~99 % de la producción). https://www.worlddiamondcouncil.org/wp-content/uploads/2022/02/The-Kimberley-Process-Fact-Sheet.pdf ↩

[7] Environmental Justice Foundation — *Thailand's Seafood Slaves* (esclavitud a bordo; la isla de Benjina). https://ejfoundation.org/reports/thailands-seafood-slaves ↩

[8] Science Advances (Park et al.) — *Illuminating Dark Fishing Fleets in North Korea* (>900 barcos; >164.000 t; >440 M$). https://www.science.org/doi/10.1126/sciadv.abb1197

[9] Ledger Insights — *Everledger bankruptcy* (el riesgo de centralizar la trazabilidad de diamantes en una sola empresa). https://www.ledgerinsights.com/everledger-bankruptcy-esg-blockchain-traceability/ ↩

[10] The Africa Report — *Rubaya coltan mine at the heart of M23 financing* (~800.000 $/mes para un grupo armado). https://www.theafricareport.com/375904/drc-rwanda-rubaya-coltan-mine-at-the-heart-of-m23-financing/ ↩

Filantropía: adónde va mi euro

«Cualquiera puede dar dinero; pero darlo a quien es debido, en la medida debida, cuando es debido, por el motivo debido y como es debido, eso ya no está al alcance de todos, ni es fácil.»

— Aristóteles, Ética a Nicómaco, II, 9 (1109a)

Después del terremoto de Haití de 2010, la Cruz Roja Americana recaudó casi **quinientos millones de dólares**, mientras prometía barrios enteros de casas nuevas a un pueblo devastado. En 2015, los periodistas Justin Elliott, de ProPublica, y Laura Sullivan, de la radio pública NPR, recorrieron el terreno para ver el resultado. Encontraron **seis casas permanentes** acabadas en todo el país. Sobre el papel, la organización decía haber «dado un hogar a más de 130.000 personas», pero aquella cifra incluía gente que había asistido a un seminario de reparación o que había recibido un refugio temporal ya en ruinas [1]. Un detalle lo resumía todo: un ingeniero haitiano sénior cobraba 42.000 dólares mientras un jefe de proyecto expatriado cobraba 140.000.

Aquellas seis casas contienen la pregunta de este capítulo, que es la del donante, no la del beneficiario. En el capítulo 49 vimos cómo probar que la ayuda **llega** a quien la necesita; aquí la pregunta es anterior y complementaria: **¿adónde va mi euro entre el clic y el impacto, y es real el impacto que me venden?** Porque entre la donación y la causa hay un trayecto oscuro —captadores, gastos, subcontratistas, cifras infladas— donde se pierde mucho más de lo que se roba en el reparto final.

¿Adónde va mi euro?

La opacidad de este trayecto es sistémica y, a veces, criminal. Como hemos visto, en 2015 la comisión de comercio estadounidense y los cincuenta estados demandaron a cuatro organizaciones falsas contra el cáncer, controladas por la familia Reynolds, por estafar **más de 187 millones de dólares**: menos del **3 %** llegaba a los pacientes, y los teleoperadores se quedaban el 85 % o más de cada donación, que se gastaba en cruceros, motos de agua y entradas a conciertos [2]. Pero no hace falta llegar al fraude para perderse por el camino: según el informe anual de la fiscalía de Nueva York, los captadores profesionales se quedaron el **25 % de cada dólar** en 2024, y en la mitad de las campañas la entidad recibió **menos de la mitad** de lo que se recaudó [4]. Y el problema crece: la oficina de delitos informáticos del FBI cifró en unos **96 millones de dólares** el fraude de falsas caridades y campañas de catástrofe en 2024, con la inteligencia artificial fabricando apariencia de legitimidad [3].

Ante esto, el sector ha aprendido una lección contraintuitiva. En 2013 los responsables de los tres grandes evaluadores de ONG —**GuideStar, Charity Navigator y la BBB Wise Giving Alliance**— firmaron una carta abierta, *El mito del overhead*, advirtiendo que fijarse solo en el porcentaje de gastos administrativos es un **mal indicador**: empuja a las ONG a la «inanición», a no invertir en los sistemas que las harían eficaces [6]. La pregunta correcta, como defiende el evaluador de eficacia **GiveWell**, no es cuánto gasta una ONG en sí misma, sino **cuántas vidas cambia por dólar** —y calcula que las mejores pueden evitar una muerte por entre tres mil y cinco mil quinientos dólares [7]. Para el donante, como resume Daniel Borochoff, fundador de **CharityWatch**, lo que debe guiar no es el marketing, sino la **transparencia financiera auditable**.

Cuando la donación limpia una reputación

Hay un fraude más sutil que el del dinero: el de la **reputación**. En diciembre de 2021, el Museo Metropolitano de Nueva York retiró el nombre de la familia Sackler de siete galerías. Los Sackler, propietarios de Purdue Pharma —el fabricante que promovió agresivamente el OxyContin en plena epidemia de opioides—, habían estado «entre nuestros donantes más generosos». Como documenta el periodista **Patrick Radden Keefe** en su libro *Empire of Pain*, aquella filantropía funcionó como un **lavado de reputación**: donaciones millonarias a museos que compraban una fachada de virtud mientras la familia nunca destinó fondos a tratar la adicción que su empresa había esparcido. La donación, aquí, no roba dinero al donante; roba la verdad al público.

La prueba de existencia: sellar la promesa y la evidencia de impacto

Es aquí donde **t2p** ofrece una capa que saca los *claims* de la palabra de la organización y los ancla en evidencia verificable. No certifica que una ONG sea honesta, pero sella **pruebas en cada nodo del recorrido del dinero**. Primero, la **promesa**: en el instante de donar, el importe, el propósito restringido y la promesa publicada se resumen en una **huella SHA-512**, se anclan a la **blockchain pública** y se sellan con el sello de tiempo eIDAS. Esto fija de manera inalterable *qué se prometió* y *para qué* se restringió el fondo, impidiendo reescribir después la promesa —el patrón de Haití, donde una «comunidad nueva» se convirtió en un «seminario». Segundo, cada **desembolso** —una factura pagada, una transferencia a un subcontratista— se sella con su importe y su fecha, creando un rastro encadenado del overhead real frente al prometido. Y tercero, la **prueba de impacto** —la foto de la obra, el acta firmada, el recuento de entregables— se captura con **GPS forense**, **sello de tiempo** y **prueba de vida**, y se empaqueta en un contenedor **.asice** verificable fuera de línea.

El efecto para el donante es que puede **auditar** si el 75 % que dice llegar a la causa coincide con los desembolsos sellados, y que una foto de impacto lleva coordenadas, hora y prueba de captura en vivo —no una imagen reciclada de otra catástrofe. Un evaluador independiente como CharityWatch, un regulador o el propio donante pueden verificar el contenedor sin depender del servidor de la ONG.

Hay que decir el límite con toda la crudeza, porque aquí es sutil. «Basura a la entrada, basura en la cadena»: el sello garantiza que un dato existía y cuándo, no que el dinero se gastara bien. El **problema de la última milla** es estructural: cuando la ONG paga en efectivo a un proveedor local, aquella transacción sale del rastro verificable. Un acta de impacto puede estar **sellada, geolocalizada y mentir a la vez**; seis casos reales se pueden fotografiar y presentar como prueba de «130.000 ayudados», si la métrica declarada es tramposa —la prueba de existencia no juzga la *definición* del *claim*, solo su existencia. No detecta el lavado de reputación ni el origen sucio del dinero del donante: sellar una donación de los Sackler la hace más auditable, no más limpia. Y no sustituye el juicio de eficacia —si son tres mil dólares por vida o un proyecto inútil—, que exige la evaluación de GiveWell y la auditoría humana. **t2p** aporta **integridad del expediente**, no **mérito** del programa.

La promesa y el peligro

La promesa es restaurar la confianza que sostiene toda la filantropía. Una capa que selle la promesa restringida, cada desembolso y la evidencia de impacto daría al donante la capacidad de auditar su euro, haría mucho más difícil inflar beneficiarios o reciclar fotos, y premiaría a las ONG honestas con una transparencia demostrable en lugar de penalizarlas por un overhead mal entendido. En un sector que vive de la confianza, hacer el expediente inalterable es proteger tanto al donante como a las organizaciones que hacen bien su trabajo.

El peligro pide los matices que hemos mencionado. El primero, la última milla: el rastro se acaba donde alguien deja de capturar evidencia honesta. El segundo, no confundir integridad con verdad: una métrica tramposa sellada sigue siendo tramposa. El tercero, que el sello no limpia dinero sucio ni juzga la eficacia. Y el cuarto, la captura selectiva: si la ONG elige qué sella, el rastro tendrá agujeros. La prueba de existencia es una herramienta poderosa para la transparencia del trayecto, no un certificado de honestidad ni un sustituto de la evaluación de impacto.

Es hora de actuar

Para los donantes: exigir la promesa restringida y la evidencia de impacto selladas, y centrarse en el coste por resultado, no en el overhead. Para las ONG: sellar cada desembolso y cada prueba de impacto, convirtiendo la transparencia en una ventaja demostrable. Para los evaluadores y reguladores (CharityWatch, las fiscalías): reconocer el contenedor sellado como base de auditoría independiente. Y para las plataformas de captación (el crowdfunding): ligar cada campaña a una promesa y una evidencia verificables, para que una página falsa no pueda cobrar en nombre de una víctima.

Medio millar de millones de dólares produjeron seis casas, y nadie lo supo hasta que dos periodistas lo contaron. Dar a cada donación una prueba sellada de su trayecto —sin olvidar nunca que hacen falta la evaluación de impacto y la auditoría humana— es, en este frente que sostiene la generosidad, time2act.

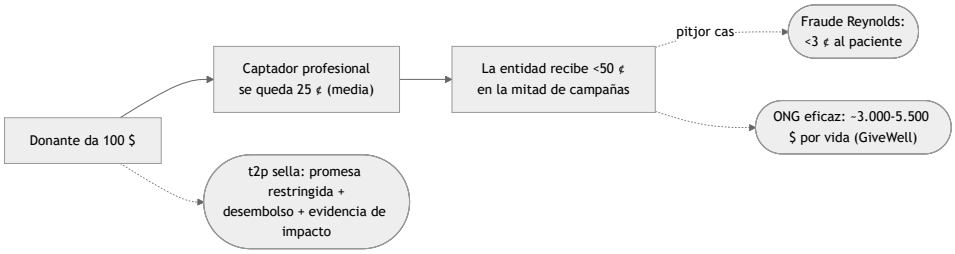


Figura 73.1 — El recorrido de un dólar donado, con sus fugas reales: el captador profesional se queda 25 céntimos de media (fiscalía de Nueva York, 2024), y en la mitad de las campañas la entidad recibe menos de la mitad; en el fraude Reynolds, menos de 3 céntimos llegaban al paciente; en el proyecto de Haití, un 40 % se perdía en overhead. Como contrapunto, una ONG eficaz evita una muerte por unos 3.000-5.500 dólares (GiveWell). t2p sella tres nodos —la promesa restringida, cada desembolso y la evidencia de impacto (GPS + hora + prueba de vida)—, convirtiendo el «confía en el informe» en evidencia auditable. Límite: no juzga si la métrica declarada es honesta ni la eficacia del programa. Fuentes: fiscalía de Nueva York; FTC; ProPublica; GiveWell.

---

[1] ProPublica / NPR (Justin Elliott y Laura Sullivan) — *How the Red Cross raised half a billion dollars for Haiti and built six homes* (2015). https://www.propublica.org/article/how-the-red-cross-raised-half-a-billion-dollars-for-haiti-and-built-6-homes ↩

[2] Federal Trade Commission — *FTC, all 50 states and D.C. charge four cancer charities with bilking over $187 million* (familia Reynolds; <3 % a los pacientes). https://www.ftc.gov/news-events/news/press-releases/2015/05/ftc-all-50-states-dc-charge-four-cancer-charities-bilking-over-187-million-consumers ↩

[3] FBI Internet Crime Complaint Center — *PSA: charity and disaster-relief fraud* (2024; ~96 M$; la IA aumenta la legitimidad aparente). https://www.ic3.gov/PSA/2025/PSA250116 ↩

[4] New York Attorney General (Letitia James) — *Pennies for Charity 2025* (los captadores se quedan el 25 %; <50 % en la mitad de campañas). https://ag.ny.gov/press-release/2025/attorney-general-james-releases-annual-pennies-charity-report ↩

[5] CBS News — *CBS News investigates Wounded Warrior Project spending* (de 1,7 a 26 M$ en conferencias; directivos destituidos en marzo de 2016). https://www.cbsnews.com/news/cbs-news-investigates-wounded-warrior-project-spending/

[6] GuideStar, Charity Navigator y BBB Wise Giving Alliance — *The Overhead Myth* (2013; el overhead, mal indicador). https://learn.guidestar.org/news/news-releases/2013/2013-06-17-overhead-myth ↩

[7] GiveWell — *How much does it cost to save a life?* (entre ~3.000 y 5.500 $ por vida). https://www.givewell.org/how-much-does-it-cost-to-save-a-life ↩

[8] CharityWatch (Daniel Borochoff) — *Our charity rating process* (≥75 % a programa; ≤25 $ por recaudar 100 $). https://www.charitywatch.org/our-charity-rating-process

[9] CBS News / Patrick Radden Keefe (*Empire of Pain*) — *The Met removes the Sackler name* (la filantropía como «reputation laundering»). https://www.cbsnews.com/news/metropolitan-museum-of-art-sackler-family-name-removed-purdue-pharma/

[10] Federal Trade Commission — *Reported fraud losses hit $12.5 billion in 2024* (contexto del fraude). https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

Cajas negras: el dato que el fabricante decía que no existía

«Los hechos son tozudos; y sean cuales sean nuestros deseos, nuestras inclinaciones o los dictados de nuestras pasiones, no pueden alterar el estado de los hechos y de las pruebas.»

— John Adams, defensa en los juicios de la Masacre de Boston (1770)

El 25 de abril de 2019, en Key Largo (Florida), un Tesla con el Autopilot activado causó un accidente mortal. Cuando los abogados de la víctima reclamaron los datos del coche, Tesla respondió primero que **no existían**; después dijo a la policía que estaban «corruptos», e invocó una función de **autoborrado que no existía**. Todo era falso: sus propios servidores habían recibido una **instantánea de colisión** —vídeo, datos del bus del coche y del registrador— unos **tres minutos después del impacto**. Un perito externo, Alan Moore, lo recuperó todo haciendo una **imagen bit a bit de la memoria** de la unidad de control. «Los ingenieros de Tesla dijeron que no se podía hacer… y lo hizo gente de fuera de Tesla.» En agosto de 2025, un jurado de Miami condenó a Tesla a pagar **243 millones de dólares**, de los cuales 200 en daños punitivos [1][2].

Aquel forcejeo por un dato contiene la pregunta de este capítulo, distinta de las del capítulo 20 (la evidencia de atrocidades para un tribunal) y del capítulo 57 (los registros de una intrusión informática). Aquí el dato es **telemetría de máquina** —velocidad, frenada, clasificación de objetos, parámetros de vuelo— y el conflicto típico no es «nos piratearon», sino **«el coche dice X, el conductor dice Y»** y, sobre todo, **quién controla y recorta el dato del fabricante**. Porque el problema, como veremos, no es que falten datos: es que quien los custodia puede hacerlos desaparecer.

La caja negra existe; el problema es quién la controla

Los registradores modernos son prodigiosos. Una caja negra de avión sobrevive a un impacto de 3.400 g, a 1.100 grados de fuego durante media hora y a la presión del agua a seis mil metros, y registra más de ochenta y ocho parámetros [5]. El registrador de un coche captura ahora los veinte segundos previos a un choque diez veces por segundo [7]. El dato está ahí. El problema es la **custodia y la selección**. En el atropello mortal de Elaine Herzberg por un Uber autónomo en Tempe en 2018, la telemetría reveló que el sistema **detectó a la peatón 5,6 segundos antes** pero nunca la supo clasificar —objeto, vehículo, bicicleta— mientras el frenado de emergencia estaba desactivado; la caja negra no captó una avería, sino una **indecisión algorítmica** milisegundo a milisegundo [3]. Y el caso de Cruise en San Francisco mostró el peligro en su forma más pura: después de que un robotaxi arrastrara a una peatón seis metros, la empresa enseñó a la autoridad de tráfico de California un **vídeo recortado que acababa antes del arrastre**; la **DMV le suspendió los permisos** por tergiversar la información de seguridad [4]. Cuando quien controla el dato es el mismo que se investiga, **la elección de lo que se enseña se convierte en el problema central**.

Cuando la caja no llega al final, o no resuelve la causa

Pero la caja negra tiene dos límites que ninguna tecnología puede borrar. El primero es que solo sirve si graba hasta el final. En el accidente de Jeju Air en Corea del Sur en diciembre de 2024, con 179 muertos, tanto la grabadora de voz como la de datos se detuvieron unos cuatro minutos antes del impacto y dejó fuera de la caja la franja decisiva [9].

El segundo límite es aún más profundo: la caja fija los hechos físicos, pero no resuelve la interpretación. En el accidente de EgyptAir 990 de 1999, con los mismos datos auténticos e íntegros, la autoridad estadounidense concluyó una acción deliberada del copiloto, mientras que la egipcia la atribuyó a una avería mecánica [10]. Los bits eran los mismos; su significado, en disputa. La cadena de bloques no es perito.

La prueba de existencia: sellar la caja negra

Es aquí donde **t2p** aporta una capa de **integridad probatoria**, no solo de captura. Sella la caja negra para que nadie pueda decir después «este no es el dato original». En el momento en que el registrador

cierra un evento —una instantánea de colisión, un bloque de datos de vuelo o un registro de aterrizaje de un dron—, el dispositivo calcula la **huella SHA-512** y la ancla a la **blockchain pública** con un **sello de tiempo RFC 3161** conforme a eIDAS. Solo se publica la huella; el dato crudo permanece privado, pero queda probada su existencia y su contenido exacto en aquel instante.

Esto contrarresta directamente los casos que hemos visto: si la huella de la instantánea completa se ancla tres minutos después del impacto, un dato posterior «distinto» no coincidirá con el sello, y un vídeo truncado como el de Cruise mostrará una huella incompatible con la del clip íntegro. El **GPS forense** y el sello de tiempo para drones y vehículos permiten refutar la afirmación «yo no estaba en zona restringida», como en el caso de Cabo Cañaveral, donde los registros del propio dron contradecían al operador [8]. La **prueba de vida** en el momento de la extracción certifica que una persona identificada sacó el dato en tal fecha, sellando la cadena de custodia desde el primer minuto.

Hay que señalar tres limitaciones. Primero, «basura a la entrada, basura en la cadena»: el sello no corrige el dato de origen; si un sistema clasifica mal a un peatón, solo certifica que el error existió en aquel momento. Segundo, **no resuelve la interpretación**: como demuestra el caso del EgyptAir 990, la prueba habría blindado los bits pero la disputa pericial sobre qué significan quedaría intacta. Tercero, **no graba lo que la máquina nunca captó**: en Jeju Air las cajas dejaron de registrar cuatro minutos decisivos y el sello solo cierra el vacío. Finalmente, el anclaje **debe ocurrir en el dispositivo y de manera inmediata**; si el fabricante controla el momento del sellado —como hoy controla la instantánea — podría sellar una versión ya modificada. El valor es real solo con un **sellado automático, en el dispositivo e instantáneo**, fuera del control discrecional de quien se investiga.

La promesa y el peligro

La promesa es cerrar la asimetría que costó a Tesla **243 millones de dólares** probar en su contra; una caja negra sellada en origen haría imposible negar, corromper o recortar el dato después del hecho, y daría a los investigadores y a los tribunales una cadena de custodia inatacable desde el minuto cero, protegiendo tanto a las víctimas como a los fabricantes honestos, que podrían demostrar que su dato es el original. En un mundo donde los accidentes los deciden algoritmos, hacer la caja negra inalterable es restaurar la confianza en lo que pasó de verdad.

El peligro pide los matices que hemos dicho. Primero, no confundir integridad con verdad ni con causa: el sello blinda los bits, pero no resuelve su significado. Segundo, no rellena los vacíos de lo que el sensor no captó. Y tercero, y más importante, si el sellado no es inmediato y en el dispositivo, el fabricante puede seguir curando el dato antes de sellarlo. La prueba de existencia es una capa poderosa de integridad probatoria, no un perito ni un sustituto de una grabación completa.

Es hora de actuar

Para los fabricantes (de coches, aviones, drones): sellar cada bloque de datos en el dispositivo y en el instante de su cierre, fuera de su propio control discrecional. Para los reguladores (organismos de seguridad del transporte, aviación, tráfico): exigir el sellado en origen como parte de la homologación de los registradores. Para los investigadores y tribunales: sellar la extracción con prueba de vida, para que la cadena de custodia sea inatacable. Y para los operadores: un dato que los proteja tanto si tienen razón como si no, para que la verdad del accidente no dependa de quién controla el servidor.

Un fabricante dijo que un dato no existe, y un perito de fuera lo encontró en sus servidores. Dar a cada caja negra una prueba sellada en el momento de nacer —sin olvidar nunca que el sello no resuelve la causa ni rellena lo que no se grabó— es, en este frente donde deciden las máquinas, time2act.



Figura 74.1 — Los registradores (la caja negra de avión con más de 88 parámetros y ahora hasta 25 h de voz; el registrador del coche con los 20 s previos al choque; el registro de vuelo de un dron) capturan el dato. t2p no mejora la captura: en el instante en que el registrador cierra un evento, calcula su huella SHA-512 en el dispositivo y la ancla a la blockchain pública con sello eIDAS, de manera que negar el dato (Tesla), recortarlo (Cruise) o alterarlo deja una huella que no cuadra. Límite: el sello no corrige un dato erróneo, no resuelve la disputa pericial sobre la causa (EgyptAir 990), y no rellena lo que el sensor

no grabó (Jeju Air, donde la grabación se cortó 4 minutos antes). Fuentes: NTSB; California DMV; caso Benavides contra Tesla.

---

[1] NPR — *Tesla ordered to pay $243 million in fatal Autopilot crash* (Benavides contra Tesla; 200 M$ en daños punitivos; 33 % de responsabilidad). https://www.npr.org/2025/08/02/nx-s1-5490930/tesla-autopilot-crash-jury-240-million-florida ↩

[2] Electrek — *Tesla withheld data and misdirected police in Autopilot crash* (la instantánea de colisión a +3 min; la imagen NAND; el perito Alan Moore). https://electrek.co/2025/08/04/tesla-withheld-data-lied-misdirected-police-plaintiffs-avoid-blame-autopilot-crash/ ↩

[3] National Transportation Safety Board — *Collision Between an Uber ATG Test Vehicle and a Pedestrian (HAR-19-03)* (5,6 s; frenado de emergencia desactivado). https://www.ntsb.gov/investigations/Pages/HWY18MH010.aspx ↩

[4] California DMV — *Statement on Cruise LLC suspension* (24-oct-2023; el metraje del arrastre, omitido). https://www.dmv.ca.gov/portal/news-and-media/dmv-statement-on-cruise-llc-suspension/ ↩

[5] National Transportation Safety Board — *Cockpit Voice Recorders and Flight Data Recorders* (supervivencia; ≥88 parámetros). https://www.ntsb.gov/news/Pages/cvr_fdr.aspx ↩

[6] Federal Register / FAA — *25-hour Cockpit Voice Recorder requirement for new aircraft* (2026; de 2 a 25 horas). https://www.federalregister.gov/documents/2026/02/02/2026-02110/25-hour-cockpit-voice-recorder-cvr-requirement-new-aircraft-production

[7] eCFR — *49 CFR Part 563: Event Data Recorders* (captura pre-choque de 5 s a 20 s a 10 Hz). https://www.ecfr.gov/current/title-49/subtitle-B/chapter-V/part-563 ↩

[8] DroneXL — *Drone pilot sentenced over Cape Canaveral Space Force base flights* (los registros de geofencing contradicen al operador). https://dronexl.co/2025/08/28/drone-pilot-sentenced-cape-canaveral-space-force-base/ ↩

[9] CNN — *Jeju Air black boxes stopped recording before the crash* (los 4 minutos decisivos, fuera de la caja). https://www.cnn.com/2025/01/11/asia/south-korean-airline-black-boxes-stopped-recording-intl-hnk/index.html ↩

[10] National Transportation Safety Board — *EgyptAir 990 Aircraft Accident Brief (AAB-02/01)* (los mismos datos, causas opuestas). https://www.ntsb.gov/investigations/AccidentReports/Reports/AAB0201.pdf ↩

La caja negra personal: evidencia preventiva para víctimas y para inocentes

«Más vale una onza de prevención que una libra de remedio.»

— Benjamin Franklin, Pennsylvania Gazette (1735)

El 20 de marzo de 2024 no pasó nada que se viera a simple vista. Ninguna sirena, ningún titular. Aquel día, el sistema Cometa —el servicio estatal que registra cada movimiento de los agresores con pulsera antimaltrato— cambiaba de manos: de Telefónica a la unión temporal de empresas formada por Vodafone y Securitas. En la migración, los historiales de posicionamiento anteriores a aquella fecha quedaron inaccesibles para los juzgados [1]. Los meses siguientes, en salas de vistas de toda España, fiscales que querían probar quebrantamientos de órdenes de alejamiento se encontraron con el vacío: la memoria anual de la Fiscalía General del Estado, conocida en septiembre de 2025, reconoce «numerosas absoluciones y sobreseimientos provisionales» por la pérdida de aquellos datos, en un sistema con unas 4.500 pulseras activas, y habla de una potencial desprotección de las víctimas [1][2]. El Gobierno conocía incidencias desde enero de 2024 [3]. La caja negra que debía proteger a miles de mujeres falló en silencio, y parte de la prueba murió con ella.

Este capítulo trata la caja negra personal: la certificación preventiva de tu propia vida —el audio de una conversación amenazadora, el clip de la cámara del coche, la foto datada— sellada en el dispositivo por si un día eres víctima o te acusan falsamente. Las cajas negras de los fabricantes están en el capítulo 74; la cadena de custodia judicial, en el capítulo 77; la reclamación de seguros, en el capítulo 28; la documentación del daño en línea, en los capítulos 83 y 84. La pregunta clave: ¿cómo puede una persona corriente guardarse la verdad sin convertirse en espía de nadie? La respuesta es **t2p**: el contenido no sale nunca del teléfono; solo la huella SHA-512, con el anclaje de la huella en la blockchain pública y el sello de tiempo RFC 3161/eIDAS complementario dentro de un contenedor .asice, queda fijada para siempre [18]; y revelarla o no es siempre decisión tuya. La neutralidad es radical: la misma herramienta sirve a la víctima que documenta —el caso de cada día— y al inocente que se defiende —el caso raro, pero devastador. La prueba no tiene bando.

Cuando la caja negra del Estado falla

Vale la pena mirar de cerca el caso Cometa, porque es una parábola entera. La infraestructura probatoria más sensible del país —la que registra los movimientos de los agresores para proteger a víctimas de violencia de género— dependía de una migración de base de datos entre contratistas. En el cambio de Telefónica a la UTE de Vodafone y Securitas, los posicionamientos anteriores al 20 de marzo de 2024 se volvieron inaccesibles para las autoridades judiciales [1]. Cuando un fiscal necesitaba demostrar que un agresor se había acercado a su víctima antes de aquella fecha, el dato ya no estaba: de ahí las absoluciones y los sobreseimientos provisionales que la Fiscalía acabó reconociendo en su memoria anual [2]. El Gobierno tenía constancia de incidencias desde enero de 2024 [3]; la gestión costó una reprobación parlamentaria a la ministra y unas disculpas públicas a las víctimas, sin descartar penalizaciones al contratista [4]. El análisis jurídico posterior lo resumió sin rodeos: un sistema «en crisis» [5].

La lección no es partidista, es estructural: cuando la prueba vive en un único depósito centralizado, un cambio de contrato, un error de migración o una decisión administrativa la pueden borrar. No hace falta ninguna malicia; basta con la fragilidad. La prueba de existencia invierte el diseño: si cada posición y cada alerta se hubiera anclado en origen —huella SHA-512 y sello de tiempo, en el mismo instante de producirse [18]—, el contenido se habría podido perder igualmente, pero habría sido imposible discutir qué existía, qué se registró y cuándo. Ninguna defensa habría podido fundamentarse en la duda sobre si los datos existieron alguna vez.

Y aquí nace la pregunta que da sentido a todo el capítulo: si esto le puede pasar al Estado, con 4.500 pulseras y un contrato millonario, ¿qué no le puede pasar al ciudadano que, ante un conflicto, solo tiene su palabra?

El derecho a grabar tu propia vida

La regla de base la fijó el Tribunal Constitucional hace cuatro décadas, y nació, precisamente, de una grabación aportada en un conflicto laboral. La STC 114/1984, de 29 de noviembre, establece que grabar una conversación en la que participas no vulnera el secreto de las comunicaciones del artículo 18.3 de la Constitución —«no hay secreto para aquel a quien la comunicación va dirigida»— y que la grabación propia es admisible como prueba documental, con un límite: no invadir la esfera íntima del otro [6]. El Tribunal Supremo lo ha confirmado de manera constante [7]. Tu teléfono puede ser, legalmente, tu testigo.

La línea roja también es nítida. Grabar conversaciones ajenas —aquellas en las que no participas— con artificios técnicos de escucha o grabación es delito de descubrimiento y revelación de secretos: el artículo 197.1 del Código Penal lo castiga con prisión de uno a cuatro años y multa, y si el material se difunde, la pena sube de dos a cinco años [8]. La caja negra personal no es un micrófono oculto en casa ajena: es el registro de tu propia vida, de las conversaciones que tú mantienes y de lo que pasa ante tu parabrisas.

El subcaso del parabrisas merece su propio mapa, porque el mosaico europeo es instructivo. En España, la Agencia Española de Protección de Datos admite la cámara de a bordo (*dashcam*) con condiciones: grabación limitada al incidente —unos veinte segundos antes y después—, preferiblemente sin sonido y minimizando los datos de terceros; con estos límites, la grabación vale como prueba, amparada por el interés legítimo y la tutela judicial efectiva [13]. Alemania la admite como prueba limitada al momento del siniestro; Francia hace al conductor responsable del tratamiento de los datos; y Portugal aplica la política más dura de Europa: la Ley 58/2019 prohíbe las *dashcams* hasta el punto de que ni siquiera se pueden llevar en el coche [14]. El derecho a tu propia prueba existe, pues, pero es estrecho y exige un respeto escrupuloso por la intimidad ajena. Es exactamente el diseño de t2p: solo huellas en la cadena, contenido en el dispositivo, revelación voluntaria ante el juez [18].

La grabación ya no se cree

Dos fuerzas han chocado en esta década: nunca había sido tan fácil grabarlo todo, y nunca había sido tan fácil falsificarlo todo. Con la tecnología actual se clonan voces convincentes a partir de tres a cinco minutos de audio limpio, y algunos sistemas tienen bastante con treinta segundos [9]: cualquier fragmento de conversación puede ser imitado por una máquina que reproduce el timbre, el ritmo y las imperfecciones del hablante.

Los tribunales lo saben, y han movido ficha. En el proceso, impugnar la autenticidad de un audio desplaza la carga de la prueba hacia quien lo presenta; y la jurisprudencia reciente del Tribunal Supremo ya no acepta la impugnación genérica —el «podría ser falso»—, sino que exige una impugnación técnica y fundamentada, con los criterios de admisión cada vez más estrictos: análisis forense, cadena de custodia completa, integridad acreditada, contraste con otras pruebas [10].

Para el ciudadano, la consecuencia es incómoda: tu grabación verídica, por sí sola, vale cada día menos. Al día siguiente de un conflicto, la otra parte siempre podrá sembrar la duda —«es un montón de bits, editados quién sabe cuándo»—, y el peritaje que lo resuelve es caro, lento y cada generación de síntesis lo hace más difícil [9][10].

La salida estructural es la del capítulo 15: no detectar la falsedad a posteriori, sino acreditar la autenticidad a priori. Una grabación con la huella SHA-512 sellada en el momento de la captura y anclada a la blockchain pública [18] llega al juzgado con la pregunta clave ya resuelta: este fichero, exactamente este, existía en aquella fecha y no se ha tocado desde entonces. La duda razonable cambia de bando: quien quiera negarla tendrá que explicar cómo se falsifica un sello criptográfico hacia atrás en el tiempo.

La caja negra que ya llevas encima

La caja negra personal no es vigilancia: es memoria certificada propia, activada cuando tú quieres. Un botón antes de una reunión tensa; un modo en el coche que solo conserva el incidente; una foto que se sella al hacerse. El contenido permanece cifrado en el dispositivo; solo la huella viaja [18]. No se trata de grabar la vida entera, sino de abrir un canal controlado para aquellos fragmentos que pueden decidir tu destino.

El Estado, de hecho, ya apunta hacia aquí. La aplicación oficial AlertCops, de la Secretaría de Estado de Seguridad, incorpora un botón SOS que, pulsado cinco veces en menos de seis segundos, envía a las fuerzas de seguridad la ubicación y diez segundos de audio; las víctimas de violencia de género se registran

con el código AVDG para el aviso automático a los cuerpos competentes [15]. Es el reconocimiento institucional de que un audio inmediato y datado puede romper el círculo de la palabra contra palabra.

La víctima de acoso —laboral, vecinal, doméstico— encuentra aquí el primer uso: acumular durante meses conversaciones propias selladas, amparadas por la STC 114/1984 [6]. Cuando decida denunciar, no llevará recuerdos dispersos: llevará una cronología verificable.

El inocente acusado falsamente encuentra el segundo. Es un caso estadísticamente raro —las denuncias por violencia de género que acaban en condena firme por denuncia falsa son el 0,0082 % de casi tres millones de denuncias, según la serie de la Fiscalía [11][12], y este libro lo subraya para no alimentar ningún mito—, pero para quien lo padece es devastador. Una agenda sellada —dónde estabas, qué dijiste— puede ser la única defensa posible contra una difamación o una acusación errónea.

Y el conductor encuentra el tercero, frente a las mafias del siniestro simulado: las aseguradoras detectan unos 400.000 intentos de fraude al año, con un coste potencial de 2.000 millones de euros; seis de cada cien lesiones declaradas esconden fraude, y los accidentes simulados son el 3,2 % de los declarados pero el 18 % del coste de los siniestros investigados [16]. En julio de 2025, una sola trama acabó con 32 detenidos por siete accidentes simulados en ocho meses [17]. La *dashcam* con sello en origen, dentro de los límites de la AEPD [13], es la caja negra sobre ruedas del particular.

La prueba de existencia aplicada

Una persona corriente, un teléfono corriente, y una decisión: guardarse la verdad por si alguna vez hay que enseñarla.

1. La víctima que documenta

Una mujer que sufre amenazas reiteradas graba las conversaciones en las que participa, amparada por la STC 114/1984 [6]. Cada noche, el móvil calcula la huella SHA-512 de los ficheros, le añade el sello de tiempo RFC 3161/eIDAS y la ancla a la blockchain pública [18]. El contenido no sale del teléfono: ni nubes, ni terceros, ni riesgo de filtración. El día que denuncia, su abogada aporta una cronología de evidencia con fecha cierta que ninguna impugnación genérica puede tumbar [10]. Si el agresor borra sus mensajes o niega las llamadas, el registro de ella sigue existiendo —y no depende de ningún contratista ni de ninguna migración de bases de datos [1]. Complementa, no sustituye, los canales oficiales: AlertCops y el 016 [15].

2. El inocente que se defiende

Un hombre acusado de haber dicho o hecho algo en un momento concreto aporta su agenda sellada: el audio de la reunión real, la ubicación datada, el mensaje original. No es una herramienta de sospecha contra nadie —las condenas firmes por denuncia falsa son ínfimas [11][12]—, sino un seguro de bajo coste contra el peor día de una vida. La clave es técnica: el sello se creó antes del conflicto, y nadie fabrica una coartada retroactiva contra una cadena de bloques [18].

3. La caja negra sobre ruedas

Un conductor con la cámara configurada en el modo que recomienda la AEPD —solo el incidente, unos veinte segundos antes y después, sin sonido [13]— se topa con un frenazo sospechoso: dos coches coordinados, cuatro ocupantes, lesiones declaradas al día siguiente. El clip sellado en origen —huella y hora ancladas en el mismo minuto [18]— desmonta el guion de la trama [16][17]: contra un sello criptográfico no hay versión coordinada que aguante. Para la aseguradora, peritaje más rápido; para el conductor honesto, el fin del «tú contra cuatro testigos».

4. El contrato de palabra

La autónoma que cierra un encargo por teléfono, el inquilino que acuerda una reparación con el propietario, la familia que pacta los turnos de cuidado de un padre mayor: conversaciones propias, grabadas legalmente [6] y selladas al momento [18]. Si todo va bien, nadie las escuchará nunca. Si alguien niega su palabra, la fecha cierta convierte el «yo nunca dije eso» en una posición insostenible.

Hay que decir también, con la misma claridad, qué no hace el sello: acredita cuándo existía un fichero y que no se ha alterado, pero no acredita que lo que se dice en él sea verdad; no convierte en lícita una grabación que no lo era —grabar conversaciones ajenas sigue siendo delito del artículo 197 [8]—; y no

libera al juez de valorar la prueba en su contexto. La caja negra personal es memoria blindada, no veredicto.

La promesa y el peligro

La promesa es triple: que ninguna víctima vuelva a perder un juicio porque la prueba vivía en un servidor ajeno y desapareció con un contrato [1][2]; que ningún inocente dependa solo de su palabra; y que la grabación verídica recupere el valor probatorio que la clonación de voz y la síntesis le están erosionando [9][10]. Pero este es, quizá, el capítulo donde los peligros piden más franqueza de todo el libro.

El primero es **la sociedad de la sospecha**. Si todo el mundo graba siempre a todo el mundo «por si acaso», la confianza íntima muere: una sociedad de cajas negras mutuas es una sociedad vigilada desde dentro. Por eso la caja negra personal ha de ser defensiva y excepcional: se activa con intención, no por defecto; registra tu vida, no la de los demás; y el diseño de solo-huellas [18] garantiza que nada se puede difundir que no se haya revelado formalmente. La herramienta es para la sala de vistas, no para las redes.

El segundo es **la línea penal y la esfera íntima**. El derecho ampara la grabación propia (STC 114/1984 [6]) y castiga la interceptación de la conversación ajena (artículo 197 del Código Penal [8]). Ningún sello blanquea una captación ilícita, y la difusión fuera del proceso puede ser delito aunque la grabación fuera lícita. La frontera entre prueba legal y exposición pública ha de quedar grabada en el propio diseño de la herramienta.

El tercero es **la revocabilidad y el olvido**. Las huellas de tu vida han de poder invalidarse a petición tuya, y no puede haber ningún registro central de huellas personales. La inmutabilidad protege la prueba; no puede convertirse en una condena perpetua de la propia memoria.

Y el cuarto es **la excusa para no arreglar el Estado**. La caja negra personal no exime a la Administración de hacer funcionar Cometa, AlertCops o el 016 [1][15]. Que el ciudadano tenga que blindarse la prueba es un síntoma, no un ideal: la promesa solo es justa si convive con instituciones que también hacen su trabajo.

Es hora de actuar

La prueba de tu vida no puede depender ni de la memoria ni de un contrato de mantenimiento.

Para ti, ciudadano: conoce tu derecho —grabar las conversaciones en las que participas es legal desde la STC 114/1984 [6]; grabar las ajenas, delito [8]. Activa la caja negra con intención —la reunión difícil, el trayecto en coche, el incidente— y sella en el dispositivo [18]. Y no difundas nunca: revela solo ante el juez.

Para las víctimas de violencia de género y de acoso: registraos en AlertCops con el código AVDG [15]; documentad con grabaciones propias selladas y buscad asesoramiento legal. Una cronología verificable vale más que mil recuerdos dolorosos.

Para abogados, jueces y peritos: exigid y valorad el sello de captura; una huella anclada resuelve de entrada la impugnación de autenticidad que hoy encarece y alarga los procedimientos [10].

Para las administraciones: anclad en origen los sistemas probatorios públicos —que ninguna migración vuelva a borrar la protección de 4.500 mujeres [1][2][3]— y reconoced valor probatorio cualificado a la evidencia ciudadana sellada.

Para las aseguradoras: premiad la cámara de a bordo conforme a la AEPD con sello en origen [13]: menos fraude [16][17], peritajes más cortos y clientes honestos mejor tratados.

Para los legisladores: estableced la presunción de autenticidad para la prueba sellada en captura; garantizad su revocabilidad; y ni un paso hacia la obligatoriedad —la caja negra personal es un derecho, nunca un deber.

La caja negra del Estado falló un 20 de marzo sin que nadie lo viera [1]. La tuya no depende de ningún contrato, de ninguna migración ni de ninguna empresa: solo de ti y de la matemática. Por la verdad de cada uno, **time2act**.

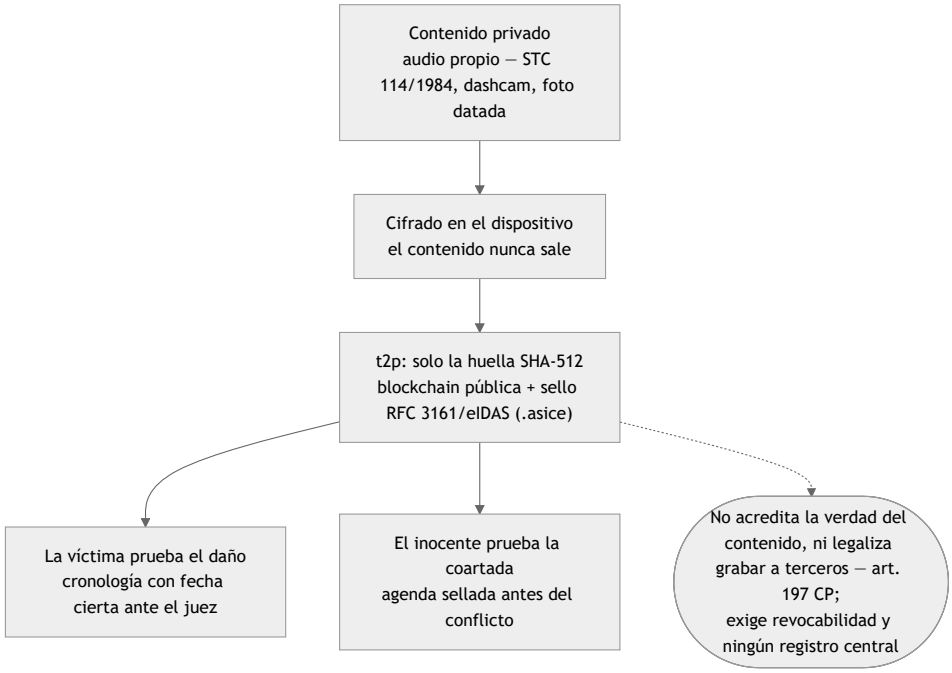


Figura 75.1 — La caja negra personal: el audio de una conversación propia (STC 114/1984), el clip de la dashcam (límites AEPD) o la foto datada se cifran y NO salen nunca del dispositivo; solo la huella SHA-512 con sello de tiempo RFC 3161/eIDAS se ancla a la blockchain pública (.asice). La revelación es decisión del titular, ante el juez. Dos salidas simétricas: la víctima que prueba el daño y el inocente que prueba la coartada. Límites: no acredita la verdad del contenido, no legaliza la grabación de un tercero (art. 197 CP), exige revocabilidad y ningún registro central. Fuentes: STC 114/1984; Fiscalía General del Estado (Cometa; denuncias falsas 0,0082 %); AEPD; UNESPA.

---

[1] Euronews — *Un fallo informático en las pulseras antimaltrato en España absuelve a decenas de agresores* (18 de septiembre de 2025; migración Telefónica → UTE Vodafone+Securitas; datos anteriores al 20 de marzo de 2024 inaccesibles; memoria de la Fiscalía General del Estado; ≈4.500 pulseras activas). https://es.euronews.com/2025/09/18/un-fallo-informatico-en-las-pulseras-antimaltrato-en-espana-absuelve-a-decenas-de-agresore ↩

[2] Diario Socialista — *Fallo en pulseras «antimaltrato» provoca absoluciones y pérdida de pruebas en casos de violencia machista* (18 de septiembre de 2025; «numerosas absoluciones y sobreseimientos provisionales»). https://diariosocialista.net/2025/09/18/fallo-en-pulseras-antimaltrato-provoca-absoluciones-y-perdida-de-pruebas-en-casos-de-violencia-machista/ ↩

[3] OKDiario — *El Gobierno reconoce ahora que conocía desde «enero de 2024» los fallos en las pulseras antimaltrato*. https://okdiario.com/espana/pulseras-gobierno-reconoce-ahora-que-sabia-desde-enero-2024-fallos-pulseras-antimaltrato-15967835 ↩

[4] La Nación (agencias) — *Redondo aborda en el Senado la gestión de pulseras para maltratadores tras ser reprobada en el Congreso* (septiembre de 2025; disculpas a las víctimas; posibles penalizaciones al contratista). https://www.lanacion.com.ar/agencias/redondo-aborda-este-miercoles-en-el-senado-la-gestion-de-pulseras-para-maltratadores-tras-ser-nid28092025/ ↩

[5] Hay Derecho — Nuria Barona Martínez, *Pulseras antimaltrato: análisis jurídico y político de un sistema en crisis* (8 de octubre de 2025). https://www.hayderecho.com/2025/10/08/pulseras-antimaltrato-analisis-juridico-politico/ ↩

[6] Tribunal Constitucional — *STC 114/1984, de 29 de noviembre* (grabar una conversación propia no vulnera el art. 18.3 CE; admisible como prueba documental; límite de la esfera íntima; origen laboral del caso). https://hj.tribunalconstitucional.es/es/Resolucion/Show/367 · https://www.boe.es/buscar/doc.php?id=BOE-T-1984-27955 ↩

[7] Legal Today — *La grabación de las conversaciones entre particulares y su manifestación jurisprudencial* (doctrina consolidada del TS sobre grabaciones de participantes); Iberley — *La validez de las grabaciones privadas aportadas como prueba en el proceso penal.* https://www.legaltoday.com/practica-juridica/derecho-penal/penal/la-grabacion-de-las-conversaciones-entre-particulares-y-su-manifestacion-jurisprudencial-2014-08-14/ · https://www.iberley.es/revista/la-validez-las-grabaciones-privadas-aportadas-como-prueba-proceso-penal-1221 ↩

[8] Gerson Vidal (abogados) — *¿Es delito grabar una conversación sin consentimiento?* (art. 197.1 CP: prisión de 1 a 4 años y multa de 12 a 24 meses; difusión: 2 a 5 años); Noticias Jurídicas — *Voces ocultas: la delgada línea entre grabar legalmente y cometer un delito.* https://www.gersonvidal.com/blog/delito-grabar-conversacion/ · https://noticias.juridicas.com/conocimiento/tribunas/18542-voces-ocultas:-la-delgada-linea-entre-grabar-legalmente-y-cometer-un-delito-/ ↩

[9] Digital Perito — *Clonación de voz: deepfakes de audio y detección forense* (clones convincentes con 3-5 minutos de audio; algunos sistemas con 30 segundos; análisis de espectrogramas y prosodia). https://digitalperito.es/glosario/clonacion-voz/ ↩

[10] Economist & Jurist — *La prueba sintética en el proceso judicial: retos probatorios de los deepfakes* (impugnar desplaza la carga; el TS exige impugnación técnica, no genérica; criterios de admisión reforzados); Rubén Blázquez (Instituto Vasco de Derecho Procesal) — *Deepfakes en el procedimiento probatorio*. https://www.economistjurist.es/noticias-juridicas/la-prueba-sintetica-en-el-proceso-judicial-retos-probatorios-de-los-deepfakes/ · https://www.institutovascodederechoprocesal.com/sites/default/files/files/Ruben%20Blazquez2.pdf ↩

[11] ICPM — *La Fiscalía señala que sólo el 0,01 % de las denuncias por violencia machista son falsas* (79 condenas firmes, el 0,0075 %). https://www.icpm.es/actualidad_noticias.asp?id=2382 ↩

[12] Efeminista — *Casi 3 millones de denuncias por violencia de género en España desde 2004 y solo un 0,0082 % son falsas* (serie 2009-2024); ANAVID — *¿De dónde sale la cifra del 0,01 %?* (matiz metodológico: solo falsedad acreditada con dolo). https://efeminista.com/denuncias-falsas-violencia-de-genero-espana/ · https://anavid.es/de-donde-sale-la-cifra-del-001-de-denuncias-falsas-de-violencia-de-genero-por-parte-de-la-fiscalia-del-estado-y-el-cgpj/ ↩

[13] Motorpasión — *¿Puedes usar una dashcam en España?* (criterios AEPD: grabación limitada al incidente, ~20 segundos antes y después, preferible sin sonido; válida como prueba por interés legítimo y tutela judicial); Adasfera — *Legalidad dashcam España: guía DGT y AEPD (2026)*. https://www.motorpasion.com/seguridad/pregunta-puedes-usar-dashcam-espana-respuesta-puedes-meterte-buen-lio-no-sabes-como · https://adasfera.com/2026/01/legalidad-dashcam-espana-dgt-multasson-legales-las-dashcams-en-espana-en-2026-guia-definitiva-dgt-y-aepd/ ↩

[14] TodoDashcam — *Legislación sobre dashcams en España y Europa* (Portugal: Ley 58/2019, prohibido incluso llevarla; Alemania: admisión limitada al incidente; Francia: CNIL, conductor responsable del tratamiento). https://www.tododashcam.es/pages/blog-legislacion-dashcams-espana ↩

[15] AlertCops (Secretaría de Estado de Seguridad, Ministerio del Interior) — *AlertCops incorpora un botón SOS* (5 pulsaciones en menos de 6 segundos; ubicación + 10 segundos de audio a las FCSE; código AVDG para víctimas de violencia de género). https://alertcops.ses.mir.es/publico/alertcops/actualidad/detalleActualidad.html?entrada=AlertCops-incorpora-un-bot-n-SOS ↩

[16] Rastreator — *Guardia Civil y UNESPA, contra el fraude* (≈400.000 intentos de fraude anuales; ≈2.000 M€; 6 de cada 100 lesiones; accidentes simulados: 3,2 % de los declarados, 18 % del coste investigado; Procedimiento Operativo GC-UNESPA). https://www.rastreator.com/seguros/noticias/guardia-civil-y-unespa-luchan-contra-el-fraude-en-el-seguro.aspx ↩

[17] Infobae — *Detenidas 32 personas que fingían accidentes de tráfico para estafar al seguro* (2 de julio de 2025; siete accidentes simulados en ocho meses). https://www.infobae.com/espana/2025/07/02/detenidas-32-personas-que-fingian-accidentes-de-trafico-para-estafar-al-seguro-una-agencia-de-detectives-presento-la-denuncia/ ↩

[18] t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; el contenido no sale nunca del dispositivo; revelación voluntaria). Véanse los capítulos 13 y 15. ↩

Datos genómicos: el consentimiento de uno expone a muchos

«...una de las ideas más poderosas y peligrosas de la historia de la ciencia: el "gen", la unidad fundamental de la herencia.»

— Siddhartha Mukherjee, El gen: una historia íntima (2016)

El 24 de abril de 2018, la policía de Sacramento detuvo a Joseph James DeAngelo, un expolicía de setenta y dos años, como el «Golden State Killer», responsable de más de doce asesinatos y cincuenta violaciones en los años setenta y ochenta. La pista no salió de ninguna base de datos policial. Los investigadores subieron un perfil de ADN de la escena del crimen a una base genealógica pública, GEDmatch, y la genealogista forense Barbara Rae-Venter lo rastreó a través de **primos de tercer y cuarto grado** que sí habían subido su ADN voluntariamente [7]. Al asesino no lo delató su propio ADN, sino **el árbol genealógico de su familia**.

Aquel caso, a la vez una victoria de la justicia y una pesadilla de la privacidad, contiene la paradoja central de este capítulo, distinta de la del capítulo 47 —«¿quién eres?»— y de la del capítulo 49 —la biometría del refugiado vulnerable. Aquí el sujeto es el **consumidor** que paga voluntariamente por un test de ADN, y el dato tiene una propiedad que ningún otro tiene: **es tuyo y de tu familia a la vez, es irrevocable y delata a personas que nunca consintieron nada**. El consentimiento de uno expone a muchos.

El dato que no puedes cambiar ni recuperar

La fragilidad de este dato quedó desnuda en octubre de 2023, cuando 23andMe sufrió una brecha. Los atacantes entraron directamente en solo unas catorce mil cuentas —el 0,1 %—, pero desde allí, a través de la función que conecta parientes, expusieron los datos de **6,9 millones de usuarios** [1]. E hicieron algo escalofriante: publicaron listas segmentadas por origen étnico —un millón de perfiles etiquetados como judíos asquenazíes, cien mil como chinos— a la venta por unos pocos dólares. El dato genético es, por construcción, un dato de **pertenencia a un grupo**. Lo peor es que no se puede deshacer: a diferencia de una contraseña, no puedes «cambiar tu ADN» después de una fuga.

Y en 2025 llegó el segundo golpe. 23andMe, que custodiaba los datos de cerca de **quince millones de personas**, quebró; en veinticuatro horas el tráfico a su web subió un 526 % y cerca de **1,9 millones de personas** pidieron borrar su ADN, al descubrir que la genética que habían confiado a una startup era ahora un **activo concursable** que se subastaría [3]. Una coalición de **28 fiscales generales**, encabezada por la de Nueva York, Letitia James, demandó a la empresa con un argumento contundente: «23andMe no puede subastar la información genética de millones de personas sin su consentimiento» [4]. Los datos acabaron en manos de una fundación de la cofundadora por 305 millones de dólares, y el regulador británico multó a la empresa con 2,31 millones de libras —castigando, como subrayó, la **custodia**, no el contenido [6]. Y la ley estadounidense de no discriminación genética, recordémoslo, **no cubre los seguros de vida** [9].

La familia que nunca consintió

Aquí está la verdad más incómoda, y es matemática. Los investigadores **Yaniv Erlich y sus colegas** demostraron, como hemos visto, que basta con que el **2 % de una población** esté en una base de datos genética para identificar a casi cualquier persona a través de un pariente lejano; ya hoy, cerca del 60 % de los estadounidenses de ascendencia europea son identificables aunque **nunca se hayan hecho un test** [2]. La privacidad genética, pues, no es un derecho individual, sino **colectivo y familiar**. Como argumenta el jurista **Taner Kuru**, subir tu ADN no convierte el ADN de tu primo en «público»: ninguna firma tuya puede legitimar un dato que delata a hijos, primos y descendientes aún no nacidos. Y lo mismo vale para la biometría de consumo —la cara, el iris—, que tampoco se puede cambiar: bajo la ley de Illinois, Facebook pagó 650 millones de dólares por etiquetar caras sin consentimiento.

La prueba de existencia: sellar el consentimiento, no el genoma

Es aquí donde **t2p** ha de ser especialmente humilde, porque lo que puede hacer es valioso pero limitado. No ancla **la secuencia de ADN** —ponerla en la cadena sería catastrófico—, sino **el acto y los términos del consentimiento**. El cliente firma un formulario que fija exactamente para qué autoriza el uso —el test, la conexión con parientes, la investigación, el acceso policial—; en el dispositivo se calcula la **huella SHA-512**, y solo esta se ancla a la **blockchain pública** con un **sello de tiempo eIDAS** y **GPS forense**. El resultado es una prueba inalterable de *qué consintió esta persona, cuándo y dónde*. La **prueba de vida** ligará el consentimiento a una persona viva y presente, y el **versionado** de cada política de privacidad —como el cambio de GEDmatch en 2019 o la transferencia a la fundación en 2025— deja un registro verificable de qué base de consentimiento amparaba realmente cada transferencia. El contenedor **.asice** se entrega al consumidor, que conserva así su **propia copia probatoria** de lo que autorizó, sin depender del servidor de una empresa que puede quebrar.

Hay que decir el límite con toda la crudeza, porque aquí es lo más duro de todo el libro. «Basura a la entrada, basura en la cadena», y peor: **el dato genético no es de quien lo sella**. Primero, la prueba de existencia **no da privacidad, da trazabilidad**: sellar el consentimiento demuestra que existió, pero no impide que el dato se filtre, se subaste en una quiebra o lo use una aseguradora de vida; la integridad no es confidencialidad. Segundo, y lo más grave, el dato es **irrevocable** y el consentimiento es estructuralmente imposible de dar del todo, porque **tu consentimiento sella el ADN de tu familia**; la prueba puede demostrar que *tú* consentiste, pero no crea el consentimiento de tu primo tercero. Tercero, no resuelve la asimetría de la letra pequeña: un *opt-in* sellado a la perfección sigue siendo lo mismo que el usuario aceptó sin leer —la cadena da fe del clic, no de que el clic fuera informado. Y cuarto, borrar la huella **no borra la muestra física**, ni los *backups*, ni las copias ya compartidas con investigadores o atacantes. **t2p** puede aportar **soberanía probatoria sobre el consentimiento**, pero no puede devolver la privacidad a un dato que, por naturaleza, ya pertenece también a otros y no se puede deshacer.

La promesa y el peligro

La promesa, bien acotada, es real. Dar a cada persona una prueba sellada y en manos propias de qué consintió exactamente y cuándo haría mucho más difícil que una empresa en quiebra subaste datos con un consentimiento que nadie dio o que reescribiera los términos a posteriori. En un mundo donde la genética que confías a una startup puede acabar en una subasta, tener tu propia copia de lo que autorizaste es un escudo real contra el repudio corporativo.

El peligro, aquí, es prometer lo que no se puede cumplir. Vender la prueba de existencia como una garantía de privacidad genética sería una mentira peligrosa: el sello da trazabilidad, no confidencialidad, y no puede legitimar un dato que compromete a la familia. El consentimiento verdaderamente informado, la prohibición de subastar genomas, el cierre del agujero de los seguros de vida y la minimización del dato son problemas de derecho y de gobernanza, no de criptografía. La prueba de existencia es una herramienta para la soberanía sobre el consentimiento, no un sustituto de una ley que proteja un dato que no se puede cambiar.

Es hora de actuar

Para los consumidores: pensárselo dos veces antes de entregar un dato que también pertenece a sus hijos y primos, y conservar una prueba de lo que autorizan. Para las empresas de genómica y biometría: sellar el consentimiento y su versionado, y exigir un opt-in real antes de cualquier venta o transferencia. Para los reguladores: castigar la mala custodia, como hizo el regulador británico, y cerrar el agujero de los seguros de vida. Y para los legisladores: reconocer que la privacidad genética es familiar y colectiva, y que ninguna firma individual puede vender el ADN de una estirpe entera.

Un asesino cayó porque un pariente había subido su ADN; millones de personas vieron su genoma a la venta después de que una empresa quebrara. Dar a cada persona una prueba de lo que ha consentido —sin olvidar nunca que el sello no devuelve la privacidad a un dato irrevocable y compartido— es, en este frente que toca lo más íntimo de todos, time2act.

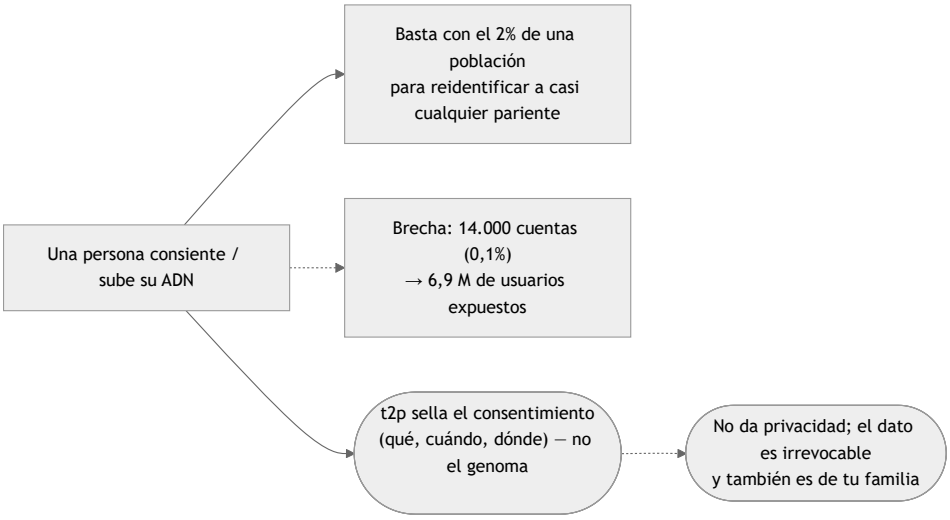


Figura 76.1 — Dos verdades del dato genético. A la izquierda, el efecto familiar: basta con que el 2 % de una población esté en una base de datos para reidentificar a casi cualquier persona a través de un pariente lejano, y cerca del 60 % de los de ascendencia europea ya son identificables aunque nunca se hayan hecho un test (Erlich et al., 2018). A la derecha, el efecto multiplicador de la brecha: el ataque a 14.000 cuentas (el 0,1 %) expuso a 6,9 millones de usuarios a través de la función que conecta parientes. t2p puede sellar el acto de consentimiento —qué, cuándo y dónde—, pero no puede devolver la privacidad a un dato irrevocable que también es de tu familia. Fuentes: Science (Erlich et al.); TechCrunch; fiscalía de Nueva York.

---

[1] TechCrunch — *23andMe confirms hackers stole ancestry data on 6.9 million users* (2023; las listas segmentadas por origen étnico). https://techcrunch.com/2023/12/04/23andme-confirms-hackers-stole-ancestry-data-on-6-9-million-users/ ↩

[2] Yaniv Erlich, Tal Shor, Itsik Pe'er y Shai Carmi (Science) — *Identity inference of genomic data using long-range familial searches* (2018; el 2 % de la población basta). https://www.science.org/doi/10.1126/science.aau4832 ↩

[3] CNBC — *23andMe bankruptcy: selling and deleting DNA* (2025; +526 % de tráfico; ~1,9 M de solicitudes de borrado). https://www.cnbc.com/2025/03/30/23andme-bankruptcy-selling-deleting-dna-genetic-testing.html ↩

[4] New York Attorney General (Letitia James) — *AG James sues 23andMe to protect genetic data* (coalición de 28 fiscales generales). https://ag.ny.gov/press-release/2025/attorney-general-james-sues-23andme-protect-new-yorkers-genetic-data ↩

[5] Bio-IT World — *Anne Wojcicki buys back 23andMe for $305M* (Regeneron, 256 M$ → TTAM, 305 M$; cierre el 14-jul-2025). https://www.bio-itworld.com/news/2025/07/02/anne-wojcicki-buys-back-23andme-for-305m-promises-data-security

[6] Information Commissioner's Office (Reino Unido) — *ICO fines 23andMe £2.31 million* (155.592 residentes británicos; la sanción castiga la custodia). https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/06/23andme-fined-for-failing-to-protect-uk-users-genetic-data/ ↩

[7] NPR — *In hunt for the Golden State Killer, investigators uploaded his DNA to a genealogy site* (el ADN lo subió un familiar). https://www.npr.org/sections/thetwo-way/2018/04/27/606624218/in-hunt-for-golden-state-killer-investigators-uploaded-his-dna-to-genealogy-site ↩

[8] The Legal Genealogist — *GEDmatch reverses course* (opt-out por defecto; solo ~14 % optaron por participar). https://www.legalgenealogist.com/2019/05/19/gedmatch-reverses-course/

[9] National Human Genome Research Institute — *GINA: Genetic Information Nondiscrimination Act (2008)* (no cubre vida, invalidez ni cuidados de larga duración). https://www.genome.gov/27026050/president-bush-signs-the-genetic-information-nondiscrimination-act-of-2008 ↩

[10] Taner Kuru (Computer Law & Security Review) — *Investigative genetic genealogy in Europe* (2025; subir tu ADN no hace «público» el de tus parientes). https://www.sciencedirect.com/science/article/pii/S0267364925000019

Justicia penal: la prueba que el tribunal tiene que poder creer

«Es mejor que diez culpables escapen a que un inocente sufra.»

— William Blackstone, Commentaries on the Laws of England, IV, 27 (1769)

El 24 de enero de 2017, el agente de policía de Baltimore Richard Pinheiro entró en un patio lleno de basura, colocó una bolsa de cápsulas dentro de una lata de sopa, salió al callejón y *entonces* encendió su cámara corporal para grabar el «descubrimiento» de la droga. Lo que no sabía es que aquel dispositivo conserva automáticamente los **treinta segundos anteriores a la activación, sin sonido**. Aquellos treinta segundos mudos lo delataron: fue condenado por fabricar pruebas, y el caso de drogas se hundió [4]. La misma tecnología pensada para vigilar al ciudadano había grabado al vigilante.

Aquel caso contiene las dos caras de este capítulo, distinto del capítulo 20 —que trataba la evidencia de atrocidades ante un tribunal internacional. Aquí el terreno es la **justicia penal ordinaria**: la cámara corporal de un agente, el audio de un divorcio, el vídeo de un juicio nacional. Y plantea la pregunta que hoy resquebraja los tribunales de todo el mundo: en una era en que cualquier sonido o imagen se puede falsear de manera convincente, **¿cómo puede un tribunal saber qué prueba debe creer?**

El dividendo del mentiroso dentro de la sala

La amenaza tiene dos direcciones. La primera es el falso que engaña: un audio o vídeo fabricado con inteligencia artificial presentado como auténtico. En un caso de familia británico, una madre aportó un audio en el que el padre supuestamente hacía amenazas violentas; los peritos demostraron, analizando los metadatos, que había sido editado después de la llamada para insertar palabras que el padre nunca dijo [9].

La segunda dirección es más insidiosa y tiene nombre propio. Los juristas Robert Chesney y Danielle Citron, en su artículo de referencia *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* (2019), la bautizaron como el «dividendo del mentiroso»: a medida que todo el mundo asume que todo se puede falsear, algunos eludirán su responsabilidad denunciando como deepfake una grabación auténtica [6].

Y ya ha llegado a los tribunales. En el litigio por la muerte de un ingeniero al volante de un Tesla, los abogados de la empresa llegaron a sostener que los vídeos en los que Elon Musk promociona la seguridad de su sistema «podrían ser *deepfakes*». La jueza **Evette Pennypacker** lo calificó de «profundamente inquietante»: con aquella lógica, cualquier figura pública podría decir lo que quisiera y después negarlo [1]. Y en el juicio de Kyle Rittenhouse, la defensa consiguió que el juez dudara de que ampliar un vídeo en una tableta —una simple interpolación de píxeles— lo «alterara con inteligencia artificial», y dio a la fiscalía solo veinte minutos para traer a un ingeniero de Apple; la imagen ampliada no se mostró nunca al jurado [2]. Cuando clonar una voz convincente requiere solo unos segundos de audio y, según un estudio de 2025, solo el 0,1 % de las personas distingue con fiabilidad lo real de lo falso, la duda se convierte en un arma.

Quién controla el archivo

Hay un tercer problema, más prosaico pero igual de corrosivo: **quién custodia la prueba**. La cámara corporal se vendió como una herramienta de transparencia, pero a menudo se ha convertido en una herramienta controlada por la propia policía. Una investigación de **ProPublica** encontró que, de setenta y nueve homicidios policiales con cámara en Estados Unidos, solo el 42 % tenía la grabación publicada un año y medio después, y que en aproximadamente uno de cada cinco casos el departamento dijo falsamente al órgano de control que la grabación **no existía** [5]. En Inglaterra y Gales, una investigación de la BBC documentó más de ciento cincuenta informes de mal uso de cámaras —agentes que las apagaban, borraban o compartían grabaciones—, hechos que, según un alto mando, «van al corazón de lo que socava la confianza en la policía» [10]. Como resume The Sedona Conference, el think tank de derecho probatorio, en la era digital la prueba no se «guarda», se **custodia con trazabilidad**: sin una cadena demostrable, el dato más valioso es impugnable.

La prueba de existencia: sellar en el segundo de grabación

Es aquí donde **t2p** ataca el problema en su origen exacto. En el instante de la captura, la cámara corporal o el móvil del testigo calcula **en el dispositivo** la huella SHA-512 del fichero —que no sale nunca; solo viaja la huella—, la ancla a la **blockchain pública** y le adjunta un **sello de tiempo RFC 3161** conforme a eIDAS, un **GPS forense** y un contenedor **.asice**. El sello no se pone *después*, en la sala de pruebas: se pone **en el segundo de grabación**, cerrando la ventana de manipulación.

El efecto sobre las dos amenazas es directo. Contra la edición o el borrado posterior —el caso de Baltimore o los ciento cincuenta informes de la BBC—, cualquier corte o «pérdida» de un clip sellado fallaría la verificación. Y contra el dividendo del mentiroso, ante el «este vídeo es un *deepfake*», el anclaje independiente prueba que **aquel fichero exacto existía intacto antes de tal instante**, desplazando la carga de la duda a quien lo impugna. Todo esto encaja con el derecho existente: la regla federal estadounidense 902(14) ya admite el **hash** como vía de autoautenticación de copias digitales, y el reglamento europeo eIDAS da al sello de tiempo cualificado una **presunción legal** de integridad y fecha. Y el contenedor .asice permite que tanto la defensa como la fiscalía verifiquen la integridad **sin la aplicación y sin confiar en t2p**, con herramientas abiertas: una garantía de igualdad de armas, porque la defensa puede auditar de manera independiente la prueba de cargo.

Hay que decir el límite con toda la crudeza, porque el caso de Baltimore es el ejemplo demoledor. Una cámara corporal sellada **en el momento** de grabar a Pinheiro plantando la droga habría certificado, con un sello inalterable, una escena fraudulenta. «Basura a la entrada, basura en la cadena»: si el agente actúa de mala fe ante la cámara, la cadena certifica la mentira con fecha cierta. El sello prueba integridad, instante, lugar y persona, **no la verdad de la escena**. Y hay límites específicos de este frente. Primero, la prueba solo sirve si el sello se aplica **en origen**: no rescata las grabaciones históricas sin sellar, que hoy son el 99,9 % de la prueba real en los juzgados. Segundo, **no obliga a la policía a encender la cámara**: el problema de ProPublica no es la integridad del clip, sino su *inexistencia*, y ningún sello crea grabaciones que nadie hizo. Tercero, ante el dividendo del mentiroso, el ancla solo ayuda si la prueba **estaba** sellada; para el océano de material sin sellar, la duda sigue intacta, y un sistema que solo avale el material sellado podría, perversamente, **aumentar** la sospecha sobre todo lo demás. Y cuarto, la admisibilidad final la decide el juez según las reglas nacionales, no la cadena de bloques: el hash autoautentica el *fichero*, no su relevancia ni la legalidad de su obtención.

La promesa y el peligro

La promesa es restaurar la base de hechos sin la cual ningún juicio es posible. Una prueba sellada en el origen daría al tribunal una manera de distinguir el fichero íntegro del fabricado, blindaría la cadena de custodia de la cámara corporal y rompería el dividendo del mentiroso para el material protegido. El mismo órgano que escribe las reglas probatorias en Estados Unidos, el Advisory Committee presidido por el profesor Daniel Capra, ya debate nuevas reglas para la prueba generada por máquina, reconociendo que ni las herramientas ni los jueces saben todavía distinguir los *deepfakes* con fiabilidad. El sello de origen es exactamente el refuerzo de autenticación que este debate busca.

El peligro pide los matices que hemos dicho, y aquí son cruciales. El primero, no confundir integridad con verdad: una cámara sellada que graba un montaje certifica el montaje. El segundo, que el sello no obliga a encender la cámara ni rescata el material antiguo. Y el tercero, el más sutil: si solo se confía en lo que está sellado, se puede acabar desconfiando injustamente de todo lo demás. La prueba de existencia es un refuerzo poderoso de la autenticación probatoria, no un detector de mentiras ni un sustituto del juicio humano.

Es hora de actuar

Para los **cuerpos policiales**: sellar cada grabación en el segundo de la captura y hacer obligatoria la activación de la cámara, para que la integridad y la existencia del clip no queden en manos de quien se investiga. Para los **tribunales y quienes escriben las reglas** (el Advisory Committee, los legisladores): reconocer el sello de origen como vía de autoautenticación y adaptar las normas a la prueba generada por máquina. Para la **defensa y la fiscalía**: exigir contenedores verificables de forma independiente, para garantizar la igualdad de armas. Y para los **ciudadanos**: una manera de probar que lo que grabaron es exactamente lo que pasó.

Un agente fue delatado por su propia cámara, pero una cámara sellada habría podido certificar igual de bien su mentira si la hubiera grabado con cara de póquer. Dar a cada prueba una huella sellada en el momento de nacer —sin olvidar nunca que el sello no hace verdad la escena— es, en este frente del que depende la justicia, time2act.

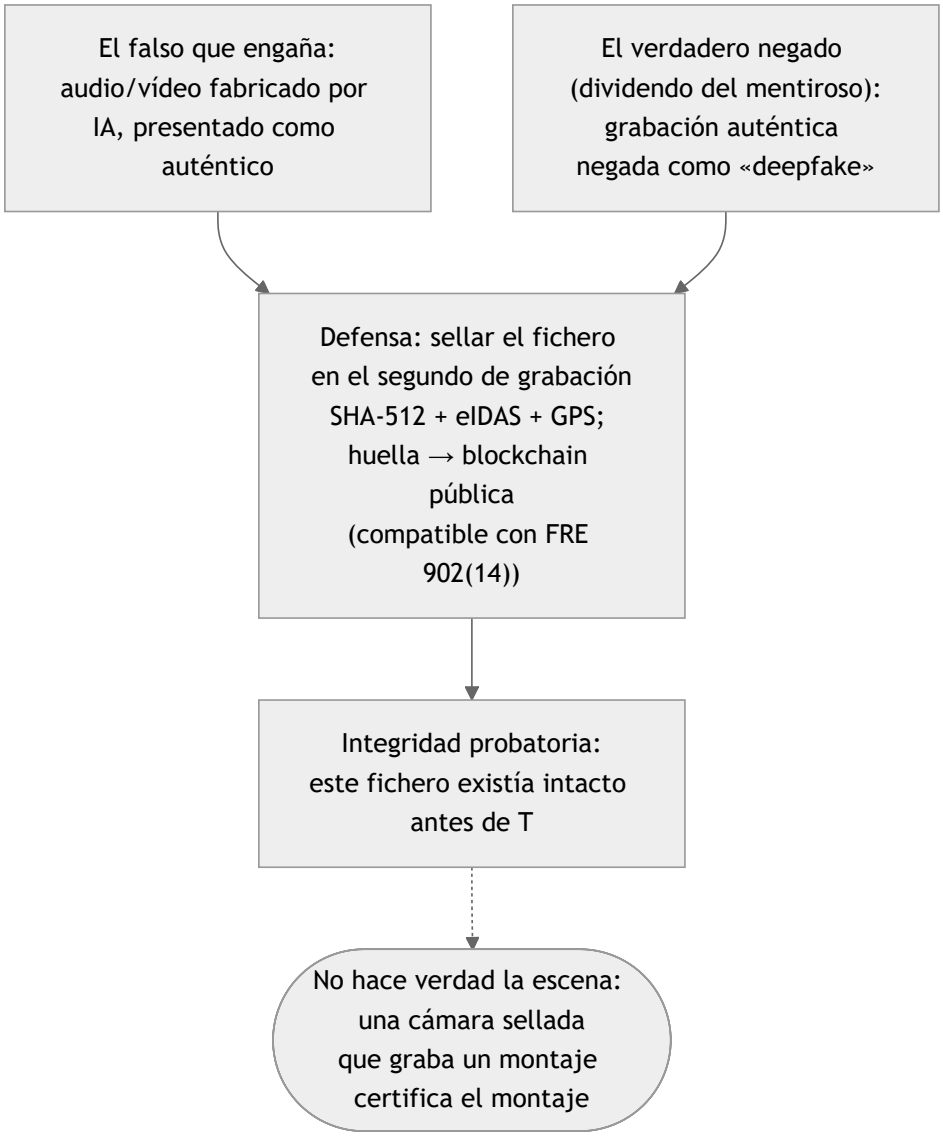


Figura 77.1 — La prueba digital sufre dos ataques opuestos. A la izquierda, el falso que engaña: un audio o vídeo fabricado con IA presentado como auténtico (como el audio editado de un caso de familia británico). A la derecha, el dividendo del mentiroso: una grabación auténtica negada como «deepfake» para eludir la responsabilidad (como en el litigio Huang contra Tesla, donde se alegó que los vídeos de Musk «podrían ser deepfakes»). La misma defensa vale para ambos: sellar el fichero en el segundo de la grabación con huella SHA-512, sello eIDAS y GPS (compatible con la regla 902(14): el hash autoautentica copias). Límite: el sello prueba integridad y momento, no la verdad de la escena —una cámara sellada que graba un montaje certifica el montaje. Fuentes: Chesney y Citron (2019); ProPublica; casos Tesla y Baltimore.

---

[1] Fortune — *Tesla lawyers argue recordings of Musk touting Autopilot could be deepfakes* (Huang contra Tesla; jueza Evette Pennypacker). https://fortune.com/2023/04/27/elon-musk-lawyers-argue-recordings-of-him-touting-tesla-autopilot-safety-could-be-deepfakes/ ↩

[2] 9to5Mac — *Rittenhouse lawyer's pinch-to-zoom argument* (la carga trasladada a la fiscalía; 20 minutos para un perito de Apple). https://9to5mac.com/2021/11/11/rittenhouse-lawyer-pinch-to-zoom/ ↩

[3] NBC News — *Washington state judge blocks use of AI-enhanced video evidence* (State contra Puloka; juez Leroy McCullough; 29-mar-2024). https://www.nbcnews.com/news/us-news/washington-state-judge-blocks-use-ai-enhanced-video-

evidence-rcna141932

[4] NPR — *Baltimore police caught planting drugs in body-cam footage* (el agente Pinheiro; el búfer de 30 segundos sin sonido). https://www.npr.org/sections/thetwo-way/2017/07/20/538279258/baltimore-police-caught-planting-drugs-in-body-cam-footage-public-defender-says ↩

[5] ProPublica — *How police have undermined the promise of body cameras* (solo el 42 % de 79 homicidios; «no existe» falso en 1 de cada 5). https://www.propublica.org/article/how-police-undermined-promise-body-cameras ↩

[6] Robert Chesney y Danielle Keats Citron — *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* (107 California Law Review 1753, 2019; el «dividendo del mentiroso»). https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security ↩

[7] U.S. Courts — *Advisory Committee on Evidence Rules: propuesta de Regla 707 (prueba generada por máquina) y 901(c)* (comentario hasta el 16-feb-2026). https://www.uscourts.gov/sites/default/files/document/2025-11_evidence_rules_commitee_agenda_book_final.pdf

[8] American Bar Association — *New rules for self-authenticating electronic evidence (FRE 902(13)/(14))* (el valor hash autoautentica copias digitales). https://www.americanbar.org/groups/litigation/resources/newsletters/trial-evidence/new-rules-self-authenticating-electronic-evidence/

[9] CYFOR / Expatriate Law — *Deepfake audio evidence used in a UK court* (audio editado después de la llamada para insertar amenazas). https://cyfor.co.uk/deepfake-audio-evidence-used-in-uk-court-to-discredit-father/ ↩

[10] BBC (via LBC) — *150 reports of police officers misusing body cameras* (Inglaterra y Gales; Jim Colwell, NPCC). https://www.lbc.co.uk/article/150-reports-police-officers-misusing-body-cameras-investigation-england-wales-DWzgZZ_2/ ↩

Historiales médicos: quién tocó el registro, y cuándo

«Puede parecer un principio extraño enunciar como el primerísimo requisito de un hospital que no haga ningún daño al enfermo.»

— Florence Nightingale, Notes on Hospitals (1863)

En Chicago, una madre demandó al Rush University Medical Center en nombre de su hijo, nacido con una lesión cerebral por falta de oxígeno durante el parto. Para probar qué había pasado minuto a minuto en la sala, necesitaba una cosa concreta: el **registro de auditoría** del historial electrónico, el rastro que muestra quién escribió, modificó o borró cada anotación y cuándo. Durante más de tres años, el hospital entregó un simple registro de accesos en lugar del rastro completo e hizo afirmaciones sobre su capacidad de producirlo que el juez consideró **falsas**. En 2022, el juez James O'Hara impuso una sanción equivalente a una **sentencia en rebeldía**: la culpabilidad quedaba fijada, solo faltaba ponerle la cifra [1]. La ironía es cruel: el documento sobre el que se litigaba era, precisamente, el que debía decir la verdad de lo que pasó.

Aquel rastro retenido contiene la pregunta de este capítulo, distinta de la del capítulo 18 —que trata la imagen médica y las recetas. Aquí no hablamos del *contenido* clínico, sino de la **gobernanza del registro**: **¿quién accedió a un historial, quién lo alteró, cuándo, y lo consintió el paciente?** Porque un historial electrónico, por muy sofisticado que parezca, es un registro que se puede reescribir, retrodatar y esconder.

El registro que se puede reescribir

La manipulación del historial es un fraude documentado y técnicamente sencillo. Los forenses han encontrado casos en que las notas de un turno se redactaron **después de la muerte del paciente y con fecha retroactiva**, hechas desde una estación de trabajo no clínica horas después de la parada cardíaca: lo que en papel parecía contemporáneo, en los metadatos era posterior. Por eso la normativa de la agencia del medicamento estadounidense es taxativa: un cambio en un registro electrónico **no puede ocultar la información anterior** [3]. A mayor escala, el fraude toma la forma del **copiar-pegar**: la oficina de inspección del sistema de salud estadounidense encontró que solo una cuarta parte de los hospitales tenía políticas sobre esta función, y que las estancias facturadas al nivel de gravedad más alto crecieron casi un 20 % en cinco años, hasta representar **casi la mitad de todo el gasto** de Medicare en hospitalizaciones [4][5]. Y está el fisgoneo: el cotilleo en los historiales de famosos costó al hospital de la UCLA una multa de **865.500 dólares** en 2011, y otro exempleado del mismo centro, **Huping Zhou**, que había accedido a registros **323 veces**, fue **la primera persona encarcelada en Estados Unidos por una violación de la ley de privacidad sanitaria** [6][7]. El registro de auditoría revela todos estos fraudes —pero, como mostró el caso Prieto, también se puede retener.

El consentimiento como recibo, no como casilla

Hay una segunda dimensión, la del **consentimiento**. Hoy el consentimiento del paciente suele ser una casilla perdida en un formulario, imposible de auditar y fácil de fabricar a posteriori. La iniciativa **Kantara**, en su especificación de *recibo de consentimiento* —base de la norma internacional ISO 27560—, propone una idea sencilla y poderosa: que el consentimiento se materialice en un **recibo legible por humanos y procesable por máquinas**, como el de una compra, que registre quién consintió, para qué finalidad y bajo qué política. Así el consentimiento se vuelve **auditable y revocable**, no una casilla olvidada. Y la ley estadounidense ya empuja en esta dirección: la Cures Act obliga a dar a los pacientes acceso a su información de salud y prohíbe el «bloqueo de información» —exactamente lo que hizo el hospital del caso Prieto.

La prueba de existencia: sellar el evento, no la imagen

Es aquí donde **t2p** aporta una capa de integridad al registro y al consentimiento. Lo que se sella **no es la imagen ni el dato clínico** —que queda en el servidor del hospital—, sino el **evento**. Cada vez que se crea, modifica o se borra una anotación, el dispositivo calcula la **huella SHA-512** del par formado por el

contenido de la entrada y sus metadatos de auditoría —identificador del usuario, rol, hora, tipo de acción —, y esta huella se ancla a la **blockchain pública** con un **sello de tiempo eIDAS**. Se genera una prueba pública e inalterable de que *aquella* entrada existía con *aquel* contenido en *este* instante. Lo mismo se aplica al **recibo de consentimiento** —demostrando cuándo se concedió y, sobre todo, cuándo se **revocó**, impidiendo el consentimiento retroactivo fabricado— y al **recibo de acceso**, que crea un registro de quién ha consultado el historial y que ya no puede desaparecer, como en el caso de la UCLA.

El efecto es directo. La **prueba de vida** liga la firma de una nota a un clínico real y presente, no a una sesión robada; el **GPS forense** corrobora que la entrada se hizo desde una ubicación clínica plausible, no desde una estación remota; el **sello de tiempo** fija el instante de manera independiente del reloj manipulable del historial; y el contenedor **.asice** empaqueta la entrada, su recibo de consentimiento y la prueba de anclaje para que un perito los pueda verificar **sin acceso al sistema del hospital**. La retrodatación, la sobreescritura y el filtrado selectivo del rastro en un litigio se vuelven detectables.

Hay que decir el límite con toda la crudeza, porque aquí es fundamental. «Basura a la entrada, basura en la cadena»: el sellado prueba la **integridad temporal y de autoría** del registro, no la **verdad clínica**. Si un médico escribe en tiempo real una observación falsa —«paciente estable» cuando no lo estaba— y la sella al instante, t2p certificará para siempre que aquella mentira existió en aquel momento y de aquella mano, y la hará **más** difícil de retractar, no menos. La prueba no detecta la negligencia ni el error clínico; solo congela lo que se escribió. Además, no sustituye el registro de auditoría nativo del historial: si el hospital no genera o no sella un evento, no hay nada que anclar, y un acceso fuera del flujo sellado es invisible a la cadena. El recibo de consentimiento prueba que el paciente firmó, no que lo entendiera ni que el consentimiento fuera libre. Y el registro de quién mira puede revelar **patrones** sensibles, algo que exige gobernanza. La prueba de existencia da integridad al registro, no veracidad a su contenido.

La promesa y el peligro

La promesa es restaurar la confianza en el documento del que dependen la vida y la justicia. Un historial con cada evento sellado en origen haría imposible retrodatar una nota después de un mal resultado, esconder la huella en un litigio como el del caso Prieto, o borrar las huellas de un fisgón. Y daría al paciente un control real sobre su consentimiento, con un recibo que demuestra qué autorizó y cuándo lo revocó. En un sistema donde el registro se puede reescribir, hacer el evento inalterable es proteger tanto al paciente como al clínico honesto, que podría demostrar que su nota es exactamente la que escribió.

El peligro pide los matices que hemos dicho. El primero, no confundir integridad con verdad: una nota falsa sellada sigue siendo falsa y ahora, además, inmutable. El segundo, que el sello no sustituye el registro nativo ni rescata lo que no se selló. Y el tercero, la privacidad de la propia huella de acceso, que hay que proteger para que no se convierta en una herramienta de vigilancia del clínico. La prueba de existencia es una capa poderosa de gobernanza del registro, no un certificado de buena práctica ni un sustituto del juicio pericial que sabe leer un audit-trail.

Es hora de actuar

Para los **hospitales y los fabricantes de historiales** (Epic, Cerner): sellar cada evento de escritura, acceso y consentimiento en origen, para que el rastro no se pueda retrodatar ni esconder. Para los **reguladores** (las agencias de salud, del medicamento, de interoperabilidad): reconocer el sello de origen como cumplimiento de los controles de auditoría e integridad que la ley ya exige. Para los **pacientes**: un recibo de consentimiento en manos propias que demuestre qué autorizaron y cuándo lo revocaron. Y para los **tribunales**: tratar el registro de auditoría sellado como la prueba fiable que faltó en el caso Prieto.

Una madre luchó tres años por un registro que debía decir la verdad del parto de su hijo, y el hospital lo escondió. Dar a cada evento de un historial una prueba sellada de quién lo tocó y cuándo —sin olvidar nunca que el sello no hace verdadero lo que se escribe en él— es, en este frente que toca la salud y la justicia, time2act.

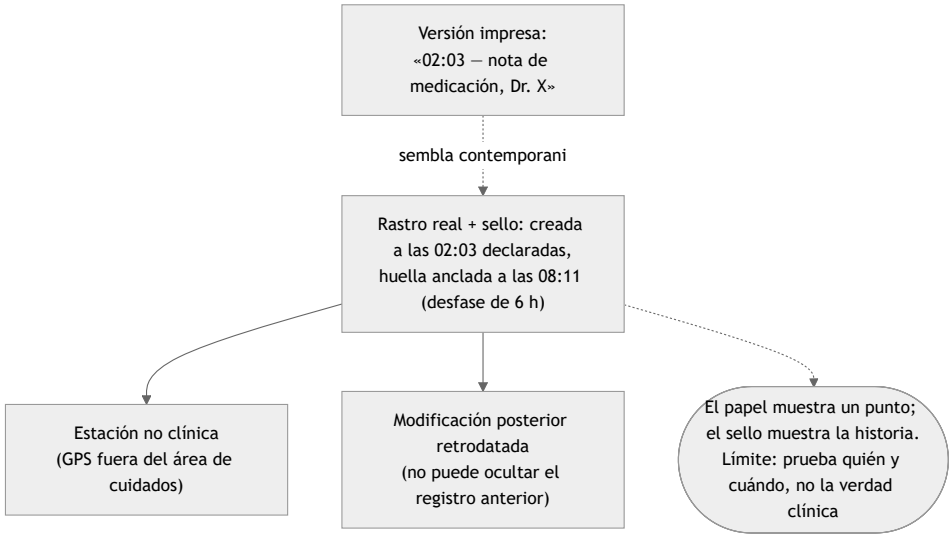


Figura 78.1 — Una nota clínica vista en dos carriles. Arriba, la versión impresa: un solo punto, «02:03 — nota de medicación, Dr. X». Abajo, el rastro de auditoría real con sello de t2p: el evento de creación declarado a las 02:03 pero con la huella anclada a la blockchain pública a las 08:11 —un desfase de seis horas—, hecho desde una estación no clínica (GPS forense fuera del área de cuidados), con una modificación posterior retrodatada que no puede ocultar la información anterior (21 CFR 11.10(e)). El papel muestra un punto; el sello muestra la historia. Límite: el sello prueba quién y cuándo, no la verdad clínica de lo que se escribió. Fuentes: HIPAA y FDA (controles de auditoría); caso Prieto contra Rush; análisis forense de historiales.

---

[1] Enigma Forensics — *Judge sanctions hospital for not producing complete EMR audit trail* (Prieto contra Rush University Medical Center; juez James O'Hara; «information blocking»). https://enigmaforensics.com/blog/judges-order-sanctions-hospital-not-producing-complete-emr-audit-trail/ ↩

[2] Cornell Law (Legal Information Institute) — *45 CFR §164.312: HIPAA technical safeguards* (controles de auditoría obligatorios; integridad de la ePHI). https://www.law.cornell.edu/cfr/text/45/164.312

[3] Cornell Law (Legal Information Institute) — *21 CFR §11.10: FDA electronic records* (audit trails con sello de tiempo; un cambio no puede ocultar el registro anterior). https://www.law.cornell.edu/cfr/text/21/11.10 ↩

[4] HHS Office of Inspector General — *Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology* (OEI-01-11-00570, 2013; solo ~25 % con políticas de copiar-pegar). https://oig.hhs.gov/oei/reports/oei-01-11-00570.asp ↩

[5] HHS Office of Inspector General — *Trend Toward More Expensive Inpatient Hospital Stays in Medicare* (OEI-02-18-00380, 2021; casi la mitad del gasto al nivel máximo de severidad). https://oig.hhs.gov/oei/reports/OEI-02-18-00380.pdf ↩

[6] ProPublica / HHS OCR — *UCLA Health System pays $865,500 to settle celebrity-privacy allegations* (2011; el snooping en los historiales). https://www.propublica.org/article/ucla-health-system-pays-865000-to-settle-celebrity-privacy-allegations ↩

[7] U.S. Department of Justice — *Former UCLA healthcare worker sentenced (Huping Zhou)* (323 accesos; la primera condena de prisión por una violación de HIPAA). https://www.justice.gov/archive/usao/cac/Pressroom/pr2010/004.html ↩

[8] Federal Register / ONC — *21st Century Cures Act: interoperability and information blocking* (2020; acceso del paciente a su información de salud). https://www.federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification

[9] Kantara Initiative — *Consent Receipt Specification v1.1* (base de la norma ISO/IEC TS 27560:2023). https://kantara.atlassian.net/wiki/spaces/archive/pages/3508790/Consent+Receipt+Specification

[10] Dean F. Sittig y Adam Wright (Applied Clinical Informatics) — *Identifying a Clinical Informatics or EHR Expert Witness* (2023; el log es prueba que hay que interpretar). https://pmc.ncbi.nlm.nih.gov/articles/PMC10033222/

Modelos de IA: con qué se entrenaron, y qué ejecutamos realmente

«Más vale que estemos bien seguros de que el propósito puesto en la máquina es el propósito que de verdad deseamos.»

— Norbert Wiener, «Some Moral and Technical Consequences of Automation», Science (1960)

En diciembre de 2023, un equipo del **Observatorio de Internet de Stanford** miró dentro de algo que hacía años que nadie había auditado de verdad: **LAION-5B**, el conjunto de cinco mil millones de pares de imagen y texto con los que se habían entrenado Stable Diffusion y buena parte de la generación de imágenes por IA. Encontraron miles de enlaces a material de abuso sexual infantil —más de **3.200 casos sospechosos**, una parte confirmada por terceros— escondidos entre los datos raspados de la web [1]. LAION retiró el conjunto de la red, y el informe recomendaba **deprecar y discontinuar** los modelos entrenados con él; meses después publicó una versión limpiada, Re-LAION-5B, de la que eliminó más de dos mil enlaces [1][2]. El problema de fondo no era solo el contenido: era que **nadie —ni quienes lo habían creado— podía decir con certeza qué había dentro** hasta que alguien de fuera lo auditó. Un modelo que ya se habían descargado millones de personas se había entrenado sobre una pila de datos que resultaba ser, en parte, ilegal, y no existía ningún registro fiable que lo dijera.

Esta es la pregunta de este capítulo, distinta de la del capítulo 40 —que trata los derechos de quien crea una obra. Aquí no hablamos de la autoría del contenido, sino de la **procedencia del modelo mismo**: con qué datos se entrenó, quién lo construyó, cuándo, y —no menos importante— si los **pesos** que te has descargado y ejecutas son exactamente los que alguien evaluó. Porque un modelo de IA, por impresionante que sea, es un artefacto opaco: un fichero de pesos y una tarjeta de documentación que se pueden reescribir, retrodatar y, como veremos, hasta infectar.

El modelo que nadie puede auditar

La opacidad tiene tres caras. La primera son los **datos**: los grandes modelos se entrenan sobre corpus raspados de todo internet, tan enormes que su composición solo se conoce por aproximación; el caso de LAION mostró que ni siquiera los creadores saben a ciencia cierta qué contienen. La segunda es la **documentación**: desde 2019, las *model cards* propuestas por Mitchell y colegas estandarizan cómo declarar el uso previsto, el rendimiento y los límites de un modelo [9]; pero una tarjeta de modelo es un documento voluntario que vive en un repositorio que el proveedor controla, y que puede editar —o suavizar— después de un incidente. Y la tercera, la más inquietante, es la **integridad de los pesos**. En 2024, los investigadores de JFrog encontraron **un centenar de modelos maliciosos** colgados en Hugging Face: aprovechando el formato de serialización *pickle* —el estándar para empaquetar modelos—, escondían código que se ejecutaba al cargar el fichero y abría una **puerta trasera** en la máquina de la víctima [3][4]. La consecuencia es demoledora: el modelo que descargas puede **no ser** el que el laboratorio evaluó y declaró seguro. Entre la evaluación y tu GPU hay una cadena de custodia que hoy nadie sella.

La ley pide papel; falta el ancla

La ley ha empezado a responder. El Reglamento europeo de IA obliga, desde el 2 de agosto de 2025, a los proveedores de modelos de propósito general a mantener documentación técnica —arquitectura, número de parámetros, recursos de cómputo, descripción de los datos— y a publicar un «resumen suficientemente detallado» del contenido de entrenamiento según una plantilla de la Oficina de IA [5][6]. El incumplimiento se paga caro: hasta 15 millones de euros o el 3 % de la facturación mundial, y a partir del 2 de agosto de 2026 la Oficina podrá verificarlo; desde la misma fecha, el artículo 50 exige marcar de manera legible por máquina el contenido generado por IA [5][6]. La industria ha propuesto un AI-BOM, la lista de materiales de un modelo como la que ya existe para el software. El estándar CycloneDX le añadió el ML-BOM —datasets, modelos y configuraciones con su procedencia— (como hemos visto) y el proyecto AIBOM de OWASP impulsa su estandarización [7][8]. Pero aquí chocamos con el mismo muro: un BOM, como una tarjeta de modelo o un resumen de entrenamiento, es tan fiable como la voluntad de quien lo firma; un PDF de cumplimiento es solo un PDF y nada impide retocarlo mañana.

Por qué el manifiesto por sí solo no salva

Hay que decirlo con crudeza: publicar un resumen de entrenamiento o un *hash* de los pesos en un fichero LÉEME no demuestra nada si aquel fichero se puede cambiar sin dejar rastro. Un proveedor que, después de un incidente como el de LAION, editara discretamente su tarjeta de modelo para quitar una fuente incómoda, no dejaría ninguna huella de haberlo hecho. Un *hash* de pesos sin una **fecha cierta e independiente** no distingue el original de la versión retocada a posteriori. Y un AI-BOM almacenado en el mismo repositorio que controla quien lo ha de explicar es, en una disputa, papel de parte. Lo que falta no es el documento: es **un anclaje inalterable que fije quién declaró qué, y cuándo**.

La prueba de existencia aplicada

Es aquí donde **t2p** aporta la capa que falta, y lo hace sobre el artefacto digital, no sobre una foto del terreno. Al publicar un modelo se calcula la **huella SHA-512** del fichero de pesos y la del **manifiesto AI-BOM** —el resumen de datos de entrenamiento, el informe de evaluación y de seguridad, las licencias— y ambas se anclan con un **sello de tiempo RFC 3161 conforme a eIDAS** a la blockchain pública, dentro de un contenedor **.asice** verificable fuera de línea. Esto genera una prueba pública e inalterable de que *aquel* día el proveedor declaró *aquel* resumen de entrenamiento y *aquel* resultado de evaluación, y que *estos* pesos —por su huella— son los evaluados.

El efecto es directo sobre las tres opacidades. Sobre los **datos**, el resumen de entrenamiento queda con fecha cierta: si mañana hay que deprecar el modelo como LAION, no se puede fingir que nunca se declaró lo que se declaró. Sobre la **documentación**, la edición silenciosa posterior se vuelve detectable, porque el auditor puede confrontar la tarjeta actual con la versión sellada el día cero. Y sobre los **pesos**, cualquiera que despliegue el modelo recalcula la huella y la compara con el ancla: una sustitución al estilo *nullifAI* **falla la comprobación** antes de llegar a producción. Es, sobre el modelo, el complemento de lo que proponen los capítulos 13 y 15 respecto a la salida: la marca C2PA y SynthID sellan **lo que un modelo produce** —Google ya ha marcado con SynthID más de cien mil millones de contenidos [10]—; t2p sella **lo que un modelo es**.

Ahora el límite, con toda la crudeza, porque aquí es esencial. «Basura a la entrada, basura en la cadena»: el sello prueba que el proveedor **se comprometió** con un resumen de entrenamiento determinado y que los pesos coinciden con una huella en un instante; **no prueba que el resumen sea verdad** —que los datos fueran realmente solo los declarados—, ni que el modelo sea seguro, ni detecta un envenenamiento hábil del conjunto. Liga una afirmación a una fecha y a un autor; no verifica su contenido. En Stanford el material ilegal lo han tenido que encontrar **humanos** auditando; ningún sello lo habría hecho por su cuenta. La prueba de existencia no sustituye la auditoría del *dataset*, el *red-teaming* ni la marca de agua: los hace **responsables**, porque impide negar después lo que se declaró antes.

La promesa y el peligro

La promesa es un ecosistema de IA donde el linaje es **verificable**: poder demostrar con qué datos, qué versión y qué evaluación se construyó un modelo, y que los pesos que corren en producción son los auditados, con una responsabilidad que sobrevive a los incidentes. En una industria donde un fichero de pesos viaja de mano en mano sin ningún recibo, hacer el origen inalterable protege tanto al desplegador honesto como al público.

El peligro pide los matices de siempre. Primero, hay que recordar que **el sello no prueba la veracidad del resumen de entrenamiento**; un documento falso y sellado sigue siendo falso, y ahora, además, inmutable, y genera una falsa tranquilidad —«está anclado, luego es seguro»— que no se corresponde con nada. Segundo, la **concentración**: si solo los grandes laboratorios pueden sellar y documentar, el estándar puede expulsar a los modelos abiertos en lugar de fortalecerlos, consolidando un poder de mercado que podría limitar la diversidad y la innovación. Tercero, la tensión entre publicar el resumen de entrenamiento como prueba de gobernanza y preservar el secreto industrial legítimo; hay que equilibrar la transparencia necesaria con la protección de propiedades intelectuales y ventajas competitivas. La prueba de existencia es una capa de gobernanza del modelo, no un certificado de bondad ni un sustituto del juicio experto que sabe auditar un corpus.

Además, sellar la procedencia de un modelo no resuelve la dificultad fundamental de comprender los criterios de decisión que se generan dentro de las redes neuronales profundas. Como señala Cathy O'Neil,

estos sistemas son «opacos e invisibles excepto para los sacerdotes del sector: los matemáticos y los ingenieros» [11]. Esto crea una nueva forma de poder concentrado: solo quien tiene acceso a la expertise interna puede descifrar o manipular las lógicas subyacentes, mientras que el público e incluso los reguladores se quedan con un sello de autenticidad sin saber *por qué* el modelo actúa como lo hace. En paralelo, el marco legal que debería frenar esta asimetría retrocede: como hemos visto, la Unión Europea ha aplazado las obligaciones para la IA de alto riesgo de 2026 hasta el periodo 2027-2028 [12], y el estado de Colorado ha suprimido completamente su ley de IA, eliminando el deber de no discriminar [12]. Este retroceso normativo favorece un entorno donde la vigilancia se vuelve más difícil y el poder de quienes controlan los modelos se intensifica sin ningún contrapeso efectivo.

Un refuerzo inesperado viene de las propias IA públicas, ya que muchas de ellas producen registros intrínsecamente auditables. La herramienta **Policy Synth**, diseñada por Beth Noveck, genera un registro detallado —cita a cita— de todas las acciones de sus agentes, y cada salida viene acompañada de su origen documental [13]. Esto significa que, más allá del sello blockchain que garantiza la inmutabilidad, ya existe una capa de trazabilidad: cualquier auditor puede seguir el hilo de decisiones hasta la fuente original sin depender de un único proveedor. A escala municipal, ciudades como Helsinki y Ámsterdam publicaron sus primeros inventarios algorítmicos (2020), exponiendo los datos de entrenamiento y los mecanismos de supervisión humana para cada sistema [14]. Anclar estos logs e inventarios con una prueba de existencia neutral los convierte en **no repudiables** y verificables por cualquier actor, eliminando la necesidad de «confiar en la web de la administración» y añadiendo un nuevo nivel de confianza descentralizada al tejido de gobernanza algorítmica.

Es hora de actuar

Para los **proveedores de modelos** (OpenAI, Google, Meta, Mistral, los laboratorios de peso abierto): sellar el AI-BOM al publicar —huella de los pesos, resumen de entrenamiento e informe de evaluación— para que el linaje tenga fecha cierta. Para los **desplegadores y las empresas** que integran modelos: verificar que los pesos que ejecutan coinciden con la huella sellada antes de desplegarlos y exigir un AI-BOM anclado al proveedor como requisito de compra. Para los **repositorios de modelos** (Hugging Face): anclar la huella de cada modelo al subirlo, de manera que una sustitución maliciosa sea detectable. Y para los **auditores y reguladores** (la Oficina de IA): reconocer el AI-BOM sellado como evidencia de la documentación que el artículo 53 ya exige y tratar la fecha cierta como la diferencia entre una declaración y una coartada fabricada después.

En Stanford, un grupo de investigadores tuvo que auditar desde fuera un modelo que ya corría en todo el mundo para descubrir qué contenía. Dar a cada modelo una prueba sellada de con qué se ha entrenado, quién lo ha hecho y qué pesos son los correctos —sin olvidar nunca que el sello no hace verdadero lo que se declara en él— es, en este frente donde la máquina aprende de nosotros, **time2act**.

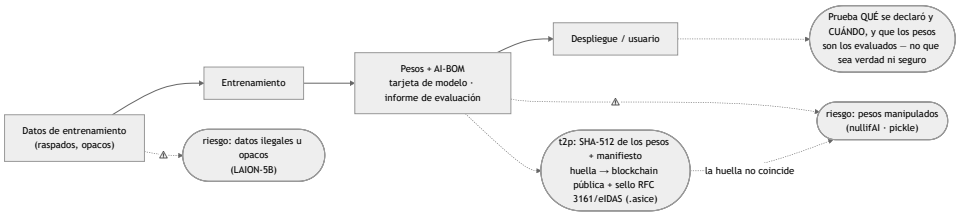


Figura 79.1 — El ciclo de vida de un modelo en cuatro eslabones: datos de entrenamiento → entrenamiento → pesos + AI-BOM (tarjeta de modelo, informe de evaluación) → despliegue. t2p ancla la huella SHA-512 de los pesos y del manifiesto en la blockchain pública, con sello RFC 3161/eIDAS complementario (.asice). Dos puntos de riesgo: datos ilegales u opacos en el origen (LAION-5B) y pesos manipulados entre el laboratorio y el usuario (puerta trasera nullifAI *vía* pickle*), que la comprobación de huella detecta. Límite: el sello prueba qué se declaró y cuándo, y que los pesos son los evaluados; no prueba que la declaración sea cierta ni que el modelo sea seguro. Fuentes: Stanford Internet Observatory (LAION-5B); JFrog (modelos maliciosos); Reglamento europeo de IA, art. 53 y 50; CycloneDX ML-BOM.*

[1] Stanford Internet Observatory / 404 Media — *Largest Dataset Powering AI Images Removed After Discovery of Child Sexual Abuse Material* (diciembre de 2023; 3.226 casos sospechosos en LAION-5B; recomendación de deprecar los modelos). https://www.404media.co/laion-datasets-removed-stanford-csam-child-abuse/ ↩

[2] LAION — *Releasing Re-LAION-5B: transparent iteration on LAION-5B with additional safety fixes* (agosto de 2024; 2.236 enlaces eliminados). https://laion.ai/blog/relaion-5b/ ↩

[3] JFrog Security Research — *Data Scientists Targeted by Malicious Hugging Face ML Models with Silent Backdoor* (2024; técnica *nullifAI*, abuso de *pickle*, puerta trasera). https://jfrog.com/blog/data-scientists-targeted-by-malicious-hugging-face-ml-models-with-silent-backdoor/ ↩

[4] The Hacker News — *Over 100 Malicious AI/ML Models Found on Hugging Face Platform* (marzo de 2024). https://thehackernews.com/2024/03/over-100-malicious-aiml-models-found-on.html ↩

[5] EU Artificial Intelligence Act — *Article 53: Obligations for providers of general-purpose AI models* (documentación técnica Anexo XI; resumen del contenido de entrenamiento; sanciones de hasta 15 M€ o 3 %). https://artificialintelligenceact.eu/article/53/ ↩

[6] Comisión Europea — *General-Purpose AI Models in the AI Act: Questions & Answers* (plantilla del resumen de entrenamiento; aplicación desde el 2 de agosto de 2025; marcado del art. 50 desde el 2 de agosto de 2026). https://digital-strategy.ec.europa.eu/en/faqs/general-purpose-ai-models-ai-act-questions-answers ↩

[7] CycloneDX (OWASP) — *Machine Learning Bill of Materials (AI/ML-BOM)* (datasets, modelos y configuraciones con procedencia; desde la v1.5, 2023). https://cyclonedx.org/capabilities/mlbom/ ↩

[8] *Operationalising AI bills of materials for verifiable AI provenance and lifecycle assurance* (Frontiers in Computer Science, 2026). https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2026.1735919/full ↩

[9] Margaret Mitchell et al. — *Model Cards for Model Reporting* (2019). https://arxiv.org/abs/1810.03993 ↩

[10] Google / C2PA — *How Google and the C2PA are increasing transparency for gen AI content* (SynthID: más de 100.000 millones de contenidos marcados según Google I/O 2026 (mayo de 2026); credenciales de contenido). https://blog.google/innovation-and-ai/products/google-gen-ai-content-transparency-c2pa/ ↩

[11] Cathy O'Neil — *Armas de destrucción matemática* (Capitán Swing, 2018). ↩

[12] Consejo de la UE / Pinsent Masons (2026). https://www.pinsentmasons.com/out-law/news/rules-high-risk-ai-delayed-under-eu-omnibus-deal ↩

[13] Beth Simone Noveck — *Reboot* (Yale UP, 2026), cap. 6. ↩

[14] VentureBeat (2020). https://venturebeat.com/ai/amsterdam-and-helsinki-launch-algorithm-registries-to-bring-transparency-to-public-deployments-of-ai ↩

Los agentes de IA: el mandato verificable

«Como ahora no tenemos ninguna manera de hacer sabios a los ordenadores, ahora no deberíamos encargarles tareas que exigen sabiduría.»

— Joseph Weizenbaum, Computer Power and Human Reason (1976)

Noviembre de 2022. Jake Moffatt, un canadiense que acaba de perder a su abuela, consulta la web de Air Canada el mismo día. El chatbot de la compañía le explica, servicial, una política que no existe: que puede comprar el billete a precio completo y pedir después, en 90 días, la tarifa de duelo. Moffatt compra —1.630,36 dólares canadienses. Cuando reclama, la compañía le responde que la política real no se aplica a viajes ya hechos, y se niega. En febrero de 2024, el tribunal civil de la Columbia Británica condena a Air Canada a pagarle 812 dólares: la compañía «no tuvo el cuidado razonable de garantizar que su chatbot fuera exacto» [1]. Y deja una frase para la historia: «debería ser obvio para Air Canada que es responsable de toda la información de su web; da igual que venga de una página estática o de un chatbot». Por el camino, la compañía había llegado a alegar que el chatbot era «una entidad legal separada», responsable de sus propios actos. El tribunal no se lo tragó [1].

Aquello era solo un chatbot que informaba. Lo que ya está aquí son agentes que actúan: compran billetes, contratan servicios, responden a clientes, mueven dinero. Cada acto de un agente es un acto jurídico de quien lo ha activado —y cada error, una disputa a tres bandas: el usuario, que sostiene que no autorizó aquello; la plataforma del agente, que asegura que ejecutó lo que le ordenaron; y el comercio, que recibió una orden aparentemente válida.

Este capítulo trata la delegación en máquinas que se equivocan. Qué es el modelo por dentro —los datos, los pesos, el AI-BOM— se trata en el capítulo 79; los registros de acciones de los agentes del sector público, en el capítulo 107; la identidad de quien contratas en remoto, en el capítulo 91; la suplantación de directivos que ordena transferencias, en el capítulo 87. Pregunta clave: cuando la compra sale mal, ¿cómo se prueba qué autorizaste exactamente —y qué hizo exactamente el agente? Respuesta: con el mandato y el registro de acciones sellados con **t2p** —el paquete probatorio del capítulo 13 [3]— en una capa neutral que ninguna de las tres partes interesadas controla.

La industria ya construye el mandato

Lee el panorama con los ojos de este libro, porque es revelador [2]. Visa, con Intelligent Commerce, emite credenciales tokenizadas de alcance limitado para agentes: un token para el agente de viajes válido solo para una aerolínea y una ventana de fechas; un token con límite de 200 dólares que no puede autorizar una compra de 500. Mastercard anunció en abril de 2025 Agent Pay: agentes verificados que transaccionan con «Agentic Tokens» que ligan la credencial de pago a un agente concreto, un ámbito de comercios y una política de consentimiento. Y Google publicó en septiembre de 2025 el protocolo abierto AP2, con más de sesenta socios —Mastercard, American Express, PayPal, Coinbase, Salesforce—, que define dos piezas con nombres reveladores: el «Intent Mandate» —qué quiere el usuario— y el «Cart Mandate» —qué propone comprar el agente—, ambos firmados como credenciales verificables [2]. Mientras tanto, los agentes mismos ya son productos de consumo: Operator de OpenAI, Project Mariner de Google, Computer Use de Anthropic, los agentes de Microsoft Copilot [2].

Fíjate en el vocabulario: mandatos, credenciales verificables, alcance, consentimiento. Es el lenguaje del derecho civil de toda la vida, reescrito en criptografía. La industria de pagos ha entendido antes que nadie que el problema de los agentes es el mandato.

Pero cada solución vive dentro de su ecosistema —la de Visa mira el pago Visa; la de Google, su protocolo — y todas miran el momento de pagar. La disputa, en cambio, llega después y es más amplia: qué autorizaste, qué vio el agente, qué hizo, en qué orden. Y la evidencia de esto no puede vivir en casa de ninguna de las tres partes interesadas —ni en el móvil del usuario que reclama, ni en los servidores de la plataforma que se defiende, ni en los sistemas del comercio que cobró. Falta la capa neutral.

La prueba de existencia aplicada

Cuatro gestos convierten la delegación en un hecho auditable [3].

1. El mandato sellado

Antes de activar el agente, el usuario —o la empresa— redacta el mandato: presupuesto máximo, ámbitos permitidos, vetos, duración. El documento se sella con t2p: huella SHA-512 calculada en el dispositivo, fecha cierta, anclaje [3]. No hace falta que nadie más lo vea: el día de la disputa, el mandato existía con este contenido exacto antes de la primera acción del agente. El «yo no autoricé esto» y el «sí que lo autorizaste» dejan de ser un pulso de memorias: hay un texto, con una fecha.

2. El registro de acciones anclado

El agente genera su registro —qué ha hecho, cuándo, sobre qué sitios— y este registro se sella periódicamente por lotes: la huella de cada tramo, encadenada con la anterior [3], como los registros de facturación del capítulo 34. La plataforma que lo ofrece de serie convierte la caja negra de su agente en un historial auditable —y se protege a sí misma: ante el cliente que niega haber recibido el resumen, o el comercio que alega una orden fantasma, el registro anclado responde.

3. El instante de la oferta

Los precios y las condiciones cambian por segundos; el agente decide sobre lo que ve ahora. La captura certificada de lo que el agente tenía delante —la página de la oferta, con imagen completa y código fuente [3]— congela el instante de la decisión. Cuando el comercio diga «este precio nunca existió», o el usuario diga «la oferta prometía otra cosa», la pantalla de aquel momento tiene fecha cierta. Es la lección de Air Canada [1], llevada al mundo de los agentes: la información sobre la que se actuó, preservada.

4. La autorización fuerte

Por debajo del umbral que el usuario haya fijado en el mandato, el agente va solo; por encima —la compra grande, el contrato nuevo, el pago inusual—, el acto requiere la aprobación humana explícita: la firma con vídeo-selfie de t2p, con sus dos retos de vida aleatorios y la verificación biométrica del dispositivo [3]. La aprobación queda ligada al acto concreto, con fecha cierta. Ni el usuario puede negar lo que aprobó mirando a la cámara, ni nadie puede hacer pasar por aprobado lo que nunca se sometió.

Los límites, dichos claramente: el sello no hace al agente más listo —no evita la alucinación ni el error: los detecta, los data y los hace atribuibles. La responsabilidad final la reparten los contratos y los tribunales —y Air Canada [1] fijó el principio: quien despliega el agente responde de lo que el agente dice y hace. Y no todo tiene que ser un agente: hay actos —los más personales— que merecen manos humanas de principio a fin.

La promesa y el peligro

La promesa: delegación con confianza —el usuario que activa un agente sabiendo que el mandato y cada acción tienen fecha cierta [3]; disputas que se resuelven en minutos comparando mandato, registro y captura, en lugar de años de litigio [1]; plataformas que compiten por auditabilidad; y la infraestructura de mandatos que la industria ya construye [2], completada con la capa neutral que ninguna de las partes controla.

Los peligros, mirados de cara.

El primero es **la vida entera en el registro**. El registro de acciones de un agente personal es un diario íntimo: qué compras, qué lees, qué negocias. Ha de quedar en el dispositivo o en los sistemas del usuario —solo huellas en la cadena [3]—, con revelación selectiva del tramo disputado, nunca de la vida entera.

El segundo es **el agente como coartada**. «Lo hizo el agente» no puede convertirse en la versión digital de «no fui yo». El mandato datado delimita responsabilidades, no las borra: quien activa un agente con un mandato amplio asume lo que cabe dentro; quien lo despliega comercialmente responde ante el cliente —el principio de Air Canada [1]. El rastro sirve para repartir bien las culpas, no para hacerlas desaparecer.

El tercero es **la carrera de agentes**. El comercio también tiene sus agentes, y la asimetría se reproduce: el gigante con flota de agentes y registros perfectos frente al consumidor con un móvil. La neutralidad de la prueba es el mínimo; la protección del más débil, como siempre, es regulatoria.

Y el cuarto es **el tecnosolucionismo agéntico**. Ningún sello hace que delegar sea siempre buena idea. El agente es una herramienta para tareas delegables; el criterio sobre qué se delega —y qué no— sigue

siendo la decisión más humana de todas.

Es hora de actuar

Que la delegación tenga memoria.

Para quien activa agentes —personas y empresas: mandato por escrito y sellado antes de activar [3]; umbrales de aprobación humana para los actos grandes; y el registro, exportado y anclado periódicamente.

Para las plataformas de agentes: registro de acciones auditable y anclado de serie [2][3] —vuestra defensa en la disputa y vuestro argumento de venta; y que el mandato del usuario sea un objeto verificable, no una casilla aceptada.

Para los comercios: capturad y anclad lo que servís a los agentes —la oferta, el precio, las condiciones del instante [3]; la disputa de mañana se gana con la pantalla de hoy.

Para las redes de pago y los protocolos: vuestros mandatos firmados [2] son el fundamento; abridlos al anclaje neutral para que la prueba sobreviva a cualquiera de vosotros.

Para los reguladores y legisladores: el principio de Air Canada [1] —quien despliega responde— merece rango de norma; y todo agente que actúe ante consumidores debería tener mandato datado y registro auditable como condición de operación.

Delegamos porque la vida no nos cabe en las manos; que la delegación tenga memoria. Cuando tu agente compre, contrate y responda por ti, que tú puedas probar qué le ordenaste —y él, qué hizo. Por una delegación con fecha cierta, **time2act**.

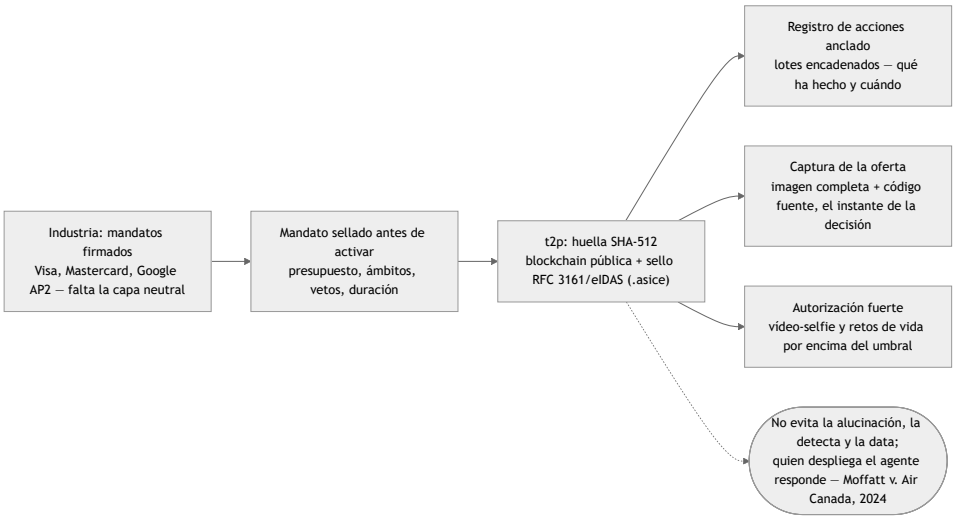


Figura 80.1 — El mandato verificable para agentes de IA con prueba de existencia (sellado con t2p — capítulo 13): el mandato sellado antes de activar (presupuesto, ámbitos, vetos), el registro de acciones anclado por lotes encadenados, la captura certificada de la oferta que el agente vio (imagen + código fuente) y la autorización fuerte con vídeo-selfie por encima del umbral. Contexto: la industria ya construye mandatos firmados (Visa Intelligent Commerce, Mastercard Agent Pay, Google AP2 —Intent/Cart Mandate como credenciales verificables); la capa que falta es la neutral entre usuario, plataforma y comercio. Precedente: Moffatt v. Air Canada (2024) —quien despliega el agente responde. Fuentes: tribunal de la Columbia Británica; Visa/Mastercard/Google AP2.

---

[1] CBC News — *Air Canada found liable for chatbot's bad advice on bereavement rates* (Moffatt v. Air Canada, B.C. Civil Resolution Tribunal, febrero de 2024: el chatbot inventó una política de tarifa de duelo; 812 $ canadienses de compensación sobre 1.630,36 pagados; «Air Canada no tuvo el cuidado razonable de garantizar que su chatbot fuera exacto»; «es responsable de toda la información de su web —da igual que venga de una página estática o de un chatbot»); Forbes — *What Air Canada Lost In 'Remarkable' Lying AI Chatbot Case* (la alegación de que el chatbot era «una entidad legal separada»); McCarthy Tétrault — *Moffatt v. Air Canada: A Misrepresentation by an AI Chatbot*. https://www.cbc.ca/news/canada/british-columbia/air-canada-chatbot-lawsuit-1.7116416 · https://www.forbes.com/sites/marisagarcia/2024/02/19/what-air-canada-lost-in-remarkable-lying-ai-chatbot-case/ · https://www.mccarthy.ca/en/insights/blogs/techlex/moffatt-v-air-canada-misrepresentation-ai-chatbot ↩

[2] Visa — *Intelligent Commerce* (credenciales tokenizadas de alcance limitado para agentes; servidor MCP; un token de 200 $ no puede autorizar 500 $); Mastercard — *Agent Pay* (anunciado el 29-4-2025: Agentic Tokens que ligan credencial, agente,

ámbito de comercios y política de consentimiento; «Agent Pay for Machines», junio de 2026); Google AP2 (septiembre de 2025, 60+ socios: Intent Mandate + Cart Mandate firmados como credenciales verificables); Eco/Paz — guías del comercio agéntico 2026 (runtimes: OpenAI Operator, Google Project Mariner, Anthropic Computer Use, Microsoft Copilot). https://www.visa.com/en-us/solutions/intelligent-commerce · https://www.mastercard.com/us/en/news-and-trends/press/2026/june/mastercard-launches-agent-pay-for-machines.html · https://eco.com/support/en/articles/14839400-what-is-agentic-commerce-the-2026-guide · https://www.paz.ai/glossary/agentic-commerce-protocol-acp ↩

[3] t2p — manual de producto (certificar cualquier fichero —el mandato y los registros, solo la huella viaja; captura de página web con imagen completa + código fuente; firma con vídeo-selfie, dos retos de vida aleatorios y verificación biométrica del dispositivo; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; la procedencia de los modelos, en el capítulo 79; los agentes del sector público, en el capítulo 107. ↩

Tu cara, tu voz: derechos de imagen y réplicas digitales

«El número de serie de un ejemplar humano es la cara, esa combinación accidental e irrepetible de rasgos.»

— Milan Kundera, La inmortalidad (1990)

En octubre de 2023, **Tom Hanks** tuvo que avisar a sus seguidores por Instagram de algo extraño: «Hay un vídeo por ahí que promociona un plan dental con una versión de IA de mí. No tengo nada que ver con él» [1]. Meses después, la actriz **Scarlett Johansson** explicaba que había rechazado la petición de OpenAI de prestar su voz a ChatGPT, y que la empresa había lanzado igualmente una voz —«Sky»— que se le parecía tanto que un análisis forense de la Universidad Estatal de Arizona la encontró más parecida a la de Johansson que la del **98 %** de las demás actrices examinadas; OpenAI la retiró tras recibir cartas de sus abogados [2]. En ambos casos, la persona tuvo que salir a desmentirlo **después**, sin ninguna manera de probar, de entrada, que nunca había dado permiso. La carga recaía sobre la víctima.

Esta es la pregunta de este capítulo, distinta de la del capítulo 40 —la autoría de una obra— y de la del capítulo 67 —la actuación en directo y los derechos de reproducción. Aquí la **obra protegida eres tú**: tu cara, tu voz, tu cuerpo. Y la pregunta no es quién lo ha hecho, sino **¿lo consentiste, para qué uso, y se puede demostrar?** Porque generar una réplica digital de alguien se ha vuelto trivial, y desmentirla, no.

Una cara que ya no es tuya

El problema tiene tres formas. La primera son los **anuncios fraudulentos**: rostros famosos —Hanks, Johansson— pero también personas anónimas— pegados a productos que nunca han avalado, en una oleada de estafas que se multiplica porque fabricarlas cuesta minutos. La segunda es el **miedo de los profesionales de la voz y la imagen**: como hemos visto, en 2023 los actores de Hollywood hicieron huelga durante meses y una de sus líneas rojas eran precisamente las **réplicas digitales**; el acuerdo que cerró la huelga exige consentimiento informado para crear o reutilizar la réplica de un intérprete, con una «descripción razonablemente específica» del uso previsto, y un consentimiento **nuevo** —y una paga nueva — si la réplica se traslada a otro proyecto [3]. La tercera es la **resurrección de los muertos**: voces y caras de difuntos reanimadas para vender o entretener sin que nadie pueda decir si la familia lo autorizó. En las tres, la misma asimetría: es fácil falsificar y difícil desmentir, y quien sufre el daño ha de perseguir cada copia una por una.

La ley reconoce el derecho; falta el recibo

La ley ha reaccionado con una rapidez inusual. En Tennessee, la **ELVIS Act** —*Ensuring Likeness, Voice and Image Security*— entró en vigor el 1 de julio de 2024 e incorporó la **voz** al derecho de publicidad, creando incluso responsabilidad para quien distribuya una herramienta de IA cuya finalidad principal sea imitar la voz o la imagen de alguien [4]. En Estados Unidos, la **NO FAKES Act** —que crearía un derecho federal sobre la réplica digital— superó el 18 de junio de 2026 la Comisión Judicial del Senado por unanimidad, aunque todavía ha de pasar el pleno del Senado y la Cámara de Representantes [5]. Y Dinamarca ha dado el paso más radical: en junio de 2025 presentó una reforma de su ley de propiedad intelectual —aún en trámite parlamentario, con entrada en vigor prevista a mediados de 2026— para dar a **cada persona un derecho de tipo copyright sobre su propia cara, cuerpo y voz**, con derecho a exigir la retirada de los *deepfakes* y una compensación, protección hasta cincuenta años después de la muerte y excepciones para la parodia y la sátira [6]. En Europa, el artículo 50 del Reglamento de IA obligará a **marcar** el contenido generado por IA [véase capítulo 79]. Pero todas estas leyes chocan, a la hora de la verdad, con una sola pregunta: **¿esta persona consintió este uso, y dónde está la prueba?** Hoy el consentimiento es un PDF en un cajón —o no es nada.

Por qué la ley por sí sola no salva

Hay que decirlo con crudeza: un derecho de publicidad vale tanto como la evidencia que lo sostiene. Cuando aparece un anuncio con tu cara, tienes que demostrar que **no** consentiste —probar un hecho negativo—, y la plataforma ha de decidir en horas si lo retira. Un contrato de cesión guardado en el

servidor de un estudio se puede retocar o retrodatar; un estudio sin escrúpulos puede alegar «ya estuvo de acuerdo» y enseñar un papel. Sin un registro de consentimiento **verificable y con fecha cierta**, cada disputa se convierte en tu palabra contra la suya, y gana quien tiene más abogados. El derecho existe; lo que falta es el **recibo inalterable**.

La prueba de existencia aplicada

Es aquí donde **t2p** aporta dos capas complementarias. La primera la controla la **persona**: con una **prueba de vida**, crea un *registro de consentimiento de la imagen* que liga una **referencia biométrica** —la huella SHA-512 de una muestra de rostro o voz, que **no sale del dispositivo**— a una concesión explícita y **acotada**: qué usos autoriza, para quién y hasta cuándo. Todo ello se sella con un **sello de tiempo RFC 3161/eIDAS** y se ancla a la **blockchain pública** dentro de un contenedor **.asice**. Una réplica digital legítima lleva entonces un **puntero verificable** a un consentimiento sellado y vigente; y la **revocación** también queda sellada y datada, de manera que nadie puede alegar un permiso que ya se había retirado. La segunda capa la sella el **estudio o el anunciante** en el momento de firmar: el consentimiento informado al estilo del acuerdo de los actores, con la descripción específica del uso y la prueba de vida del intérprete, de manera que reutilizar la réplica en otro proyecto sin un consentimiento nuevo se vuelve **detectable**.

El efecto es que la carga de la prueba cambia de bando. El caso de Hanks deja de depender de su palabra: puede mostrar que **nunca** emitió ninguna concesión sellada para aquel anuncio dental, y la **ausencia** de un permiso anclado se convierte, ella misma, en prueba de la falta de consentimiento. Se combina con la procedencia de los capítulos 13 y 15: la marca C2PA o SynthID dice «esto es sintético»; el registro de consentimiento añade «y nadie autorizó esta cara».

Ahora el límite, con toda la crudeza. «Basura a la entrada, basura en la cadena»: el sello prueba que el consentimiento se dio —o no—, de quién y cuándo; **no detecta el *deepfake*** por su cuenta (eso depende de la marca de procedencia y de los detectores), **no impide su creación**, y un consentimiento sellado bajo presión sigue siendo un consentimiento viciado, ahora además inmutable. Prueba el **acto** de consentir, no su **justicia**. Lo que hace es sacar las disputas del terreno de la palabra contra palabra y llevarlas al de «enseña la concesión sellada».

La promesa y el peligro

La promesa es un mundo donde tu cara y tu voz vuelven a ser tuyas de manera **demostrable**: los intérpretes licencian sus réplicas con un consentimiento datado, acotado y revocable; las plataformas y los tribunales disponen de un registro para distinguir el uso autorizado de la violación; y los difuntos quedan protegidos por concesiones selladas por sus herederos. En una época en que cualquier cara se puede clonar en minutos, hacer el consentimiento inmutable es devolver el control a la persona.

El peligro pide matices. Primero, un consentimiento **arrancado por coacción** y sellado no deja de ser injusto porque sea inmutable. Segundo, construir un registro de referencias biométricas es sensible: por eso la regla de oro —la cara **no sale del dispositivo**, solo se sella una huella— ha de sustituir cualquier base central de rostros que sería un sueño para la vigilancia. Tercero, hay que evitar que los estudios acaben custodiando las fichas de imagen de todo el mundo. Y cuarto, no hay que confundir la ausencia de consentimiento con usos legítimos —parodia, sátira, crítica, información— que la normativa ya protege. La prueba de existencia es una capa de control sobre la propia imagen, no un permiso automático ni un detector de falsedades.

Además, delegar la gestión biométrica a redes descentralizadas no elimina el riesgo de que el control efectivo se concentre en manos de unos pocos actores técnicos. La infraestructura necesaria para crear y validar huellas digitales requiere servidores potentes, acceso a bases de datos masivas y una capa de software compleja que solo un número limitado de empresas puede desarrollar y mantener. Como señala Marc Goodman, Facebook —y no un programa estatal— es «el almacén más extenso de datos biométricos que hay sobre la Tierra, superando con creces el de cualquier gobierno»[11]. Esto muestra cómo una plataforma privada puede acumular información biográfica a escala global, convirtiéndose en un punto de entrada privilegiado para la captura y la explotación de las huellas. Por tanto, incluso con protocolos que garantizan que la cara no salga del dispositivo, hay que establecer mecanismos de gobernanza y auditoría independientes que impidan que esta concentración técnica se traduzca en un poder real sobre la identidad de las personas.

Como hemos visto, el ejemplo de **PalmerAI** en el caucus demócrata de Samoa Americana ilustra cómo la pregunta ya no es «¿es real el vídeo?», sino «¿qué dijo la persona y qué dice la réplica?»[12]. El avance de un avatar que reproducía la voz y el aspecto de Jason Palmer, capaz de ganar una elección con 51-40 puntos, pone de relieve un vacío: el votante necesita saber si el mensaje proviene del candidato o de una entidad digital. Un anclaje neutral en blockchain puede registrar cada declaración con una prueba de existencia inmutable, vinculada al certificado de consentimiento original y a la clave privada del titular. Así, cualquier observador podría trazar el origen del discurso y validarlo sin depender de plataformas centralizadas. No obstante, el mismo mecanismo puede crear un nuevo riesgo: si las claves se comprometen o se emplean por parte de un grupo de poder, la cadena certificadora podría ser utilizada para legitimar réplicas manipuladas, convirtiéndose en una «capa de confianza» que, mal gobernada, refuerza la concentración de control sobre el discurso político y social.

Es hora de actuar

Para las **personas y los intérpretes**: sellar un registro de consentimiento de la imagen acotado y revocable, manteniendo la referencia biométrica privada en el dispositivo. Para los **estudios, anunciantes y proveedores de herramientas de IA**: sellar el consentimiento informado al firmar, con el alcance específico del uso, y **verificar una concesión vigente** antes de generar ninguna réplica. Para las **plataformas** donde corren los anuncios: exigir un puntero de consentimiento verificable para cualquier aval sintético, y tratar su ausencia como señal de retirada. Y para los **legisladores y tribunales** (ELVIS Act, NO FAKES, Dinamarca, el Reglamento europeo): reconocer el registro de consentimiento sellado como evidencia con fecha cierta del consentimiento —o de su falta.

Tom Hanks tuvo que salir a decir que la cara que vendía planes dentales no era la suya. Dar a cada persona una prueba sellada de qué autoriza su imagen, para quién y hasta cuándo —sin olvidar nunca que el sello prueba el consentimiento, no su justicia— es, en este frente donde nos pueden robar la cara, **time2act**.

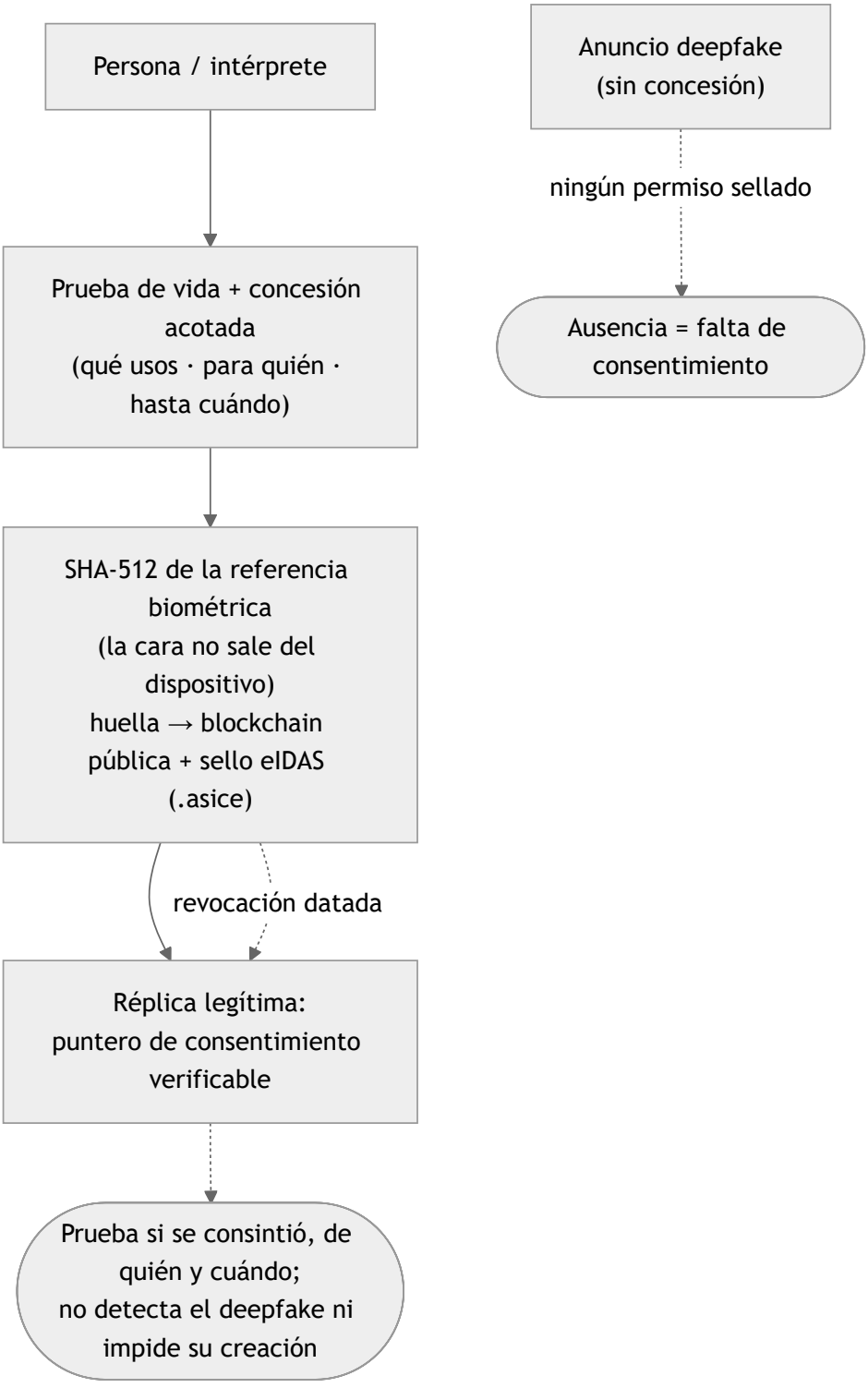


Figura 81.1 — Dos vías. Arriba: la persona crea, con prueba de vida, una concesión de consentimiento acotada (qué usos, para quién, hasta cuándo) ligada a una referencia biométrica (huella SHA-512; la cara no sale del dispositivo), anclada a la blockchain pública, con sello eIDAS complementario (.asice); una réplica legítima lleva un puntero verificable, y la revocación queda datada. Abajo: un anuncio deepfake sin ninguna concesión sellada —la ausencia misma demuestra la falta de consentimiento. Límite: el sello prueba si se consintió, de quién y cuándo; no detecta el deepfake ni impide su creación, y no juzga si el consentimiento fue libre. Fuentes: caso Tom Hanks; caso Johansson–OpenAI; acuerdo SAG-AFTRA; ELVIS Act; reforma danesa.

[1] Voicebot.ai — *Tom Hanks Warns of Deepfake Hanks Dental Ad* (octubre de 2023; «I have nothing to do with it»). https://voicebot.ai/2023/10/02/tom-hanks-warns-of-deepfake-hanks-dental-ad/ ↩

[2] NPR — *OpenAI pulls AI voice that was compared to Scarlett Johansson in the movie 'Her'* (mayo de 2024; análisis forense de la Universidad Estatal de Arizona: más parecida que el 98 % de las actrices). https://www.npr.org/2024/05/20/1252495087/openai-pulls-ai-voice-that-was-compared-to-scarlett-johansson-in-the-movie-her ↩

[3] SAG-AFTRA / Perkins Coie — *How the 2023 SAG-AFTRA contract addresses generative AI and digital replicas* (consentimiento informado; descripción específica del uso; consentimiento nuevo para la reutilización). https://perkinscoie.com/insights/blog/generative-ai-movies-and-tv-how-2023-sag-aftra-and-wga-contracts-address-generative ↩

[4] Davis Wright Tremaine — *Tennessee Passes ELVIS Act (Ensuring Likeness, Voice and Image Security Act)* (en vigor el 1 de julio de 2024; la voz al derecho de publicidad; responsabilidad de las herramientas de IA). https://www.dwt.com/blogs/artificial-intelligence-law-advisor/2024/04/tennessee-elvis-act-ai-voice-replica ↩

[5] United States Senate Judiciary Committee — *NO FAKES Act (Nurture Originals, Foster Art, and Keep Entertainment Safe)* (derecho federal sobre la réplica digital; versión revisada de 2026, aprobada por la Comisión Judicial del Senado el 18 de junio de 2026). https://www.judiciary.senate.gov/no-fakes-act ↩

[6] World Economic Forum — *Deepfake legislation: Denmark takes action* (presentada en junio de 2025; derecho de tipo copyright sobre cara, cuerpo y voz; retirada y compensación; excepciones de parodia; en trámite parlamentario, entrada en vigor prevista a mediados de 2026). https://www.weforum.org/stories/2025/07/deepfake-legislation-denmark-digital-id/ ↩

[7] Variety — *Scarlett Johansson Reacts to OpenAI Sky Voice: 'Shocked' and 'Angered'* (mayo de 2024). https://variety.com/2024/digital/news/scarlett-johansson-responds-shocked-angered-openai-chatgpt-her-1236011135/

[8] SAG-AFTRA — *Digital Replicas 101* (tipología y derechos de consentimiento del intérprete). https://www.sagaftra.org/sites/default/files/sa_documents/DigitalReplicas.pdf

[9] Wikipedia — *ELVIS Act* (Ensuring Likeness, Voice and Image Security Act of 2024; reforma de la Personal Rights Protection Act de 1984). https://en.wikipedia.org/wiki/ELVIS_Act

[10] EU Artificial Intelligence Act — *Article 50: transparency obligations* (marcado del contenido generado o manipulado por IA). https://artificialintelligenceact.eu/article/50/

[11] Marc Goodman — *Delitos del futuro* (Ariel, 2015). ↩

[12] Wikipedia, *Jason Palmer (politician)*; TIME, *Albania's AI minister Diella* (2025). https://time.com/7324934/albania-ai-minister-diella/ ↩

Sharenting: la imagen de quien no puede consentir

«No hay niños: hay personas; pero con otra escala de conceptos, otro caudal de experiencia, otros impulsos, otro juego de sentimientos.»

— Janusz Korczak, Cuando vuelva a ser niño (1925)

El primer día de escuela, con la mochila nueva y la sonrisa a medio hacer. La fiesta de cumpleaños, los globos, el pastel. La tarde de playa. Y el gesto automático de cada vez: publicar. Ninguna malicia —amor, orgullo y la costumbre del siglo. El dato que lo enmarca [1]: un niño aparece de media en 1.300 fotografías publicadas en línea antes de cumplir los 13 años —un álbum público que él no ha elegido, indexado, replicable y permanente. Y los riesgos que el legislador francés enumeró al tramitar su ley no son hipotéticos: usurpación de identidad, chantaje, ciberacoso —y los peores [1].

El matiz que hace el capítulo entero: esto no va de culpar a padres. Va de una pregunta jurídica que nadie se había hecho hasta hace poco —¿quién consiente la imagen de quien todavía no puede consentir, y dónde queda escrito? ¿Quién puede demostrar que una publicación tenía el permiso de ambos progenitores, o que uno se negó? ¿Dónde está la autorización que la escuela dice que tenía?

Este capítulo trata el consentimiento sobre la imagen de los menores —y cómo acreditarlo. El derecho de imagen de los adultos —la obra protegida eres tú— está en el capítulo 81; la difusión de imágenes íntimas, en el capítulo 83; el odio y el acoso a los jóvenes, en el capítulo 84; la coparentalidad —donde el menor nunca es objeto de registro—, en el capítulo 53; la escuela, en el capítulo 19. Pregunta clave: ¿cómo se protege el derecho de alguien que todavía no lo puede ejercer? Respuesta: documentando las decisiones de los adultos que lo custodian —la autorización, la negativa, la petición de retirada— con fecha cierta: **t2p**, la mecánica de siempre, la del capítulo 13 [3]. Se documentan consentimientos; nunca el menor —la línea del capítulo 53, aquí, es sagrada.

Francia escribe lo que nadie había escrito

El 19 de febrero de 2024, el Parlamento francés aprobó —por unanimidad— la Ley 2024-120, que garantiza el respeto del derecho a la imagen de los niños [1]. La reforma toca el corazón del derecho de familia: el artículo 371-1 del Código civil dice ahora, expresamente, que la autoridad parental incluye la protección de la vida privada del menor y de su derecho a la imagen; que los padres lo protegen en común; y que han de asociar al niño según su edad y madurez. Y la pieza más contundente: si la difusión de la imagen del hijo por sus propios padres atenta gravemente contra su dignidad o su integridad moral, el juez puede delegar en un tercero el ejercicio del derecho de imagen del menor —retirárselo a los padres [1].

En España, el marco protege al menor con intensidad —la ley orgánica que ampara el honor, la intimidad y la propia imagen, la de protección jurídica del menor, la vigilancia del Ministerio Fiscal [2]— y los tribunales ya exigen el acuerdo de ambos progenitores para publicar imágenes de los hijos: la negativa de uno debería detener la difusión [2].

Y aquí, el diagnóstico de este libro: el consenso legal existe; su prueba, no. Todo el edificio —el consentimiento común, la negativa de un progenitor, la autorización escolar, la petición de retirada— funciona sobre actos que nadie puede acreditar después: el «yo nunca autoricé esto» del padre separado, el «la escuela tenía permiso» que no se encuentra, el «pedí que lo borraran hace un año» sin fecha. Declaraciones que pesan poco cuando llega el conflicto —porque no tienen fecha ni forma.

La prueba de existencia aplicada

Se documentan las decisiones de los adultos —nunca el menor [3].

1. La autorización que dice qué

La autorización escolar o de extraescolar —a menudo una casilla genérica— convertida en un documento preciso y sellado: qué usos (¿la web del centro? ¿redes? ¿el grupo de familias?), qué canales, cuánto tiempo; firmada con fecha cierta [3]. La escuela que la tiene anclada sabe qué puede hacer; la familia sabe

qué ha permitido; y el «teníamos permiso» se convierte en un hecho consultable, no en una discusión de inicio de curso.

2. El desacuerdo que consta

Cuando un progenitor no quiere que se publiquen imágenes del hijo —el caso clásico de la separación—, su negativa, comunicada y sellada con fecha cierta [3]: al otro progenitor, a la escuela, al club. Los tribunales ya exigen el acuerdo de ambos [2]; lo que faltaba era que la negativa tuviera fecha. La lógica es la del capítulo 53 —documentar los acuerdos y desacuerdos de los adultos, nunca el menor— aplicada a la imagen.

3. La retirada datada

La petición de borrar una foto —al otro progenitor, al abuelo entusiasta, a la plataforma— enviada y capturada con fecha cierta; y el silencio o la negativa, también datados [3]. Si el conflicto escala —hasta el juez que la ley francesa ya prevé [1]—, la cronología entera existe: se pidió tal día; no se atendió; esto es lo que había publicado.

4. La huella para el futuro

La foto publicada —o el álbum entero— registrada por huella: la SHA-512 en el dispositivo de la familia, nada del contenido en ninguna parte [3]. Parecería paradójico —documentar lo que querríamos que no existiera—, pero es el regalo probatorio al hijo mayor: el día que quiera ejercer sus derechos —retirada, olvido, o simplemente saber—, podrá acreditar qué se publicó de él y cuándo, sin depender de la memoria de nadie ni de la memoria caché de ningún buscador. Su infancia digital, auditable por él.

Los límites, antes de que nadie se haga ilusiones: el sello acredita consentimientos, negativas y fechas —no decide qué es el interés superior del menor: eso lo hacen los padres que se entienden y, cuando no, el juez [1][2]. Nada de esto es una invitación a documentar al niño —la línea del capítulo 53 manda: se registran las decisiones de los adultos. Y la mejor protección sigue siendo la más antigua: publicar menos, pensar antes, y preguntar al hijo cuando tenga edad de responder —la ley francesa lo dice con una palabra preciosa: asociarlo [1].

La promesa y el peligro

La promesa: escuelas con autorizaciones precisas y consultables [3]; progenitores separados que discuten el fondo —qué conviene al hijo— y no los hechos; peticiones de retirada que no se pierden en conversaciones; y una generación que, al cumplir 18 años, podrá mirar su infancia digital con los derechos en la mano [1] —porque alguien tuvo el cuidado de datarla.

Ahora, los peligros.

El primero es **el expediente contra la expareja**. El desacuerdo documentado puede convertirse en munición del conflicto parental. El contrapeso es el del capítulo 53: el rastro es para proteger al menor, no para ganar la guerra —el diseño bilateral y el interés superior del menor como norte; y los jueces detectan enseguida quién documenta por el hijo y quién contra el otro.

El segundo es **la burocratización de la ternura**. Si publicar la foto del cumpleaños exige un trámite, la vida familiar se hace imposible. La respuesta es la proporcionalidad: el consentimiento preciso es para las instituciones —escuelas, clubes, medios— y para los desacuerdos; entre adultos que se entienden, basta con el respeto.

El tercero es **el falso sello de legitimidad**. Una autorización datada no hace buena una publicación que hace daño. El consentimiento de los padres tiene límites —la dignidad del menor los marca, y la ley francesa lo ha escrito [1]: hay difusiones que ninguna firma parental ampara.

Y el cuarto, el más íntimo: buscar en una herramienta la excusa para no pensar. Ninguna huella sustituye el criterio. La pregunta antes de publicar no es «¿tengo el permiso?», sino «¿le gustará, dentro de quince años, que esto exista?». La prueba de existencia ordena los consentimientos; la prudencia los hace innecesarios.

Es hora de actuar

Que cada imagen de un niño tenga detrás una decisión que se pueda enseñar.

Para madres y padres: pensad antes de publicar —y cuando el hijo tenga edad, preguntadle [1]; si hay desacuerdo entre vosotros, que conste con fecha [3]: el hijo merece que su imagen no sea campo de batalla.

Para las escuelas, clubes y entidades: autorizaciones precisas, selladas y renovadas [3] —la casilla genérica de principio de curso no protege ni a las familias ni al centro.

Para las plataformas: peticiones de retirada de imágenes de menores con respuesta datada y trazable —el silencio también es una decisión, y debería constar.

Para los legisladores: Francia ha marcado el camino [1] —el derecho a la imagen del menor como deber común de los padres, con el juez como última garantía; que la transposición de esta idea venga con consentimientos y negativas acreditables.

Para los hijos, cuando seáis mayores: vuestra infancia digital es vuestra; reclamadla —y que las huellas datadas [3] os ahorren tener que probar lo evidente.

Las 1.300 fotos [1] ya están; las siguientes todavía no. Que cada imagen de un niño tenga detrás un consentimiento que se pueda enseñar —y un adulto que se haya detenido a pensar. Por quienes todavía no pueden decir que no, **time2act**.

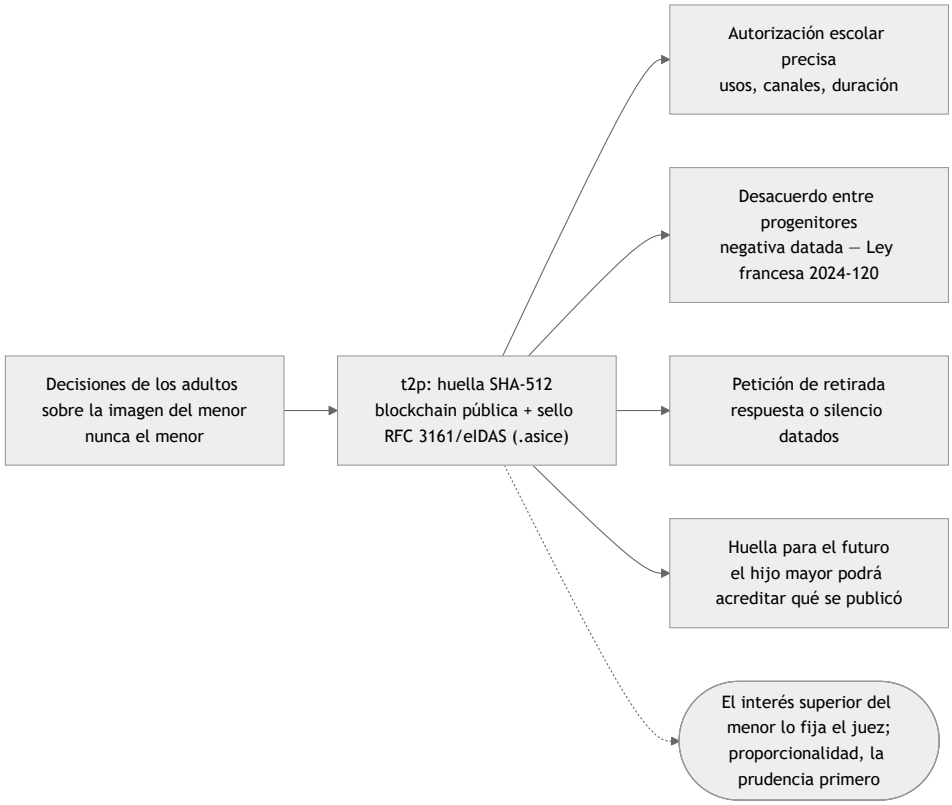


Figura 82.1 — La imagen del menor con prueba de existencia (sellado con t2p — capítulo 13) —se documentan las decisiones de los ADULTOS, nunca el menor: la autorización escolar precisa y sellada (usos, canales, duración), el desacuerdo entre progenitores datado, la petición de retirada con respuesta o silencio datados, y la huella de la publicación para el futuro (el hijo mayor podrá acreditar qué se publicó de él, sin que ningún contenido viaje). Contexto: un niño aparece en ~1.300 fotos en línea antes de los 13 años; Ley francesa 2024-120 (derecho a la imagen dentro de la autoridad parental, ejercido en común; delegación judicial en casos graves). Límites: el interés superior del menor lo fija el juez; proporcionalidad; la prudencia primero. Fuentes: Légifrance; DAJ.

---

[1] Légifrance — *Ley núm. 2024-120, de 19 de febrero de 2024, para garantizar el respeto del derecho a la imagen de los niños* (modificación del art. 371-1 del Código civil: la autoridad parental incluye la protección de la vida privada y del derecho a la imagen del menor; protección ejercida en común por los dos progenitores, asociando al niño según edad y madurez; delegación judicial del ejercicio del derecho de imagen en caso de atentado grave a la dignidad o la integridad moral); DAJ/economie.gouv.fr — *Respect du droit à l'image des enfants: les apports de la loi* (contexto: un niño aparece de media en 1.300 fotografías en línea antes de los 13 años; riesgos: usurpación, chantaje, ciberacoso); Actu-Juridique — *Les 5 apports de la loi*. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049163317 · https://www.economie.gouv.fr/daj/lettre-de-la-daj-

respect-du-droit-limage-des-enfants-les-apports-de-la-loi-du-19-fevrier-2024 · https://www.actu-juridique.fr/civil/personnes-famille/le-respect-du-droit-a-limage-des-enfants-et-les-5-apports-de-la-loi-du-19-fevrier-2024/ ↩

[2] Marco español (LO 1/1982 sobre el honor, la intimidad y la propia imagen; LO 1/1996 de protección jurídica del menor; intervención del Ministerio Fiscal; doctrina judicial que exige el acuerdo de ambos progenitores para publicar imágenes de los hijos). Véase el capítulo 81 para el derecho de imagen general y el capítulo 53 para los registros de coparentalidad. ↩

[3] t2p — manual de producto (escáner de documentos; captura de pantalla y correo certificados; certificar cualquier fichero — solo la huella viaja, el contenido no sale nunca del dispositivo; firma con vídeo-selfie; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; la coparentalidad, en el capítulo 53; la difusión íntima, en el capítulo 83. ↩

Imágenes íntimas no consentidas: el daño, la prueba y la retirada

«A las chicas de todas partes: estoy con vosotras. Las noches en que os sintáis solas, estoy con vosotras. Cuando la gente dude de vosotras o os menosprecie, estoy con vosotras.»

— Chanel Miller, declaración de impacto de la víctima, caso People v. Turner (2016)

En septiembre de 2023, en **Almendralejo**, un pueblo de Extremadura, decenas de adolescentes descubrieron que circulaban por WhatsApp imágenes suyas desnudas que nunca habían existido. Alguien había cogido fotos vestidas de sus cuentas de Instagram y, con una aplicación de IA, las había convertido en desnudos falsos. Las víctimas tenían entre doce y catorce años. «Muchas niñas estaban completamente aterrorizadas y tenían ataques de ansiedad tremendos porque lo sufrían en silencio», explicó una madre [1]. Un juzgado de menores de Badajoz condenó a quince chicos —de trece a quince años— por veinte delitos de creación de material de abuso infantil y veinte más contra la integridad moral de las víctimas [2]. El daño ya estaba hecho: las imágenes eran falsas, pero la humillación y el miedo eran reales.

Este capítulo trata una de las caras más crueles de las *deepfakes*, distinta de la del capítulo 81 —el uso comercial de la imagen. Aquí no hablamos de dinero ni de marca, sino de **dignidad**. Y hay que decir una cifra que lo enmarca todo: más del **90 % del contenido *deepfake*** que circula por la red es pornográfico, y casi todo tiene como víctima a una **mujer** [6]. La pregunta de este capítulo no es cómo evitar que exista —no se puede del todo—, sino cómo dar a la víctima **prueba del daño y una retirada demostrable** sin obligarla a revivirlo.

Un daño fácil de infligir, difícil de reparar

El caso de Almendralejo no es aislado. En enero de 2024, imágenes sexuales falsas de **Taylor Swift** inundaron la red X: una sola publicación se vio más de **47 millones de veces** antes de que la retiraran, y la plataforma bloqueó las búsquedas de su nombre durante dos días [3]. Si esto le pasa a una de las mujeres más poderosas del planeta, imaginemos a una adolescente anónima. La asimetría es brutal: fabricar la imagen cuesta minutos y es gratuita; retirarla obliga a la víctima a perseguir cada copia en cada plataforma, demostrar que es ella y a menudo **volver a mirar** aquello que la hiere para aportarlo como prueba.

Ya existe una defensa que, no por casualidad, usa exactamente el principio de este libro. **StopNCII.org** permite a una víctima generar en su dispositivo una **huella** (un *hash*) de la imagen íntima; **solo la huella —nunca la imagen— sale del teléfono**, y se comparte con Meta, TikTok, Reddit o Google para que bloqueen las subidas coincidentes. Desde 2021 ha protegido más de **500.000 imágenes** y ha impedido más de **10.000 intentos** de publicación, con un éxito superior al 90 % [7]. Es la prueba de que se puede defender a la víctima **sin centralizar** ni una sola imagen.

La ley ya está; falta la prueba inalterable

La respuesta legal ha sido rápida y contundente. En Estados Unidos, la **TAKE IT DOWN Act**, firmada el 19 de mayo de 2025, criminaliza la publicación de imágenes íntimas no consentidas —incluidas las *deepfakes*— y obliga a las plataformas a retirarlas en un máximo de **48 horas** desde el aviso; desde el **19 de mayo de 2026** la FTC ya aplica el cumplimiento a las plataformas [4]. En Europa, la **Directiva (UE) 2024/1385** sobre la violencia contra las mujeres, en vigor desde junio de 2024 y a transponer antes de junio de 2027, tipifica la producción y difusión no consentida de material íntimo manipulado y obliga a los estados a ofrecer **órdenes de retirada y preservación rápida de pruebas** [5]. La ley, pues, ya pide dos cosas: retirar deprisa y **conservar la prueba**. Y aquí vuelve el muro de siempre: una captura de pantalla es manipulable, el aviso a la plataforma puede no dejar rastro datado, y la víctima acaba teniendo que custodiar ella misma el material que la hiere.

Por qué la denuncia por sí sola no salva

Hay que decirlo con crudeza, porque aquí es especialmente delicado. Para que un tribunal condene —como en Almendralejo— y para que una retirada sea exigible, hace falta **evidencia admisible**: que esta

imagen existía, dónde, cuándo, y que se pidió retirarla. Hoy esta evidencia es frágil: una captura sin sello no prueba la fecha; demostrar que la plataforma recibió el aviso y no actuó en 48 horas depende de correos y registros que se pueden discutir; y conservar la prueba significa, demasiado a menudo, que la víctima ha de guardar y volver a enseñar su propia imagen. Falta una manera de **fijar la prueba del daño y del aviso con fecha cierta, sin revivirlo ni almacenarlo**.

La prueba de existencia aplicada

Es aquí donde **t2p** extiende la lógica de StopNCII con la pieza que falta. Cuando una víctima, una entidad de apoyo o una plataforma detecta una imagen no consentida, se calcula en el dispositivo la **huella SHA-512** del contenido y se sella, junto con **dónde y cuándo** se ha encontrado (la URL, la hora) y la **solicitud de retirada**, con un **sello de tiempo RFC 3161/eIDAS** anclado a la **blockchain pública** dentro de un contenedor **.asice**. Lo que resulta es una **cadena de custodia inalterable y datada** —útil para la fiscalía, como en el caso de Almendralejo, y para demostrar que la plataforma fue avisada en tal momento y tenía 48 horas para actuar— **sin que la víctima tenga que almacenar ni volver a compartir la imagen**: solo se sella su huella. La fecha cierta demuestra que *aquel* contenido existía y fue marcado como abuso en *aquel* instante, y el acusado ya no puede alegar que la prueba se fabricó después.

Hay una segunda aplicación, para la cara inversa del problema: la **sextorsión** y la falsa acusación. Cuando alguien amenaza a una víctima con difundir una imagen que parece real, la **procedencia** —la ausencia de ningún origen sellado, combinada con la marca C2PA de los capítulos 13 y 15— ayuda a establecer que la imagen es **sintética**, y a quitarle el poder de chantaje.

Ahora el límite, con toda la crudeza, porque aquí engañarse haría daño. «Basura a la entrada, basura en la cadena»: el sello **no retira la imagen**, **no impide su creación**, **no detecta** por sí solo que sea una *deepfake* y no puede hacer que lo que se ha visto deje de verse. Lo que hace es dar **prueba del daño y retirada demostrable**, no prevención. E impone una línea roja absoluta: **nunca** puede convertirse en un registro de imágenes íntimas; solo huellas calculadas en el dispositivo, como en StopNCII. La protección real sigue siendo la suma de la huella, la ley y el deber de la plataforma; el sello añade la prueba inalterable.

La promesa y el peligro

La promesa es devolver a la víctima un poco de poder: una **prueba datada y admisible** del daño y del aviso, y una retirada **exigible y verificable** en todas las plataformas, sin tener que rendir ni una sola imagen ni revivirla cada vez. El agresor y la plataforma lenta pierden la posibilidad de negarse; la niña de Almendralejo tendría, mañana, una prueba que ningún abogado podría discutir.

El peligro exige los matices más estrictos del libro. Primero: **nada de imágenes centralizadas**; solo huellas en el dispositivo. Segundo: no convertir el proceso de denuncia en una nueva fuente de trauma; la herramienta ha de acompañar, no obligar a mirar. Tercero: la gobernanza del banco de huellas, que ha de ser auditada y a prueba de abuso. Y cuarto: recordar siempre que el sello demuestra **el acto de marcar** un contenido como no consentido, con fecha y autor; la determinación de quién lo creó corresponde a la investigación. La prueba de existencia es una herramienta de dignidad y de justicia, no un escudo tecnológico que borre el daño.

Además, la inmutabilidad inherente a los registros basados en blockchain puede convertirse en una cadena invisible de persecución para las víctimas que buscan recuperar la vida después del trauma. Una vez grabada una huella de una imagen no consentida, esta queda inscrita para siempre en el libro público de pruebas; el hecho de que no se pueda eliminar también implica que no hay ningún mecanismo natural para retirarla cuando las circunstancias cambian o cuando la víctima decide dejar atrás aquel capítulo. Como advierte Edward Snowden, la existencia de un «pasado del que me arrepentía por completo, pero que apenas recordaba» puede quedar «tan inextricable y tecnológicamente ligado» a la identidad de la persona afectada, aumentando el riesgo de revictimización a largo plazo [11]. Por eso, cualquier arquitectura de sello digital ha de incluir una capa de caducidad o revocabilidad controlada por una autoridad independiente, que permita borrar o invalidar la huella cuando la prueba ya no sea necesaria o resulte contraproducente. Esta salvaguarda equilibraría la necesidad de certeza legal con el derecho al olvido y a la rehabilitación personal.

Como hemos visto, la magnitud del problema ya supera el terreno de la empresa y llega a las alturas de la política: el American Sunlight Project constató que, en diciembre de 2024, cerca de uno de cada seis

congresistas estadounidenses son víctimas de imágenes íntimas no consentidas generadas por IA, una cifra que revela un patrón sistemático de abuso y vulnerabilidad a escala institucional [12]. Esta realidad obliga a las plataformas a adoptar mecanismos «Take It Down» capaces de responder en tiempo real, pero sin una prueba de existencia anclada a la blockchain la retirada se queda en el aire: no hay ningún registro inmutable que demuestre que la denuncia se ha hecho y que el contenido ha sido eliminado. El anclaje neutral de la evidencia, independiente del creador y de terceros, convierte cada solicitud de eliminación en una pista verificable para el tribunal, evitando que las víctimas tengan que asumir la carga de demostrar el daño y garantizando que las autoridades puedan actuar con la certeza legal necesaria.

Es hora de actuar

Para las víctimas y las entidades de apoyo (StopNCII, líneas de ayuda): sellar la huella y las circunstancias del daño como prueba, sin almacenar la imagen. Para las plataformas: conservar el banco de huellas y emitir recibos sellados por cada aviso y retirada, demostrando el cumplimiento de las 48 horas. Para la policía y los tribunales: tratar la huella sellada con sello de tiempo como cadena de custodia, como se hizo en el caso de Almendralejo. Para los legisladores (TAKE IT DOWN Act, Directiva 2024/1385): reconocer la prueba sellada como evidencia válida y garantizar su preservación rápida. Y para los proveedores de aplicaciones de IA que «desnudan» fotos: asumir la responsabilidad de la herramienta, tal como ya exigen las nuevas leyes sobre imagen.

En Almendralejo unas niñas sufrieron en silencio un daño hecho con un clic. Dar a cada víctima una prueba sellada del daño y una retirada que se pueda exigir —sin centralizar nunca su imagen ni obligarla a revivirla— es, en este frente que toca la dignidad más íntima, time2act.

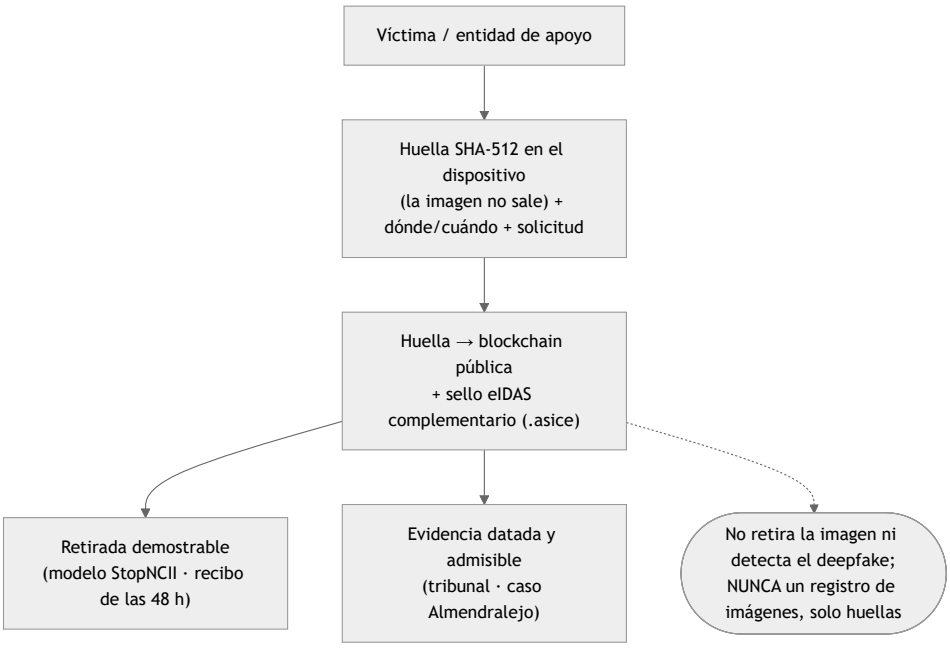


Figura 83.1 — La víctima o la entidad de apoyo calcula en el dispositivo la huella SHA-512 del contenido (la imagen no sale del teléfono) y le añade dónde y cuándo se ha encontrado; la huella del conjunto se ancla en la blockchain pública, con sello eIDAS complementario (.asice). Dos resultados: a la izquierda, la retirada demostrable en todas las plataformas (modelo StopNCII, con recibo sellado de las 48 horas); a la derecha, evidencia datada y admisible para el tribunal (como en Almendralejo). Límite: el sello no retira la imagen, no impide crearla ni detecta el deepfake; nunca un registro de imágenes, solo huellas. Fuentes: caso Almendralejo; caso Taylor Swift; TAKE IT DOWN Act; Directiva (UE) 2024/1385; StopNCII.org.

[1] Euronews — *The Almendralejo case: when AI deepfakes are used to undress teenagers* (septiembre de 2023; testimonio de una madre; víctimas de 12-14 años). https://www.euronews.com/next/2023/11/15/the-case-of-almendralejo-when-deepfakes-are-used-to-undress-teenagers-euronews-tech-talks- ↩

[2] Scottish Legal News / Reuters — *Spain: court punishes schoolboys for spreading AI deepfakes of girls* (julio de 2024; 15 menores condenados; 20 delitos de material de abuso infantil y 20 contra la integridad moral).

https://www.scottishlegal.com/articles/spain-court-punishes-schoolboys-for-spreading-ai-deepfakes-of-girls ↩

[3] Wikipedia — *Taylor Swift deepfake pornography controversy* (enero de 2024; una publicación vista más de 47 millones de veces; X bloquea las búsquedas de su nombre). https://en.wikipedia.org/wiki/Taylor_Swift_deepfake_pornography_controversy ↩

[4] Congress.gov / The White House — *TAKE IT DOWN Act* (S.146; firmada el 19 de mayo de 2025; retirada en 48 h; cumplimiento a plataformas aplicado por la FTC desde el 19 de mayo de 2026; primera condena penal en abril de 2026). https://www.congress.gov/bill/119th-congress/senate-bill/146 ↩

[5] Council of Europe — *Directive (EU) 2024/1385 of 14 May 2024 on combating violence against women and domestic violence* (en vigor el 13 de junio de 2024; tipifica el material íntimo manipulado; órdenes de retirada y preservación de pruebas). https://www.coe.int/en/web/cyberviolence/-/european-parliament-and-council-directive-eu-2024-1385-of-14-may-2024-on-combating-violence-against-women-and-domestic-violence ↩

[6] Euronews — *Nude deepfakes: is the EU doing enough to tackle the issue?* (2024; más del 90 % del contenido deepfake es pornográfico, casi todo contra mujeres). https://www.euronews.com/next/2024/03/17/nude-deepfakes-is-the-eu-doing-enough-to-tackle-the-issue ↩

[7] StopNCII.org — *How StopNCII.org works* (huella generada en el dispositivo; la imagen no sale nunca; más de 500.000 imágenes protegidas; socios Meta, TikTok, Reddit, Google). https://stopncii.org/how-it-works/ ↩

[8] Skadden — *'Take It Down Act' requires online platforms to remove unauthorized intimate images and deepfakes when notified* (análisis del mecanismo de aviso y retirada). https://www.skadden.com/insights/publications/2025/06/take-it-down-act

[9] RAINN — *TAKE IT DOWN Act* (perspectiva de las víctimas de violencia sexual). https://rainn.org/federal-legislation/take-it-down-act/

[10] EU Artificial Intelligence Act — *Article 50: transparency obligations* (marcado del contenido generado o manipulado por IA). https://artificialintelligenceact.eu/article/50/

[11] Edward Snowden — *Vigilancia permanente* (Planeta, 2019). ↩

[12] The Markup (2024). https://themarkup.org/artificial-intelligence/2024/12/11/1-in-6-congresswomen-targeted-by-ai-generated-sexually-explicit-deepfakes ↩

El odio en las redes: el daño, la prueba y la dignidad

«Si pones la vergüenza en una placa de Petri, necesita tres cosas para crecer exponencialmente: secretismo, silencio y juicio. Si la rocías con empatía, no puede sobrevivir.»

— Brené Brown, «Listening to Shame», TED (2012)

En 2013, en Novara, Italia, Carolina Picchio, una adolescente de 14 años, vio cómo un vídeo suyo —aparentemente bebida en una fiesta— se esparcía por Facebook. El clip desencadenó una oleada de insultos que llenó su bandeja de entrada con unos 2.600 mensajes de burla, amenazas y difamación, enviados por su exnovio y el grupo de amigos que lo secundaba. La presión psicológica fue tan intensa que Carolina se lanzó por la ventana de su casa. El caso se convirtió en el impulso legislativo de la Ley 71/2017, la primera norma europea específica contra el ciberacoso, promovida por la senadora Elena Ferrara y dedicada a la víctima [1]. Este episodio muestra cómo las palabras digitales, aunque se puedan suprimir o editar en un instante, dejan una huella real y devastadora en la vida de un joven.

Este capítulo se centra exclusivamente en el odio, el acoso y la humillación en las redes sociales —no en el sexo ni en la difusión de contenido íntimo (capítulos 83 y 81)—; el marco general de la crisis de la verdad se encuentra en el capítulo 10, mientras que los enjambres de bots y la prueba de personalidad cívica se explican en el capítulo 108. La pregunta clave es: ¿cómo podemos ofrecer a las víctimas —a menudo menores— una **prueba** tangible del daño y una retirada demostrable sin obligarlas a custodiar el contenido que las ha herido? La respuesta se encuentra en **t2p**, la prueba de existencia basada en blockchain que sella en el dispositivo la huella SHA-512 del contenido de odio, junto con la URL y la marca horaria de detección, y registra la solicitud de retirada. Esta cadena de custodia datada es inalterable y admisible en un tribunal, todo ello sin almacenar ni reexponer el material ofensivo [15]. La tecnología aporta la pieza que falta: una prueba fiable del daño que no depende de plataformas centralizadas y que protege la dignidad de la víctima manteniendo la neutralidad total.

Un daño fácil de infligir, difícil de reparar

El odio en las redes se propaga con la misma facilidad que un mensaje de texto: unos cuantos clics y una conexión a Internet son suficientes para crear una explosión de insultos, rumores o amenazas. En cambio, el proceso de reparación es una marcha atrás interminable. Cada copia del contenido ofensivo se replica en miles de dispositivos, se almacena en servidores que a menudo no ofrecen ningún rastro de origen y, aun cuando la víctima consigue hacer desaparecer el post original, las huellas digitales persisten en memorias colectivas y algoritmos que recomiendan contenido similar. La carga recae totalmente sobre quien ha sufrido la agresión: hay que localizar cada fragmento, demostrar que es una extensión del daño y, a menudo, volver a mirar el material para identificarse como objeto del odio, un proceso que reabre las heridas psicológicas y consume recursos económicos y temporales.

Esta asimetría se hace especialmente evidente entre los jóvenes. Un estudio del Pew Research Center muestra que el 46 % de los adolescentes estadounidenses (13-17 años) ha sufrido al menos una de seis formas de ciberacoso, con un 32 % de insultos y un 10 % de amenazas físicas [2]. La Organización Mundial de la Salud, a través del proyecto HBSC, confirma esta tendencia en Europa: el 16 % (aproximadamente uno de cada seis) de los jóvenes de 11, 13 y 15 años ha sido víctima de ciberacoso, y la incidencia ha aumentado entre 2018 y 2022 [3]. En España, el informe conjunto de las fundaciones ANAR y Mutua Madrileña indica que el 12,3 % del alumnado declara haber experimentado acoso o ciberacoso, una cifra superior al 9,4 % del año anterior [4]. De estos casos, el 91,7 % de los acosadores son compañeros del mismo centro educativo y un 14,2 % ya usan inteligencia artificial para crear vídeos falsos o suplantaciones de identidad. El impacto se traduce en una realidad palpable: la ADL informa de que el 50 % de los adolescentes ha sufrido acoso en línea durante los últimos doce meses, y un 36 % afirma que esta experiencia ha desembocado en acoso presencial [5].

Estos números no son meras estadísticas; son testimonios de una crisis de confianza que se extiende más allá del ciberespacio. Cuando la violencia verbal se convierte en una forma de control social, el bienestar mental de los jóvenes queda comprometido y sus oportunidades educativas y profesionales se ven erosionadas. La magnitud del problema es evidente: no se trata de un fenómeno marginal o puntual, sino de una amenaza ambiental que afecta a la salud colectiva y al tejido social. Cada vez que una víctima ha de perseguir un rastro digital para demostrar su daño, la sociedad renuncia a su propia responsabilidad de

proteger a los más vulnerables y perpetúa un ciclo de silencio e impunidad. La solución no puede limitarse a sancionar al agresor; hace falta una prueba fiable del daño que sea independiente de las plataformas, neutral y admisible en tribunales —exactamente lo que ofrece t2p.

La herida invisible y el debate honesto

El 30 de septiembre de 2022, el dictamen forense de Andrew Walker rompió un silencio que parecía inexpugnable: la muerte de Molly Russell, una adolescente británica de 14 años, se vinculaba directamente a los efectos nocivos del contenido en línea. De los 16.300 mensajes que la joven había guardado en Instagram durante los seis meses previos a su suicidio, 2.100 mostraban temáticas de autolesión, depresión e incitaciones a la autodestrucción [6]. Este primer dictamen mundial demostró que no se trataba de una simple coincidencia trágica, sino de un contenido que había erosionado la salud mental de Molly hasta el punto letal.

El debate académico actual gira en torno a dos perspectivas opuestas. Jonathan Haidt sostiene que la proliferación masiva de teléfonos móviles y plataformas digitales ha provocado un «gran recableado» del cerebro adolescente, alimentando una epidemia de salud mental entre las generaciones más jóvenes [7]. En contraposición, Candice Odgers refuta esta correlación directa y argumenta que no hay evidencia empírica que demuestre que las redes «recableen» el cerebro ni que sean la causa única de los trastornos observados; señala, en cambio, factores sociales, económicos y familiares como contribuyentes complejos [7].

El odio en línea se manifiesta como una herida invisible que, aunque efímera o manipulada digitalmente, deja cicatrices profundas. Las directrices del DSA (2025) imponen verificación de edad y persiguen el contenido nocivo, mientras el anteproyecto de ley orgánica español (2024) crea el alejamiento en línea como agravante [10][11]. Sin embargo, estas normas dependen de pruebas fiables del daño: sin una evidencia inmutable, los jueces disponen solo de una prueba frágil.

Aquí t2p aporta la pieza que falta: una prueba inmutable del daño —sellada en el dispositivo y anclada a la blockchain pública dentro de un contenedor .asice [15]— que permite a las autoridades actuar con certeza y restaurar, aunque parcialmente, la dignidad de las personas jóvenes víctimas de odio digital.

Odio que nadie escribió: deepfakes y enjambres

En enero de 2024, en la Pikesville High School (Maryland), un sencillo clip de audio se convirtió en el arma más corrosiva de un odio sintético. Dazhon Darien, director deportivo del centro, utilizó una herramienta de inteligencia artificial para crear un deepfake sonoro que hacía sonar al director Eric Eiswert pronunciando frases racistas y antisemitas. El audio, difundido en las redes sociales en cuestión de minutos, desencadenó críticas y amenazas contra el director y lo convirtió en objeto de difamación y represalia. La policía identificó el contenido como falso y detuvo a Darien en abril de 2024, pero no se pudo revertir el daño inmediato: los comentarios y las capturas de pantalla ya habían circulado, alimentando una narrativa de odio que nadie había escrito [8]. El caso muestra cómo la tecnología de síntesis puede fabricar «palabras que nadie ha dicho nunca» y convertir el odio en un producto manipulable, totalmente desconectado de la persona suplantada.

La otra cara de la herramienta es la ampliación masiva de un discurso de odio ya existente. Un estudio publicado en *PNAS* en 2025, centrado en la plataforma X bajo la dirección de Musk, reveló que la tasa semanal de contenido odioso había subido aproximadamente un 50 % después de la adquisición, y que los «me gusta» asociados a este tipo de publicación se habían incrementado un 70 % [9]. No siempre se trata de una comunidad real: a menudo lo que parece una multitud es la maniobra de un único troll o de un grupo coordinado de cuentas falsas, capaces de multiplicar la visibilidad del mensaje odioso con pocas interacciones. Esta dinámica de autenticidad débil alimenta la crisis de confianza descrita en el capítulo 108, donde la prueba de personalidad cívica intenta desvelar quién hay realmente detrás de un perfil digital.

En ambos escenarios, el daño es tangible y real, aunque el contenido sea efímero o manipulable. Las leyes actuales —como el art. 510 del Código Penal español o la Online Safety Act del Reino Unido— castigan la incitación al odio y el acoso, pero dependen de una prueba robusta que a menudo falta: capturas de pantalla modificables, avisos sin rastro horario y contenido que el agresor puede borrar. Aquí entra *t2p*, aplicando la receta forense del capítulo 13/15: se calcula en el dispositivo una huella SHA-512 del contenido odioso, junto con la URL y la hora exactas donde se ha encontrado, y se sella con un sello de

tiempo RFC 3161/eIDAS anclado a la blockchain pública dentro de un contenedor .asice. El resultado es una cadena de custodia inmutable y admisible. Esta prueba no elimina el post ni impide la creación de odio, ni tampoco lo detecta; pero ofrece una evidencia verificable que las autoridades pueden usar para aplicar la ley sin depender de una captura manipulable.

La ley ya está; falta la prueba inalterable

Desde que la Unión Europea publicó las directrices del DSA sobre protección de menores (14 de julio de 2025) [10], los estados miembros deben impulsar medidas concretas contra el ciberacoso y el grooming. En España, el anteproyecto aprobado el 4 de junio de 2024 [11] introduce el llamado «alejamiento en línea» y refuerza el marco penal existente: el artículo 510 del Código Penal castiga el odio con prisión de 1 a 4 años y multas, y el artículo 172 ter tipifica el acoso reiterado con penas de entre tres meses y dos años [12]. En el Reino Unido, la Online Safety Act de 2023, en vigor desde el 25 de julio de 2025, obliga a las plataformas a proteger a los menores contra el bullying y el contenido de odio, estableciendo multas que pueden llegar al 10 % de la facturación mundial [13]. Australia ha ido un paso más allá con la Online Safety Amendment (Social Media Minimum Age) Act de 2024, que prohíbe el acceso a las redes sociales a cualquier menor de 16 años a partir del 10 de diciembre de 2025, con sanciones de aproximadamente 50 millones de dólares australianos para las empresas infractoras [14].

Todas estas regulaciones convergen en un requisito fundamental: la necesidad de **probar** qué ha sucedido, cuándo ha pasado y qué solicitud de retirada se ha formulado. En la práctica, este requerimiento choca con el mismo muro que ha dificultado la defensa de las víctimas durante años. Una captura de pantalla, por muy detallada que sea, no garantiza la fecha exacta; los metadatos pueden ser manipulados o eliminados. Un aviso enviado a la plataforma a menudo desaparece sin dejar ningún rastro horario verificable, y el contenido ofensivo se puede borrar antes de que las autoridades puedan recoger pruebas sólidas.

Esta fragilidad de la prueba no es solo una cuestión técnica, sino un obstáculo legal que impide la aplicación efectiva de las leyes: **la falta de evidencia fiable libera a los agresores**, perpetúa el silencio de las víctimas y mantiene vivo el ciclo de odio y acoso en línea.

Como hemos visto, **t2p** calcula la huella SHA-512 del contenido de odio directamente en el dispositivo de la víctima, sin que el material salga nunca del teléfono. A esta huella se asocia la información de **dónde** (URL o identificador) y **cuándo** (marca horaria exacta), junto con la solicitud formal de retirada; el sello de tiempo, basado en el protocolo RFC 3161/eIDAS y anclado a la blockchain pública, crea una cadena de custodia datada y verificable dentro de un contenedor .asice [15]. Este proceso produce una prueba **neutral**, independiente de cualquier creador o intermediario, que se puede presentar ante los tribunales como evidencia admisible.

La prueba de existencia aplicada

En las aulas de Barcelona, una profesora de secundaria recibe un correo electrónico con un enlace a la captura de un chat donde un grupo de alumnos ha enviado mensajes de odio y falsas acusaciones contra una compañera de 14 años. El contenido ya no está disponible: el teléfono del remitente solo muestra la notificación «mensaje eliminado». Sin pruebas tangibles, la escuela queda atrapada entre la necesidad de actuar y la imposibilidad de demostrar que el acoso reiterado (art. 172 ter) se ha producido realmente. Es aquí donde **t2p** entra en juego: calcula en el dispositivo una huella SHA-512 del mensaje, le añade el enlace y la marca horaria de detección, y lo sella todo con un sello de tiempo —como hemos visto— anclado a la blockchain pública dentro de un contenedor .asice. El resultado es una cadena de custodia inalterable que se puede presentar como prueba admisible tanto en el expediente escolar como ante el juez.

1. El expediente escolar

Según el informe de la Fundación ANAR y Mutua Madrileña, ese elevado porcentaje de ciberacosadores que son compañeros del mismo centro ya se ha señalado [4]. Estas dinámicas a menudo se traducen en un «no se hace nada», dejando a las víctimas sin recurso. Con **t2p**, la alumna puede aportar una prueba digital que rompe este silencio: la huella demuestra que el mensaje existía, cuándo y dónde se publicó, y que se solicitó su retirada. La escuela, obligada por las directrices del DSA a proteger a los menores [10],

puede actuar inmediatamente, abrir una investigación formal e imponer medidas disciplinarias contra el agresor, sin necesidad de conservar el contenido completo.

2. La denuncia penal

El artículo 510 del Código Penal español castiga la incitación pública al odio con prisión de hasta cuatro años y multas [12]. Para demostrar que una serie de publicaciones constituyen un acoso «insistente y reiterado» (art. 172 ter), hay que probar la continuidad temporal y la intención dañosa. La cadena de custodia generada por **t2p** ofrece exactamente eso: cada huella incluye la hora y el lugar, y crea un registro cronológico que se puede presentar como prueba directa del carácter repetitivo del odio. Así, la víctima no ha de almacenar ni reexponer los mensajes ofensivos; solo presenta la huella, que es inmutable y admisible.

3. Notice-and-action para las plataformas

El DSA europeo y la Online Safety Act del Reino Unido imponen a las redes sociales la obligación de retirar el contenido ilegal en un plazo razonable [10][13]. Un recibo sellado generado en el momento de la denuncia funciona como prueba de que la plataforma ha sido notificada y cuándo. Esto impide el «memory-holing»: aunque el agresor borre el post, la huella y la fecha demuestran inequívocamente que el contenido existió y que se cumplió la respuesta requerida.

Casos complementarios

En casos como el de Pikesville, donde un audio sintético difamó al director de un centro [8], la procedencia —la marca C2PA y el requisito de etiquetado del AI Act [16]— es el complemento que ayuda a establecer que un contenido es sintético, y t2p le añade la prueba neutral y datada del daño. Además, la prueba de personalidad en el dispositivo, como hemos visto en el capítulo 108, permite verificar «una persona, una voz» sin recurrir a la desanonimización biométrica, y preserva la libertad de expresión y la privacidad.

En resumen, **t2p** no elimina el odio ni impide que se generen nuevos mensajes nocivos; tampoco crea un registro centralizado del contenido abusivo. Su fuerza radica en proporcionar una huella inmutable en el dispositivo de la víctima, que demuestra la existencia y la fecha del daño sin exponer el contenido mismo [17]. Esta es la pieza clave que transforma las obligaciones legales en acciones viables, y defiende la dignidad digital de los jóvenes frente al odio en línea.

La promesa y el peligro

En un mundo donde cada comentario, meme o vídeo se puede capturar, replicar y difundir en segundos, la víctima de odio digital a menudo se encuentra sin una prueba sólida del daño que ha sufrido. La promesa de **t2p** es devolver poder a esta persona: generar, en su propio dispositivo, una huella SHA-512 del contenido ofensivo, añadirle la URL y la hora exacta, y registrar a la vez la solicitud de retirada. Este sello de tiempo, conforme a las especificaciones que ya hemos citado y anclado a la blockchain pública dentro de un contenedor .asice, crea una cadena de custodia inmutable y datada que se puede presentar ante los tribunales como prueba admisible, sin necesidad de almacenar ni reexponer el contenido. Así, la víctima dispone de una evidencia verificable del daño y del aviso legal, capaz de hacer cumplir las obligaciones establecidas contra el ciberacoso y los artículos 510 y 172 ter del Código Penal español [12].

Sin embargo, esta tecnología conlleva una serie de peligros que hay que reconocer con la misma claridad con que se presenta la promesa. Primero, **no crea ningún registro centralizado** del contenido abusivo: todas las huellas se generan y se conservan únicamente en el dispositivo de la víctima, tal como hace el modelo de StopNCII.org [17]. Esto evita que una base de datos global de abusos se convierta en un instrumento de vigilancia masiva.

En segundo lugar, **nunca puede servir para desanonimizar ni vigilar** a los usuarios. El sello demuestra la existencia de un daño sufrido por una persona, pero no revela quién es exactamente; convertirlo en una herramienta para identificar cualquier voz iría contra la libertad de expresión y amenazaría la sátira, el whistleblowing y otras formas legítimas de disidencia (véase el capítulo 62). Desanonimizar el discurso podría helar el debate público y proteger solo a los poderosos; por eso el valor de la prueba es, precisamente, su neutralidad.

Un tercer peligro es la **necesidad de una caducidad o revocabilidad** de la huella. La inmutabilidad que garantiza la validez judicial también puede convertirse en un registro perpetuo de la victimización, vulnerando el derecho al olvido y perpetuando el daño psicológico. Por eso cualquier implementación ha de permitir borrar o invalidar las huellas cuando la víctima lo pida.

Finalmente, hay que recordar que **el sello es infraestructura de prueba, no cura**. La raíz del problema radica en los modelos de negocio basados en la atención que premian la indignación, como muestra el «como hemos visto» del discurso de odio en X tras el cambio de propiedad [9]. Sin cambios estructurales en estas plataformas —y sin un debate honesto sobre la verificación de edad, que protege a los menores pero también puede vigilarlos [10][14]— ninguna herramienta técnica será más que un parche. La promesa de **t2p** es poderosa; el peligro es confiar en que la tecnología pueda sustituir las reformas legales y sociales necesarias para garantizar dignidad y seguridad a los jóvenes en línea. El sello es una herramienta de dignidad y de justicia, no un escudo tecnológico que borre el daño.

Es hora de actuar

La violencia digital no es una sombra efímera: deja cicatrices reales en jóvenes que viven la adolescencia entre pantallas y notificaciones. El 46 % de los adolescentes estadounidenses ha sufrido alguna forma de ciberacoso [2] y la mitad lo ha padecido durante el último año [5]; en Europa, uno de cada seis jóvenes (16 %) ya ha experimentado alguna, con una tendencia al alza desde 2018 [3]. Leyes como la Ley 71/2017, nacida del caso de Carolina Picchio, han establecido penas claras contra el ciberacoso y el odio en línea, pero el problema persiste porque la prueba del daño sigue siendo débil: capturas manipulables, avisos sin marca temporal y contenido que el agresor borra antes de ser documentado.

Para las víctimas y familias: el primer paso es sellar en el dispositivo una huella SHA-512 del contenido ofensivo, junto con la URL y la hora exacta de detección. Esta huella se combina con una solicitud formal de retirada y se registra en un contenedor .asice, con la huella anclada en la blockchain pública y un sello de tiempo RFC 3161/eIDAS complementario [15]. Así, la víctima conserva una prueba inalterable del daño sin tener que guardar el contenido ofensivo y evita revivirlo cada vez.

Para los centros educativos: las escuelas han de tratar la huella sellada como un documento del expediente. Cada caso registrado puede ser revisado por equipos multidisciplinares (psicólogos, trabajadores sociales y juristas) que, sobre una cadena de custodia verificable, pueden aplicar medidas rápidas y legalmente sólidas: apoyo psicológico, sanciones o mediación.

Para las plataformas: el DSA europeo y la Online Safety Act del Reino Unido imponen obligaciones claras; cada aviso ha de generar un recibo sellado, con fecha y hora, que se entregue al denunciante y se archive como huella solo en el dispositivo. Este mecanismo cumple las directrices del DSA sobre la protección de los menores [10] y evita crear bases de datos centralizadas que vulneren la privacidad.

Para la policía y los tribunales: la huella datada se ha de aceptar como prueba admisible para los artículos 510 y 172 ter del Código Penal español, ya que constituye una cadena de custodia inalterable que demuestra la presencia y el contenido del discurso de odio en el momento exacto. Los jueces pueden usar esta evidencia para emitir órdenes de retirada e imponer sanciones sin depender de pruebas que se puedan borrar o alterar.

Para los legisladores: hay que reconocer legalmente la prueba sellada como forma legítima de evidencia, con una disposición que garantice su preservación y, a la vez, el derecho al olvido, de manera que el daño no se perpetúe pero la responsabilidad sea rastreable.

Como recuerda el caso de Carolina Picchio [1], la Ley 71/2017 nació para dar voz a chicos como ella; ahora podemos ofrecer a cada joven una prueba sellada del daño y una retirada exigible —sin centralizar nunca el contenido ni obligarla a revivirlo—. En este frente que toca la dignidad, **time2act**.

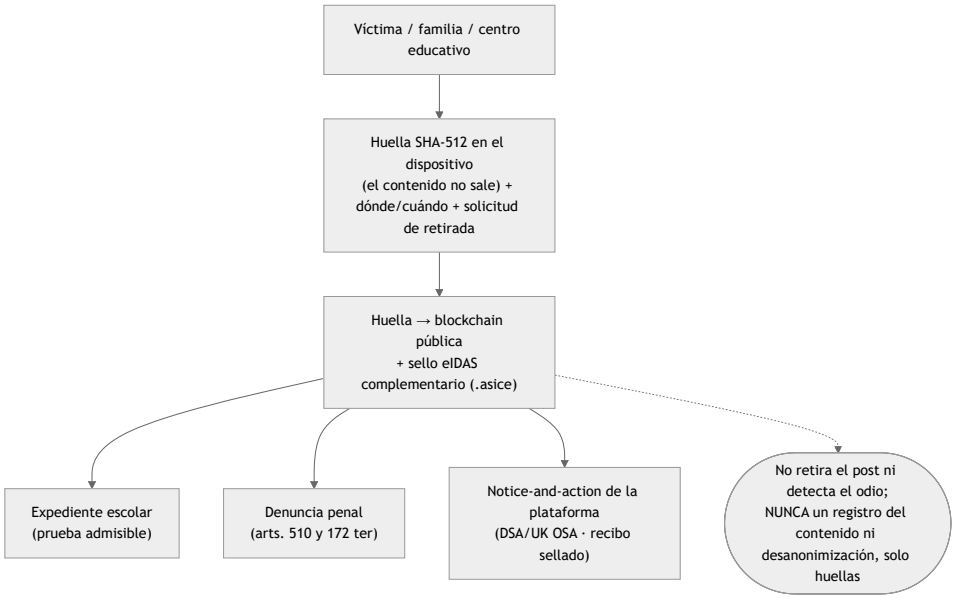


Figura 84.1 — La víctima, la familia o el centro educativo calcula en el dispositivo la huella SHA-512 del contenido de odio (el contenido no sale del teléfono) y le añade dónde y cuándo se ha encontrado y la solicitud de retirada; la huella del conjunto se ancla en la blockchain pública, con sello eIDAS complementario (.asice). Tres salidas: el expediente escolar, la denuncia penal (arts. 510 y 172 ter) y el notice-and-action de la plataforma (DSA/UK OSA), con recibo sellado. Límite: el sello no retira el post, no impide crear odio ni lo detecta; nunca un registro del contenido ni una herramienta de desanonimización, solo huellas en el dispositivo. Fuentes: caso Picchio; Molly Russell; ANAR; StopNCII.

---

[1] The Local (Italia) — *Italy unanimously passes anti-cyberbullying law* (mayo 2017; Ley 71/2017; Carolina Picchio, 14 años, 2013; senadora Elena Ferrara). https://www.thelocal.it/20170517/italy-unanimously-passes-anti-cyberbullying-law-online-abuse-trolling ↩

[2] Pew Research Center — *Teens and Cyberbullying 2022* (15 de diciembre de 2022; 46 %; insultos 32 %, rumores 22 %, amenazas 10 %). https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/ ↩

[3] OMS-Europa y estudio HBSC — *One in six school-aged children experiences cyberbullying* (27 de marzo de 2024; 16 %; 44 países; ≈280.000 jóvenes). https://www.who.int/europe/news/item/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study ↩

[4] Fundación ANAR y Fundación Mutua Madrileña — *VIII Informe de Prevención del Acoso Escolar* (2025; 12,3 % vs 9,4 %; 14,2 % con IA; 91,7 % del mismo centro; 17.562 alumnos). https://www.anar.org/crece-el-acoso-escolar-impulsado-por-el-ciberbullying-y-el-uso-de-la-ia-para-cometerlo/ ↩

[5] ADL — *Online Hate and Harassment: The American Experience 2024* (junio de 2024; adolescentes 50 %; 36 % salto al mundo físico). https://www.adl.org/resources/report/online-hate-and-harassment-american-experience-2024 ↩

[6] CBS News / ITV News — *Molly Russell inquest* (30 de septiembre de 2022; forense Andrew Walker; 2.100 de 16.300 posts; primer dictamen mundial). https://www.cbsnews.com/news/molly-russell-suicide-death-coroner-social-media-instagram-pinterest/ ↩

[7] Candice Odgers — *The great rewiring: is social media really behind an epidemic of teenage mental illness?* (Nature, marzo de 2024; réplica a Jonathan Haidt, *The Anxious Generation*, 2024). https://www.nature.com/articles/d41586-024-00902-2 ↩

[8] CNN — *Pikesville principal's voice on racist recording was an AI-generated deepfake* (Dazhon Darien / Eric Eiswert; enero-abril de 2024). https://www.cnn.com/2024/04/26/us/pikesville-principal-maryland-deepfake-cec/index.html ↩

[9] PNAS — *X under Musk's leadership: substantial hate and no reduction in inauthentic activity* (2025; +≈50 % odio; +70 % «me gusta»; actividad coordinada sin reducir). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11819532/ ↩

[10] Comisión Europea — *Guidelines on the protection of minors under the Digital Services Act* (14 de julio de 2025; ciberacoso, verificación de edad; riesgos sistémicos = discurso de odio ilegal). https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors ↩

[11] La Moncloa — *Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales* (Consejo de Ministros, 4 de junio de 2024; «alejamiento en línea»; verificación de edad). https://www.lamoncloa.gob.es/consejodeministros/resumenes/Paginas/2024/040624-rueda-de-prensa-ministros.aspx ↩

[12] Código Penal (España) — arts. 510 (delito de odio; prisión 1-4 años) y 172 ter (acoso/stalking; agravado por la edad de la víctima). https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444 ↩

[13] Ofcom / GOV.UK — *Online Safety Act 2023: protection of children codes* (deberes en vigor el 25 de julio de 2025; bullying y contenido de odio; multas hasta el 10 % de la facturación mundial). https://www.gov.uk/government/collections/online-safety-act ↩

[14] eSafety Commissioner (Australia) — *Social media age restrictions* (Act 2024; menores de 16 desde el 10 de diciembre de 2025; primer país). https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions ↩

[15] t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice). Véanse los capítulos 13 y 15. ↩

[16] EU Artificial Intelligence Act — *Article 50: transparency obligations* (marcado del contenido generado o manipulado por IA). https://artificialintelligenceact.eu/article/50/ ↩

[17] StopNCII.org — *How StopNCII.org works* (huella generada en el dispositivo; el contenido no sale nunca; modelo de solo-huellas). https://stopncii.org/how-it-works/ ↩

Personas mayores: la voz clonada y el abuso invisible

«Los viejos, ¿son hombres? Viendo cómo los trata nuestra sociedad, es lícito dudarlo.»

— Simone de Beauvoir, La vejez (1970)

Una tarde cualquiera, en un piso cualquiera, el móvil de una madre mayor se ilumina: «Hola mamá, se me ha roto el móvil, este es mi nuevo número. Escríbeme por WhatsApp cuando puedas.» El texto, sencillo y urgente, es el cebo de una de las estafas más extendidas en España. El estafador ha sacado el nombre y la relación familiar de redes sociales o de bases de datos filtradas y ha fabricado una urgencia creíble —la variante reciente dice «se me ha mojado el móvil»—; el INCIBE recomienda verificar siempre por otra vía, y la Policía Nacional ha alertado repetidamente [1]. Y esto es solo la versión escrita. Con la inteligencia artificial actual, la llamada siguiente puede traer la voz clonada del hijo de verdad, fabricada a partir de unos segundos de audio sacados de un vídeo público (véase el capítulo 68) [3].

Las cifras del termómetro estadounidense dan la escala de lo que se acerca. Según el FBI, en 2024 los mayores de 60 años perdieron cerca de 4.900 millones de dólares en ciberdelitos, un 43 % más que el año anterior; en 2025, las denuncias subieron a 201.266 y las pérdidas a 7.750 millones (+59 %), con más de 3.100 denuncias de séniores que mencionaban la IA —más de 352 millones perdidos— y más de 5 millones de dólares en estafas de angustia con voz clonada [2].

Este libro ha dedicado un capítulo al daño digital sobre los jóvenes (capítulo 84); este es su espejo para las personas mayores. La tecnología de la voz clonada se explica en el capítulo 68; el testamento y la herencia, en el capítulo 52; la fe de vida, en el capítulo 64; el fraude financiero corporativo, en el capítulo 16. La pregunta clave: ¿cómo protegemos a nuestros mayores —de la estafa, del abuso y de la presión— sin convertirlos en menores de edad vigilados? La respuesta es darles, a ellos y a sus familias, evidencia verificable con **t2p** —la huella SHA-512 en el dispositivo, el anclaje de la huella en la blockchain pública y el sello de tiempo RFC 3161/eIDAS complementario [11]—, bajo un principio irrenunciable que la ley española ya ha hecho suyo: apoyo, no sustitución (Ley 8/2021 [10]).

La estafa que llama a casa

La suplantación familiar ha dado el salto del texto a la voz. El FBI alertó en diciembre de 2024 de que la IA generativa se usa para clonar voces de familiares en las llamadas estafas «del abuelo» o de angustia: la llamada que llora y pide dinero urgente ya no necesita ningún actor —basta con unos segundos de audio del nieto o del hijo sacados de un vídeo colgado en cualquier red [3]. En 2025, las pérdidas declaradas por estas estafas de angustia con voz clonada superaron los 5 millones de dólares, dentro de un total de más de 352 millones perdidos por los séniores en fraudes con mención de IA [2]. Cada llamada es una invasión de la intimidad más profunda: el sonido de una voz querida, vuelto contra quien más la quiere.

La estafa romántica completa el cuadro. La FTC estadounidense recibió cerca de 60.000 denuncias en 2024, con pérdidas de 1.200 millones de dólares; y es la franja de 65 a 74 años la que sufre las pérdidas más altas —más ahorros acumulados, menos familiaridad con las tácticas digitales [4]. En España la modalidad está plenamente activa, con detenciones anunciadas por el Ministerio del Interior [6], y ha llegado al extremo más oscuro: el crimen de Morata de Tajuña, en 2023 —tres hermanos mayores asesinados después de haber sido víctimas de una estafa del amor de hasta 263.000 euros [5].

El patrón común de todas estas modalidades es doble. Primero, el estafador explota la mejor virtud de la víctima: la confianza en la familia y en el afecto. Segundo, cuenta con la mejor aliada posible: la vergüenza de denunciar. Cuando la víctima calla, no hay prueba, no hay estadística y no hay escarmiento. Y todavía hay un tercer frente, el más incómodo de todos: cuando el peligro no viene de fuera, sino de dentro —de quien cuida, o de quien espera la herencia—, la prueba se hace casi imposible. Los dos apartados siguientes entran de lleno en ello.

El abuso que no se ve

En enero de 2022, el periodista Victor Castanet publicó en Francia *Les Fossoyeurs* («Los enterradores»), una investigación sobre Orpea, uno de los grandes grupos europeos de residencias, con unos 260.000 residentes: racionamiento de comida y de productos de higiene para recortar costes en un grupo

subvencionado con dinero público, y desatención médica. La fiscalía francesa abrió investigaciones penales por indicios de maltrato, malversación de fondos públicos e infracciones laborales, con decenas de denuncias de familias —algunas por homicidio involuntario—; el Gobierno francés anunció una amplia operación de control de las residencias del grupo, y el Estado acabó inyectando 605 millones de euros a cambio de una participación mayoritaria [7]. La lección es estructural: el abuso en el cuidado pasa detrás de puertas cerradas, se borra en la rutina, y la palabra de una persona con demencia no pesa como prueba. Sin evidencia, ni las familias ni los inspectores pueden distinguir la residencia ejemplar de la que raciona pañales.

España ofrece el contrapunto en pequeño formato, y con salida. En una residencia de El Escorial, las hijas de una interna con demencia —informadas de que su madre podía estar siendo maltratada— instalaron una cámara oculta. La trabajadora fue condenada, con una multa de 480 euros y una indemnización de 3.000 confirmadas por la Audiencia Provincial de Madrid, y la cámara fue avalada como prueba válida [8]. Lo hace posible la doctrina del Tribunal Supremo: con sospecha previa y fundada de un delito grave, una cámara temporal y enfocada al lugar concreto supera el triple juicio de proporcionalidad —idoneidad, necesidad y proporcionalidad estricta— y vale en el proceso penal, aunque administrativamente pueda suponer una infracción de protección de datos [9]. El matiz es esencial: no es barra libre para espiar a cuidadores; es una excepción rigurosa para la sospecha fundada.

Y sin embargo, queda un vacío: la grabación casera, sin fecha cierta ni integridad acreditada, sigue siendo el flanco débil de cualquier procedimiento —«¿cuándo se grabó esto? ¿quién nos dice que no se ha editado?». Es exactamente el vacío que la prueba de existencia cierra, como veremos a continuación.

La última voluntad bajo presión

El capítulo 52 trató el testamento falsificado: la firma falsa, el documento alterado. Aquí el problema es más sutil y más frecuente: el testamento auténtico de una voluntad presionada. El familiar que aísla, el «cuidador» que sugiere, la visita al notario arrancada en un mal día. Ninguna falsificación en ninguna parte —y sin embargo, ninguna voluntad libre.

El marco legal español dio un giro de paradigma con la Ley 8/2021, de 2 de junio: de la sustitución al apoyo [10]. La persona mayor o con discapacidad puede testar si en aquel momento tiene aptitud para comprender y expresar su voluntad; puede ordenar ante notario medidas voluntarias —poderes preventivos, autocuratela, voluntades anticipadas—; quien le presta apoyo ha de rendir cuentas; y la curatela se vuelve excepcional. Es una arquitectura de dignidad: decide la persona, no la familia.

Pero la disputa llega años después, a menudo cuando la persona ya no está. ¿Había aptitud? ¿Había presión? El notario da fe del acto —de aquel momento, ante él—, pero los meses de aislamiento o de influencia previa no los ve nadie. La prueba de existencia aporta lo que faltaba: profundidad temporal. Las conversaciones propias selladas —la persona mayor que documenta, en su propio dispositivo, las presiones que recibe—; la decisión expresada y datada cuando aún está serena; la rendición de cuentas de quien presta apoyo, anclada para que nadie la pueda reescribir [11]. La voluntad deja de ser una foto de un instante para convertirse en una línea coherente en el tiempo —mucho más difícil de capturar, y mucho más difícil de discutir.

La prueba de existencia aplicada

La misma tecnología que clona la voz de un hijo puede certificar la voz del hijo de verdad.

1. El hijo de verdad

Contra la llamada clonada, la verificación familiar. La familia acuerda una palabra de seguridad y un protocolo: ante cualquier urgencia con dinero, se cuelga y se rellama al número de siempre [1]. Y el hijo de verdad puede enviar una prueba de vida sellada: un audio o vídeo corto respondiendo el reto acordado, con la huella SHA-512 calculada en el dispositivo y el sello de tiempo del minuto exacto [11]. La voz clonada puede imitar el timbre, pero no puede responder el reto ni fabricar un sello criptográfico del presente —es el mismo principio de reto y frescura de la fe de vida del capítulo 64, llevado a la escala de la familia (la autenticación de la red telefónica se trata en el capítulo 68). La regla de la casa se vuelve simple: quien llama pidiendo dinero y no puede sellar la respuesta, miente —por defecto.

2. La familia que vigila con respeto

Dentro de los límites estrictos de la doctrina del Supremo —sospecha fundada, cámara temporal y enfocada [9]—, la grabación que una familia se ve obligada a hacer vale mucho más si nace sellada: cada segmento con huella y hora ancladas [11], una cadena de custodia impecable desde el primer minuto, inmune al «esto está editado». En un caso como el de El Escorial [8], este blindaje habría ahorrado cualquier discusión sobre la autenticidad de las imágenes. Y la simetría que lo hace justo: las residencias también salen ganando. Registros de cuidado anclados —medicación, higiene, turnos, visitas— protegen al profesional diligente de la acusación injusta y hacen detectable el racionamiento sistémico que destapó el caso Orpea [7] antes de que se convierta en escándalo. La prueba no tiene bando: ampara a la interna, a la familia y al buen cuidador.

3. La voluntad acreditada

Una persona mayor que quiere blindar su última voluntad —no contra la familia, sino contra la duda— puede acompañar las medidas de la Ley 8/2021 [10] con evidencia anclada: el vídeo del momento de la decisión, con fecha cierta; las conversaciones donde expresa esta voluntad a lo largo de meses, con huella en su propio dispositivo; la rendición de cuentas de quien le presta apoyo, anclada [11]. Si alguna vez alguien alega captación —o si la captación existe de verdad—, habrá cronología verificable en lugar de recuerdos interesados. No sustituye al notario: lo complementa con lo que ningún acta puede contener — la consistencia de una voluntad en el tiempo.

4. El corazón verificado

Contra la estafa romántica, la prueba de existencia corta en las dos direcciones. Quien se relaciona en línea puede pedir al pretendiente pruebas de vida selladas —quien no puede acreditar ni un minuto verificable de su existencia real, sospecha por defecto [11]. Y la víctima que empieza a dudar puede sellar las conversaciones y los justificantes de pago en su dispositivo —sin vergüenza, sin tener que explicárselo todavía a nadie—, de manera que, si un día denuncia [6], lleve una cronología completa y no un puñado de capturas. Las cifras [4] y el recuerdo de Morata de Tajuña [5] dicen bastante claro qué hay en juego.

Hay que decir también qué no hace el sello: no detecta la mentira ni el amor fingido; no sustituye la llamada de cada domingo, ni la compañía, ni la financiación digna de los cuidados —el caso Orpea es un modelo de negocio, no un fallo criptográfico [7]. La prueba de existencia da a las personas mayores y a sus familias aquello que la vergüenza y la puerta cerrada les quitaban: la posibilidad de probarlo.

La promesa y el peligro

La promesa es un país donde la llamada del falso hijo se topa con una pregunta que no puede responder [11], donde el abuso en el cuidado deja de ser palabra contra silencio [8], y donde la última voluntad llega a los tribunales acreditada en el tiempo y no reconstruida de memoria [10]. Pero este capítulo toca a personas en situación vulnerable, y los peligros piden la máxima franqueza.

El primero es **la vigilancia paternalista**. Proteger no puede querer decir vigilar. Si la familia convierte el móvil de la abuela en un dispositivo monitorizado, habremos sustituido al estafador por la tutela — exactamente lo que la Ley 8/2021 quiso desterrar [10]. La regla de diseño: las herramientas las controla la persona mayor —su dispositivo, sus huellas, su decisión de revelar. El apoyo se presta con ella, nunca sobre ella.

El segundo es **la cámara como norma**. La doctrina del Supremo ampara una excepción —sospecha fundada, temporal, enfocada [9]—, no la videovigilancia permanente de los cuidadores, que vulneraría sus derechos y convertiría la desconfianza en estándar del cuidado. El sello hace sólida la prueba lícita; no hace lícita la captación que no lo era.

El tercero es **el registro que no debe existir**. La verificación familiar funciona con retos y huellas en el dispositivo de cada uno; un repositorio central de voces «auténticas» sería a la vez un botín para los clonadores y una infraestructura de vigilancia masiva. Solo huellas, revocables, sin biometría centralizada y sin desanonimización [11].

El cuarto peligro no es ninguna estafa: es poner tecnología donde falta compañía. Ningún sello cura la soledad —que es la puerta de entrada de la estafa romántica [4] y de la captación de la voluntad. La prevención real es compañía, atención y cuidados bien financiados; la criptografía solo garantiza que, cuando haga falta probar, se pueda. Si la tecnología sirve de excusa para llamar menos a casa, habremos perdido mucho más de lo que ningún estafador podía llevarse.

Es hora de actuar

La generación que nos enseñó a dar la palabra merece herramientas para poder demostrarla.

Para las familias: acordad una palabra de seguridad y el protocolo de rellamada [1]; ante cualquier urgencia con dinero, verificación sellada antes que transferencia [11]; y hablad de ello abiertamente en casa —la vergüenza es el arma del estafador.

Para las personas mayores: tu móvil puede ser tu memoria certificada. Sella las conversaciones que te presionan, los acuerdos que te prometen y tu voluntad cuando la tengas clara [10][11]; revelarlo —o no— será siempre decisión tuya.

Para residencias y cuidadores: anclad los registros de cuidado —medicación, higiene, turnos, visitas —: protegen al profesional honesto y hacen visible el racionamiento antes de que se convierta en escándalo [7].

Para notarios y juristas: combinad la fe pública con la profundidad temporal —las medidas de la Ley 8/2021 acompañadas de cronologías selladas de la voluntad [10][11].

Para bancos y plataformas: ante transferencias inusuales de clientes mayores, ofreced —nunca impongáis— la pausa de verificación: un reto de prueba de vida al presunto familiar antes de ejecutar el pago [3][11].

Para los legisladores: reconoced la prueba sellada en captura en los procedimientos de abuso y de captación de la voluntad; y financiad la inspección de residencias —ninguna cadena de bloques sustituye a un inspector [7].

El próximo «hola mamá» puede traer la voz exacta de tu hijo. Que la respuesta de tu casa sea una pregunta que solo tu hijo puede responder —y un sello que ninguna máquina puede falsificar. Por quienes nos dieron la palabra, **time2act**.

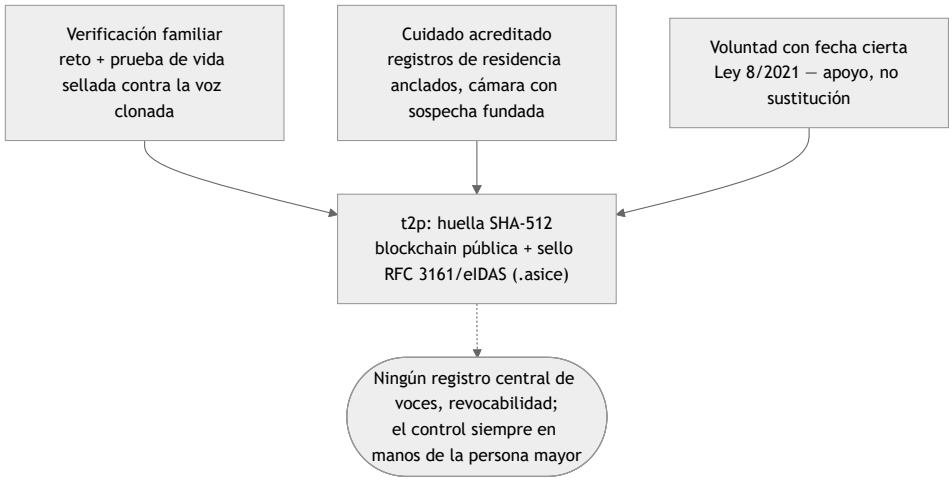


Figura 85.1 — Tres escudos para las personas mayores con una sola lógica (huella SHA-512 en el dispositivo, sello de tiempo RFC 3161/eIDAS, anclaje a la blockchain pública, .asice): la verificación familiar contra la voz clonada (reto + prueba de vida sellada), el cuidado acreditado (registros de residencia anclados; cámara solo dentro de la doctrina de proporcionalidad del TS) y la voluntad con fecha cierta (Ley 8/2021: apoyo, no sustitución). Límites: ningún registro central de voces, revocabilidad, y el control siempre en manos de la persona mayor. Fuentes: INCIBE; FBI/IC3; elDiario.es (El Escorial); Ley 8/2021.

[1] INCIBE / Infobae — *El teléfono de tu hijo no se dañó: la estafa en WhatsApp que pide dinero para una emergencia* (8 de mayo de 2025; mecánica del «hola mamá», variantes, recomendaciones de verificación); Policía Nacional (alerta) — OKDiario; Valencia News — *Así funciona la estafa del «hijo en apuros» por SMS y WhatsApp.* https://www.infobae.com/tecno/2025/05/08/el-telefono-de-tu-hijo-no-se-dano-la-estafa-en-whatsapp-que-pide-dinero-para-solucionar-una-emergencia/ · https://okdiario.com/curiosidades/policia-nacional-alerta-sobre-esta-estafa-hola-mama-telefono-esta-roto-10582931 · https://valencianews.es/tendencias/mama-se-me-ha-roto-el-movil-asi-funciona-estafa-del-hijo-en-apuros-sms-y-whatsapp/ ↩

[2] HousingWire — *FBI: Seniors lost $7.75B to cybercrime in 2025 — a 59% jump* (201.266 denuncias de mayores de 60; 4.900 M$ en 2024, +43 %; >3.100 denuncias sénior con IA y >352 M$; >5 M$ en estafas de angustia con voz clonada); PPC Land — *AI-linked fraud costs Americans $893 million* (22.364 denuncias de IA en 2025). https://www.housingwire.com/articles/fbi-seniors-cybercrime-2025/ · https://ppc.land/ai-linked-fraud-costs-americans-893-million-fbi-reports-for-2025/ ↩

[3] FBI / IC3 — *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud* (PSA-241203, 3 de diciembre de 2024; clonación de voz en estafas de angustia y suplantación de familiares). https://www.ic3.gov/PSA/2024/PSA241203 ↩

[4] Factchequeado — *Qué son las estafas de romance y cómo identificarlas* (FTC: ≈60.000 denuncias y 1.200 M$ en 2024; la franja 65-74 con las pérdidas más altas); AARP — *Los estafadores de romance engañan a sus víctimas con fraudes de criptomonedas*. https://factchequeado.com/teexplicamos/20240126/estafa-romance-scam/ · https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2023/enganos-de-romance-con-criptomoneda.html ↩

[5] Wikipedia — *Estafa romántica* (crimen de Morata de Tajuña, 2023: tres hermanos mayores asesinados; estafa de hasta 263.000 €). https://es.wikipedia.org/wiki/Estafa_rom%C3%A1ntica ↩

[6] Ministerio del Interior — *Detenidas dos personas por la estafa conocida como «Romance Scam», timo del amor*. https://www.interior.gob.es/opencms/es/detalle/articulo/Detenidas-dos-persona-por-la-estafa-conocida-como-Romance-Scam-timo-del-amor/ ↩

[7] Infobae — *Francia anuncia control de residencias de ancianos tras escándalo* (1 de febrero de 2022; «Les Fossoyeurs» de Victor Castanet; Orpea ≈260.000 residentes; racionamiento; investigaciones penales por maltrato, malversación e infracciones laborales; denuncias por homicidio involuntario); infoLibre — *El último escándalo de Orpea* (inyección estatal de 605 M€ por una participación mayoritaria). https://www.infobae.com/america/agencias/2022/02/01/francia-anuncia-control-de-residencias-de-ancianos-tras-escandalo/ · https://www.infolibre.es/politica/ultimo-escandalo-orpea-negocios-trama-societaria-oculta-luxemburgo_1_1232899.html ↩

[8] elDiario.es — *Condenada la trabajadora de una residencia cazada con una cámara oculta mientras maltrataba a una interna* (El Escorial; multa de 480 € e indemnización de 3.000 € confirmadas por la Audiencia Provincial de Madrid; cámara de las hijas avalada como prueba). https://www.eldiario.es/madrid/condenada-trabajadora-residencia-cazada-camara-oculta-maltrataba-interna_1_12498186.html ↩

[9] El Foro de Labos — *El Tribunal Supremo confirma la validez de una prueba obtenida con cámara oculta* (2022); Pardo Geijo Abogados — *¿Es legal poner cámaras ocultas en casa?* (sospecha fundada de delito grave; cámara temporal y enfocada; triple juicio de proporcionalidad). https://www.elforodelabos.es/2022/09/el-tribunal-supremo-confirma-la-validez-de-una-prueba-obtenida-con-camara-oculta/ · https://pardogeijo.com/es-legal-grabar-camaras-ocultas-casa/ ↩

[10] BOE — *Ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica* (apoyo, no sustitución; medidas voluntarias ante notario; aptitud para testar; rendición de cuentas; curatela excepcional); El Notario — *Una visión práctica de la Ley 8/2021*. https://www.boe.es/buscar/act.php?id=BOE-A-2021-9233 · https://www.elnotario.es/practica-juridica/11767-una-vision-practica-de-la-ley-8-2021-de-2-de-junio-sobre-personas-con-discapacidad ↩

[11] t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; prueba de vida con reto; contenido nunca fuera del dispositivo; revelación voluntaria). Véanse los capítulos 13, 15 y 64. ↩

Comunicaciones oficiales: ¿quién certifica que el jefe de Estado ha dicho esto?

«Las palabras tuvieron que cambiar su significado ordinario y tomar el que ahora se les daba.»

— Tucídides, Historia de la guerra del Peloponeso, III, 82

A mediados de junio de 2025, alguien creó una cuenta de Signal con el nombre visible «marco.rubio@state.gov». Con una voz clonada por IA e imitando el estilo de escritura del secretario de Estado de EE. UU., **Marco Rubio**, el impostor contactó al menos con **tres ministros de exteriores extranjeros, un senador de EE. UU. y un gobernador**: dejó mensajes de voz en Signal a dos de los contactados y, en un caso, envió un mensaje de texto invitando al interlocutor a pasar a la misma aplicación. Un cable del Departamento de Estado del **3 de julio de 2025** alertó a los empleados: el objetivo probable era acceder a información o a cuentas, y el autor no se ha identificado [3]. No hacía falta piratear ningún sistema; bastó con una voz y un nombre en una aplicación de mensajería para hacer pasar por buena la palabra de la diplomacia estadounidense.

El precedente canónico se remonta al **16 de marzo de 2022**, cuando unos atacantes piratearon el canal ucraniano **Ukraine 24** y difundieron en él un deepfake del presidente **Volodímir Zelenski** que parecía ordenar a los soldados deponer las armas, mientras el teletipo pirateado afirmaba que había huido de Kíiv; Zelenski lo desmintió en horas con un selfie real desde el centro de Kíiv («provocación infantil») [1] —es el caso que hemos analizado en el capítulo 20. La pregunta que ambos episodios dejan abierta vertebra este capítulo: cuando un mensaje oficial se puede falsificar y empujar por un canal de confianza —o por uno personal, como Signal—, ¿cómo puede el público confirmar de manera rápida e independiente qué ha dicho de verdad su gobierno?

Este capítulo es distinto del capítulo 48 —la integridad electoral, donde el blanco es la campaña, el candidato y el voto— y del capítulo 20 —la defensa y los derechos humanos, donde hablamos de mando en el campo de batalla y prueba de crímenes de guerra. Aquí el sujeto es la **autenticidad de las comunicaciones oficiales de crisis y de las declaraciones que mueven mercados**: lo que dice un Estado o una institución en el momento que más importa. La pregunta no es si una falsedad se puede crear —se puede—, sino cómo una autoridad puede publicar su palabra de manera que cualquier periodista o ciudadano la pueda **verificar en segundos** como genuina, y cómo una falsificación se puede **desmentir contra el original** antes de que el pánico haga su trabajo. Es la tesis de este libro aplicada al momento más frágil de todos: la emergencia.

Cuando el canal de confianza se vuelve el arma

El caso de Ukraine 24 no es anecdótico: como hemos visto, es el patrón. El **22 de mayo de 2023**, una imagen generada por IA de una explosión cerca del **Pentágono**, difundida por una cuenta falsa que se hacía pasar por «Bloomberg» y amplificada por la rusa RT, hizo caer brevemente el **S&P 500 alrededor de un 0,3 %** (unos 30 puntos) y el Dow unos 80 puntos entre las 10:06 y las 10:10 de la mañana, recuperándose a las 10:13; Bloomberg lo describió como «posiblemente la primera vez que una imagen generada por IA mueve el mercado» [2]. La falsedad vivió cuatro minutos y movió miles de millones: no hacía falta que fuera buena, solo que llegara por un canal que parecía de confianza.

En **abril de 2025**, la **Channel 14** de Israel emitió en directo, sin verificarlo, un deepfake de origen iraní del exministro de Defensa **Yoav Gallant** afirmando falsamente que EE. UU. no podía derrotar a los hutíes; el presentador lo cortó a mitad («parad el vídeo… esto es falso») y la cadena se disculpó [4].

Del fraude financiero al pánico de masas

La rama preferida de los estafadores son las figuras que encarnan la confianza institucional. En febrero de 2024, Mugur Isărescu, el gobernador del banco central más longevo del mundo, apareció en un deepfake que promocionaba inversiones fraudulentas —parte de una oleada que ha golpeado a los jefes de banco central: el luxemburgués Gaston Reinesch, el gobernador del Reserve Bank de la India y, en junio de 2026, una falsificación del gobernador del Banco de Inglaterra, Andrew Bailey [5]. Si se puede fabricar la cara que dice «vuestro dinero está seguro», el fraude no solo roba ahorros: erosiona el fundamento de todo el sistema.

La otra cara es el pánico. Como hemos visto el **13 de enero de 2018**, una alerta oficial en Hawái —no un deepfake, sino un error humano genuino— anunció «AMENAZA DE MISIL BALÍSTICO ENTRANTE A HAWÁI. BUSQUEN REFUGIO INMEDIATO. ESTO NO ES UN SIMULACRO», y la corrección se retrasó **38 minutos** [6]; una situación que habría podido generar un pánico de masas y decisiones irreversibles si hubiera sido falsificada. El **16 de mayo de 2026**, la policía de Singapur reveló una videollamada de Zoom con deepfakes de altos cargos, incluido el primer ministro Lawrence Wong, que supuso una pérdida mínima de **4,9 millones de dólares singapurenses** (3,8 millones de dólares de EE. UU.); Wong ya había advertido en marzo de 2025 del uso indebido de su imagen para estafas [8].

El marco: autenticar en la emisión, pero no en la distribución

Los reguladores y las agencias de seguridad ya han actuado, sobre todo por el lado de la emisión. Como hemos visto, el Reglamento europeo de IA, artículo 50 (Reglamento 2024/1689), obliga a los desplegadores —incluidas las autoridades públicas en asuntos de interés público— a revelar el contenido deepfake (definido en el art. 3.60) a partir del 2 de agosto de 2026, con sanciones de hasta 15 millones de euros o el 3 % de la facturación mundial [7]. En EE. UU., el sistema de alertas IPAWS de FEMA ya firma digitalmente cada alerta oficial (EAS/WEA, mensajes CAP) y la autentica vía IPAWS-OPEN para evitar la suplantación, con certificados que se renuevan cada tres años: la línea base de autenticación en la emisión. Una hoja informativa de ciberseguridad de la NSA/CISA y sus socios de los Five Eyes (29 de enero de 2025) recomienda las Content Credentials C2PA y la procedencia duradera para los medios gubernamentales y de infraestructura crítica, en línea con eIDAS y los sellos cualificados.

El agujero, sin embargo, es evidente: toda esta arquitectura protege el momento en que la autoridad emite. No protege el momento en que el mensaje se distribuye y se reemite —el teletipo de Ukraine 24, la reemisión no verificada de Channel 14, la imagen falsa de «Bloomberg». Es en este tramo donde el público queda sin defensa.

Por qué la firma en la emisión por sí sola no salva

Hay que decirlo con crudeza. Que IPAWS firme una alerta o que un comunicado lleve un sello cualificado eIDAS resuelve la autenticidad en el origen, pero no llega al ciudadano que recibe el mensaje reenviado por WhatsApp, visto en una noticia televisiva extranjera o leído en un teletipo pirateado. La firma vive en un sistema cerrado; el periodista que ha de decidir en dos minutos si emite o no un clip no tiene ningún botón universal para comprobarla.

Peor, ninguno de estos controles existe en el lugar donde ocurrió el daño. Ukraine 24 no falló en la emisión de Zelenski —falló porque otra persona empujó una falsedad por un canal que el público creía suyo. La firma en el origen solo certifica lo que la autoridad emitió, no desmiente lo que un atacante ha distribuido. Falta una comprobación pública, neutral respecto del proveedor y fuera de línea, junto a la distribución, que cualquiera pueda hacer en segundos sin pedir permiso a nadie.

La prueba de existencia aplicada

Es aquí donde **t2p** aporta la pieza que faltaba sobre el artefacto oficial mismo. El objeto sellado es la **declaración oficial autorizada en el momento de emisión**: el vídeo o audio de la oficina de prensa, el comunicado PDF firmado, la decisión del banco central o la carga útil de la alerta de emergencia, antes de que salga del órgano emisor. En la oficina de prensa o en el centro de operaciones, la aplicación de captura calcula en el dispositivo la **huella SHA-512** —el fichero no sale nunca—, obtiene un **sello de tiempo RFC 3161/eIDAS** y ancla la huella a la blockchain pública, produciendo un contenedor **.asice** verificable fuera de línea. Para declaraciones en directo del principal —un jefe de Estado grabando un desmentido, un ministro en el atril—, una **prueba de vida** y el **GPS forense** ligan el acto a aquella persona, aquel lugar y aquel minuto. La autoridad publica entonces el **handle de verificación** (un QR o URL en el canal oficial) para que cualquiera confirme en segundos que *este* fichero exacto viene de la fuente genuina, a la hora declarada, bit a bit inalterado.

Así, un teletipo pirateado, una reemisión no verificada o un clip falsificado se pueden **desmentir contra el original sellado** en minutos —como el selfie de Zelenski, pero criptográficamente demostrable. Complementa, no sustituye, los controles en la emisión: las firmas IPAWS, la procedencia C2PA/Content

Credentials (como hemos visto en el capítulo 13 y 15), los sellos cualificados eIDAS y las herramientas de detección.

El sello prueba **el origen, la hora, el autor y la integridad** del artefacto oficial —no que su contenido sea verdad, legal o de interés público. Si un cargo autorizado emite una declaración falsa, presa del pánico o inconstitucional —o comete un error honesto como la alerta de Hawái de 2018—, un sello válido demostrará que el mensaje equivocado vino realmente del despacho correcto. No detiene un deepfake que no se compara con el original, ni impide que el público ignore el handle de verificación; tampoco sustituye la verificación editorial, la credibilidad institucional o las capas existentes de C2PA/SynthID, firma IPAWS y detección.

La promesa y el peligro

La promesa es cerrar el agujero de la distribución: devolver a la autoridad —y al público— una manera **rápida, pública e independiente** de separar la palabra oficial auténtica de la falsificación, en el momento de crisis en que cada minuto cuenta. El selfie de Zelenski funcionó porque él es Zelenski y lo podíamos creer; un handle de verificación sellado funcionaría para cualquier funcionario, sin depender de la fama ni de la improvisación, y con prueba matemática en lugar de confianza ciega.

El peligro pide matices. El primero: la **falsa seguridad** —«está sellado, luego es cierto»—, cuando el sello solo garantiza el origen, no la verdad ni la legalidad del contenido. El segundo: si los sistemas emisores se piratean para que firmen una carga maliciosa, el sello **autenticaría la mentira** con toda la solemnidad; la seguridad del emisor es condición previa, no consecuencia. Y el tercero: el **dividendo del mentiroso** se agrava si el público aprende que «sin sello» equivale a «falso», porque entonces cualquier declaración incómoda no sellada se puede descartar como falsa. La prueba de existencia es una capa de verificación pública, no un certificado de veracidad ni un sustituto del criterio.

Además, el diseño descentralizado del protocolo puede ser una fachada que esconde una concentración de poder real: ¿quién define las reglas de actualización y qué nodos tienen la autoridad para firmarlas? Si la comunidad se limita a votar sobre propuestas presentadas por un pequeño grupo de expertos o por entidades corporativas, el consenso aparente se convierte en una decisión impuesta desde dentro. En este escenario, el control del código —y, por tanto, del mecanismo de sellado— pasa a manos de una élite que puede ajustar las condiciones de emisión para favorecer intereses particulares, como suprimir declaraciones incómodas o introducir filtros ocultos. Como advierte Marc Goodman, «quien controle el código controlará el mundo, para bien y para mal»[12]; la vulnerabilidad no reside solo en la tecnología, sino en quién tiene la clave de actualización y qué transparencia ofrecen sus decisiones. Por tanto, la promesa de confianza pública se ve amenazada si la gobernanza del protocolo se mantiene opaca o centralizada bajo una capa de descentralización aparente.

Es hora de actuar

Para las **oficinas de prensa y los gabinetes de gobierno**: sellar cada comunicado, vídeo y audio oficial en el momento de emisión y publicar su handle de verificación en el canal oficial. Para las **autoridades de emergencia** (FEMA y sus homólogas): extender la firma tipo IPAWS con un sello público y verificable fuera de línea que el ciudadano pueda comprobar sin acceso al sistema cerrado. Para las **redacciones y las agencias de noticias**: exigir y comprobar el handle de verificación antes de reemitir un clip oficial —el reflejo que faltó a Channel 14. Para los **bancos centrales y las instituciones financieras**: sellar toda declaración que mueva mercados, para que un deepfake de Isărescu o de Bailey se pueda falsificar en segundos. Y para los **reguladores** (la Oficina de IA, bajo el artículo 50): reconocer el handle sellado como medio de cumplimiento de la transparencia y como evidencia admisible de lo que dijo la autoridad y cuándo.

En Kíiv, un presidente tuvo que grabarse un selfie para demostrar que seguía en su puesto. Dar a cada autoridad —y a cada ciudadano— una manera de probar criptográficamente qué se dijo oficialmente, sin depender de la fama ni de la suerte, y sin olvidar nunca que el sello no hace verdad lo que se declara en él, es, en este frente donde la palabra oficial es la última línea de defensa, time2act.

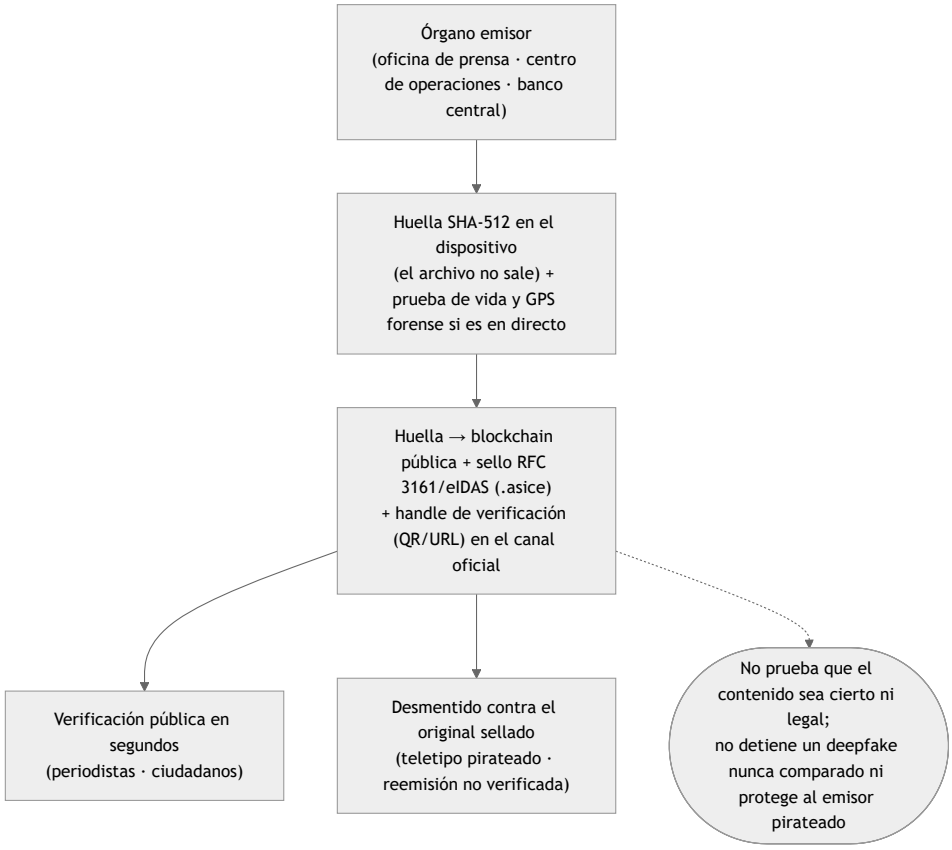


Figura 86.1 — El órgano emisor (oficina de prensa, centro de operaciones, banco central) calcula en el dispositivo la huella SHA-512 de la declaración oficial —vídeo, comunicado, decisión o alerta— sin que el fichero salga; para declaraciones en directo del principal le añade prueba de vida y GPS forense. La huella del conjunto se ancla en la blockchain pública, con sello RFC 3161/eIDAS complementario (.asice), y se publica su handle de verificación (QR/URL) en el canal oficial. Dos resultados: a la izquierda, verificación pública en segundos por parte de periodistas y ciudadanos; a la derecha, el desmentido de una falsificación (teletipo pirateado, reemisión no verificada) contra el original sellado. Límite: el sello prueba origen, hora, autor e integridad, no que el contenido sea cierto, legal ni sensato; no detiene un deepfake nunca comparado ni protege al emisor de ser pirateado. Fuentes: caso Ukraine 24/Zelenski; imagen falsa del Pentágono; caso Rubio; caso Channel 14/Gallant; alerta de Hawái de 2018; artículo 50 del Reglamento de IA; IPAWS; CSI Content Credentials NSA/CISA.

---

[1] Atlantic Council — *Russian War Report: Hacked news program and deepfake video spread false Zelenskyy claims* (16 de marzo de 2022; pirateo del teletipo y la web de Ukraine 24; deepfake de rendición; desmentido con selfie de «provocación infantil»). https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-hacked-news-program-and-deepfake-video-spread-false-zelenskyy-claims/ ↩

[2] NPR — *Fake viral images of an explosion at the Pentagon were probably created by AI* (22 de mayo de 2023; cuenta falsa de «Bloomberg», amplificación de RT, caída breve del mercado). https://www.npr.org/2023/05/22/1177590231/fake-viral-images-of-an-explosion-at-the-pentagon-were-probably-created-by-ai ↩

[3] NPR — *Impostor uses AI to impersonate Rubio and contact foreign and U.S. officials* (julio de 2025; voz clonada del secretario de Estado en Signal; cable del Departamento de Estado del 3 de julio). https://www.npr.org/2025/07/09/nx-s1-5462195/impostor-ai-impersonate-rubio-foreign-officials ↩

[4] Clarity — *Iranian Deepfake of Israeli Defense Minister Airs Live* (abril de 2025; reemisión no verificada de Channel 14 de un deepfake de Yoav Gallant; corte en directo y disculpa). https://www.getclarity.ai/ai-deepfake-blog/iranian-deepfake-of-israeli-defense-minister-airs-live----and-how-clarity-caught-it-instantly ↩

[5] Romania Insider — *Romanian central bank governor Mugur Isarescu targeted by deepfake* (febrero de 2024; deepfake de inversiones fraudulentas; patrón en varios bancos centrales). https://www.romania-insider.com/bnr-mugur-isarescu-deepfake-february-2024 ↩

[6] Wikipedia — *2018 Hawaii false missile alert* (13 de enero de 2018; falsa alerta WEA de misil balístico; corrección de 38 minutos; error genuino). https://en.wikipedia.org/wiki/2018_Hawaii_false_missile_alert ↩

[7] EU Artificial Intelligence Act — *Article 50: Transparency Obligations* (revelación de deepfakes, incluidas autoridades públicas; aplicable desde el 2 de agosto de 2026; definición en el art. 3.60; sanciones de hasta 15 M€ / 3 %).

https://artificialintelligenceact.eu/article/50/ ↩

[8] NSA/CISA et al. — *Content Credentials: Strengthening Multimedia Integrity in the Generative AI Era* (CSI, 29 de enero de 2025; guía Five Eyes que avala las Content Credentials C2PA para medios gubernamentales y de infraestructura crítica). https://media.defense.gov/2025/Jan/29/2003634788/-1/-1/0/CSI-CONTENT-CREDENTIALS.PDF ↩

[9] FEMA — *Integrated Public Alert & Warning System (IPAWS)* (alertas oficiales firmadas digitalmente por la autoridad emisora y autenticadas por IPAWS-OPEN; línea base de autenticación en la emisión). https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system

[10] Singapore Police Force — *Footage from Zoom video conference involving impersonation of senior government officials* (16 de mayo de 2026; deepfake del PM Lawrence Wong, el presidente Tharman y representantes de la MAS; pérdida de 4,9 M$ SGD por una sola víctima). https://www.police.gov.sg/media-hub/news/2026/05/20260516_footage_from_zoom_video_conference_involving_impersonation_of_senior_government_officials

[11] Bulletin of the Atomic Scientists — *AI misinformation is threatening emergency communications. Here's how to fix that* (septiembre de 2025; alertas oficiales falsas, el «dividendo del mentiroso» y la autenticación de las comunicaciones de emergencia). https://thebulletin.org/2025/09/ai-misinformation-is-threatening-emergency-communications-heres-how-to-fix-that/

[12] Marc Goodman — *Delitos del futuro* (Ariel, 2015). ↩

Suplantar al director financiero: ¿quién ha autorizado de verdad este pago?

«Es de prudencia no fiarse nunca del todo de quienes nos han engañado una vez.»

— René Descartes, Meditaciones metafísicas, I (1641)

En enero de 2024, en la oficina de Hong Kong de la empresa británica de ingeniería y diseño **Arup**, un empleado del departamento financiero recibió la instrucción de transferir unos **200 millones de dólares de Hong Kong** —alrededor de **25,6 millones de dólares** de Estados Unidos. Al principio sospechó: el correo que originaba la orden le parecía una estafa de *phishing*. Pero lo invitaron a una **videoconferencia** donde estaba el director financiero del grupo, con sede en el Reino Unido, y varios colegas más; todos tenían la cara y la voz exactas de quien decían ser. Tranquilizado por lo que veía y oía, el empleado ejecutó **15 transferencias** a cinco cuentas bancarias de Hong Kong a lo largo de una semana. Todos los participantes de la llamada, salvo él, eran *deepfakes* generados por IA. El director global de sistemas de información de Arup, Rob Greig, lo confirmó meses después: «podemos confirmar que se usaron voces e imágenes falsas», y que ningún sistema interno había sido comprometido —el fraude funcionó **puramente suplantando una autorización** [1]. En 2025 no se había detenido a nadie ni se habían recuperado los fondos.

Este capítulo trata una cara muy concreta del fraude, distinta de la del capítulo 16 —que cubre el paisaje amplio del crimen financiero y el cumplimiento normativo. Aquí no hablamos de la detección genérica del fraude, sino de un acto único y puntual: **la autorización de un pago o una instrucción ejecutiva**. La pregunta no es si la cara de la pantalla es real —ya hemos visto que es imposible de garantizar—, sino cómo demostrar que **una directiva proviene de verdad del directivo**. La tesis del libro se aplica directamente: en lugar de perseguir la falsedad, sellamos la verdad en el origen.

Un fraude que no necesita romper nada

Lo que hace estremecer del caso Arup es que no se vulneró ningún sistema: no hubo intrusión, ni software malicioso, ni contraseñas robadas. El fraude explotó lo único que ningún *firewall* protege: la **confianza humana en una cara y una voz conocidas**. Greig fue explícito en que los sistemas internos no se tocaron; la debilidad era de proceso, no técnica, porque la compañía no podía distinguir una autorización genuina del director financiero de una fabricada, ya que la autorización misma nunca se había sellado.

Como hemos visto en marzo de 2025, un director financiero de una multinacional en **Singapur** autorizó un pago de **499.000 dólares** durante una llamada de Zoom donde el director ejecutivo y otros directivos eran todos *deepfakes* generados por IA; ningún participante era real [7]. En **julio de 2024**, un directivo de **Ferrari** desbarató una clonación de voz del consejero delegado, Benedetto Vigna —empujada por un número de WhatsApp desconocido para firmar con urgencia un acuerdo de confidencialidad sobre una adquisición secreta— con una pregunta que solo el Vigna real podía responder: el título de un libro que había recomendado hacía poco. La llamada se cortó de golpe [5]. Y en **mayo de 2024**, unos estafadores suplantaron al consejero delegado de **WPP**, Mark Read, con una cuenta falsa de WhatsApp, una reunión de Microsoft Teams, una voz clonada e imágenes de YouTube; el intento fracasó sin pérdidas, y Read advirtió al personal de que «todos debemos estar atentos a las técnicas que van más allá de los correos para aprovechar reuniones virtuales, IA y *deepfakes*» [6]. La diferencia entre Arup y Ferrari fue, literalmente, una pregunta a contracorriente.

La escala del problema, en cifras

La suplantación de directivos no es una anécdota: es una industria en crecimiento. El **compromiso del correo corporativo** (BEC) sigue siendo una de las categorías más costosas que rastrea el centro de denuncias del FBI (IC3): alrededor de **3.000 millones de dólares** en pérdidas declaradas, y casi **8.500 millones** perdidos por BEC en los tres últimos años [8]. Y la IA generativa le echa gasolina. El **Center for Financial Services de Deloitte** proyecta que las pérdidas por fraude habilitado por IA generativa en Estados Unidos podrían llegar a los **40.000 millones de dólares en 2027**, desde los 12.300 millones de 2023 —un crecimiento anual compuesto del **32 %**—, con el fraude por correo y BEC llegando potencialmente a los **11.500 millones** en el escenario más agresivo [2]. El caso Arup, con sus **25,6**

millones, es por ahora uno de los fraudes de pago habilitados por *deepfake* más grandes documentados, pero la tendencia indica que dejará de ser excepcional.

Lo que dicen los reguladores

Las autoridades ya han tomado nota. El **13 de noviembre de 2024**, la unidad de inteligencia financiera del Tesoro estadounidense, **FinCEN**, emitió la alerta **FIN-2024-Alert004**, advirtiendo que los criminales usan medios *deepfake* generados por IA —documentos de identidad fraudulentos, audio y vídeo— para burlar los controles de verificación de identidad y autenticación de las entidades financieras; recomienda **comprobaciones en vivo** y **autenticación multifactor resistente al *phishing*** [3]. El **15 de mayo de 2025**, el IC3 del FBI publicó el aviso **PSA250515**, alertando de que actores maliciosos envían mensajes de voz y texto generados por IA suplantando a altos cargos, y aconseja confirmar la identidad **por canales previamente verificados** y usar **frases de verificación pactadas**, porque el contenido generado por IA «ha avanzado hasta el punto de que a menudo es difícil de identificar» [4].

El marco legal europeo aporta la pieza clave: el **Reglamento eIDAS (UE) núm. 910/2014**, artículos 41 y 42, reconoce un **sello de tiempo electrónico cualificado** con presunción de exactitud e integridad que no puede ser denegado como prueba en ningún estado miembro; es la columna vertebral para sellar un artefacto de autorización. En el Reino Unido, la **Solicitors Regulation Authority** actualizó el 5 de marzo de 2024 su evaluación de riesgos de blanqueo señalando los *deepfakes* como riesgo emergente para las instrucciones de pago y las comunicaciones urgentes con clientes. Los regímenes de APP en el Reino Unido y en la UE ya tratan estos pagos fraudulentos como una categoría propia que exige reforzar los controles de autorización.

Por qué la alerta por sí sola no salva

Hay que decirlo con crudeza. Las recomendaciones de FinCEN y del FBI son sensatas —verificación en vivo, devolución de llamada por un canal conocido, frases pactadas—, pero todas dependen de que **alguien, bajo presión, recuerde y aplique un procedimiento** en el momento exacto en que un directivo aparentemente furioso exige un pago urgente. El empleado de Arup tenía buen olfato: sospechó del correo. Lo que lo venció fue la **prueba social** de una sala llena de caras conocidas. Una política de devolución de llamada no sirve de nada si la víctima cree que ya está hablando con el jefe. Una frase de verificación pactada protege si la recuerdas y si el otro también debería saberla; el directivo de Ferrari se salvó por instinto, no por procedimiento. El problema de fondo es que hoy la autorización es un **juicio subjetivo** —«esto parece el jefe»— en lugar de una **comprobación objetiva**. Mientras la pregunta sea «¿me parece real?», los *deepfakes* siempre acabarán ganando, porque cada año parecen más reales.

La prueba de existencia aplicada

Es aquí donde **t2p** invierte el modelo de confianza. El artefacto que hay que proteger no son los fondos: es la **directiva de autorización misma** —la instrucción ejecutiva. En lugar de que el equipo financiero intente (y fracase) detectar si la cara de la llamada es real, el **directivo genuino sella proactivamente cada directiva que autoriza**. Cuando se emite una orden de pago o de transferencia, el directivo la captura en su dispositivo: un texto de instrucción firmado, la aprobación de una factura en PDF o una breve autorización en vídeo o voz con **prueba de vida** y **GPS forense** que confirman una persona viva en un lugar conocido. El dispositivo calcula localmente la **huella SHA-512** —la instrucción no sale nunca del dispositivo—, obtiene un **sello de tiempo RFC 3161 conforme a eIDAS**, anclando la huella a la blockchain pública y generando un contenedor **.asice** verificable fuera de línea.

A partir de aquí, la tesorería no mueve ni un euro si la instrucción no llega con un sello válido, datado y ligado al directivo, que se verifica contra el ancla pública. La pregunta «¿el jefe lo ha aprobado de verdad?» deja de ser un juicio subjetivo y pasa a ser una comprobación criptográfica; un director financiero deepfake en una llamada de Zoom simplemente no puede producir el sello criptográfico previo del directivo real, de manera que una instrucción «urgente» sin sello es, por diseño, una bandera roja. Esto ataca el modo de fallo de Arup, donde una videoconferencia convincente sustituyó a una autorización verificable. La capa complementa, nunca sustituye, los controles existentes: convive con la devolución de llamada por canal externo, la doble firma o «cuatro ojos», el cribado de pagos y la capa de procedencia C2PA/SynthID, como hemos visto en las secciones 13 y 15.

El sello demuestra que una directiva concreta la emitió un titular de clave concreto en un instante determinado y que no se ha alterado —prueba el acto de autorizar, no que la autorización sea legítima o libre de fraude. Si el directivo es coaccionado, sobornado o engañado hasta sellar un pago fraudulento, o le roban el dispositivo o la clave de firma, el sello certificará una mala instrucción; no verifica que el beneficiario sea legítimo, ni que la factura sea real, ni impide el blanqueo de fondos. Tampoco detiene a un insider con clave legítima ni detecta un deepfake en una llamada sin sello —solo hace sospechosa la ausencia del sello. La verificación de los humanos de la llamada misma —el handshake de vida de cada participante, antes de abrir los micrófonos— se trata en el capítulo 88. La recuperación de fondos ya transferidos depende de una política «sin sello, no hay pago», y la capa refuerza las devoluciones de llamada, el doble control y el juicio humano sin sustituir la auditoría, la segregación de funciones ni un responsable financiero escéptico.

La promesa y el peligro

La promesa es convertir la autorización en algo **verificable** en lugar de creíble: pasar de «me parece el jefe» a «el sello cuadra». Una tesorería con una regla de «sin sello, no hay pago» hace que el directivo *deepfake* más perfecto del mundo sea inútil, porque le falta lo único que no puede fabricar —la clave privada del directivo real. El empleado de Arup, mañana, no tendría que decidir si una cara es real; solo tendría que comprobar un sello.

El peligro pide los matices de siempre. El primero: la **seguridad de la clave**. Si el sello se convierte en la única puerta, la clave de firma del directivo se convierte en el objetivo —hay que protegerla con hardware, biometría y recuperación robusta, o el ladrón cambia de cara por clave. El segundo: la **falsa tranquilidad**. «Está sellado, luego es bueno» es un error peligroso; el sello certifica el origen, no la bondad de la instrucción, y un directivo coaccionado sella igual. El tercero: la **concentración y la exclusión**, que la regla no deje fuera a los proveedores o socios pequeños sin capacidad de sellar, ni se convierta en una barrera que favorezca solo a los grandes. La prueba de existencia es una capa de gobernanza del pago, no un certificado de que el pago sea sensato.

Es hora de actuar

Para los directivos y consejerías delegadas (Vigna, Read, directores financieros): adoptar la costumbre de sellar cada autorización de pago en el dispositivo en el momento de emitirla, para que la tesorería pueda exigir su prueba. Para los departamentos de tesorería y finanzas: imponer la regla «sin sello, no hay pago» y combinarla con la devolución de llamada y el doble control; un sello válido tendrá que ser condición necesaria, no suficiente. Para los bancos y proveedores de pagos: ofrecer la verificación del sello como parte del cribado de transferencias, sobre todo en pagos grandes y urgentes a cuentas nuevas. Para los reguladores (FinCEN, FBI/IC3, SRA, regímenes APP): reconocer la directiva sellada con sello de tiempo eIDAS como control válido de autorización y como evidencia en las investigaciones de fraude. Y para los proveedores de software financiero y ERP: integrar el sello y la verificación en los flujos de aprobación, para que «sin sello, no hay pago» sea el camino por defecto, no una excepción heroica.

En Hong Kong, un empleado con buen olfato fue vencido por una sala llena de caras que no existían. Dar a cada autorización una prueba sellada que ningún deepfake puede fabricar —sin olvidar nunca que el sello prueba el acto, no la bondad de la instrucción— es, en este frente donde un clic mueve millones, time2act.

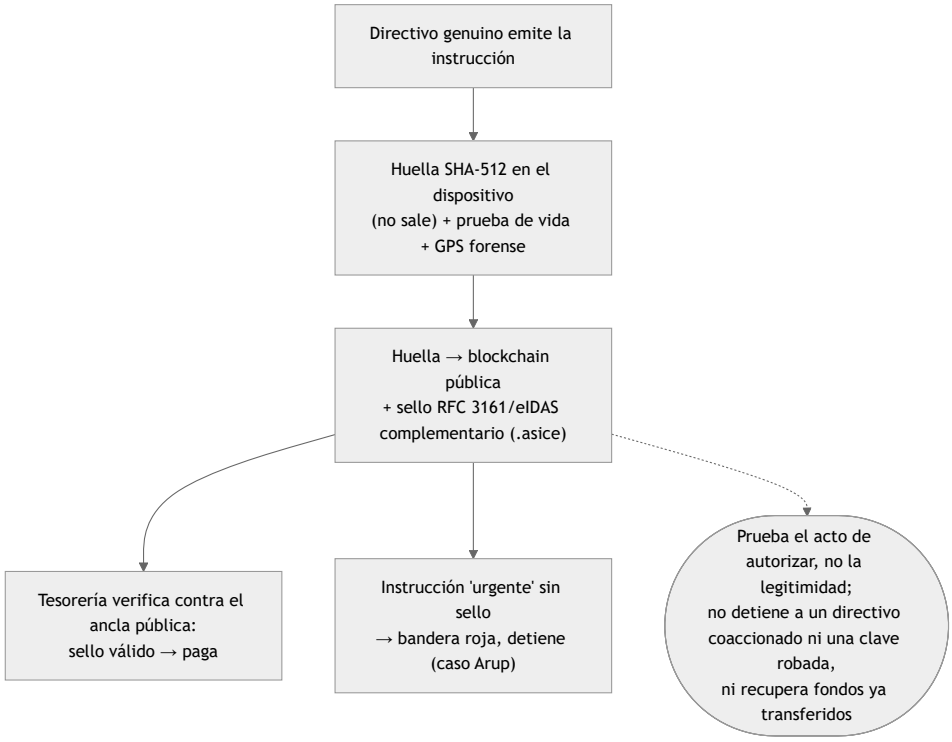


Figura 87.1 — El directivo genuino captura la instrucción de pago en el dispositivo (texto firmado, factura en PDF o vídeo con prueba de vida y GPS forense), calcula su huella SHA-512 sin que salga del dispositivo, y la ancla en la blockchain pública, con un sello de tiempo RFC 3161/eIDAS complementario (.asice). La tesorería verifica el sello contra el ancla pública: si cuadra, paga; si falta, detiene —la instrucción «urgente» sin sello es, por diseño, una bandera roja (modo de fallo de Arup). Límite: el sello prueba el acto de autorizar, no que la instrucción sea legítima; no detiene a un directivo coaccionado ni una clave robada, ni recupera fondos ya transferidos. Fuentes: caso Arup; alerta FinCEN FIN-2024-Alert004; FBI/IC3 PSA250515; eIDAS art. 41-42.

---

[1] Fortune — *A deepfake 'CFO' tricked British design firm Arup in $25 million fraud* (Arup confirmado como víctima; HK$200M/US$25,6M; 15 transferencias; declaración del CIO Rob Greig). https://fortune.com/europe/2024/05/17/arup-deepfake-fraud-scam-victim-hong-kong-25-million-cfo/ ↩

[2] Deloitte — *Generative AI is expected to magnify the risk of deepfakes and other fraud in banking* (proyección: 40.000 M$ de fraude por IA generativa en 2027 desde 12.300 M$ en 2023; 32 % de crecimiento anual; ~11.500 M$ de fraude por correo/BEC). https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html ↩

[3] FinCEN — *FinCEN Issues Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions* (alerta FIN-2024-Alert004, 13 de noviembre de 2024; recomienda verificación en vivo y MFA resistente al phishing). https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial ↩

[4] FBI/IC3 — *Senior US Officials Impersonated in Malicious Messaging Campaign* (PSA250515, 15 de mayo de 2025; voz/texto generados por IA; verificación fuera de banda y frases pactadas). https://www.ic3.gov/PSA/2025/PSA250515 ↩

[5] Fortune — *Ferrari exec foils deepfake attempt by asking the scammer a question only CEO Benedetto Vigna could answer* (julio de 2024; clonación de voz desbaratada con una pregunta de control). https://fortune.com/2024/07/27/ferrari-deepfake-attempt-scammer-security-question-ceo-benedetto-vigna-cybersecurity-ai/ ↩

[6] Marketing-Interactive — *WPP CEO Mark Read targeted by deepfake AI scam* (mayo de 2024; WhatsApp falso, Teams, voz clonada e imágenes de YouTube; intento fracasado; advertencia de Read). https://www.marketing-interactive.com/wpp-ceo-mark-read-deepfake-ai-scam ↩

[7] Tookitaki — *The Deepfake Deception: How a CEO Video Call Cost $499K in Singapore* (marzo de 2025; un director financiero autoriza 499.000 $ en una llamada de Zoom con todos los participantes deepfake). https://www.tookitaki.com/blog/deepfake-ceo-scam-singapore-2025 ↩

[8] Nacha — *FBI's IC3 Finds Almost $8.5 Billion Lost to Business Email Compromise in Last Three Years* (~3.000 M$/año; ~8.500 M$ en tres años; base del fraude de pago). https://www.nacha.org/news/fbis-ic3-finds-almost-85-billion-lost-business-email-compromise-last-three-years ↩

[9] Trend Micro — *Deepfake CFO Video Calls Result in $25MM in Damages* (análisis técnico del patrón de ataque con videollamada multiparticipante empleado contra Arup). https://www.trendmicro.com/en_us/research/24/b/deepfake-video-calls.html

[10] EUR-Lex — *Reglamento (UE) núm. 910/2014 (eIDAS), artículos 41-42* (efecto jurídico de los sellos de tiempo electrónicos: presunción de exactitud de la fecha y la hora y admisibilidad como prueba; base legal del artefacto de autorización sellado). https://eur-lex.europa.eu/eli/reg/2014/910/oj

[11] World Economic Forum — *Cybercrime: Lessons learned from a $25m deepfake attack* (febrero de 2025; análisis del caso Arup y de los fallos de control; argumento de la verificación fuera de banda). https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/

La identidad en directo: ¿quién hay de verdad al otro lado de la pantalla?

«Cuando un individuo desempeña un papel, pide implícitamente a sus observadores que se tomen en serio la impresión que se fomenta ante ellos.»

— Erving Goffman, La presentación de la persona en la vida cotidiana (1959)

El montaje que WIRED documentó en 2024 es de una sencillez estremecedora: dos móviles fijados en soportes y un aro de luz. Con el primero, el estafador hace la videollamada —a menudo por Zoom. La cámara trasera de este móvil no lo enfoca a él: enfoca la pantalla del segundo, que ejecuta una aplicación de face-swap apuntando a su cara. Lo que ve la víctima es una cara que parpadea, sonríe y responde en tiempo real —y que no existe. Las «relaciones» se alargan semanas o meses, videollamadas incluidas, hasta que llega la petición de dinero. Son los «Yahoo Boys», la cofradía de estafadores románticos que opera sobre todo desde Nigeria —y son tan descarados que presumen de los montajes en grupos de Telegram, con vídeos y todo, a veces para venderlos a otros estafadores [1]. La experta en ingeniería social Rachel Tobac lo resumía: estas aplicaciones han mejorado dramáticamente en un año —el tono de piel, el pelo, el color de ojos [1].

Y no es una anécdota artesanal: es una industria. iProov, una empresa que verifica identidades remotas para banca y gobiernos, documentó en 2024 un aumento del 2.665 % de los ataques con cámara virtual nativa —software que inyecta vídeo sintético como si viniera de la cámara del dispositivo, convertido ya en el principal vector de ataque—, un 300 % más de ataques de face-swap dirigidos precisamente contra sistemas con detección de vida, y cerca de 24.000 usuarios vendiendo tecnología de ataque como servicio; su catálogo de amenazas cuenta 127 herramientas de face-swap y 91 cámaras virtuales [2]. Y el vector nuevo es aún más barato: convertir una sola foto en vídeo animado, en dos pasos [2].

Durante un siglo, ver a alguien moverse y responder en directo fue la prueba informal definitiva de que era real y era él. Esta prueba ha muerto, y con ella la confianza de dos momentos cotidianos: cuando alguien entra —el alta en una plataforma— y cuando alguien se presenta —la videollamada, la entrevista, la primera cita. Este capítulo trata de recuperarlos. La instrucción del directivo y su llamada llena de deepfakes se trata en el capítulo 87; la identidad de quien contratas en remoto, en el capítulo 91; el KYC bancario y el crimen financiero, en el capítulo 16; la persona única del voto y la participación, en el capítulo 108; la aprobación por encima de umbral, en el capítulo 80; la voz clonada al teléfono, en el capítulo 68. La pregunta clave de este: ¿cómo puede una persona demostrar que es real, presente y que es ella, en el momento exacto que importa —y cómo puede el otro lado comprobarlo sin tener que creer a nadie? La respuesta: con la firma con vídeo-selfie de **t2p** —retos de vida aleatorios, verificación biométrica del dispositivo, huella SHA-512, sello de tiempo RFC 3161/eIDAS, ancla a la blockchain pública y un certificado que cualquiera puede verificar [8].

El directo ya no es una prueba

Tres frentes, un mismo fallo: la confianza en el movimiento de una cara. El frente sentimental ya lo hemos visto [1]. En el frente laboral, el FBI alertaba en junio de 2022 —antes del estallido de la IA generativa actual— de un aumento de denuncias por el uso de deepfakes y datos personales robados para conseguir empleos remotos: puestos de TI, programación, bases de datos y software, algunos con acceso a datos de clientes, información financiera y sistemas corporativos [4]. Las señales que entonces delataban el engaño —labios que no cuadran con el sonido, una tos que no se ve— eran ya sutiles; cada generación de herramientas las borra un poco más [4][2]. Y el frente ejecutivo tiene capítulo propio: la sala de Hong Kong donde todas las caras eran falsas y se autorizaron 25,6 millones de dólares, en el capítulo 87.

El papel tampoco salva. OnlyFake, el servicio clandestino destapado en febrero de 2024, generaba carnets y pasaportes falsos «con redes neuronales» por 15 dólares —Estados Unidos, Italia, China, Rusia, Argentina, Chequia, Canadá—; los periodistas de 404 Media superaron con uno de estos carnets el control KYC del exchange OKX, que usa un verificador externo profesional [5]. El documento solo está muerto; la selfie sola, herida de muerte [2].

La propia industria lo admite. Gartner preveía que en 2026 el 30 % de las empresas ya no considerarían fiables las soluciones de verificación de identidad y autenticación por sí solas, por culpa de los deepfakes contra la biometría facial [3]. Los ataques de inyección —el vídeo sintético servido directamente al flujo de

la cámara— crecieron un 200 % en 2023, y los estándares de detección de ataques de presentación, pensados para la máscara y la foto impresa, no cubren la inyección digital [3]. Traducción: el sector que vive de verificar caras reconoce que le han cambiado el tablero.

La respuesta instintiva es una carrera de detectores: adivinar si la cara es falsa. El libro ya ha mostrado adónde lleva: el detector se equivoca en los dos sentidos y el mentiroso cobra el dividendo (capítulo 15). La salida es otra: dejar de preguntar «¿es falsa esta cara?» y empezar a exigir «acredita que eres un humano vivo, presente y dispuesto a firmarlo —ahora». No detectar al impostor: hacer que acreditarse sea trivial para el humano real y caro para el impostor. Y que la prueba la pueda comprobar cualquiera, sin confiar en ningún proveedor.

Acreditarse en lugar de detectar: qué hace exactamente el vídeo-selfie

El gesto, paso a paso. La firma con vídeo-selfie es la firma más fuerte de t2p. La persona abre el documento —un PDF: un formulario de alta, la hoja de una reunión, una declaración— y empieza: la cámara frontal graba un vídeo breve mientras la app le plantea retos de vida aleatorios —parpadea con naturalidad, y dos más entre girar la cabeza, sonreír o inclinarla— que hay que completar en menos de 60 segundos; el dispositivo exige la verificación biométrica —la huella dactilar, o el PIN como alternativa— y, superado todo, la persona dibuja su firma manuscrita en la pantalla. Al certificar, la app genera dos transacciones en la blockchain pública —una por la firma, una por el vídeo— y un certificado dedicado: un PDF de una página con el documento, la firma, la evidencia en vídeo y las dos transacciones [8]. Solo se puede ver a una persona en el encuadre; si alguien abandona o se agota el tiempo, no queda nada.

Qué contiene la prueba. El certificado lleva la huella SHA-512 del fichero —calculada en el dispositivo—, el sello de tiempo RFC 3161 conforme a eIDAS, el ancla a la blockchain pública, un código QR y una verificación de seguridad forense: GPS contra simulación, coherencia temporal, integridad del dispositivo y attestation de hardware [8]. Este último detalle importa más de lo que parece: una cámara virtual que inyecta vídeo sintético necesita normalmente un dispositivo trucado, y el certificado deja constancia de ello. El paquete de evidencia .asice —estándar ETSI— se verifica completamente fuera de línea, con herramientas abiertas, sin la app y sin confiar en el fabricante [8]. Y la privacidad por diseño: el vídeo no sale del móvil —a la cadena solo viaja la huella [8]; compartir la evidencia es siempre una decisión de quien firma.

Qué prueba y qué no prueba. El vídeo-selfie sellado acredita que una persona real y presente ejecutó aquel acto de firma en aquel instante —un humano vivo respondiendo retos imprevisibles, no un vídeo enlatado. Lo que no hace es decir el nombre civil de nadie: la «identidad verificada» que muestra la app es la de la cuenta y la biometría del dispositivo, no la de un registro civil. Quién es la cara del vídeo lo establece el receptor —comparándola con la persona que conoce, con la de la pantalla, con la del selfie fundacional de la cuenta— o bien la capa institucional que llega: la cartera de identidad europea, que cada estado miembro ha de ofrecer en diciembre de 2026 [7]. La división del trabajo es limpia: t2p pone el artefacto de evidencia; el receptor o la institución, el nombre. La identidad civil como infraestructura —el quién eres ante el Estado, con sus promesas y sus peligros— es la materia del capítulo 47.

La frescura. Un vídeo-selfie de hace un mes no acredita nada sobre hoy. Por eso el documento firmado es el reto: si contiene el contexto de ahora —la reunión de tal día, el alta con tal nombre de usuario, una frase elegida hace un minuto—, la prueba no se puede reciclar (no-antes), y el ancla pone el techo por el otro lado (no-después). Es el sándwich temporal que el libro ya conoce del compromiso y revelación (capítulos 45 y 46), aplicado a la persona.

La prueba de existencia aplicada

Tres momentos, tres variantes del mismo gesto.

1. El handshake de la reunión

Antes de la videollamada que importa —el cierre, la due diligence, la entrevista final, el consejo—, el anfitrión redacta la hoja de la reunión: un PDF de una página con la fecha, la hora, los participantes y una frase de contexto recién elegida. Cada participante la firma con su vídeo-selfie en su dispositivo y deja el certificado en el chat de la reunión [8]. Un minuto antes de abrir micrófonos, cada uno tiene de los demás: un vídeo con retos de vida superados hace un momento, una firma manuscrita, una fecha cierta posterior a la convocatoria —y una cara nítida para comparar con la ventanita de la llamada. El face-swap en directo

puede imitar una cara dentro de Zoom [1][2]; lo que no puede hacer con la misma facilidad es producir el certificado de esta firma: haría falta superar retos aleatorios con la cara suplantada ante la cámara nativa de un dispositivo cuya integridad queda evaluada en el certificado [8]. Y si la duda persiste, la pregunta a contracorriente —el título del libro que le recomendaste hace una semana— sigue siendo gratuita y letal (capítulo 87). El handshake acredita a los humanos de la sala; la instrucción que salga de ella, si mueve dinero, pide además su propio sello —la regla «sin sello, no hay pago» del capítulo 87.

2. El alta como humano

El registro en una plataforma —el marketplace, la red social, la app de citas— es el otro momento. El formulario de alta como documento-reto: la persona lo firma con vídeo-selfie y la plataforma recibe un artefacto verificable —una persona real y presente se ha dado de alta hoy, con este nombre de usuario— sin quedarse ninguna biometría: el vídeo lo conserva el usuario, y en la cadena solo hay huellas [8]. Es la versión practicable de aquello que la investigación académica reclama con el nombre de «credenciales de personalidad»: demostrar que eres una persona real —no una IA— sin revelar ningún dato personal; la propuesta que investigadores del MIT, de OpenAI y de Microsoft publicaron en 2024, con emisión presencial o institucional y verificación criptográfica [6]. Seudónimo-pero-humano: la cuenta puede llamarse como quiera; lo que no puede es ser un guion que abre diez mil. Para los servicios que exigen el nombre legal —el banco, la edad—, la cartera europea que llega en diciembre de 2026 pone la identidad civil [7]. Y el contramodelo también tiene nombre: escanear iris a cambio de criptomonedas y concentrar la biometría de medio planeta en una sola base de datos —el libro ya ha hablado de ello (capítulo 108). Aquí es al revés: la biometría se queda en el dispositivo de cada uno.

3. El regreso: quién vuelve, y quién llama de nuevo

La identidad en directo no es solo el primer día. La cuenta que vuelve para una operación sensible —cambiar el correo de recuperación, vaciar la cartera, vender lo que tiene— puede reacreditarse con un vídeo-selfie nuevo sobre el documento de la operación: el receptor compara la cara de hoy con la del selfie fundacional de la cuenta —la continuidad es una cadena de vídeos datados, y la comparación la hace quien verifica, nunca la app [8]. El «madre, soy yo, me ha cambiado el número» que pide dinero se responde con el gesto del capítulo 85: un reto de vida antes de mover un euro. Y la primera videocita después de semanas de chat —el territorio exacto de los Yahoo Boys [1]— admite el mismo ritual que una reunión de consejo: un handshake de un minuto. Quien te quiere, lo hará sonriendo —literalmente: sonreír es uno de los retos [8]; quien no existe, no lo puede hacer.

El límite, dicho claramente: el sello no reconoce caras ni pone nombres —la comparación es del receptor, humana o pericial; no es un detector de deepfakes —es una carga de la prueba invertida; no sustituye el KYC donde la ley lo exige —lo complementa con un artefacto que el cliente controla; y no todo pide handshake: la llamada de cada día con quien conoces de toda la vida no es una due diligence. El criterio de siempre: cuanto más alto el riesgo, más fuerte el gesto —el umbral del capítulo 80.

La promesa y el peligro

La promesa: reuniones donde cada silla viene acreditada por un certificado que cualquier participante puede verificar sin confiar en nadie [8]; altas donde crear diez mil cuentas falsas deja de ser gratis, porque cada alta exige un humano vivo respondiendo retos ante una cámara; estafadores que, para intentarlo, han de dejar un artefacto datado, firmado y ligado a una cuenta —evidencia que trabaja para la víctima desde el minuto cero; y la infraestructura institucional que llega —la cartera europea [7]— completada por una capa de evidencia neutral que no custodia ningún gobierno ni ninguna plataforma.

El liveness también es atacable —honestidad antes que marketing: iProov documenta face-swaps dirigidos precisamente contra sistemas con detección de vida [2], y el manual de t2p no promete ningún escudo anti-deepfake [8]. Los retos gestuales no son una muralla: son un listón —más alto en una app nativa, con la integridad del dispositivo y la attestation de hardware en el certificado [8], que en una webcam cualquiera—, pero ningún listón es infinito. La respuesta es la de todo el libro: capas —el certificado, la comparación humana de caras, la pregunta a contracorriente (capítulo 87), el canal alternativo— y el coste asimétrico: quien salta el listón deja una prueba datada y firmada de su propio fraude. El deepfake que firma queda notariado.

La fricción —dos créditos y un minuto por persona no es para cada llamada ni para cada alta. Es para los momentos que lo valen: el importe alto, el primer contacto, la operación irreversible. El umbral lo pone

cada uno —y el capítulo 80 ya ha mostrado cómo.

La biometría como peaje —la línea ética del libro no se mueve: la prueba de vida es una opción de quien quiere acreditarse, nunca un peaje universal. El vídeo permanece en el dispositivo; en la cadena, solo huellas [8]; ha de haber alternativas para quien no puede o no quiere —el PIN ya lo es dentro del gesto [8]—, y el anonimato sigue siendo legítimo y vital allí donde enseñar la cara mata (capítulo 113).

La exclusión —quien no tiene móvil con biometría, quien no puede pagar créditos, quien tiene setenta y ocho años y tiembla ante un reto cronometrado: si la acreditación en directo se vuelve condición de acceso, hemos construido una puerta nueva para dejar gente fuera. Toda plataforma que lo adopte necesita un camino presencial o asistido equivalente —y que no sea un camino de segunda.

El registro que persigue —un mundo donde cada alta y cada reunión dejan ancla es también un mundo correlacionable: quién se acreditó, cuándo, para hablar con quién. Las anclas no han de ser enlazables entre sí, la revelación ha de ser selectiva —el tramo disputado, nunca la vida entera— y el control de cada campo, de quien firma (capítulo 112).

Es hora de actuar

Que «soy real y soy yo» vuelva a poder demostrarse.

Para las plataformas de reuniones y videollamadas: dad al handshake un lugar nativo —una sala de espera donde adjuntar y comprobar los certificados antes de abrir micrófonos; que «todos los participantes acreditados» se vea como se ve el candado del navegador. La detección puede ayudar; la acreditación decide.

Para las plataformas de consumo —redes, marketplaces, apps de citas: ofreced el alta como humano —verificar el artefacto del vídeo-selfie sin custodiar ninguna biometría [8][6]— y señalizad las cuentas que la han superado; sin convertirla en obligación ni penalizar el anonimato legítimo.

Para las empresas: política de handshake para las videollamadas por encima de umbral —la contratación remota, el proveedor nuevo, la operación grande— encajada con la regla del capítulo 87: el handshake acredita a los humanos de la reunión; el sello de la instrucción, la autorización que salga de ella. Dos capas, dos preguntas diferentes.

Para los ciudadanos: antes de enviar dinero a alguien que solo has visto por pantalla —la videocita que se vuelve urgente, el «hijo» con número nuevo, el reclutador del trabajo perfecto—, pide un minuto de handshake con retos de vida [8]. Quien es real, lo pasa sonriendo; quien se niega o se enfada, ya te ha respondido.

Para los reguladores y los estándares: la cartera europea ha de llegar a tiempo [7] y convivir con la evidencia de humanidad de capas neutrales que el ciudadano controla; y los estándares de prueba de vida han de cubrir el ataque de inyección, no solo la máscara y la foto [3] —el agujero está ahí.

La pantalla nos enseñó a vernos de lejos; los deepfakes nos han quitado el derecho de creer lo que vemos en ella. Se puede recuperar: no adivinando quién es falso, sino dando a cada humano la manera de probar que es real —aquí, ahora, firmando esto. Que cada «soy yo» —en el alta, en la sala de reuniones, en la noche en que alguien que quieres te pide ayuda— pueda llevar su prueba. Por mirar la pantalla y saber quién hay, **time2act**.

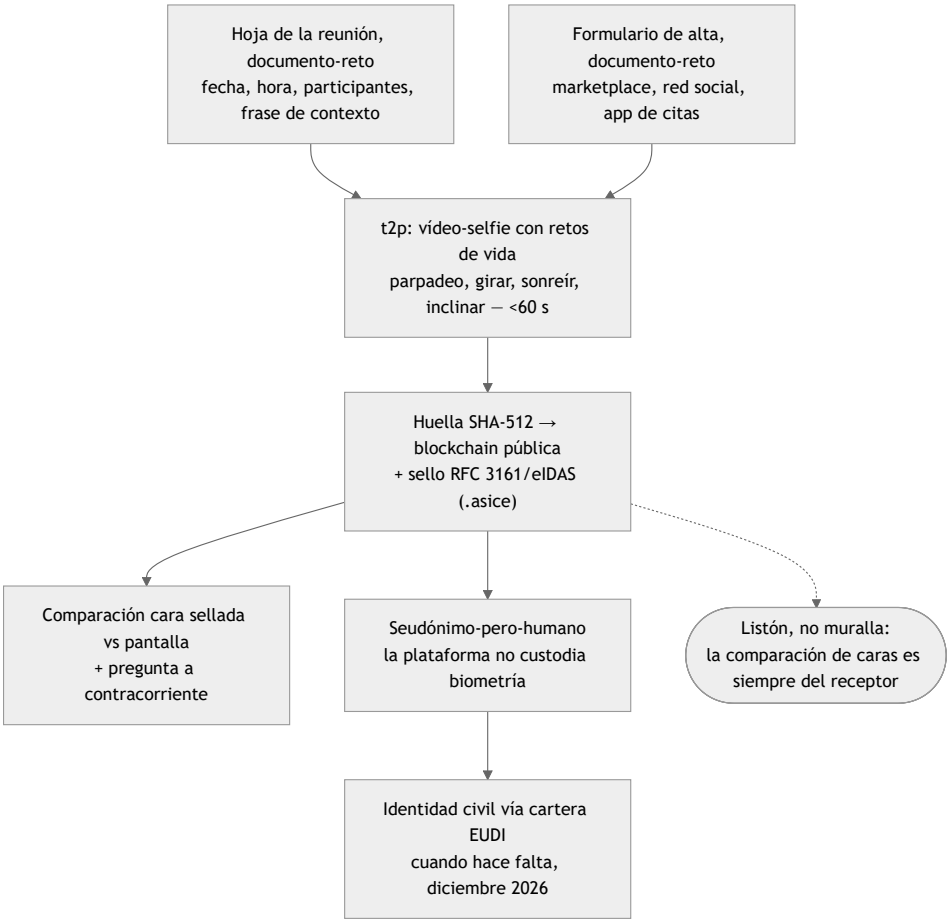


Figura 88.1 — La identidad en directo con prueba de existencia (t2p: vídeo-selfie con retos de vida aleatorios —parpadear, girar, sonreír, inclinar— en <60 s, biometría o PIN del dispositivo, huella SHA-512, sello RFC 3161/eIDAS, ancla a la blockchain pública, certificado con la evidencia en vídeo y attestation de hardware, paquete .asice verificable fuera de línea): a la izquierda, el handshake de la reunión (hoja de la reunión como documento-reto firmado por cada participante antes de abrir micrófonos; comparación de la cara sellada con la de pantalla; la pregunta a contracorriente como capa extra); a la derecha, el alta como humano (el formulario de alta firmado con vídeo-selfie: seudónimo-pero-humano, la plataforma verifica sin custodiar biometría; identidad civil vía cartera EUDI cuando hace falta). Contexto: face-swap en tiempo real comercializado (Yahoo Boys), +2.665 % de ataques de cámara virtual nativa y +300 % de face swaps contra sistemas con liveness (iProov 2025), 30 % de desconfianza empresarial prevista (Gartner). Límites: los retos gestuales son un listón, no una muralla —capas y coste asimétrico (el fraude que firma queda notariado); la comparación de caras es del receptor, nunca de la app. Fuentes: WIRED/9to5Mac; iProov; Gartner; FBI IC3; Decrypt; arXiv/MIT; CE (EUDI).

---

[1] 9to5Mac (sobre el reportaje de WIRED) — *Latest romance scam tactic uses two phones with face-swap app* (abr-2024: los «Yahoo Boys» y el face-swap en tiempo real dentro de videollamadas —dos móviles en soportes y aro de luz, o portátil con webcam; presumen de los montajes en Telegram y los venden; Rachel Tobac: las apps han mejorado dramáticamente en un año). https://9to5mac.com/2024/04/18/romance-scam-face-swap/ ↩

[2] iProov — *Threat Intelligence Report 2025: Remote Identity Under Attack* (ataques de cámara virtual nativa +2.665 %; face swaps +300 % respecto de 2023, dirigidos contra sistemas con protocolos de detección de vida; ~24.000 usuarios vendiendo tecnologías de ataque como servicio; la conversión de imagen a vídeo como vector nuevo; 127 herramientas de face-swap, 91 cámaras virtuales y 10 emuladores catalogados). https://www.iproov.com/reports/threat-intelligence-report-2025-remote-identity-attack · https://www.iproov.com/press/annual-identity-verification-threat-intelligence-report ↩

[3] Gartner (vía FutureCIO) — *Deepfakes to render identity verification and authentication solutions inefficient* (predicción de feb-2024: en 2026, el 30 % de las empresas ya no considerarán fiables aisladamente las soluciones de verificación de identidad y autenticación, por los deepfakes contra la biometría facial; ataques de inyección +200 % en 2023; los estándares de detección de ataques de presentación no cubren la inyección digital; Akif Khan: combinar PAD, IAD e inspección de imagen). https://futurecio.tech/deepfakes-to-render-identity-verification-and-authentication-solutions-inefficient/ ↩

[4] FBI / IC3 — *Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions* (PSA del 28-jun-2022: deepfakes y datos personales robados para optar a empleos remotos de TI, programación, bases de datos y software —algunas con acceso a datos de clientes y sistemas corporativos; señales: labios y sonido desincronizados, tos o estornudos que no cuadran con la imagen). https://www.ic3.gov/PSA/2022/psa220628 ↩

[5] Decrypt — *People Are Using Basic AI to Bypass KYC — But Should You?* (feb-2024: OnlyFake, carnets y pasaportes falsos generados «con redes neuronales» por 15 $ —EE. UU., Italia, China, Rusia, Argentina, Chequia, Canadá—; 404 Media superó el

KYC del exchange OKX, que usa el verificador externo Jumio; usuarios los usaban para abrir cuentas bancarias y desbloquear cuentas cripto). https://decrypt.co/216188/ai-generated-fake-id-bypass-kyc-aml-banks-crypto-onlyfakes ↩

[6] Adler, Hitzig, Jain et al. (arXiv) / MIT News — *Personhood credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online* (ago-2024; 32 autores, con investigadores del MIT, de OpenAI y de Microsoft: credenciales digitales para demostrar que eres una persona real —no una IA— sin revelar ningún dato personal; emisión presencial o institucional; verificación criptográfica; «AI is moving very fast, certainly much faster than the speed at which governments adapt»). https://arxiv.org/abs/2408.07892 · https://news.mit.edu/2024/3-questions-proving-humanity-online-0816 ↩

[7] Comisión Europea / Corbado — el Reglamento (UE) 2024/1183 de identidad digital europea: los estados miembros han de ofrecer una cartera EUDI a ciudadanos, residentes y empresas (plazo: diciembre de 2026); menos de un tercio de los estados cumplen hoy el listón de preparación (observatorio del Politecnico di Milano). https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/915931811/The+European+Digital+Identity+Regulation · https://www.corbado.com/blog/eudi-wallet-2026-deadline-rollout-eic-2026 ↩

[8] t2p — manual de producto (firma con vídeo-selfie: «la firma más fuerte de la app» —la cámara frontal graba mientras firmas, parpadeo y dos retos de vida aleatorios (girar la cabeza, sonreír, inclinarla) en menos de 60 segundos, verificación biométrica del dispositivo obligatoria con PIN como alternativa, firma manuscrita, 2 créditos y dos transacciones; certificado dedicado con el documento, la firma, la evidencia en vídeo y las dos transacciones; solo una persona en el encuadre; certificado con SHA-512, sello RFC 3161/eIDAS, ancla a la blockchain pública, QR y verificación forense con integridad del dispositivo y attestation de hardware; paquete .asice ETSI verificable fuera de línea sin confiar en el fabricante; los ficheros permanecen en el dispositivo — solo la huella viaja; la prueba de vida confirma «una persona real y presente» al firmar). Véanse los capítulos 13 y 15; la suplantación de directivos y la regla «sin sello, no hay pago», en el capítulo 87; quién contratas en remoto, en el capítulo 91; el compromiso y revelación, en los capítulos 45 y 46; la persona única de la participación, en el capítulo 108. ↩

Información que mueve mercados: quién lo ha dicho, y cuándo lo dijo

«El Rumor: ningún otro mal es más veloz; se nutre del movimiento y, andando, gana fuerzas.»

— Virgilio, Eneida, IV, 174-175

El 10 de noviembre de 2022, a la 1:36 de la tarde, un impostor con el sello de «verificado» de Twitter Blue de **8 dólares** (@EliLillyandCo, con el logotipo de Lilly) publicó: «Estamos encantados de anunciar que la insulina ahora es gratuita». La acción real de **Eli Lilly** cayó de unos 368 a unos 346 dólares en veinte minutos, borrando momentáneamente unos **15.000 millones de dólares** de valor y forzando a la compañía a pedir disculpas y a remitir a los inversores a su cuenta auténtica, @LillyPad [1]. Seis meses después, la misma mecánica encontró un blanco más grande: el 22 de mayo de 2023, la imagen generada por IA de una explosión junto al **Pentágono** —el caso que abría el capítulo 17—, amplificada por cuentas con el sello de «verificado» que se hacían pasar por «Bloomberg News» (@BloombergFeed) y por la cuenta estatal rusa RT, hizo caer el S&P 500 alrededor de un 0,26-0,3 % hasta el mínimo de la sesión —el Dow perdió unos ochenta puntos entre las 10:06 y las 10:10— antes de recuperarse del todo en pocos minutos, cuando el cuerpo de bomberos del condado de Arlington y el Pentágono confirmaron que no había habido ninguna explosión [2]. Fue, según la propia Bloomberg, posiblemente la primera vez que una imagen de IA movía el mercado.

Este capítulo no habla de las cuentas anuales ni de la auditoría —que ya son el terreno del capítulo 55— ni del fraude publicitario del capítulo 56. Aquí el artefacto no es un balance retrospectivo, sino una **única revelación en directo**, una noticia o un rumor que se publica y mueve el precio de un valor en cuestión de segundos. La pregunta es sencilla y brutal: en un mercado donde los algoritmos reaccionan a un titular en milisegundos, **¿cómo puede saber el mercado, al instante, si una «noticia» viene realmente del emisor que dice ser su origen?** Y la tesis del libro encaja directamente: ante la falsificación, la prueba de existencia no juzga la verdad, pero fija **quién** lo dijo y **cuándo**.

Una mentira más rápida que cualquier desmentido

El caso de Lilly y el del Pentágono comparten una raíz con un precedente más antiguo y brutal. El 23 de abril de 2013 —el «Hack Crash»— una cuenta pirateada de la agencia Associated Press publicó que había habido explosiones en la Casa Blanca y que el presidente Obama había resultado herido. El Dow cayó 143,5 puntos y se borraron más de **136.000 millones de dólares** del valor del S&P 500 en pocos segundos, antes de corregirse [3]. La lección es que los **operadores algorítmicos y de alta frecuencia** leen el texto de las redes sociales y reaccionan a él en milisegundos: mucho antes de que ningún humano —y no digamos ninguna empresa— pueda desmentirlo. La asimetría es total; publicar una falsa revelación cuesta segundos, mientras corregirla depende de una autoridad o de la propia compañía que lo verifique y lo desmienta por un canal reconocido por el mercado.

No siempre se trata de una broma que se deshace en minutos. En 2025, en el esquema de Ostin Technology (NASDAQ: OST), vídeos *deepfake* del estratega de Goldman Sachs David Kostin, de Elon Musk y de Mark Zuckerberg, combinados con identidades robadas de asesores registrados en la FINRA, inflaron la cotización un **1.175 %** —de 0,78 a 9,40 dólares entre mediados de abril y finales de junio— antes de un desplome del **94 % en un solo día**. El Departamento de Justicia de EE. UU. presentó cargos por fraude de valores, fraude electrónico y conspiración en septiembre de 2025; el esquema habría evaporado más de **950 millones de dólares** [4]. Aquí el *deepfake* ya no es un titular fugaz, sino el motor de un *pump-and-dump* completo.

El rumor como arma, y el fraude de los canales legítimos

El problema no es solo la suplantación de emisores cotizados. Es también la suplantación de quien da **consejos**. La Bolsa de Bombay (**BSE**) ha tenido que emitir avisos repetidos —el 12 de enero de 2026, de nuevo el 8 de marzo, y un cuarto incidente hacia abril— por vídeos *deepfake* de su consejero delegado, **Sundararaman Ramamurthy**, dando supuestos consejos de bolsa y prometiendo «beneficios extraordinarios». La bolsa ha tenido que aclarar que ni él ni ningún directivo de la BSE hace recomendaciones ni gestiona grupos de WhatsApp o Telegram, y ha prometido acciones legales [5].

Y todavía hay un tercer vector, el más inquietante para un editor: los **canales legítimos** también se pueden envenenar. Un comunicado de prensa falso distribuido a través de **GlobeNewswire** afirmó que Walmart aceptaría la criptomoneda **Litecoin**; el precio de Litecoin subió más de un **30 %** antes de que Walmart lo desmintiera [7]. Si incluso los teletipos regulados —los que el mercado trata como autorizados — pueden vehicular una revelación falsificada, la pregunta del origen auténtico deja de ser teórica.

Qué dice la ley sobre quien disemina

El derecho ya persigue esta conducta, pero desde el otro extremo. En Europa, el Reglamento de abuso de mercado (MAR) (Reglamento UE núm. 596/2014, artículo 12) incluye expresamente dentro de la «manipulación de mercado» la difusión de información a través de los medios de comunicación —incluido internet— que dé o pueda dar señales falsas o engañosas sobre la oferta, la demanda o el precio de un instrumento financiero, incluyendo rumores, cuando quien la difunde sabía o debería haber sabido que era falsa. El artículo 17 del mismo MAR obliga a los emisores a comunicar la información privilegiada al público **lo antes posible** y por canales oficiales; las enmiendas de la Listing Act, aplicables desde el 5 de junio de 2026, ajustan su régimen de retraso.

En Estados Unidos, la Regla 10b-5 y la Sección 9(a)(2) de la Securities Exchange Act, que aplica la SEC, abarcan las falsas declaraciones y los esquemas que mueven precios, con cargos paralelos del DOJ por fraude de valores y conspiración —como en el caso Ostin. La Reg FD y el Formulario 8-K definen los canales legítimos de la revelación corporativa: EDGAR más los teletipos reconocidos (Dow Jones, Bloomberg, Business Wire, PR Newswire). En un aviso conjunto del 25 de enero de 2024, la SEC, la FINRA y la NASAA advierten de que los defraudadores pueden usar vídeos *deepfake* para imitar al consejero delegado de una empresa anunciando noticias falsas con la intención de manipular el precio de una acción [6]. Como hemos visto, el arsenal sancionador es contundente: en el ejercicio 2025, la SEC abrió 456 acciones y ordenó 17.900 millones de dólares en sanciones por manipulación de mercado y fraude de revelación [8].

Por qué la ley por sí sola no salva

Hay que decirlo con crudeza: el MAR y la Regla 10b-5 castigan **después**, cuando el mal ya se ha hecho y el precio ya se ha movido. Persiguen a quien difunde la mentira, pero no dan al mercado ninguna manera de saber, **en el segundo en que aparece el titular**, si viene de verdad de Lilly o de un impostor de 8 dólares. El canal legítimo —EDGAR, el 8-K, el teletipo regulado— es exactamente lo que la suplantación explota: nadie puede comprobar, al instante y en línea, que este tuit o este comunicado tengan el origen que dicen. El fallo es de **origen auténtico verificable**, y ninguna cuantía de sanciones a posteriori lo cierra. Mientras el mercado no pueda distinguir lo genuino de lo falso en milisegundos, el algoritmo reaccionará primero y preguntará después.

La prueba de existencia aplicada

Es aquí donde **t2p** aporta la pieza que falta, no como oráculo de verdad, sino como **referencia criptográfica del artículo genuino**. Cuando el equipo de relaciones con inversores de un emisor —o su agente de presentación, o el teletipo— publica un elemento sensible al precio (un formulario 8-K, un anuncio de información privilegiada bajo el artículo 17 del MAR, una declaración del consejero delegado, un resultado trimestral, una publicación oficial en las redes o un vídeo), el artefacto se sella **en el dispositivo**: se calcula localmente la **huella SHA-512** —el fichero no sale nunca—, se envuelve en un **sello de tiempo RFC 3161 conforme a eIDAS**, se ancla a la blockchain pública y se emite como contenedor **.asice** verificable fuera de línea. Cuando un directivo aparece filmando la declaración, se le añade el **GPS forense** y una **prueba de vida**. El emisor publica la huella de verificación junto a su cuenta oficial y a su página de relaciones con inversores, de manera que cualquier periodista, bolsa, regulador, *bróker* o canal algorítmico de noticias puede confirmar en milisegundos si un tuit, captura o comunicado «de última hora» viene realmente de la compañía —o es el impostor: el falso tuit de @EliLillyandCo, la falsa cuenta de Bloomberg del Pentágono, el vídeo *deepfake* del consejero de la BSE, las identidades robadas de Ostin. No sustituye nada: se sienta **debajo** de EDGAR/8-K, la Reg FD, el MAR y los teletipos regulados como **capa de autenticidad**, y se complementa con la procedencia de contenido C2PA/SynthID de los capítulos 13 y 15 —el sello prueba «esto viene del emisor», la procedencia marca «esto está generado por IA», y el regulador sigue juzgando el abuso.

Ahora el límite, con toda la crudeza. «Basura a la entrada, basura en la cadena»: el sello prueba que un fichero concreto fue emitido por una fuente autenticada en un instante con la integridad intacta; **no prueba que la revelación sellada sea verdad**, completa, legal o no manipulativa. Una empresa puede sellar a la perfección un comunicado que sea él mismo una mentira —un comunicado de *pump-and-dump* sellado por la sociedad pantalla de los propios defraudadores es auténtico-pero-falso—, y el sello no detiene a un emisor que quiere engañar ni atrapa la revelación engañosa por omisión: eso sigue siendo tarea de la SEC, la ESMA, la FINRA, la vigilancia de las bolsas y los auditores. Tampoco hace «fallar» un rumor no sellado: solo permite que los verificadores confirmen que el genuino no coincide con él —y eso depende de que los emisores sellen de verdad sus revelaciones reales y de que el mercado las compruebe. No demuestra por sí solo que un vídeo sea real y no IA (eso es C2PA/SynthID y la detección), no evalúa la materialidad ni la intención de uso de información privilegiada, y no impide la reacción algorítmica en milisegundos antes de que la verificación pueda producirse. Es una capa de autenticidad y de fecha cierta, no un oráculo de verdad.

La promesa y el peligro

La promesa es ofrecer al mercado un **patrón de referencia genuino** contra el cual contrastar cualquier copia viral: si Lilly hubiera podido publicar la huella de su comunicado real, cualquier verificador habría visto en un segundo que el tuit del impostor no coincidía. El emisor honesto recupera el control de su propio origen; el periodista, el *bróker* y el canal de noticias ganan una comprobación instantánea antes de amplificar.

El peligro pide los matices de siempre. El primero, la **falsa seguridad**: «está sellado, luego es cierto» es precisamente la confusión entre integridad y verdad que un *pump-and-dump* sellado explotaría. El segundo, la **cobertura desigual**: si solo los grandes emisores sellan, la ausencia de sello en una empresa pequeña y honesta se podría leer, injustamente, como sospecha. Y el tercero, la **velocidad**: mientras la verificación no esté integrada de manera nativa en los canales de noticias algorítmicos, el sello llegará tarde para la primera oleada de milisegundos. La prueba de existencia es una capa de autenticidad, no un sustituto del juicio humano ni regulador.

Además, el hecho de que el sello de prueba de existencia se convierta en una fuente de datos masivos para modelos predictivos genera un riesgo de **poder sobre la conducta colectiva**. Cada vez que una entidad puede anticipar qué contenidos serán considerados auténticos o falsos, adquiere la capacidad de influir —o incluso de modelar— las decisiones de los usuarios antes de que estos actúen. Como advierte Carissa Véliz, «todo intento de predecir el comportamiento humano es también un intento de controlarlo, lo que, en su extremo, conduce al autoritarismo»[11]. Si los algoritmos que procesan las huellas se concentran en manos de unas pocas corporaciones o gobiernos, la información sobre qué mensajes están «verificados» puede ser utilizada para restringir la libertad de expresión e imponer narrativas oficiales. Por eso, el diseño del registro ha de garantizar una arquitectura descentralizada y transparente, con mecanismos de gobernanza que impidan la acumulación de poder predictivo en ninguna entidad única, asegurando que la capa de autenticidad siga sirviendo a la confianza colectiva y no a la vigilancia autoritaria.

Es hora de actuar

Para los **emisores y sus equipos de relaciones con inversores** (como Lilly después de su propio caso): sellar cada revelación sensible al precio en el momento de emitirla y publicar su huella junto a la cuenta oficial. Para las **bolsas y los reguladores** (SEC, ESMA, FINRA, BSE, SEBI): reconocer el origen sellado como señal de verificación e integrar su comprobación en la vigilancia de mercado. Para los **teletipos regulados** (Business Wire, PR Newswire, GlobeNewswire): sellar en el origen cada comunicado para cerrar la brecha que permitió el fraude Walmart-Litecoin. Para los **medios y los canales algorítmicos de noticias** (Bloomberg, Dow Jones, agregadores): comprobar la huella antes de amplificar un titular «de última hora». Y para los **brókers y las plataformas** (X y el resto de redes donde nace el rumor): exponer el estado de verificación junto al contenido financiero, para que el sello azul de 8 dólares no vuelva a confundirse con una fuente autorizada.

Como hemos visto el 22 de mayo, una imagen que no mostraba nada real movió el S&P 500 antes de que nadie pudiera desmentirla. Ofrecer al mercado una manera de comprobar, en el mismo segundo, quién lo ha dicho y cuándo lo ha dicho —sin pretender nunca que el sello diga si es verdad— es, en este frente donde los milisegundos valen millones, **time2act**.

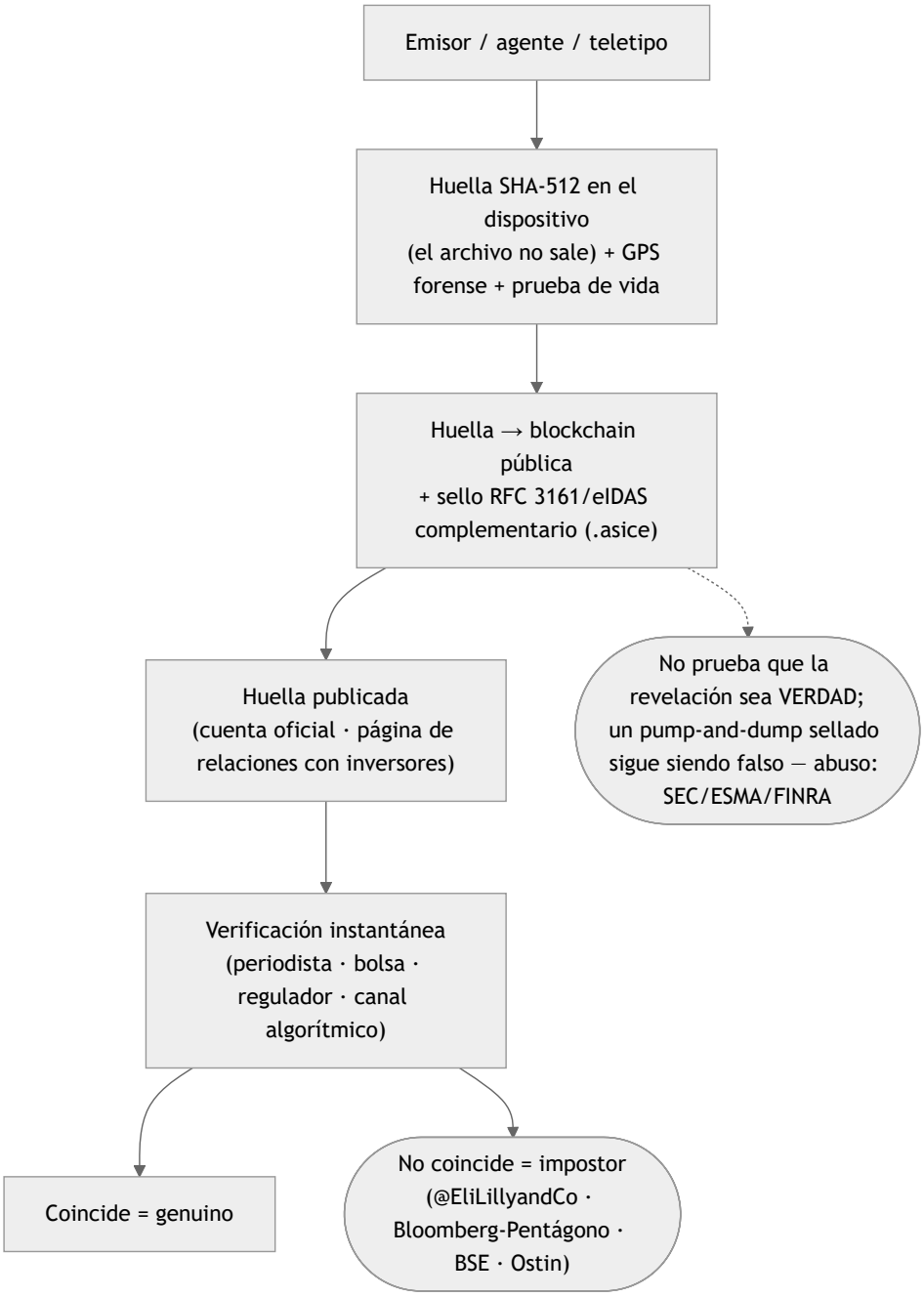


Figura 89.1 — El emisor (o su agente o teletipo) sella la revelación sensible al precio en el momento de emitirla: huella SHA-512 en el dispositivo → blockchain pública, con sello de tiempo RFC 3161/eIDAS complementario (.asice), con GPS forense y prueba de vida si hay un directivo filmando. La huella se publica junto a la cuenta oficial; cualquier periodista, bolsa, regulador o canal algorítmico confirma en milisegundos si un tuit o comunicado «de última hora» coincide con el genuino (Lilly, Pentágono-Bloomberg, BSE, Ostin) o es el impostor. Límite: el sello prueba quién lo emitió y cuándo, no que la revelación sea verdad; un comunicado de pump-and-dump sellado sigue siendo falso, y la manipulación sigue siendo tarea de la SEC/ESMA/FINRA y las bolsas. Fuentes: caso Eli Lilly; imagen falsa del Pentágono; Hack Crash de 2013; caso Ostin Technology; aviso SEC/FINRA/NASAA; MAR art. 12.

---

[1] 340B Report — *Fake Lilly Twitter account tweets 'Insulin Is Free Now,' temporarily wiping billions from company's stock value* (10 nov. 2022, 1:36 p.m. ET; caída de ~368 a ~346 $; ~15.000 M$ borrados; disculpa de la empresa y cuenta @LillyPad). https://340breport.com/fake-lilly-twitter-account-tweets-insulin-is-free-now-temporarily-wiping-billions-from-companys-stock-value/ ↩

[2] NPR — *Fake viral images of an explosion at the Pentagon were probably created by AI* (22 mayo 2023; difundida por cuentas verificadas incluida una falsa Bloomberg; breve caída del S&P 500; desmentida por los bomberos de Arlington).

https://www.npr.org/2023/05/22/1177590231/fake-viral-images-of-an-explosion-at-the-pentagon-were-probably-created-by-ai ↩

[3] University at Buffalo — *With one false tweet, computer-based 'Hack Crash' led to real panic* (23 abril 2013; tuit pirateado de AP; Dow −143,5 puntos; >136.000 M$ borrados en segundos; reacción algorítmica y de alta frecuencia). https://www.buffalo.edu/news/releases/2015/05/037.html ↩

[4] InvestmentNews — *Shareholders accuse Ostin Technology of deepfake-driven $950M pump-and-dump scheme* (2025; *deepfakes* de Kostin/Musk/Zuckerberg; identidades robadas de asesores FINRA; inflación del 1.175 %; caída del 94 % en un día; acusación del DOJ el sept. 2025). https://www.investmentnews.com/regulation-legal-compliance/legal-shareholders-accuse-ostin-technology-of-deepfake-driven-950m-pump-and-dump-scheme/265308 ↩

[5] The Hans India — *BSE warns investors about fake deepfake video misusing CEO's identity* (avisos de 2026 sobre vídeos *deepfake* del consejero delegado Sundararaman Ramamurthy; incidentes recurrentes enero-abril; promesa de acciones legales). https://www.thehansindia.com/business/bse-warns-investors-about-fake-deepfake-video-misusing-ceos-identity-1038779 ↩

[6] SEC / FINRA / NASAA — *Investor Alert: Artificial Intelligence (AI) and Investment Fraud* (Investor.gov, 25 ene. 2024; aviso explícito sobre vídeos *deepfake* de consejeros delegados para «manipular el precio de una acción»). https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/artificial-intelligence-fraud ↩

[7] PRNEWS — *Hoax Releases Hit Newswire Services* (comunicado falso Walmart-Litecoin vía GlobeNewswire; Litecoin +30 %; ángulo de autenticación de los teletipos). https://www.prnewsonline.com/hoax-releases-hit-newswire-services/ ↩

[8] Sidley Austin — *SEC Enforcement FY2025 Results Signal Shift in Priorities* (456 acciones; 17.900 M$ ordenados; ajustado 1.400 M$ + 1.300 M$; prioridad a la manipulación de mercado y el fraude de revelación). https://www.sidley.com/en/insights/newsupdates/2026/04/sec-enforcement-fy2025-results-signal-shift-in-priorities-in-direct-critique-of-prior-administration ↩

[9] EUR-Lex / Lexparency — *MAR Regulation (EU) No 596/2014, Article 12 — Market manipulation* (difusión de información falsa o engañosa y de rumores a través de los medios e internet como manipulación de mercado). https://lexparency.org/eu/32014R0596/ART_12/

[10] FINRA — *Artificial Intelligence (AI) and Investment Fraud* (versión de la FINRA del aviso; lenguaje sobre vídeos *deepfake* de consejeros delegados y noticias falsas para mover el precio de una acción). https://www.finra.org/investors/insights/artificial-intelligence-and-investment-fraud

[11] Carissa Véliz — *Prophecy: Prediction, Power, and the Fight for the Future* (2025). ↩

Titularidad real: quién es la persona de carne y hueso detrás de la empresa

«El respeto va ligado a los nombres. El anonimato y el respeto se excluyen mutuamente.»

— Byung-Chul Han, En el enjambre (2017)

El 3 de octubre de 2021, el **Consorcio Internacional de Periodistas de Investigación** (ICIJ) publicó los **Papeles de Pandora**: una filtración de **11,9 millones de documentos** —2,94 terabytes— procedentes de **catorce** despachos de servicios *offshore*. Dentro estaban los verdaderos dueños de más de **30.000 sociedades** y más de **29.000 titulares reales** ocultos tras cadenas de sociedades pantalla, fideicomisos y fundaciones repartidas por más de doscientos países. Los ficheros señalaron a **35 jefes de estado y de gobierno** en activo o pasados y a más de **330 políticos**, entre ellos el rey Abdalá II de Jordania, el entonces primer ministro checo Andrej Babiš y los presidentes de Kenia, Ecuador y Gabón, además de más de **130 milmillonarios** —46 de ellos oligarcas rusos [1]. Llegaba cinco años después de los **Papeles de Panamá** de abril de 2016 —11,5 millones de documentos de un solo despacho, Mossack Fonseca, que cerró en 2018 [2]— e identificaba aproximadamente el doble de titulares reales. El hilo común: el dueño que figuraba en el papel, un administrador fiduciario o una capa de sociedades anónimas, casi nunca era el titular real último, y ningún registro de la época podía probar **quién** era esa persona, **en qué momento** había tomado el control, ni si la declaración de propiedad era **auténtica**.

Este capítulo no trata el contrato público del capítulo 43 —licitaciones y adjudicaciones— ni la factura del capítulo 54 —el fraude documental en el comercio—, sino aquello que hay **aguas arriba** de cualquier operación: probar el **titular real último** que hay detrás de la persona jurídica, sea lo que sea que esta empresa compre, venda o financie después. La pregunta es quirúrgica: ¿cómo fijamos **quién** declara ser el dueño, **qué** declara y **cuándo**, de manera que la declaración no se pueda retrodatar ni manipular en silencio? Es la tesis del libro aplicada al corazón de la opacidad societaria: la prueba de existencia no descubre el secreto, pero impide negar después lo que se declaró antes.

Una arquitectura de secreto que sobrevive a todas las filtraciones

Los Papeles de Pandora no fueron una anomalía, sino una confirmación. Ninguna de aquellas sociedades era ilegal en sí misma; lo que las hacía peligrosas era que nadie podía probar **quién** se escondía detrás. Diez años después de los Papeles de Panamá, el balance es aleccionador: las investigaciones fiscales habían recuperado unos **1.360 millones de dólares** y habían desencadenado reformas profundas —la Corporate Transparency Act estadounidense, los registros de titularidad real de la UE, el Registro de Entidades Extranjeras del Reino Unido—, y aun así Transparency International concluye con crudeza que «**la arquitectura fundamental del secreto *offshore* permanece intacta**» [3]. La razón es estructural: cada reforma ha pedido **declarar** quién es el dueño, pero casi ninguna ha podido **verificarlo** ni **datarlo** de manera inalterable.

El fraude no es, pues, solo la omisión: es la **declaración falsa**. Un cleptócrata pone un testaferro al frente, interpone un fideicomiso en una jurisdicción opaca, y el registro nacional recoge obedientemente un nombre que no es el suyo. Cuando finalmente salta una filtración —Panamá, Paraíso, Pandora—, el daño lleva años corriendo, y la pregunta judicial siempre es la misma: esta declaración, ¿era así el día que se presentó, o se ha retocado después? Sin un ancla temporal independiente, la respuesta depende de un registro que el propio declarante, o un funcionario complaciente, puede haber modificado.

Registros que se declaran solos y no se comprueban

El problema técnico tiene un nombre: **autodeclaración sin verificación**. Open Ownership, la autoridad de referencia en datos de titularidad real, es contundente: la mayoría de registros se basan en datos que el propio obligado declara, y **sin verificación** —comprobaciones de conformidad, contrastes cruzados y revisión de la evidencia de apoyo— los registros permiten introducir información falsa y estructuras de testaferro que oculten el control real [11]. Un campo de base de datos, mutable y sin sello, no es una prueba; es una afirmación.

Las cifras del despliegue lo ilustran. La **Corporate Transparency Act** estadounidense estimaba de partida unos **32 millones** de sociedades obligadas a informar, más unos 5 millones de nuevas cada año;

en noviembre de 2024 solo se habían presentado 6,5 millones [5]. Y en marzo de 2025 una norma provisional de la **FinCEN** dio la vuelta a todo el régimen: exoneró a **todas** las sociedades domésticas estadounidenses y a las personas estadounidenses, y redujo la población cubierta de unos 32 millones a **menos de 12.000** entidades —las extranjeras [4]. El registro más ambicioso del mundo, antes de consolidarse, quedó prácticamente vacío. En Europa, mientras tanto, la sentencia del **Tribunal de Justicia de la UE** del 22 de noviembre de 2022 invalidó el acceso público general a los registros de titularidad real por ser una «**injerencia grave**» en los derechos a la vida privada y a la protección de datos (artículos 7 y 8 de la Carta): el acceso queda limitado ahora a autoridades, sujetos obligados y quien acredite un interés legítimo [6]. El resultado es un mosaico donde los datos existen, pero su **fiabilidad** y su **accesibilidad** siguen en disputa.

Una marea regulatoria que pide exactitud

La respuesta normativa de 2024-2027 es la más ambiciosa de la historia en este frente. En Europa, el **Reglamento (UE) 2024/1624** —el código único antiblanqueo (AMLR)— se aplicará directamente a los 27 estados desde el **10 de julio de 2027**, y la nueva **Autoridad de Lucha contra el Blanqueo (AMLA)**, con sede en Fráncfort, es operativa desde el **1 de julio de 2025**; su mandato incluye registros de titularidad real **interoperables** a escala de la UE [7]. En el Reino Unido, la **Economic Crime and Corporate Transparency Act 2023** ha empezado a desplegar desde el **18 de noviembre de 2025** la **verificación de identidad obligatoria** para administradores y personas con control significativo; solo entre marzo de 2024 y marzo de 2025, Companies House retiró información falsa o engañosa que afectaba a **100.400 sociedades** y rechazó más de **10.200 solicitudes sospechosas** [8]. En Estados Unidos, el **16 de diciembre de 2025** el **Undécimo Circuito**, en *National Small Business United v. Treasury*, se convirtió en el tribunal estadounidense de mayor rango en confirmar la constitucionalidad de la CTA, aunque la norma de marzo limita su alcance práctico [9]. Y por encima de todo, la **Recomendación 24** del **GAFI**, revisada en marzo de 2022, exige a cada país garantizar que las autoridades competentes dispongan de información de titularidad real **adecuada, exacta y actualizada** mediante un enfoque multidimensional, incluido un registro o mecanismo equivalente [10]. Toda esta arquitectura pide algo que los documentos en papel no dan por sí solos: **exactitud verificable y datada**.

Por qué el registro por sí solo no salva

Hay que decirlo sin rodeos: un registro de titularidad real, por muy obligatorio que sea, **es tan fiable como la voluntad de quien lo rellena y la capacidad de quien lo comprueba**. Una entrada de base de datos se puede editar; una declaración presentada hoy se puede retrodatar mañana sin dejar rastro; y un funcionario puede aceptar un nombre que sabe falso. El caso de la FinCEN lo demuestra a la inversa: un régimen entero se puede vaciar con una norma administrativa, y los datos que quedaban dejan de ser comparables con los de ayer. Un PDF de declaración de titularidad es un PDF. Lo que falta no es el formulario ni la ley que lo exige —ambos ya existen—, sino una **ancla inalterable que fije quién declaró qué, y en qué instante exacto**, de manera que ni el declarante ni el custodio del registro puedan alterarlo a posteriori sin que se note.

La prueba de existencia aplicada

Es aquí donde **t2p** aporta la capa que falta, y lo hace sobre el artefacto de la declaración, no sobre la estructura societaria que nunca verá. Cuando un titular real, un administrador o un proveedor de servicios societarios presenta o actualiza una declaración de titularidad real, el sello liga **aquella declaración concreta y su evidencia** a un punto fijo en el tiempo y en la identidad. Al presentarla, el documento de declaración más la prueba subyacente —el extracto del registro de accionistas, la escritura del fideicomiso, la divulgación del acuerdo de testaferro, la página del pasaporte o del DNI, y una **prueba de vida** del declarante capturada sobre el terreno— se calcula con una **huella SHA-512 en el dispositivo** del declarante; la huella recibe un **sello de tiempo RFC 3161 conforme a eIDAS** y se ancla a la blockchain pública, produciendo un contenedor **.asice** verificable fuera de línea. Cuando una persona real afirma el control —el humano de carne y hueso detrás de la sociedad pantalla—, la captura de campo añade **GPS forense** y prueba de vida, que demuestran que un humano vivo, no una *deepfake* ni una foto reciclada, hizo la atestación en aquel lugar y en aquel momento.

Esto complementa los registros y los regímenes de verificación —la BOI de la FinCEN, los registros interoperables de la AMLR/AMLA, la verificación de identidad de Companies House, la R.24 del GAFI— sin sustituirlos: el registro sigue custodiando y divulgando los datos, y el guardián sigue filtrándolos, pero ahora cada declaración lleva un recibo a prueba de manipulación y comprobable de manera independiente que indica quién declaró qué, cuándo, y que la declaración y su evidencia no se han alterado desde entonces. Esto convierte una entrada de base de datos autodeclarada y mutable en una atestación sellada y a prueba de tribunal, y hace detectable la retrodatación silenciosa o la manipulación posterior de un registro de propiedad. Es el complemento, sobre el acto de declarar, de lo que los capítulos 13 y 15 proponen sobre la procedencia del contenido con C2PA: allí se sella lo que se produce; aquí, quién declara ser el dueño.

Ahora el límite, con toda la crudeza, porque aquí engañarse haría daño. «Basura a la entrada, basura en la cadena»: el sello prueba el acto de declarar, quién lo hizo, cuándo, y que la declaración y la evidencia adjunta están inalteradas; **no prueba que la persona declarada sea el titular real último**. Un cleptócrata puede plantarse ante la cámara, superar la prueba de vida y sellar una atestación perjura que nombra a un testaferro, u omitir por completo el fideicomiso oculto, y el sello datará fielmente la mentira. No puede atravesar una cadena de sociedades extranjeras que nunca ve, ni detecta un acuerdo de testaferro, ni sabe si un registro de accionistas notariado ya es falso en el origen. No verifica los documentos de identidad contra las autoridades emisoras, no evalúa si la estructura sirve para blanquear o evadir sanciones, y no protege el registro central de una brecha posterior —como mostró la intrusión de piratas estatales en el Tesoro y en la FinCEN en diciembre. El sello es una capa de integridad y procedencia para cada declaración; la verdad sustantiva de la propiedad depende todavía de la verificación del registro, la diligencia del guardián, el periodismo de investigación, el intercambio transfronterizo de datos y el juicio humano, ninguno de los cuales sustituye.

La promesa y el peligro

La promesa es devolver a los registros aquello que hoy falta: que cada declaración de titularidad sea **datada, atribuible y a prueba de tribunal**. Cuando vuelva a saltar una filtración como Pandora, ya no se podrá fingir que nunca se declaró lo que se declaró; el periodista, el fiscal y la autoridad tendrán un recibo inalterable de quién dijo qué y cuándo. En un mundo donde un nombre en el papel viaja sin ninguna garantía, hacer el origen de la declaración inalterable protege tanto al investigador honesto como al ciudadano.

El peligro pide los matices de siempre. Primero, no confundir **integridad con verdad**: una declaración falsa y sellada sigue siendo falsa, y ahora, además, inmutable; el sello podría dar una falsa tranquilidad —«está anclado, luego es cierto»— que no se corresponde con nada. Segundo, la **privacidad**: después de la sentencia del TJUE, sellar declaraciones no puede convertirse en una excusa para exponer datos personales más allá del interés legítimo; la huella se ancla, no los datos. Tercero, la **concentración**: si solo los grandes proveedores de servicios societarios pueden sellar con solvencia, el estándar podría expulsar a las jurisdicciones y a los actores pequeños en lugar de fortalecerlos. La prueba de existencia es una capa de gobernanza de la declaración, no un certificado de propiedad verdadera ni un sustituto de la diligencia que sabe auditar una estructura.

Además, hay que reconocer que la misma infraestructura inmutable puede convertirse en un arma de **lock-in** corporativo si no se instauran mecanismos de apertura e interoperabilidad. Cuando las grandes plataformas controlan los protocolos de sellado, cualquier cambio o migración a un entorno competidor requiere reescribir todo el historial —un coste prohibitivo que consolida su dominancia. Carissa Véliz advierte de que «los gigantes tecnológicos de hoy pueden conseguir blindar (lock-in) su posición»[12], y este escenario se materializa cuando las autoridades reguladoras no imponen normas de portabilidad o formatos abiertos. El riesgo queda agravado por el precedente de 2025, como hemos visto, en que FinCEN eximió a las empresas estadounidenses de declarar la titularidad real, vaciando el registro y dejando la estructura de confianza en manos de un número reducido de entidades privadas[13]. Sin garantías explícitas contra este encadenamiento, la transparencia registral podría retroceder, convirtiéndose en una capa que refuerza la concentración en lugar de alzar a los actores más pequeños.

Es hora de actuar

Para los registros mercantiles y las autoridades (FinCEN, AMLA, Companies House): exigir que cada declaración de titularidad real llegue con una huella sellada y datada, para que la retrodatación y la

manipulación silenciosa sean detectables. Para los proveedores de servicios societarios y los sujetos obligados (despachos, notarios, bancos): sellar la declaración y su evidencia de apoyo en el momento de presentarla, no después, y conservar el contenedor .asice como parte de la diligencia debida. Para los legisladores y el GAFI: reconocer la declaración sellada como prueba de la exactitud y la actualización que la Recomendación 24 ya exige, y tratar la fecha cierta como la diferencia entre una declaración y una coartada fabricada posteriormente. Para los periodistas de investigación y la sociedad civil (ICIJ, Open Ownership, Transparency International): poder confrontar la declaración actual con la versión sellada el día cero, para que la edición silenciosa deje de ser invisible. Y para los declarantes honestos: asumir la prueba de vida y el GPS forense como elementos que los distinguen del testaferro que se niega a poner la cara.

Como hemos visto en 2021, once millones de documentos revelaron lo que ningún registro podía probar: quién había, de verdad, detrás de treinta mil empresas. Dar a cada declaración de titularidad un recibo sellado de quién la hizo, qué dijo y cuándo —sin olvidar nunca que el sello no hace verdadero lo que se declara en él— es, en este frente donde se esconde la propiedad del mundo, time2act.

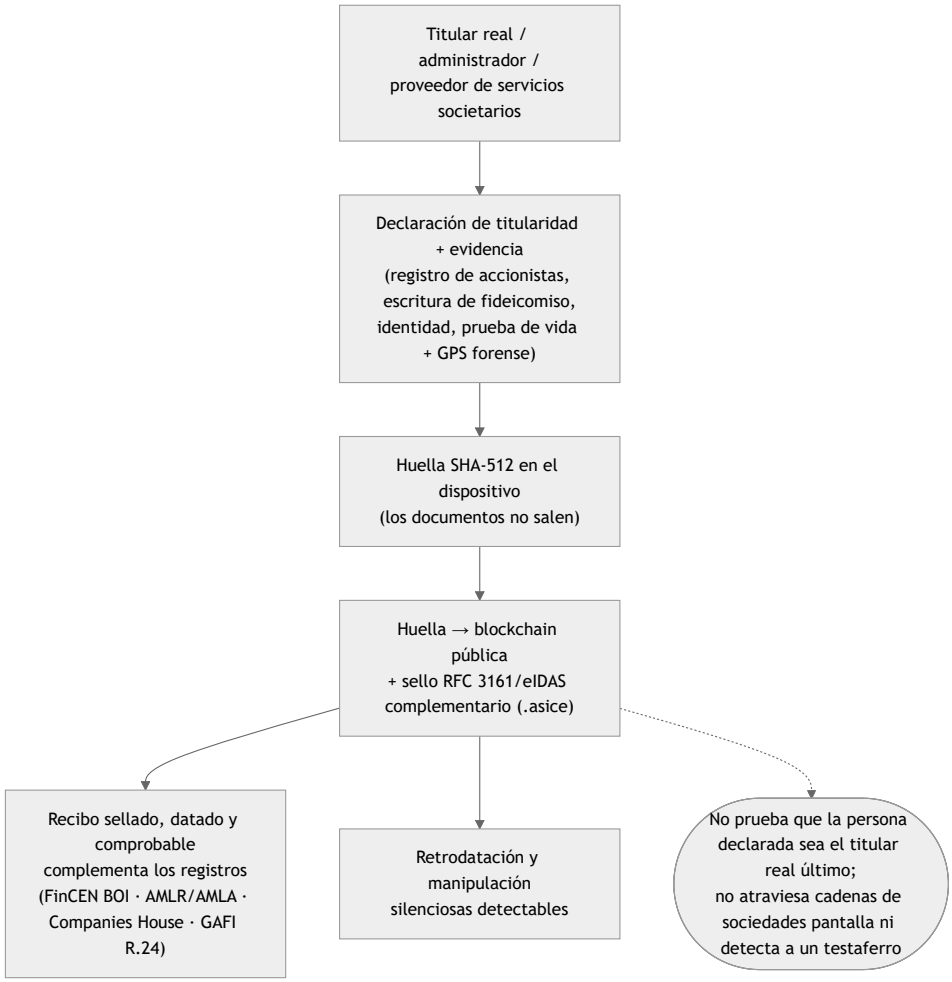


Figura 90.1 — El titular real, el administrador o el proveedor de servicios societarios presenta la declaración y su evidencia (registro de accionistas, escritura de fideicomiso, identidad, prueba de vida con GPS forense sobre el terreno); se calcula la huella SHA-512 en el dispositivo —los documentos no salen— y se ancla la huella en la blockchain pública, con sello RFC 3161/eIDAS complementario (.asice). El recibo complementa los registros (FinCEN BOI · AMLR/AMLA · Companies House · GAFI R.24): prueba quién declaró qué y cuándo, y hace detectable la retrodatación. Límite: el sello no prueba que la persona declarada sea el titular real último; no atraviesa cadenas de sociedades pantalla ni detecta un testaferro. Fuentes: Papeles de Pandora (ICIJ); Papeles de Panamá; Transparency International; FinCEN; CJUE C-37/20 y C-601/20; GAFI R.24; Open Ownership.

[1] ICIJ — *About the Pandora Papers investigation* (3 de octubre de 2021; 11,9 millones de documentos, 2,94 TB, 14 proveedores, 29.000+ titulares reales, 35 líderes y 330+ políticos). https://www.icij.org/investigations/pandora-papers/about-

pandora-papers-investigation/ ↩

[2] Wikipedia — *Panama Papers* (3 de abril de 2016; 11,5 millones de documentos de Mossack Fonseca, 214.488 entidades, 150 investigaciones en 79 países, cierre en 2018). https://en.wikipedia.org/wiki/Panama_Papers ↩

[3] Transparency International — *Panama Papers: 10 years on* (~1.360 M USD recuperados; reformas CTA, registros UE, ROE; «la arquitectura del secreto offshore permanece intacta»). https://www.transparency.org/en/news/panama-papers-10-years ↩

[4] FinCEN — *FinCEN Removes Beneficial Ownership Reporting Requirements for U.S. Companies* (norma provisional de marzo de 2025; exoneración de sociedades domésticas; población cubierta < 12.000). https://www.fincen.gov/news/news-releases/fincen-removes-beneficial-ownership-reporting-requirements-us-companies-and-us ↩

[5] Journal of Accountancy — *BOI update: 6.5 million of 32 million reports filed so far* (estimación original de 32 M de sociedades obligadas; 6,5 M presentadas en noviembre de 2024). https://www.journalofaccountancy.com/news/2024/nov/boi-update-6-5-million-of-32-million-reports-filed-so-far/ ↩

[6] Transparency International — *EU court ruling on beneficial ownership registers: legitimate access* (sentencia del TJUE de 22 de noviembre de 2022; invalidación del acceso público; marco de interés legítimo). https://www.transparency.org/en/blog/eu-court-ruling-on-beneficial-ownership-registers-legitimate-access ↩

[7] PwC Ireland — *The EU's new Anti-Money Laundering Authority* (AMLA Fráncfort operativa desde el 1 de julio de 2025; AMLR (UE) 2024/1624 aplicable el 10 de julio de 2027; registros UBO interoperables). https://www.pwc.ie/services/audit-assurance/insights/eu-new-anti-money-laundering-authority.html ↩

[8] GOV.UK — *Companies House confirms identity verification rollout from 18 November 2025* (ECCTA; verificación de identidad de administradores y PSC; 100.400 sociedades afectadas, 10.200+ solicitudes rechazadas). https://www.gov.uk/government/news/companies-house-confirms-identity-verification-rollout-from-18-november-2025 ↩

[9] Transparency International US — *Unanimous Eleventh Circuit decision upholds the Corporate Transparency Act* (16 de diciembre de 2025; tribunal de mayor rango en confirmar la constitucionalidad de la CTA). https://us.transparency.org/news/unanimous-eleventh-circuit-decision-upholds-the-corporate-transparency-act/ ↩

[10] FATF — *Beneficial Ownership* (Recomendación 24 revisada en 2022 y guía de 2023; información adecuada, exacta y actualizada; enfoque multidimensional). https://www.fatf-gafi.org/en/topics/beneficial-ownership.html ↩

[11] Open Ownership — *Verification of beneficial ownership data: Overview* (los datos autodeclarados necesitan verificación: conformidad, contrastes cruzados, evidencia de apoyo). https://www.openownership.org/en/publications/verification-of-beneficial-ownership-data/overview/ ↩

[12] Carissa Véliz (ed.) — *The Oxford Handbook of Digital Ethics* (Oxford UP, 2022). ↩

[13] FinCEN (2025). https://www.fincen.gov/news/news-releases/fincen-removes-beneficial-ownership-reporting-requirements-us-companies-and-us ↩

Identidad laboral: a quién contratamos de verdad en remoto

«El hombre es menos él mismo cuando habla en nombre propio. Dale una máscara y te dirá la verdad.»

— Oscar Wilde, «The Critic as Artist» (1891)

En julio de 2024, **KnowBe4** —una empresa estadounidense de formación en ciberseguridad— contrató a un ingeniero de software remoto para su equipo de informática interna sin saber que, al otro lado de la pantalla, había un operativo norcoreano. El candidato había usado la **identidad robada de un ciudadano de EE. UU. real** y una foto de stock retocada con IA para que cuadrara con el retrato de la solicitud; con ello superó **cuatro entrevistas por videoconferencia**, una verificación de antecedentes y la comprobación de referencias. El 15 de julio, horas después de que el portátil corporativo llegara a su dirección, el **EDR** de la empresa detectó intentos de carga de software malicioso; el centro de operaciones de seguridad aisló la máquina a las 22.20 y, con Mandiant y el FBI, estableció que el supuesto empleado era un actor de estado-nación que operaba por VPN desde Corea del Norte o China y que el portátil había ido a parar a una **«granja de portátiles» mula** en suelo estadounidense. No se perdió ningún dato, pero el consejero delegado, Stu Sjouwerman, publicó el incidente el 23 de julio como advertencia: contratar, y no solo iniciar sesión, ya es una superficie de ataque de identidad [1].

Este capítulo no trata la identidad digital del ciudadano —la credencial fundacional, gubernamental, que aborda el capítulo 47—. Aquí hablamos de la **relación laboral**: la contratación, la entrevista, la verificación de identidad, el *onboarding* y la continuidad del trabajo en remoto. La pregunta es concreta: ¿cómo demostramos que **la misma persona verificada** estuvo presente en la entrevista, en la prueba de identidad y en la entrega de credenciales y del portátil —y que quien hoy tiene acceso es, todavía, aquella persona—? Es la tesis del libro aplicada al momento exacto en que una empresa decide dar las llaves de casa a un desconocido.

Contratar ya es una superficie de ataque

El caso de KnowBe4 no es anecdótico; es el patrón. El **24 de julio de 2025**, el Departamento de Justicia de EE. UU. condenó a **Christina Marie Chapman**, de 50 años, de Litchfield Park (Arizona), a **102 meses de prisión** por haber gestionado desde casa una «granja de portátiles» que permitió a trabajadores informáticos norcoreanos hacerse pasar por ciudadanos de EE. UU. en **309 empresas** estadounidenses y dos extranjeras, usando **68 identidades robadas** y generando más de **17 millones de dólares**. Alojaba los portátiles corporativos en su casa y envió **49 al extranjero**, incluida una ciudad china en la frontera con Corea del Norte [3].

La escala del fraude sigue aumentando. En una acción coordinada del DOJ del **14 de noviembre de 2025**, se estableció que facilitadores basados en EE. UU. y en Ucrania habían ayudado a trabajadores informáticos de la RPDC a obtener empleo remoto fraudulento en **más de 136 empresas** estadounidenses, comprometiendo más de **18 identidades** reales y generando más de **2,2 millones de dólares** para el régimen [4]. Y no es un fenómeno marginal: el FBI, en la alerta I-012325-PSA del **23 de enero de 2025**, confirmó que los trabajadores norcoreanos usan **IA y tecnología de cambio de cara** durante las entrevistas en vídeo para ofuscar la identidad, y que han virado hacia la **extorsión** de los antiguos empleadores, secuestrando código y datos propietarios [2].

La puerta de delante: la entrevista y el *onboarding*

Lo que antes era una formalidad —ver la cara del candidato por pantalla— se ha convertido en el punto ciego. **Gartner** predice que, en **2028**, una de cada cuatro solicitudes (25 %) será falsa, impulsada por *deepfakes*, síntesis de voz y *chatbots*; la encuesta indica que un **6 %** de los candidatos admiten haber hecho trampas de estilo suplantación en la entrevista [5]. La detección de voz lo confirma desde el otro lado: los datos de **Pindrop** muestran audio generado por IA o reproducido en aproximadamente **1 de cada 106** reuniones monitorizadas, con la actividad de *deepfakes* multiplicada casi **13 veces (un 1.300 % interanual)** y las voces sintéticas llegando al **0,33 %** de las llamadas a los centros de contacto en el cuarto trimestre, un 173 % más que en el primero [7].

Los responsables de selección ya lo viven como la principal amenaza. Según un estudio de enero de 2026, el **69 % de los líderes de contratación del Reino Unido** identifican la suplantación con IA y las *deepfakes* como la amenaza emergente más sofisticada para la integridad de la selección (First Advantage); **Checkr** encontró que un **23 %** de las empresas detectaron fraude de identidad entre nuevas incorporaciones, y el informe de **Greenhouse** indica que el **91 %** de los responsables de selección de EE. UU. habían encontrado o sospechado respuestas de entrevista generadas por IA [6]. El fraude ya no empieza en el *login*: empieza en la primera videollamada. El handshake de vida que blinda la videollamada misma se describe en el capítulo 88; aquí nos ocupa la cadena entera de la contratación.

El marco regulador

La respuesta institucional se está construyendo. Como hemos visto en julio de 2025, el NIST publicó la versión final de las SP 800-63-4 Digital Identity Guidelines, que definen los niveles de garantía de identidad (IAL1/2/3) y una nueva taxonomía de verificación —Remoto No Atendido, Remoto Atendido (por ejemplo, una sesión de vídeo), Presencial No Atendido (quiosco) y Presencial Atendido (en persona) —, un marco al que las empresas pueden mapear el rigor de la verificación de identidad del onboarding [8]. El FBI, en la misma alerta y en sus páginas de búsqueda y recomendaciones sobre los «trabajadores informáticos remotos fraudulentos de la RPDC», recomienda implementar verificación de identidad durante la entrevista, el onboarding y toda la relación laboral remota [2].

Hay, además, una capa de riesgo legal especialmente dura. Las sanciones de la OFAC contra la RPDC convierten pagar o emplear a un trabajador norcoreano sancionado en una infracción de responsabilidad objetiva: un error de contratación se vuelve riesgo de sanciones y de blanqueo, con cargos de fraude electrónico, robo de identidad agravado e IEEPA en los casos Chapman y Jin Sung-Il. A ello se suman la verificación de elegibilidad laboral en EE. UU. (Formulario I-9 / E-Verify), la puerta legal que las identidades robadas retocadas con deepfake quieren burlar, y en Europa el marco eIDAS / eIDAS 2.0 y la cartera EUDI, con los deberes de transparencia del Reglamento europeo de IA.

Y un límite no menor: el RGPD y leyes biométricas como la BIPA de Illinois restringen cuántos datos biométricos o de prueba de vida puede recoger un empleador, lo que obliga a un sellado que preserve la privacidad.

Por qué la guía del FBI por sí sola no salva

Hay que decirlo con crudeza. KnowBe4 tenía EDR, hacía entrevistas en vídeo, comprobaba antecedentes y referencias —y aun así contrató al operativo—. Las recomendaciones existen, pero el problema es que **no dejan rastro verificable**: la entrevista en vídeo se hace y se olvida; el verificador de identidad mira un documento y una cara y saca una conclusión que vive, en el mejor de los casos, en una nota de un sistema de recursos humanos editable; la entrega del portátil es un albarán. Cuando, meses después, salta la alarma —«la persona que contratamos no es la que hoy tiene acceso»—, no hay ningún registro inalterable con que confrontarlo: está la memoria del departamento de recursos humanos y un montón de capturas. Falta una manera de **ligar, con fecha cierta y sin guardar datos sensibles, la misma persona verificada a los tres momentos críticos** de la contratación.

La prueba de existencia aplicada

Es aquí donde **t2p** aporta la pieza que falta, y lo hace sobre el evento de identidad de la contratación, no sobre una afirmación del currículum. En tres momentos se toma una captura en el dispositivo: (1) en la entrevista en directo o por vídeo, una prueba de vida del rostro del candidato más la declaración de consentimiento hablada; (2) en la verificación de identidad, el documento de identidad presentado y la coincidencia con un selfie; (3) en el onboarding, una atestación firmada que liga aquella identidad probada a la persona concreta que tendrá las credenciales y recibirá el portátil. Cada captura se cifra con **huella SHA-512 en el dispositivo** —el fichero biométrico o de documento no sale nunca—, recibe un **sello de tiempo RFC 3161 conforme a eIDAS**, se ancla a la **blockchain pública** y se empaqueta en un contenedor **.asice** verificable fuera de línea, con **GPS forense** y la prueba de vida que registran dónde y cuándo estaba realmente el humano. El valor único es la **continuidad y el no repudio**: una cadena inalterable y datada que demuestra que el mismo humano verificado estuvo presente en la entrevista, en la prueba y en la entrega del dispositivo, de manera que una disputa posterior se comprueba contra un registro sellado y no contra la memoria de recursos humanos.

Esto **complementa, nunca sustituye**, los controles existentes: convive con la verificación IAL2/3 del NIST 800-63, las comprobaciones I-9/E-Verify, el cribado de antecedentes, las auditorías de currículums duplicados y de teléfonos o correos reutilizados que recomienda el FBI, y la detección de deepfakes en tiempo real (Pindrop, Reality Defender, la procedencia C2PA/SynthID **como hemos visto**).

Ahora el límite, con toda la crudeza. «Basura a la entrada, basura en la cadena»: el sello prueba que **un rostro, un documento y una atestación concretos** se capturaron en un lugar y un instante por un autor y no se han alterado desde entonces; **no prueba que la persona sea honesta**, ni que el documento sea realmente suyo y no una identidad robada de alta calidad, ni que no sea un nacional sancionado, ni que no exfiltre datos mañana ni monte una granja de portátiles. Una deepfake impecable o una identidad robada real que supere la prueba de vida producen un sello perfectamente válido de un acto fraudulento. El contenedor garantiza la **integridad y la procedencia de la evidencia de onboarding**; no reemplaza el cribado de antecedentes, el cribado de sanciones, la detección de deepfakes, la verificación de autenticidad del documento ni la vigilancia continua de la amenaza interna y el juicio humano.

La promesa y el peligro

La promesa es convertir la contratación remota en un acto con **memoria verificable**: poder demostrar, ante un incidente como el de KnowBe4, que la persona de la entrevista, la de la prueba de identidad y la de la entrega del portátil eran la misma —o, justamente, descubrir que no lo eran— con una prueba que sobreviva a la rotación del personal y a la pérdida de correos. En un mercado donde un portátil corporativo viaja a un desconocido sin ningún recibo de identidad, hacer inalterable la cadena protege tanto a la empresa honesta como al candidato legítimo.

El peligro pide matices. El primero, no confundir **integridad con verdad**: un sello impecable de una identidad robada sigue siendo el sello de un fraude y puede generar una falsa tranquilidad —«está anclado, luego es de fiar»— que no se corresponde con nada. El segundo, la **privacidad**: el rostro, el documento y la prueba de vida son datos biométricos sensibles; el RGPD y la BIPA exigen que solo salga la huella, calculada en el dispositivo, y nunca un registro central de caras de candidatos. El tercero, el **sesgo y la exclusión**: la prueba de vida y la verificación de documentos pueden fallar más según qué colectivos o equipos, y no pueden convertirse en una barrera de acceso al empleo. La prueba de existencia es una capa de no repudio de la contratación, no un certificado de confianza ni un sustituto del juicio de selección.

Además, el peligro de confiar solo en un «clic» como forma de consentimiento se amplía cuando la información que sustenta ese acuerdo es tan opaca y desproporcionada que el usuario no puede comprender realmente qué autoriza. En el caso del reconocimiento facial de Facebook, Marc Goodman señala que las condiciones de uso tienen 9.300 palabras —un texto tan extenso que casi imposibilita una lectura crítica y, por tanto, un consentimiento auténtico y verificable [11]. Esta asimetría de información crea una brecha legal: el candidato puede firmar digitalmente una autorización sin saber qué rasgos biométricos se almacenan ni cómo se podrán reutilizar. Si la prueba de existencia no incluye un mecanismo que demuestre, de manera inequívoca y auditada, que el individuo ha entendido y aceptado las condiciones, el sistema queda expuesto a reclamaciones por violación del RGPD y la BIPA, y a una erosión de confianza que contrarresta cualquier beneficio de la cadena inmutable. Sin un consentimiento verificable y comprensible, la tecnología se convierte en una nueva forma de explotación de datos más que en una garantía de seguridad.

Una dimensión que el libro *Reboot* pone sobre la mesa es la crisis de la identidad digital cuando las plataformas se convierten en mercados de identidades ficticias. El informe de la Fiscalía de Nueva York (2021) reveló 9,3 millones de comentarios a la FCC provenientes de usuarios inventados, casi todos creados por un solo joven de 19 años, con cerca de 500.000 de origen ruso[12]. La solución propuesta por Noveck —una prueba de personalidad verificable que se genera íntegramente en el dispositivo— complementa el anclaje neutral en blockchain: el registro inmutable asegura que la prueba no ha sido alterada, mientras que una «API personal» garantiza que solo el propietario del dispositivo puede revelar su voz o su presencia digital, sin ninguna base biométrica centralizada. Así se cierra el vacío entre la inmutabilidad de la cadena y la autonomía del individuo, evitando que identidades falsas se infiltren en procesos críticos y reforzando una confianza real.

Es hora de actuar

Para los **equipos de recursos humanos y contratación**: sellar los tres momentos —entrevista, verificación de identidad y entrega del portátil— para que la continuidad de la persona tenga fecha cierta, sin guardar nunca los datos biométricos. Para los **responsables de seguridad (CISO y SOC)**: exigir el *.asice* de onboarding como parte del expediente del empleado y confrontarlo ante cualquier alerta de amenaza interna, tal como hizo KnowBe4 con el EDR. Para los **proveedores de verificación de identidad y detección de deepfakes** (NIST 800-63, Pindrop, Reality Defender): integrar el sellado en el dispositivo con la verificación IAL2/3 y la detección en tiempo real, para que prueba y detección viajen juntas. Para los **reguladores y el FBI/IC3** (OFAC, eIDAS 2.0): reconocer la cadena de identidad sellada como evidencia de diligencia debida en la contratación remota y como prueba ante el riesgo de sanciones. Y para las **plataformas de empleo y marketplaces de talento remoto**: anclar la prueba de identidad del onboarding para que una sustitución —la persona contratada no es la que se conecta— sea detectable.

En KnowBe4, un operativo de estado-nación superó cuatro entrevistas y una verificación de antecedentes antes de que el portátil fuera delatado a las 22.20; como hemos visto, dar a cada contratación remota una prueba sellada que ligue la misma persona verificada de la entrevista al teclado —sin olvidar nunca que el sello no hace honesta la cara que hay delante— es, en este frente donde contratar ya es atacar, **time2act**.

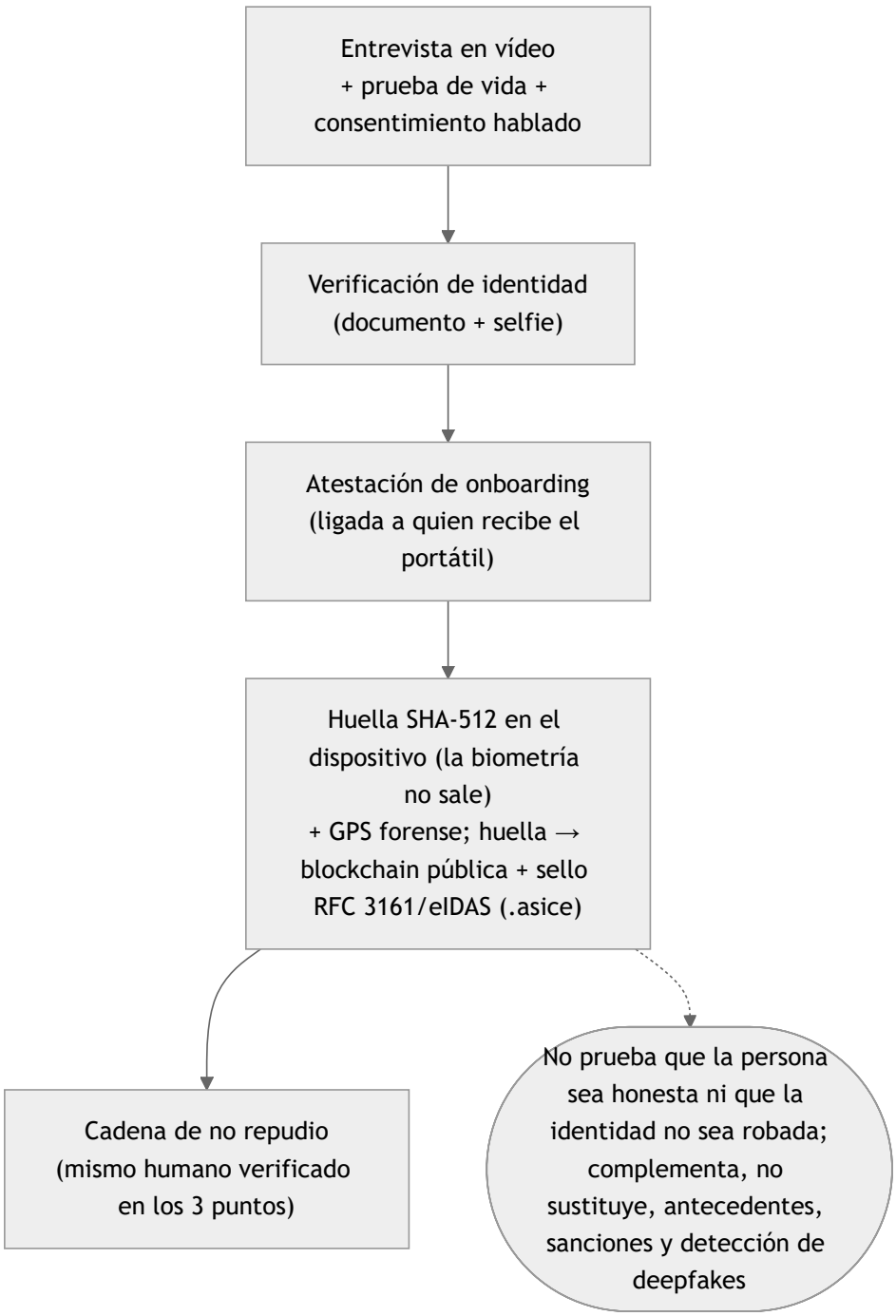


Figura 91.1 — La contratación remota sellada en tres eslabones: entrevista en vídeo con prueba de vida → verificación de identidad (documento + selfie) → atestación de onboarding *ligada a quien recibe el portátil. En cada momento se calcula la huella SHA-512 en el dispositivo (la biometría no sale), con sello RFC 3161/eIDAS, GPS forense y anclaje a la blockchain pública (.asice). Resultado: una cadena de no repudio que demuestra que el mismo humano verificado estuvo en los tres puntos. Límite: el sello no prueba que la persona sea honesta, que la identidad no sea robada ni que no sea un nacional sancionado; complementa, no sustituye, el cribado de antecedentes, de sanciones y la detección de deepfakes. Fuentes: caso KnowBe4; caso Chapman (DOJ); FBI/IC3 I-012325-PSA; NIST SP 800-63-4; Pindrop.*

---

[1] KnowBe4 — *How a North Korean Fake IT Worker Tried to Infiltrate Us* (Stu Sjouwerman; relato en primera persona: foto de stock retocada con IA, cuatro entrevistas en vídeo, detección EDR del 15 de julio de 2024, granja de portátiles mula, FBI/Mandiant). https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us ↩

[2] FBI/IC3 — *Public Service Announcement I-012325-PSA: North Korean IT Workers Conducting Data Extortion* (23 de enero de 2025; cambio de cara con IA en las entrevistas, giro hacia la extorsión, recomendaciones de verificación de identidad). https://www.ic3.gov/PSA/2025/PSA250123 ↩

[3] US DOJ (USAO-DC) — *Arizona Woman Sentenced in $17M IT Worker Fraud Scheme for North Korea* (24 de julio de 2025; Christina Chapman, 102 meses, 309 empresas, 68 identidades robadas, 17 M$, granja de portátiles, 49 portátiles enviados al extranjero). https://www.justice.gov/usao-dc/pr/arizona-woman-sentenced-17m-it-worker-fraud-scheme-illegally-generated-revenue-north ↩

[4] Crowell & Moring — *DOJ Announces Major Enforcement Actions Targeting North Korean Remote IT Worker Schemes* (14 de noviembre de 2025; más de 136 empresas víctimas, más de 18 identidades comprometidas, más de 2,2 M$ de beneficios). https://www.crowell.com/en/insights/client-alerts/doj-announces-major-enforcement-actions-targeting-north-korean-remote-it-worker-schemes ↩

[5] The Decoder — *Gartner predicts that by 2028, one in four job applicant profiles will be fake* (previsión del 25 % para 2028; admisión del 6 % de suplantación en la entrevista, encuesta a 3.000 candidatos). https://the-decoder.com/gartner-predicts-that-by-2028-one-in-four-job-applicant-profiles-will-be-fake/ ↩

[6] People Management — *Deepfakes and AI-enabled impersonation rank among top recruitment threats* (19 de enero de 2026; First Advantage 69 % de los líderes del Reino Unido; Checkr 23 % de fraude de identidad; Greenhouse 91 %). https://www.peoplemanagement.co.uk/article/1945557/deepfakes-ai-enabled-impersonation-rank-among-top-recruitment-threats-research-reveals ↩

[7] Pindrop — *The Growing Trend of Deepfakes in Interviews* (audio IA en ~1 de cada 106 reuniones; ~1.300 % interanual; voces sintéticas en el 0,33 % de las llamadas en el Q4 de 2024). https://www.pindrop.com/article/growing-trend-of-deepfakes-in-interviews/ ↩

[8] NIST — *SP 800-63-4 Digital Identity Guidelines* (final, julio de 2025; niveles de garantía IAL1/2/3 y taxonomía de verificación Remoto/Presencial × Atendido/No Atendido). https://pages.nist.gov/800-63-4/sp800-63.html ↩

[9] FBI — *Fraudulent Remote IT Workers from DPRK* (búsqueda/recomendaciones; uso de identidades robadas, ordenadores intermediarios e IA, con mitigaciones para los empleadores). https://www.fbi.gov/wanted/cyber/fraudulent-remote-it-workers-from-dprk

[10] Microsoft Security — *Fake Employees, Real Threat: Decentralized Identity to combat Deepfake Hiring* (credenciales verificables y verificación continua de la identidad de *onboarding*; contexto de solución adyacente). https://techcommunity.microsoft.com/blog/microsoft-security-blog/fake-employees-real-threat-decentralized-identity-to-combat-deepfake-hiring/4479864

[11] Marc Goodman — *Delitos del futuro* (Ariel, 2015). ↩

[12] Fiscalía General de Nueva York (2021). https://ag.ny.gov/press-release/2021/attorney-general-james-issues-report-detailing-millions-fake-comments-revealing ↩

Trabajo de plataforma: cuando el jefe es un algoritmo

«…una búsqueda, también, de sentido diario tanto como de pan diario, de reconocimiento tanto como de dinero… de una especie de vida en lugar de una especie de morir de lunes a viernes.»

— Studs Terkel, Working (1974)

Abres la aplicación a primera hora para empezar el turno y la pantalla muestra una sola línea: «Cuenta desactivada». Ningún nombre, ningún teléfono, ningún botón para pedir explicaciones. La decisión que te cuesta el sueldo la ha tomado un sistema automatizado, fuera de tu vista. Este es el punto de partida del caso conocido como «Robo-Firing» —Drivers contra Uber y Ola—, en el que un grupo de conductores tuvo que litigar años, hasta el Tribunal de Apelación de Ámsterdam (2023), solo para saber por qué: el tribunal, invocando el artículo 22 del Reglamento General de Protección de Datos, estimó su recurso en tres sentencias vinculadas y obligó a Ola a explicar la lógica de su decisión totalmente automatizada, y a Uber a dar información significativa sobre los despidos algorítmicos; Uber acabó condenada a 584.000 euros de multas coercitivas —más 4.000 euros por cada día de incumplimiento— por no cumplir la orden de explicarse [4]. Piénsalo un momento: hizo falta un tribunal de apelación europeo y multas diarias para que un trabajador conociera el motivo de su propio despido.

Este capítulo trata el trabajo gestionado por plataformas digitales —repartidores, conductores, microtrabajadores— y la relación laboral con un jefe que es un algoritmo. Quién es de verdad la persona que contratamos en remoto se trata en el capítulo 91; las condiciones laborales en la cadena de suministro global, en el capítulo 102; qué hay dentro de los modelos de IA, en el capítulo 79. Pregunta clave: cuando el jefe es un algoritmo, ¿quién levanta acta de la relación laboral? Respuesta: ambas partes, con evidencia anclada —el diario laboral sellado del trabajador y el registro de decisiones auditable de la plataforma, con **t2p**: la huella SHA-512 en el dispositivo, el anclaje de la huella en la blockchain pública y el sello de tiempo RFC 3161/eIDAS complementario dentro de un contenedor .asice [5]—, para que los derechos que Europa y España ya han escrito en el papel [1][2] se puedan probar en los hechos.

El jefe que no da la cara

Conviene describir la gestión algorítmica sin demonizarla. El algoritmo asigna encargos en tiempo real, fija tarifas dinámicas según la oferta y la demanda, puntúa el rendimiento, ordena la cola de trabajo y, al límite, desconecta. Es eficiente —por eso existe: sin esta mecánica, ninguna aplicación de reparto o de transporte podría coordinar a millones de usuarios. Pero la eficiencia tiene un coste oculto: una asimetría informativa radical.

La plataforma lo registra todo —posiciones, tiempos de respuesta, aceptaciones, clics—, en registros masivos que crecen cada segundo. El trabajador, en cambio, solo ve la interfaz del día: los encargos que le aparecen, su puntuación, la tarifa de aquel momento. Y mañana la configuración puede haber cambiado sin aviso. Cuando llega el conflicto —ante la Inspección de Trabajo, ante un juez—, una parte comparece con el registro completo del sistema y la otra con recuerdos.

El diagnóstico ya es ley en Europa. La Directiva (UE) 2024/2831, en vigor desde el 2 de diciembre de 2024 y con transposición hasta el 2 de diciembre de 2026, impone transparencia sobre los sistemas de seguimiento y los algoritmos que afectan a las condiciones de trabajo; exige supervisión humana de las decisiones y derecho a intervención humana en las decisiones importantes; y prohíbe usar datos sensibles —estado emocional, biometría, conversaciones privadas— en las decisiones automatizadas [1]. Y establece la pieza angular: la presunción de laboralidad cuando se constatan hechos que indican dirección y control, con la carga de refutarla sobre la plataforma [1].

Fijémonos en la palabra decisiva: «hechos». La Directiva es una máquina de convertir hechos en derechos. El problema es que, en este sector, los hechos los custodia en exclusiva una de las partes. Este es exactamente el agujero que la prueba de existencia cierra.

España, laboratorio: la Ley Rider y el caso Glovo

España llegó antes. La Ley 12/2021 —la «Ley Rider», en vigor desde agosto de 2021— estableció la presunción de laboralidad para el reparto cuando la empresa ejerce su organización, dirección y control

mediante la gestión algorítmica del servicio o de las condiciones de trabajo, y creó un derecho pionero: el comité de empresa ha de ser informado de los parámetros, reglas e instrucciones de los algoritmos que afectan a las condiciones de trabajo [2].

Y el caso que puso la ley a prueba fue Glovo. La justicia de Barcelona abrió causa penal contra el fundador y consejero delegado, Óscar Pierre, por el modelo de falsos autónomos; las reclamaciones por cuotas no ingresadas y las multas de la Inspección de Trabajo sumaban unos 200 millones de euros, y el competidor Just Eat reclamaba 295 más por competencia desleal [3]. El desenlace llegó entre finales de 2024 y 2025: Glovo anunció el paso al modelo laboral —entre 10.000 y 15.000 repartidores, combinando contratación directa y flotas— y Pierre reconoció ante la jueza que la regularización buscaba «paz social» y evitar «discusiones» con la Inspección, y que la presión penal y económica había forzado el cambio: «la caja no te da para operar». La matriz Delivery Hero elevó las provisiones por Glovo España a entre 440 y 770 millones de euros y estimó unos 100 millones de impacto en el resultado operativo de 2025 [3].

La lección probatoria —que es la de este libro, no el reproche político— es esta: hicieron falta años de inspecciones, actas y cruces de datos para reconstruir, desde fuera y a posteriori, una realidad laboral que ocurría cada día dentro de una aplicación. Cada euro de multa es también el precio de una evidencia que costó años de excavar. Con registros anclados desde el primer día, la misma verdad habría estado visible en semanas —para todas las partes, también para la plataforma que hubiera querido demostrar su diligencia.

El despido por algoritmo

Volvamos al «robo-firing», porque condensa la inversión de la gramática laboral. En el mundo clásico, el empresario despide y ha de motivar; en el mundo de plataforma, el sistema desconecta y es el trabajador quien ha de litigar —años, si hace falta [4]— solo para obtener la motivación. La Directiva europea responde generalizando lo que Ámsterdam tuvo que imponer caso por caso: supervisión humana y derecho a intervención humana en las decisiones importantes [1].

Pero incluso con la motivación en la mano, queda el segundo escalón: contrastarla. Si el algoritmo dice «rechazaste demasiados encargos» o «los clientes te puntuaron mal», ¿con qué lo rebate el trabajador que no tiene ningún registro propio? La plataforma custodia los datos y el criterio; él, ni siquiera su propia versión de los hechos.

La respuesta tiene dos mitades simétricas —y es importante que sean las dos. El trabajador necesita su diario laboral imborrable: su versión de los hechos, sellada día a día en su dispositivo [5]. Y la plataforma necesita —por obligación legal [1][4] y por interés propio— un registro de decisiones auditable: qué regla se aplicó, sobre qué datos, con qué revisión humana y cuándo. Ambas mitades son la misma tecnología; ninguna de las dos puede reescribirse cuando llega el conflicto.

La prueba de existencia aplicada

El mismo turno, registrado desde los dos lados de la pantalla —y ninguna de las dos versiones se puede reescribir.

1. El diario laboral sellado

Cada día de trabajo, el trabajador sella en su dispositivo su jornada: horas conectado, disponibilidad, encargos ofrecidos, aceptados y rechazados, instrucciones recibidas, capturas de las condiciones y tarifas que la aplicación mostraba aquel día [5]. No es espionaje: es su propia vida laboral, documentada desde su lado de la pantalla. El resultado es exactamente lo que la presunción de laboralidad necesita —hechos datados que indican dirección y control [1][2]—, inmune al argumento «la aplicación no decía eso»: la captura de aquella mañana lleva huella y fecha cierta. Y si un día llega la desconexión, su cronología no empieza de cero: ya existe, anclada, desde el primer turno.

2. La desactivación auditable

La plataforma que decida —o que la ley obligue [1][4]— puede anclar su registro de decisiones: cuándo el algoritmo señaló la cuenta, qué datos y qué regla aplicó, qué humano lo revisó y qué resolvió. Cada paso, con huella y datado [5]. Ante el juez de Ámsterdam, aquella cadena habría sido la respuesta que costó 584.000 euros no tener [4]; ante una acusación de discriminación o de arbitrariedad, es la defensa de la

plataforma diligente; y ante el trabajador, es el derecho a saber —artículo 22 del RGPD, Directiva [1]— cumplido por diseño, no por sentencia.

3. La inspección que no empieza de cero

El caso Glovo exigió años de actas y reconstrucciones para acreditar una relación laboral que la aplicación conocía minuto a minuto [3]. Con diarios laborales sellados de los trabajadores y registros de decisiones anclados de las plataformas, la Inspección de Trabajo y los tribunales trabajan sobre cronologías verificables desde el primer requerimiento: menos años de instrucción, menos periciales de reconstrucción, y sanciones —o absoluciones— asentadas sobre hechos con fecha cierta [5]. La presunción de laboralidad [1][2] deja de ser una batalla probatoria para convertirse en una comprobación.

4. El algoritmo con acta

La Ley Rider da al comité de empresa el derecho a conocer los parámetros, reglas e instrucciones de los algoritmos [2]; la Directiva impone transparencia continua [1]. Pero un documento entregado un martes no dice nada del cambio silencioso del viernes. La solución es el versionado sellado: cada versión de los parámetros entregados, con huella y datada [5], de manera que cualquier modificación posterior sea visible y datable. Es la misma lógica de procedencia que el libro aplica a los modelos de IA en el capítulo 79, llevada a la relación laboral: el algoritmo puede cambiar, pero no puede hacer creer que siempre había sido como ahora.

Los límites, dichos con claridad: el sello no decide si una relación es laboral —eso lo hacen las leyes y los jueces [1][2]; no abre por sí solo la caja negra del algoritmo —eso lo hacen los deberes de transparencia [1] [2] y, cuando hace falta, los tribunales [4]; y no sustituye ni el convenio, ni el sindicato, ni la negociación colectiva. La prueba de existencia hace exigible el derecho; el derecho, lo han de hacer las personas.

La promesa y el peligro

La promesa: trabajadores que ya no discuten con una pantalla muda [4]; plataformas que pueden demostrar su diligencia en lugar de pagarla por sentencia [3]; inspecciones que duran semanas y no años; y una presunción de laboralidad [1][2] que se activa con hechos datados, no con batallas de testigos. La gestión algorítmica, con acta.

Los peligros, con la misma claridad.

El primero es **la vigilancia invertida**. Sería un contrasentido trágico que la herramienta pensada para equilibrar la relación acabara justificando más monitorización del trabajador. La Directiva ya prohíbe los datos sensibles —emociones, biometría, conversaciones privadas— en las decisiones automatizadas [1]; el diario laboral sellado ha de ser del trabajador y para el trabajador: en su dispositivo, bajo su control, con revelación voluntaria y revocabilidad [5]. Ninguna plataforma puede exigirlo ni acceder a él.

El segundo es **el registro sesgado**. Quien sella elige qué sella: una plataforma podría anclar solo lo que la favorece, y un trabajador también. El sello acredita integridad y fecha, no completitud. Por eso el diseño ha de ser bilateral, y los reguladores han de poder exigir a las plataformas los registros completos —recordemos que los vacíos también quedan datados [5].

El tercero es **la reputación portátil**. Si el diario laboral sellado degenera en una «puntuación de trabajador» exportable entre plataformas, habremos construido la lista negra perfecta —inmutable y todo. La cronología es para defender derechos en caso de conflicto, no para hacer de historial de conducta permanente: caducidad, revocabilidad y prohibición expresa de usarla como filtro de contratación.

Y el cuarto es **el tecnosolucionismo laboral**. Ninguna huella sube una tarifa ni paga una cotización. Los derechos del trabajo de plataforma nacieron de la ley [1][2], de la Inspección [3], de los tribunales [4] y de la organización colectiva; la criptografía solo garantiza que, cuando haga falta probar, se pueda. Confundir la herramienta con la lucha sería repetir en un sector nuevo el error de siempre.

Es hora de actuar

Si el algoritmo dirige, que quede acta —de sus órdenes y de tu trabajo.

Para los trabajadores de plataforma: sella tu diario laboral —horas, encargos, instrucciones, capturas de condiciones [5]; conoce la presunción que te ampara [1][2]; y si llega la desconexión, exige la motivación que Europa ya te reconoce [1][4].

Para las plataformas: anclad el registro de decisiones y la revisión humana [1][4][5]; el caso Glovo enseña que la realidad acaba aflorando, y que hacerlo tarde cuesta cientos de millones [3] —ser auditable desde el primer día es más barato que serlo por sentencia.

Para sindicatos y comités de empresa: exigid los parámetros de los algoritmos [2] con versionado sellado [5] —la transparencia sin fecha cierta es una foto vieja.

Para la Inspección de Trabajo y los jueces: pedid y valorad las cronologías ancladas de ambas partes [3][5]; que la instrucción empiece con hechos datados, no con terabytes por excavar.

Para los legisladores: al transponer la Directiva antes del 2 de diciembre de 2026 [1], incorporad el deber de registro de decisiones anclado y el derecho del trabajador a su propio diario sellado —y blindadlo contra todo uso como filtro reputacional.

A los conductores de Ámsterdam les hizo falta un tribunal de apelación y 584.000 euros en multas para que una aplicación les dijera por qué los había despedido [4]. Que el próximo turno desconectado tenga la respuesta esperándolo: datada, anclada y exigible. Por el trabajo digno en la era del algoritmo, **time2act**.

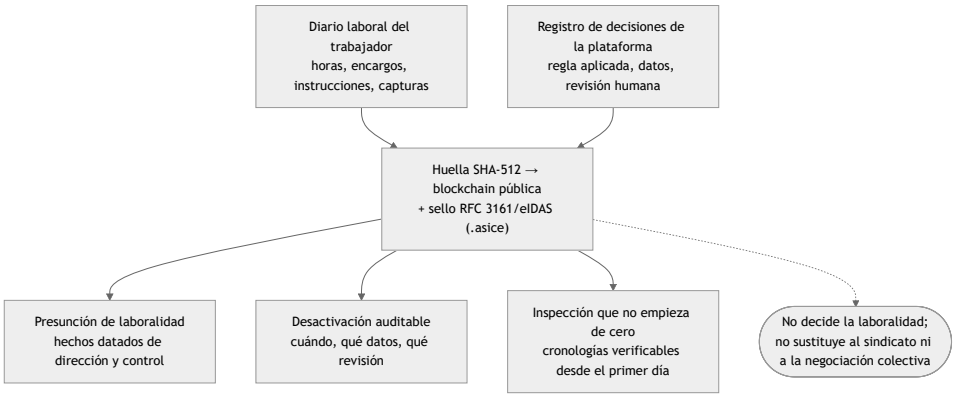


Figura 92.1 — La relación laboral de plataforma con prueba de existencia: el trabajador sella su diario laboral (horas, encargos, instrucciones, capturas de condiciones) en su dispositivo; la plataforma ancla el registro de decisiones algorítmicas y la revisión humana (art. 22 RGPD; Directiva (UE) 2024/2831); el comité recibe los parámetros del algoritmo con versionado sellado (Ley Rider). Tres salidas: la presunción de laboralidad probada con hechos datados, la desactivación auditable y la inspección que no empieza de cero. Límites: el sello no decide la laboralidad ni sustituye la negociación colectiva; el diario es del trabajador, nunca un filtro reputacional. Fuentes: DOUE (Dir. 2024/2831); BOE (Ley 12/2021); elDiario.es (caso Glovo); Worker Info Exchange (Drivers v. Uber/Ola).

---

[1] DOUE / BOE — *Directiva (UE) 2024/2831 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativa a la mejora de las condiciones laborales en el trabajo en plataformas* (en vigor el 2 de diciembre de 2024; transposición hasta el 2 de diciembre de 2026; presunción de laboralidad por hechos de dirección y control con carga de la prueba sobre la plataforma; prohibición de datos sensibles en decisiones automatizadas; transparencia, supervisión humana e intervención humana en decisiones importantes); Laboral Social — *Directiva sobre plataformas digitales de trabajo*. https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81667 · https://eur-lex.europa.eu/eli/dir/2024/2831/oj?eliuri=eli:dir:2024:2831:oj&locale=es · https://www.laboral-social.com/directiva-plataformas-digitales-trabajo-mejora-condiciones-laborales ↩

[2] BOE — *Ley 12/2021, de 28 de septiembre* («Ley Rider»: presunción de laboralidad en el reparto mediante gestión algorítmica; derecho del comité de empresa a ser informado de los parámetros, reglas e instrucciones de los algoritmos que afectan a las condiciones de trabajo; régimen en vigor desde agosto de 2021); PwC Periscopio — *¿Ha cumplido sus objetivos la Ley Rider?*. https://www.boe.es/buscar/act.php?id=BOE-A-2021-15767 · https://periscopiofiscalylegal.pwc.es/luces-y-sombras-de-la-ley-rider/ ↩

[3] elDiario.es — *El jefe de Glovo admite a la jueza que la regularización de los 'riders' busca evitar «discusiones» con Inspección de Trabajo* (causa penal en Barcelona; ≈200 M€ en cuotas y multas; Just Eat reclama 295 M€); elDiario.es — *El jefe de Glovo dice que la presión penal y las multas forzaron cambiar su modelo laboral: «La caja no te da para operar»* (10.000-15.000 riders; provisiones de Delivery Hero de 440-770 M€; impacto ≈100 M€ en el EBITDA de 2025); Crónica Global — *Óscar Pierre justifica el cambio de modelo laboral por «presión económica y penal»*. https://www.eldiario.es/catalunya/jefe-glovo-admite-jueza-regularizacion-riders-busca-evitar-discusiones-inspeccion-trabajo_1_11870197.html · https://www.eldiario.es/economia/jefe-glovo-dice-presion-penal-multas-forzaron-cambiar-modelo-laboral-caja-no-da-operar_1_12062602.html · https://cronicaglobal.elespanol.com/business/20250218/oscar-pierre-de-glovo-justifica-laboral-economica/925157487_0.html ↩

[4] Fountain Court Chambers — *Amsterdam Court Upholds Appeal in Algorithmic Decision-Making Test Case: Drivers v Uber and Ola* (abril de 2023; tres sentencias; Ola ha de explicar la lógica de la decisión totalmente automatizada, art. 22 RGPD); Worker Info Exchange — *Uber ordered to pay €584,000 for failure to comply with court order in robo-firing case* (más 4.000 €/día); UK Human Rights Blog — *Amsterdam Court orders reinstatement of Uber drivers dismissed by algorithm*. https://fountaincourt.uk/2023/04/amsterdam-court-upholds-appeal-in-algorithmic-decision-making-test-case-drivers-v-uber-and-ola/ · https://www.workerinfoexchange.org/post/uber-ordered-to-pay-584-000-for-failure-to-comply-with-court-order-in-robo-firing-case/ · https://ukhumanrightsblog.com/2021/05/18/amsterdam-court-orders-reinstatement-of-uber-drivers-dismissed-by-algorithm/ ↩

[5] t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; contenido en el dispositivo, revelación voluntaria; los vacíos de la serie quedan datados). Véanse los capítulos 13 y 15; la procedencia de los modelos de IA, en el capítulo 79. ↩

La jornada y el conflicto laboral: horas que constan

«El poder no concede nada sin una exigencia. Nunca lo ha hecho y nunca lo hará.»

— Frederick Douglass, discurso de Canandaigua (1857)

Las 19:40 en un polígono industrial cualquiera. El último pedido ha salido tarde, y el registro horario —la hoja de papel de la carpeta, o la aplicación de la empresa— marca las 18:00 en punto, como cada día. En la cafetería de un centro comercial, una camarera suma mentalmente las horas que no cobrará este mes. Ninguno de los dos gestos hará ruido hoy; ambos pesarán el día que haya conflicto.

Los datos dicen que no son anécdotas [1]: según la Encuesta de Población Activa, más del 40 % de las horas extra que se hacen en España no se remuneran. Y eso con un registro de jornada que es obligatorio para todas las empresas desde 2019. El problema no es que el registro no exista: es quién lo custodia. El papel aguanta lo que le pongan; el sistema digital de la empresa lo controla la empresa. Cuando el conflicto estalla —la reclamación de horas, la modificación de condiciones comunicada de palabra, el despido que llega justo después de reclamar—, en el juzgado de lo social hay dos memorias y un registro de parte.

Este capítulo trata la variable más básica del contrato más común del país —y la peor probada. El trabajo gobernado por un jefe algorítmico —repartidores, conductores— está en el capítulo 92; la identidad de quien contratas en remoto, en el capítulo 91; las condiciones laborales en la cadena de suministro global, en el capítulo 102; el acoso y la técnica de grabar conversaciones propias, en el capítulo 75. Pregunta clave: ¿cómo se discute la jornada cuando el reloj oficial es de una de las partes? Respuesta: con fecha cierta en los dos lados —el diario laboral del trabajador y la certificación neutral del registro oficial— mediante **t2p**: hash, hora y ancla —el trípode del capítulo 13 [3]. Y con un contexto que empuja: la reforma del registro horario digital que viene exigirá exactamente esta arquitectura.

El registro que viene: inmutable por ley

La novedad legislativa [1]: el Gobierno aprobó el 30 de septiembre de 2025 la tramitación urgente de un decreto para el registro horario digital —desacoplado de la reducción de jornada—, con el objetivo de aprobarlo durante 2026 (sin fecha de entrada en vigor publicada aún). Lo que el proyecto exige, según la documentación pública: registros electrónicos trazables e inmutables; sellado de tiempo; registro de pausas; acceso remoto y en tiempo real para la Inspección de Trabajo; y un historial de modificaciones con autoría y fecha —una corrección unilateral sin conocimiento del trabajador se podrá considerar manipulación ante un tribunal [1].

Detente en lo que esto significa para la tesis de este libro —y ponlo al lado de VeriFactu, el sistema que el capítulo 34 explica: por segunda vez en pocos años, el Estado exige por norma inmutabilidad, traza y fecha cierta para resolver un problema de confianza. Primero las facturas; ahora las horas. La prueba de existencia ya no es una propuesta: es el sentido de la marcha.

Y ahora, lo que la reforma no da. El registro, por inmutable que sea, vive en los sistemas de la empresa o de su proveedor; el acceso remoto es para la Inspección, no para el trabajador, que sigue sin una copia propia oponible de sus horas. Y la empresa honesta, ante una acusación de manipulación, ha de probar un negativo —que no tocó nada— con sus propios sistemas como único testigo. La capa que falta mira los dos lados: la copia con fecha cierta en manos del trabajador, y la certificación neutral del registro oficial que hace el cumplimiento de la empresa demostrable, no solo alegable.

La prueba de existencia aplicada

El conflicto laboral se gana o se pierde por hechos datados; que cada parte tenga los suyos [3].

1. El diario laboral del trabajador

En su dispositivo personal, el trabajador sella lo que le afecta: la foto del fichaje de hoy, la nota de las horas hechas, el turno publicado [3]. Treinta segundos al final de la jornada. Solo las huellas se anclan; el contenido queda en su móvil, y no ha de enseñárselo a nadie —hasta el día que haga falta, ante el delegado,

la Inspección o el juzgado de lo social. Meses de entradas con fecha cierta pesan más que cualquier memoria —y que cualquier registro de parte.

Y una mención que este capítulo no puede omitir: en ningún sitio vale tanto este diario como en el trabajo del hogar. Las trabajadoras domésticas —el contrato más informal del país: horas pactadas de palabra, efectivo, a menudo sin registro de ningún tipo— tienen en el mismo gesto de treinta segundos la primera evidencia laboral de su historia [3]. La dignidad de un trabajo también se mide por su capacidad de ser probado.

2. El fichaje con lugar y hora

Cuando el sistema oficial «falla» —el día que curiosamente no consta, el fichaje que alguien corrigió—, la foto de entrada y salida con el GPS forense de t2p —fijo genuino, precisión de unos 50 metros, antigüedad máxima de unos 30 segundos; la ubicación simulada bloquea la certificación [3]— acredita dónde estaba el trabajador y cuándo. Lo mismo vale para el desplazamiento que no se paga: el lugar de trabajo real, datado. Y la línea roja, dicha aquí mismo: el momento del fichaje, nunca el seguimiento continuo —se documenta la jornada, no se vigila a la persona.

3. El cuadrante y la orden

El cuadrante publicado, capturado con fecha cierta; el cuadrante cambiado a última hora, también; la orden recibida por mensaje o correo, certificada [3]. El «yo no te dije eso» y la modificación de condiciones comunicada de palabra chocan con pantallas datadas. Y si la conversación es cara a cara, la grabación propia es lícita —la técnica y los límites están en el capítulo 75.

4. El registro oficial certificado — la simetría de la empresa

La empresa que lo hace bien cierra cada mes su registro horario con una certificación por lotes: la huella del fichero mensual, encadenada con la del anterior [3] —la misma lógica que VeriFactu impone a las facturas. Ante la Inspección —que podrá acceder a él en remoto [1]— y ante el juzgado, su registro no es solo inmutable de ahora en adelante: es demostrablemente no manipulado desde cada cierre. Contra la reclamación de horas fantasma, contra la acusación de corrección retroactiva, la empresa honesta tiene fechas, no alegaciones. Y el historial de modificaciones que la reforma exige [1], anclado, se convierte en su coartada permanente.

Los límites, negro sobre blanco: el sello acredita horas y comunicaciones —no decide si la hora era extra, complementaria o voluntaria: eso lo dicen el convenio y el juez. El diario personal del trabajador no sustituye el registro legal de la empresa —lo complementa y lo contrasta. Y la proporcionalidad manda: ninguna de las dos partes puede convertir la jornada en vigilancia —ni geolocalización continua del trabajador, ni grabación ambiental de la plantilla.

La promesa y el peligro

La promesa: juicios de lo social que discuten derecho, no hechos [1][3]; el 40 % de horas extra impagadas [1] con una herramienta de reclamación al alcance de cualquier bolsillo; empresas cumplidoras que pasan inspecciones con registros demostrablemente íntegros; y la cultura del «ya lo apuntaré» sustituida por la del hecho datado —en los dos lados de la nómina.

Los peligros, sin rodeos.

El primero es **la vigilancia disfrazada de registro**. El paso del fichaje datado al trabajador rastreado es corto y tentador. La línea legal y moral: se registra el momento —entrada, salida, pausa—, nunca el recorrido; el registro sirve a la jornada, no al control de la vida.

El segundo es **la desconfianza institucionalizada**. Si cada orden se ha de capturar y cada turno sellar, la relación laboral se judicializa por adelantado. La respuesta es la de siempre en este libro: el rastro es para el conflicto, no para el día a día —y cuanto más verificable es el registro oficial, menos falta hace el paralelo.

El tercero es **la brecha del más precario**. Quien más sufre las horas impagadas es quien menos herramientas y menos margen tiene para documentarlas sin miedo. El diario personal ayuda; pero la protección real son la Inspección con acceso remoto [1], los delegados sindicales y los convenios —la prueba individual no sustituye la tutela colectiva.

Y el cuarto: **confundir medir con resolver**. El registro perfecto no paga las horas extra: las hace visibles y reclamables. Si la reclamación sigue costando el empleo, el problema no es probatorio. Hacen falta inspección, sanciones y una cultura donde pagar las horas hechas sea el mínimo, no una conquista.

Es hora de actuar

Que el reloj del trabajo tenga dos dueños.

Para ti, trabajador: treinta segundos al final de cada jornada —el fichaje, las horas, el turno [3]; el día que haga falta reclamar, tendrás meses de hechos datados. Y si la cosa va de acoso, el capítulo 75 es el tuyo.

Para las empresas: certificad el registro horario por lotes encadenados [3] antes de que la reforma [1] os lo pida a medias —el registro demostrablemente íntegro es vuestra mejor defensa ante Inspección, juzgados y reclamaciones infundadas.

Para sindicatos y delegados: haced del diario laboral sellado una herramienta básica de afiliación y defensa [3]; y negociad en los convenios el derecho del trabajador a la copia verificable de su registro.

Para la Inspección de Trabajo: el acceso remoto que la reforma os dará [1] vale lo que valga la integridad del registro —pedidlo anclado, con historial de modificaciones verificable.

Para los legisladores: la reforma del registro digital [1] es la ocasión de cerrar el círculo: registro inmutable, sí —y copia con fecha cierta para el trabajador, y valor probatorio reconocido a la certificación neutral. Que la segunda mitad de la prueba no se quede en el tintero.

Que las 19:40 del polígono y las horas de la cafetería consten —y que el próximo juicio de lo social discuta justicia, no memoria. Por las horas que son vida, **time2act**.

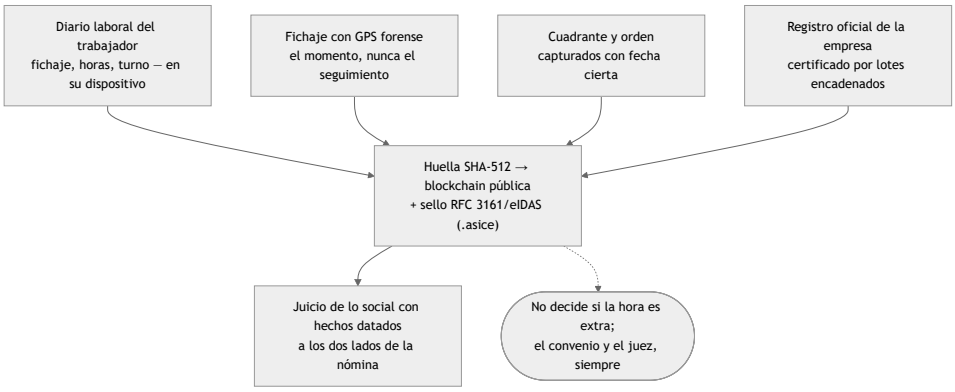


Figura 93.1 — La jornada con prueba de existencia (sellado con t2p — capítulo 13): el diario laboral del trabajador (fichaje, horas, turnos —en su dispositivo, solo huellas en la cadena), el fichaje con GPS forense (el momento, nunca el seguimiento), el cuadrante y la orden capturados con fecha cierta, y el registro oficial de la empresa certificado por lotes encadenados — demostrablemente íntegro ante Inspección y juzgado. Contexto: la reforma del registro horario digital (tramitación urgente desde el 30-9-2025) exigirá inmutabilidad, traza y acceso remoto de la Inspección; >40 % de las horas extra no se pagan (EPA). Límites: el convenio y el juez deciden el fondo; proporcionalidad siempre. Fuentes: EPA/INE; proyecto de registro horario digital.

---

[1] Ministerio de Trabajo / prensa especializada — *Registro horario digital obligatorio: la reforma en trámite* (tramitación urgente aprobada por el Consejo de Ministros el 30-9-2025, desacoplada de la reducción de jornada; objetivo de aprobación durante 2026, sin fecha de entrada en vigor publicada; requisitos del proyecto: registros electrónicos trazables e inmutables, sellado de tiempo, registro de pausas, acceso remoto y en tiempo real para la Inspección de Trabajo, historial de modificaciones con autoría y fecha); EPA/INE — más del 40 % de las horas extra no se remuneran; RD-ley 8/2019 — registro diario de jornada obligatorio. https://www.protime.eu/es-es/noticias/registro-horario-digital-obligatorio-2026 · https://factorial.es/blog/nuevo-registro-horario-digital-espana/ · https://www.inwout.com/post/registro-horario-digital-obligatorio-2026 · https://kronjop.com/es/newsroom/control-horario/digital/obligatorio/ ↩

[2] Marco laboral general (papeleta del juicio de lo social; actas de la Inspección de Trabajo; papel de los delegados). Véase el capítulo 92 para el trabajo de plataforma y el capítulo 102 para la cadena de suministro laboral.

[3] t2p — manual de producto (foto con GPS forense —fijo genuino ~50 m / ≤30 s, la ubicación simulada bloquea la certificación; captura de pantalla y correo certificados; certificar cualquier fichero —solo la huella viaja; certificación en segundo plano; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS

complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; las conversaciones propias y el acoso, en el capítulo 75. ↩

Construcción e infraestructura: quién demuestra cómo se levantó de verdad

«Todas estas construcciones deben levantarse teniendo en cuenta la solidez, la utilidad y la belleza.»

— Vitruvio, De architectura, I, 3 (s. I a. C.)

El 6 de febrero de 2023, dos terremotos (Mw 7,8 y 7,5) sacudieron el sureste de **Turquía** antes del alba. Murieron más de **55.000 personas** y se derrumbaron más de **160.000 edificios**, muchos de ellos estructuras que habían sido legalizadas a través de programas repetidos de amnistía urbanística (*imar barışı*) y levantadas con hormigón de calidad dudosa, sin certificar. El caso más crudo es el del **Isias Grand Hotel**, siete plantas en **Adıyaman** que se plegaron como un acordeón en pocos segundos y mataron a **72 personas**, entre ellas una delegación de voleibol de una escuela turcochipriota: 35 de los muertos eran niños, maestros y entrenadores. En diciembre de 2024, tras una vista de diecisiete horas, un tribunal condenó al propietario **Ahmet Bozkurt**, a su hijo **Mehmet Fatih Bozkurt** y al arquitecto **Erdem Yılmaz** a hasta **18 años** cada uno por «causar la muerte con negligencia consciente». Un informe técnico de 150 páginas concluyó que el hotel se había construido con hormigón pobre mezclado con arena y grava de río, no tenía ningún informe de estudio del terreno, y en 2016 se le había añadido una planta sin permiso [1].

Este capítulo no trata de quién es el propietario de un inmueble ni de su título legal —eso es el capítulo 35, el registro de la propiedad. Aquí hablamos del **registro de integridad física**: las pruebas de materiales, las inspecciones de obra, los estudios geotécnicos y los planos *as-built*, es decir, la prueba de **cómo se construyó de verdad una cosa y cómo se verificó**, no de quién la posee. La pregunta es incómoda porque un edificio acabado esconde su propia historia: una vez el hormigón cubre la armadura, nadie ve si las barras estaban, si el hormigón tenía la resistencia declarada, ni si la prueba del laboratorio se hizo honestamente. Y cuando esta historia se falsifica, no se pierde dinero: se pierden vidas.

La historia enterrada en el hormigón

El caso turco no es una anomalía exótica. Se estima que **13 millones de edificios** turcos —más de la mitad del parque— se levantaron incumpliendo la normativa, y al menos **75.000 construcciones** de la zona afectada habían recibido amnistías urbanísticas antes del terremoto [1]. Estas amnistías —los *Yapı Kayıt Belgesi*, certificados de registro que legalizaban retroactivamente edificios en infracción de los códigos antisísmicos— fueron calificadas por los colegios de ingenieros de Turquía como «una invitación a la muerte». El problema de fondo es que el papel que debía demostrar que un edificio era seguro o bien no existía, o bien se podía comprar a posteriori.

El mismo patrón aparece lejos de cualquier falla sísmica. El 24 de junio de 2021, en **Surfside**, Florida, la torre **Champlain Towers South** se desplomó de madrugada y mató a **98 personas**. La investigación del **NIST** —el organismo federal estadounidense— situó el inicio del colapso en un **fallo de punzonamiento** de la losa de la cubierta de la piscina: el hormigón era más débil que el que exigía el código, y la armadura se había colocado con un recubrimiento excesivo que reducía su capacidad a cortante [3]. Una losa, un detalle constructivo, años de degradación no documentada: 98 muertos. La diferencia entre Adıyaman y Surfside no es la física; es que en ambos casos el **registro de lo que realmente se construyó** era inexistente o no se podía confiar.

Cuando la prueba del material es la mentira

Hay un fraude aún más directo: falsificar la misma prueba que ha de garantizar el material. El caso más espectacular es el del **Puente Hong Kong–Zhuhai–Macao**, una de las obras más caras del planeta. Entre 2012 y 2017, la **ICAC** (la comisión anticorrupción de Hong Kong) imputó a **19 trabajadores** del laboratorio Jacobs China Limited por haber falsificado **384 informes** de ensayo de probetas de hormigón: manipulaban la fecha del ordenador y sustituían las probetas débiles por probetas de alta resistencia, e incluso por un cilindro metálico de calibración. La limpieza costó **58 millones de dólares de Hong Kong** a los contribuyentes, y en junio de 2024 el director Albert Leung Wing-keung fue encarcelado dos años y medio por defraudar al gobierno de unos 2 millones de dólares de Hong Kong [4].

En Estados Unidos, el presidente de **Testwell Laboratories**, V. Reddy Kancharla, fue condenado por haber falseado pruebas de resistencia del hormigón en **más de 100 obras** de Nueva York, entre ellas la **Freedom Tower**, el **Yankee Stadium** y el metro de la Segunda Avenida. Cuando se extrajeron y ensayaron testigos reales, el hormigón de la Freedom Tower que se había certificado a 12.000 PSI resultaba ser, de hecho, de unos 9.000 PSI. Kancharla recibió de siete a 21 años de prisión y 225.000 dólares de reparación [5]. La técnica era sencilla y devastadora: en lugar de ensayar la probeta y anotar el resultado, se escribía directamente el valor de la especificación; el documento decía lo que debía decir, pero la realidad física era otra.

Y cuando no es el material, es la inspección. El 14 de agosto de 2018, el **Puente Morandi** de **Génova** se derrumbó y mató a **43 personas**. En julio de 2022 llegaron a juicio **59 acusados**; la fiscalía concluyó que algunos documentos de inspección eran «claramente falsos» y que la operadora, Autostrade, se inspeccionaba a sí misma a través de su filial Spea. Como hemos visto, el 7 de abril de 2023 un juez aceptó un acuerdo de 30 millones de euros entre Autostrade y Spea [6]. La autovigilancia —ser juez y parte de la propia seguridad— es el agujero por donde se cuela la falsificación.

La ley ya pide el hilo; falta el ancla

La regulación ha reaccionado, y con fuerza. En el Reino Unido, después del incendio de la **Grenfell Tower** —como hemos visto— la **Building Safety Act 2022** obliga a mantener un «hilo dorado» digital: un registro trazable y con control de versiones del diseño, los productos, los materiales, las aprobaciones y la información *as-built*, conservado durante toda la vida de los edificios de alto riesgo [7]. En la Unión Europea, el **Reglamento (UE) 2024/3110** —la revisión del Reglamento de Productos de Construcción, en vigor desde el 7 de enero de 2025 y aplicable a la mayoría de productos desde el 8 de enero de 2026— convierte el **Pasaporte Digital de Producto** en un requisito legal obligatorio para el marcado CE: ha de llevar la Declaración de Prestaciones y Conformidad y la documentación técnica a través de un código QR o portador de datos [8]. A ello se suma la serie **ISO 19650**, el estándar internacional para gestionar la información con **BIM** a lo largo de todo el ciclo de vida y producir un «gemelo digital» *as-built* del activo. La ley, pues, ya pide exactamente lo que falta: un registro del *cómo se construyó*. Pero un hilo dorado almacenado en un servidor que controla quien lo ha de explicar es, en una disputa, papel de parte.

Por qué el hilo dorado por sí solo no salva

Hay que decirlo con crudeza. Un registro digital, por bien diseñado que esté, es tan fiable como la imposibilidad de alterarlo en silencio. Si el informe de inspección previa al hormigonado vive en una base de datos que la operadora puede editar —como Autostrade se inspeccionaba a sí misma—, mañana se puede retocar la fecha, sustituir una foto o borrar un ensayo incómodo sin dejar rastro. El fraude de Hong Kong consistió, literalmente, en **cambiar la fecha del ordenador**; el de Testwell, en **escribir el valor de la especificación** en lugar del valor medido. Ningún «hilo dorado» que se pueda reescribir a posteriori detiene estas dos técnicas. Lo que la ley pide es un registro; lo que falta es que ese registro sea **inalterable, datado de manera independiente y ligado a un autor y un lugar**, de manera que cualquier sustitución o retrodatación posterior se pueda demostrar.

La prueba de existencia aplicada

Es aquí donde **t2p** aporta la capa que faltaba en cada hito irreversible de la obra. **Primero**, antes del hormigonado, el inspector de campo fotografía o filma la armadura, el encofrado y el recubrimiento; el dispositivo calcula sobre la marcha la **huella SHA-512**, obtiene un **sello de tiempo RFC 3161 conforme a eIDAS**, la ancla a la **blockchain pública** y le añade el **GPS forense** y una **prueba de vida** que vincula al inspector con aquel lugar e instante. **Segundo**, el laboratorio de materiales sella cada resultado de ensayo de probeta —y los datos crudos del instrumento— en el momento exacto de la rotura a los 28 días, de manera que la fecha y el valor ya no se pueden retrodatar ni intercambiar (precisamente como hacen las técnicas de Hong Kong y Testwell). **Tercero**, el ingeniero sella el juego de planos *as-built* firmado y el informe geotécnico en el momento de la firma. Cada sello genera un contenedor **.asice** verificable fuera de línea que fluye hacia el hilo dorado (BSA 2022) y al modelo de información BIM (ISO 19650), y se empareja con la Declaración de Prestaciones y el Pasaporte Digital de Producto del Reglamento (UE) 2024/3110. Es el mismo principio de procedencia C2PA de los capítulos 13 y 15, aplicado aquí no a una imagen sintética sino a la historia física de un edificio.

Ahora el límite, con toda la crudeza. «Basura a la entrada, basura en la cadena»: el sello demuestra que *aquella* foto, *ese* resultado de ensayo o *ese* plano existían en un instante, fueron creados por un dispositivo o autor determinado y no se han alterado desde entonces. **No prueba que el edificio sea seguro**, ni que el hormigón tenga la resistencia real, ni que la armadura fotografiada sea la que quedó en su sitio, ni que el ensayo se hiciera honestamente. Un inspector corrupto puede fotografiar una armadura conforme y después verter hormigón malo; un laboratorio puede sellar un ensayo ejecutado pero deliberadamente infracargado; un propietario puede sellar el plano real de una planta ilegal. Y no puede certificar retroactivamente los millones de estructuras ya construidas y sin sellar —los 13 millones de edificios turcos no conformes. El sello estrecha el fraude porque hace **demostrable** la manipulación y la fabricación posteriores; no garantiza que la realidad física de debajo sea sólida.

La promesa y el peligro

La promesa es un registro de obra **a prueba de manipulación**: que ninguna operadora se pueda inspeccionar a sí misma en la sombra, que ningún laboratorio pueda cambiar la fecha del ordenador y que, después de un desastre, los investigadores —como el NIST en Surfside— puedan demostrar **qué registros son auténticos y contemporáneos** y cuáles se fabricaron. La prueba de existencia no sustituye los laboratorios acreditados, la inspección independiente de terceros, la firma del control de obra ni la investigación forense; los hace **responsables**.

El peligro pide los matices de siempre. El primero, la **falsa confianza**: «está anclado, luego es seguro» es exactamente la mentira que el sello no autoriza —anclar un dato no lo hace cierto. El segundo, la **concentración y el coste**: si sellar cada hito se vuelve caro o técnicamente pesado, puede expulsar a los pequeños constructores honestos en lugar de protegerlos. Y el tercero, el **fraude de captura**: si el inspector corrompido es quien sostiene el dispositivo, puede sellar una realidad tramposa con toda la fuerza probatoria de un sello; —por eso el GPS forense y la prueba de vida ligan al autor al lugar, pero no lo hacen honesto. La capa criptográfica hace la trampa demostrable; no la hace imposible.

Es hora de actuar

Para los **laboratorios de materiales y las entidades de inspección acreditadas**: sellar cada resultado de ensayo y cada inspección previa al hormigonado en el instante en que se producen, para que la fecha y el valor no se puedan tocar nunca más. Para los **promotores, constructores e ingenieros**: sellar los planos *as-built* y el informe geotécnico en el momento de la firma y volcarlos al hilo dorado. Para los **reguladores y el control de obra** (Building Safety Regulator, autoridades de marcado CE bajo el Reglamento 2024/3110): exigir el registro sellado como parte del hilo dorado y del Pasaporte Digital de Producto, y reconocerlo como evidencia. Para los **investigadores de colapsos** (NIST y equivalentes): tratar el contenedor .asice datado como la cadena de custodia que distingue el documento auténtico del fabricado después. Y para los **fabricantes de productos de construcción**: anclar la Declaración de Prestaciones de cada lote, para que una sustitución posterior falle la comprobación de huella.

Como hemos visto en Adıyaman, la muerte de decenas de personas en un hotel construido con arena de río y legalizado con un papel comprable demuestra que dar a cada hito de obra una prueba sellada de cómo se construyó y verificarla realmente —sin olvidar nunca que el sello no hace seguro lo que no lo es— es fundamental en este frente donde el hormigón esconde su propia historia, time2act.

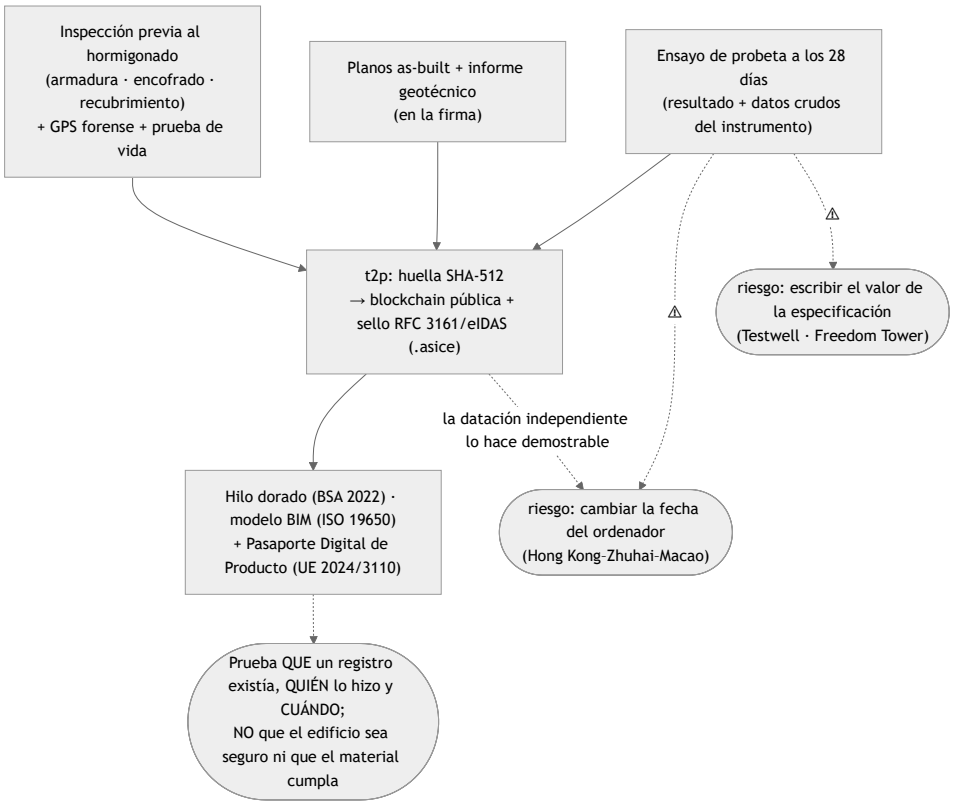


Figura 94.1 — Tres hitos irreversibles de una obra: inspección previa al hormigonado (armadura, encofrado, recubrimiento), ensayo de probeta a los 28 días, y planos as-built + informe geotécnico a la firma. En cada hito, t2p calcula la huella SHA-512, le añade GPS forense y prueba de vida si hay captura de campo, sella con RFC 3161/eIDAS y ancla a la blockchain pública (.asice); el contenedor fluye hacia el hilo dorado (BSA 2022) y el modelo BIM (ISO 19650) y se empareja con el Pasaporte Digital de Producto (Reglamento UE 2024/3110). Puntos de riesgo que la datación independiente hace demostrables: cambiar la fecha del ordenador (Hong Kong–Zhuhai–Macao) y escribir el valor de la especificación (Testwell). Límite: el sello prueba que un registro existía, quién lo hizo y cuándo, no que el edificio sea seguro ni que el material cumpla. Fuentes: terremotos de Turquía 2023 (Isias Grand Hotel); NIST (Champlain Towers South); ICAC (puente HZMB); Testwell; puente Morandi; Building Safety Act 2022; Reglamento (UE) 2024/3110.

---

[1] The Dial — *Faulty Construction* (juicios por el terremoto de Turquía; Isias Grand Hotel; condenas de 18 años en diciembre de 2024; 75.000 edificios amnistiados; unos 13 millones de edificios no conformes). https://www.thedial.world/articles/news/issue-25/turkey-earthquake-trials ↩

[2] PBS Peril & Promise — *How unenforced building codes worsened the Turkey-Syria earthquake* (julio de 2023; amnistías, no aplicación de los códigos y fallos de calidad del hormigón). https://www.pbs.org/wnet/peril-and-promise/2023/07/unenforced-building-codes-worsened-the-impacts-of-the-earthquake-that-hit-turkey-and-syria/

[3] NIST — *Champlain Towers South Collapse* (investigación federal oficial; 98 muertos; inicio por fallo de punzonamiento de la losa de la piscina; hormigón más débil que el código). https://www.nist.gov/disaster-failure-studies/champlain-towers-south-collapse ↩

[4] ICAC Hong Kong — *Consultant director jailed over false HZMB concrete cube test records* (19 trabajadores imputados; 384 informes falsificados; manipulación de fechas y sustitución de probetas; Albert Leung 2,5 años en junio de 2024). https://www.icac.org.hk/en/p/press/index_id_1890.html ↩

[5] The Real Deal — *Concrete tester exec convicted of falsifying safety reports for Yankee Stadium, Freedom Tower* (febrero de 2010; Testwell/Kancharla; Freedom Tower certificada a 12.000 PSI pero de unos 9.000 PSI; 7 a 21 años). https://therealdeal.com/new-york/2010/02/17/concrete-tester-exec-convicted-of-falsifying-safety-reports-for-yankee-stadium-freedom-tower/ ↩

[6] Wikipedia — *Ponte Morandi collapse* (Génova, 14 de agosto de 2018; 43 muertos; 59 acusados; documentos de inspección «claramente falsos»; autovigilancia vía Spea; acuerdo de 30 M€ en 2023). https://en.wikipedia.org/wiki/Ponte_Morandi_collapse ↩

[7] Seton UK — *Understanding the Golden Thread: Building Safety Act 2022* (registro digital trazable y con control de versiones para edificios de alto riesgo, posterior a Grenfell). https://www.seton.co.uk/legislationwatch/article/understanding-the-golden-thread-the-building-safety-act-2022/ ↩

[8] EUR-Lex — *Regulation (EU) 2024/3110* (Reglamento de Productos de Construcción revisado; en vigor el 7 de enero de 2025; Pasaporte Digital de Producto obligatorio para el marcado CE desde el 8 de enero de 2026). https://eur-lex.europa.eu/eli/reg/2024/3110/oj/eng ↩

[9] NIST — *Report to Congress provides update on Champlain Towers South investigation* (febrero de 2025; trabajo experimental completo, modelización en curso, presentación técnica en junio de 2025). https://www.nist.gov/news-events/news/2025/02/nist-report-congress-provides-update-champlain-towers-south-investigation

[10] BSI — *ISO 19650 Building Information Modelling standards* (gestión de la información con BIM y registro as-built / gemelo digital a lo largo del ciclo de vida). https://www.bsigroup.com/en-GB/products-and-services/standards/iso-19650-building-information-modelling-bim/

El pedigrí de una pieza: cuando un certificado falso puede matar

«Los reglamentos son papel: no amortiguarán un choque súbito de piedra y metal.»

— Ernest K. Gann, Fate Is the Hunter (1961)

Entre enero de 2019 y julio de 2023, **Jose Alejandro Zamora Yrala**, de 38 años, dirigió desde un despacho en su casa, en Surrey, una empresa británica de comercio de piezas aeronáuticas llamada **AOG Technics**. Vendió más de **60.000 piezas de motor de avión** —valoradas en unos 6,9 millones de libras— acompañadas de **certificados de aptitud falsificados** (EASA Form 1 y FAA Form 8130-3) que garantizaban fraudulentamente que las piezas eran nuevas y aeronavegables. La mayoría eran para el **CFM56**, el motor comercial más vendido del mundo, y el pedigrí falseado llegó a aerolíneas como American Airlines y Ethiopian Airlines. El fraude se deshizo a mediados de 2023, cuando una aerolínea pidió a **Safran** que verificara un certificado de AOG, Safran lo marcó como falso y, el 4 de agosto de 2023, la CAA británica, la FAA y la EASA emitieron alertas de seguridad. CFM International, la joint venture de GE Aerospace y Safran, demandó ante el High Court de Londres y acabó identificando **126 motores sospechosos**; la Serious Fraud Office británica obtuvo la declaración de culpabilidad de Zamora en diciembre de 2025 y una condena de **4 años y 8 meses** el 23 de febrero de 2026, por un fraude valorado en 39,3 millones de libras [1].

Este capítulo no habla del silicio de los chips falsificados —eso es el capítulo 70— ni de la trazabilidad genérica de mercancías del capítulo 29. Aquí el objeto es más estrecho y **crítico para la seguridad**: el **pedigrí documental de una sola pieza física**. El certificado de aeronavegabilidad de un álabe de turbina, la entrada del cuaderno de bitácora, el cuentakilómetros de un coche. La pregunta es incómoda: si la pieza es metal que no habla, y todo lo que la hace legítima es un papel que sí se puede falsificar, ¿cómo hacemos que ese papel sea inalterable y atribuible? Porque aquí un documento falso no es una molestia comercial: **puede matar**.

Un fraude de papel sobre metal que vuela

El caso AOG revela la anatomía exacta del ataque. Zamora no fabricaba piezas malas en una nave; manipulaba e inventaba los documentos que las acompañan. La demanda de CFM International identificó 78 documentos falsificados que cubrían 52 referencias de pieza del CFM56 y dos registros del CF6, con álabes de turbina incluidos, y llegaron a 68 motores montados en Boeing 737 y Airbus A320 antiguos; como hemos visto, el recuento de motores sospechosos se elevó a 126 [2]. Lo que hacía letal el fraude no era un fallo metalúrgico visible, sino la confianza ciega en un certificado: un Authorised Release Certificate con un sello y una firma que nadie podía confrontar con el origen real de la pieza.

AOG no es un caso aislado, sino la punta de un problema sistémico. Una estimación de la FAA citada por la industria calcula que cada año llegan a los aviones unos 520.000 componentes falsificados o no aprobados —cerca del 2 % de los 26 millones de piezas en servicio—, y sitúa el mercado global de piezas falsificadas por encima de los 2.000 millones de dólares anuales [3]. Cada una de estas piezas viaja con un pedigrí de papel, y cada pedigrí es tan fuerte como la dificultad de falsificarlo; hoy esta dificultad es baja: un PDF con un logotipo y una firma escaneada.

El mismo agujero, a cuatro ruedas: el cuentakilómetros

El problema del pedigrí documental no es exclusivo de la aviación; es el mismo agujero de confianza a escala que afecta a millones de consumidores. Como hemos visto, en diciembre de 2025 CARFAX estimó que circulan por las carreteras de Estados Unidos unos 2,45 millones de vehículos con el cuentakilómetros presuntamente manipulado, un aumento del 14 % respecto a 2024 y una pérdida media de unos 3.300 dólares por coche afectado [4]. La digitalización no lo ha resuelto: revertir un cuadro digital con una herramienta barata resulta más limpio y rápido que desmontar el vehículo.

En Europa la magnitud es comparable. Un estudio del Parlamento Europeo de 2018 encontró manipulación del cuentakilómetros en el 5-12 % de las ventas domésticas de coches usados y en el 30-50 % de las transfronterizas, con un daño económico estimado entre 5.600 y 9.600 millones de euros anuales en la UE [5]. La historia es la misma que en la aviación: una pieza —el vehículo— que no habla, y un

historial —los kilómetros, el libro de mantenimiento— que sí se puede reescribir. El libro de inspecciones con sello de taller es, en esencia, el hermano humilde del EASA Form 1.

El sistema que la industria ya construye

La respuesta institucional existe y avanza en la dirección correcta. Después de AOG, en febrero de 2024 se creó la Aviation Supply Chain Integrity Coalition —Airbus, Boeing, GE Aerospace, Safran, American, Delta, United y StandardAero— que el 9 de octubre de 2024 publicó 13 recomendaciones centradas en tres ejes: acreditación de proveedores, digitalización de los documentos y las firmas (FAA Form 8130, EASA Form 1) y mejora de la trazabilidad de las piezas [6]. La clave es *digitalizar*: la coalición reconoce que el papel firmado a mano es precisamente lo que AOG supo explotar.

El marco regulador ya está desde hace décadas. El Suspected Unapproved Parts (SUP) Program de la FAA, establecido en 1995, exige trazabilidad hasta la fabricación según el 14 CFR Part 21 o una determinación de aeronavegabilidad según el Part 43, verificada con las etiquetas FAA Form 8130-3, y las piezas sospechosas se reportan con la FAA Form 8120-11 [7]. En Europa, el EASA Form 1 es el equivalente y la EASA mantiene una base de datos de piezas sospechosas y emite boletines de seguridad —como el SIB 2023-05 sobre AOG Technics, de agosto de 2023—. En la carretera, la Federal Odometer Act (49 U.S.C. ch. 327) la hace cumplir la NHTSA en Estados Unidos, y en Europa la Directiva 2014/45/UE y el sistema belga Car-Pass apuntan hacia un registro de kilometraje a escala de la UE acordado en diciembre de 2025; como hemos visto, la ley pide trazabilidad, pero falta hacerla inalterable.

Por qué la digitalización por sí sola no salva

Hay que decirlo sin rodeos: digitalizar el EASA Form 1 o el libro de mantenimiento **no impide el fraude de AOG por sí solo**. Un PDF firmado es un PDF: se puede retocar, retrodatar, copiar y volver a emitir con un firmante inventado, exactamente como hizo Zamora. Si la digitalización solo sustituye el sello de tinta por una imagen de firma escaneada, hemos cambiado un papel falsificable por un fichero falsificable. Lo mismo vale para el cuadro digital del coche: un registro electrónico de kilómetros que se puede sobreescribir no es más fiable que la aguja mecánica que reemplaza.

El problema de fondo no es el soporte, sino la ausencia de una **ancla independiente** que fije *quién* declaró *qué* y *cuándo*, fuera del control de quien podría querer reescribirlo. Una base de datos centralizada ayuda, pero es tan fuerte como la confianza en el administrador y tan vulnerable como su clave. Lo que hace falta es que cada evento del pedigrí —cada certificado, cada entrada de cuaderno, cada lectura de cuentakilómetros— quede ligado a una fecha cierta y a un autor de una manera que haga **detectable** cualquier manipulación posterior.

La prueba de existencia aplicada

Aquí es donde **t2p** añade la capa que falta, y lo hace sobre el **evento de pedigrí**, no sobre el metal. Cuando un mantenimiento crea o transfiere un registro —un taller OEM/PMA que libera una pieza, un MRO que firma un formulario EASA 1 o un FAA 8130-3, un informe de desmontaje, una entrada de cuaderno de bitácora o un paquete de trazabilidad *back-to-birth*— el técnico o el responsable de calidad captura el documento en el dispositivo. Se calcula localmente la **huella SHA-512**, se aplica un **sello de tiempo RFC 3161/eIDAS**, se ancla a la blockchain pública y se genera un contenedor **.asice** verificable fuera de línea. Al añadirle un **GPS forense** y una **prueba de vida**, el firmante humano queda ligado al acto. El resultado es una **cadena de custodia inalterable**: cualquier parte posterior —la recepción de mercancías de una aerolínea, la CAMO, un regulador, un auditor o un comprador de coche usado que consulta el libro sellado y la foto del cuentakilómetros— puede verificar independientemente que *este* certificado o *esta* foto existían, sin alteración, en *este* momento, firmados por *este* autor en *este* lugar. El sistema se asienta debajo del 8130-3/Form 1 y las bases SUP y Car-Pass, encajando directamente con la recomendación de la coalición de «digitalizar documentos y firmas + mejorar la trazabilidad». Funciona junto a las capas de procedencia de los capítulos 13 (C2PA) y 15.

Ahora el límite, con toda la crudeza. «Basura a la entrada, basura en la cadena»: el sello prueba **el origen, el tiempo, el autor y la integridad** del certificado, de la foto o de la entrada de cuaderno; **no demuestra que la pieza sea genuina, nueva, aeronavegable o bien instalada**, ni que la lectura del cuentakilómetros o el registro de servicio documentado sean ciertos. Un falsificador todavía puede

sellar una mentira: si AOG hubiera sellado su propio ARC fabricado, el sello mostraría fielmente que AOG creó *este* documento en *este* instante —pero no diría que el tornillo es realmente nuevo de Safran y no uno recuperado o falsificado. Una foto de kilometraje sellada indica que el cuadro mostraba *este* número en captura, no que nunca se hubiera revertido antes. El sello no hace una inspección física, ni un ensayo metalúrgico, ni una auditoría *back-to-birth*, ni valida que la organización emisora tuviera realmente la aprobación que afirma tener. Es una capa de integridad y procedencia que hace **detectable** la manipulación retroactiva y **trazable** la responsabilidad; nunca sustituye la inspección acreditada, la autenticación del OEM, la supervisión reguladora ni el juicio de ingeniería humano.

La promesa y el peligro

La promesa es cerrar el agujero exacto que AOG explotó: hacer que **falsificar un certificado o inventar un firmante** deje una huella detectable, y convertir el pedigrí de una pieza —o el historial de un coche— en algo que cualquiera puede verificar sin confiar en la palabra del vendedor. En una cadena donde un álabe de turbina pasa de mano en mano sin ningún recibo inalterable, el anclaje del origen protege tanto al comprador honesto como al pasajero.

El peligro pide los matices de siempre. El primero: la **falsa confianza** —«está sellado, luego la pieza es buena»—, cuando el sello solo garantiza el documento, no el metal; un *.asice* impecable encima de un tornillo falsificado es más peligroso que ningún papel, porque inspira confianza. El segundo: la **concentración**, si solo los grandes OEM y MRO pueden sellar y los talleres pequeños quedan excluidos del mercado por no poder hacerlo. El tercero: la dependencia de la **captura honesta en el origen** —si el primero que rellena el Form 1 miente, el sello perpetúa la mentira con fecha cierta. La prueba de existencia es una capa de gobernanza del pedigrí, no un certificado de bondad de la pieza.

Es hora de actuar

Para los OEM y la industria del motor (GE Aerospace, Safran, CFM, Airbus, Boeing): sellar el formulario 8130-3 a la emisión, de manera que cualquier copia retocada posteriormente falle la comprobación de huella. Para los MRO y las CAMO: verificar la huella sellada al recibir la mercancía antes del montaje y exigirla como requisito de compra. Para los reguladores (FAA, EASA, CAA): reconocer el pedigrí sellado como evidencia dentro del SUP Program y tratar la fecha cierta como diferencia entre un certificado y una coartada posterior.

Para la coalición de integridad de la cadena: hacer del sello anclado el estándar técnico recomendado para «digitalizar documentos y firmas». Y para los reguladores del automóvil y los registros de kilometraje (NHTSA, Car-Pass, el futuro registro de la UE): sellar cada lectura del cuentakilómetros en la inspección, para que cualquier reversión deje un vacío detectable.

Como hemos visto, Zamora Yrala vendió sesenta mil piezas con papeles falsos desde un despacho en casa; solo cuando un responsable de Safran comprobó el certificado se detectó el fraude. Asignar a cada pieza crítica un pedigrí que ningún falsificador pueda reescribir sin dejar rastro —sin olvidar nunca que el sello no inspecciona el metal— es, en este frente donde un documento falso puede matar, time2act.

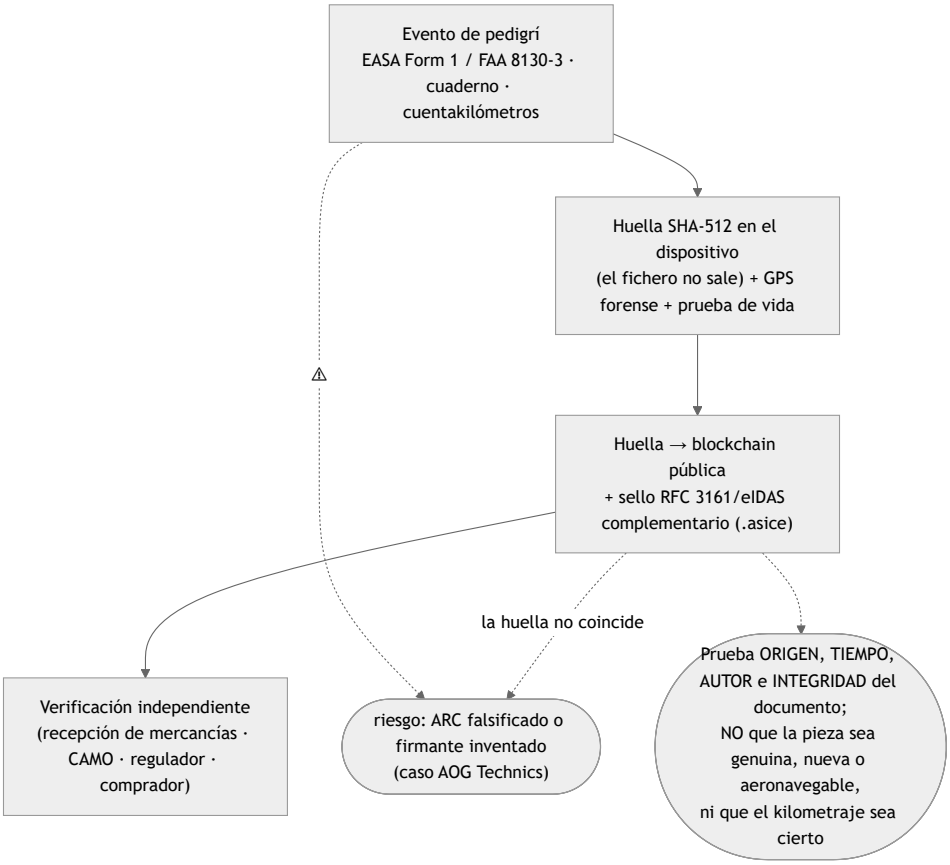


Figura 95.1 — Un evento de mantenimiento crea un registro (EASA Form 1 / FAA 8130-3, entrada de cuaderno, lectura de cuentakilómetros). El técnico calcula su huella SHA-512 en el dispositivo (el fichero no sale), le añade GPS forense y prueba de vida si hay captura de campo, y la huella del conjunto se ancla en la blockchain pública, con sello RFC 3161/eIDAS complementario (.asice). Cualquier parte posterior —recepción de mercancías, CAMO, regulador, comprador— verifica de manera independiente quién lo declaró y cuándo. Límite: el sello prueba el origen, el tiempo, el autor y la integridad del documento; no prueba que la pieza sea genuina, nueva o aeronavegable, ni que el kilometraje sea cierto —basura a la entrada, basura en la cadena. Fuentes: caso AOG Technics (SFO); demanda de CFM International; estimaciones FAA de piezas no aprobadas; CARFAX y Parlamento Europeo sobre cuentakilómetros; Aviation Supply Chain Integrity Coalition.

---

[1] SFO (GOV.UK) — *SFO secures 4-year prison sentence for aircraft parts fraud* (Zamora Yrala; 60.000 piezas; fraude de 39,3 M£; ARC falsificados; condena de 4 años y 8 meses; descubrimiento por Safran). https://www.gov.uk/government/news/sfo-secures-4-year-prison-sentence-for-aircraft-parts-fraud ↩

[2] SFO (GOV.UK) — *SFO case page: AOG Technics Ltd* (página oficial de la causa de la Serious Fraud Office). https://www.gov.uk/sfo-cases/aog-technics-ltd ↩

[3] Fortune — *Fake components went into 68 jet engines on Boeing 737 and Airbus A320 planes, lawsuit says* (demanda de CFM International: 78 documentos falsificados, 52 referencias del CFM56, 68 motores, álabes de turbina). https://fortune.com/2023/09/08/fake-components-68-jet-engines-boeing-737-airbus-a320-planes-lawsuit/ ↩

[4] FAA — *Suspected Unapproved Parts (SUP) Program* (trazabilidad según 14 CFR Part 21/43, Form 8130-3, report con Form 8120-11). https://www.faa.gov/aircraft/safety/programs/sups ↩

[5] EASA — *Suspected Unapproved Parts* (base de datos y definiciones de la UE; casos de EASA Form 1 falsificados; marco de los SIB). https://www.easa.europa.eu/en/domains/aircraft-products/suspected-unapproved-parts ↩

[6] EASA — *Safety Information Bulletin SIB 2023-05* (boletín sobre las piezas sospechosas de AOG Technics y acciones de cuarentena/reemplazo recomendadas). https://ad.easa.europa.eu/blob/EASA_SIB_2023_05.pdf/SIB_2023-05_1 ↩

[7] GE Aerospace — *Coalition delivers report to help prevent future unapproved parts entering aviation* (Aviation Supply Chain Integrity Coalition: 13 recomendaciones, 9 de octubre de 2024; digitalizar 8130-3/Form 1; trazabilidad; acreditación de proveedores). https://www.geaerospace.com/news/press-releases/coalition-delivers-report-help-prevent-future-unapproved-parts-entering-aviation ↩

[8] Connector Supplier — *Counterfeit Components Ground Airlines* (~520.000 piezas falsificadas o no aprobadas llegan a los aviones cada año, ~2 % de 26 millones; mercado de más de 2.000 M$). https://connectorsupplier.com/counterfeit-components-

ground-airlines/

[9] PR Newswire / CARFAX — *Odometer rollbacks see dramatic jump of 14% to 2.45 million vehicles* (diciembre de 2025; 2,45 millones de vehículos sospechosos; +14 % interanual; ~3.300 $ de pérdida media). https://www.prnewswire.com/news-releases/carfax-odometer-rollbacks-see-dramatic-jump-of-14-to-2-45-million-vehicles-302643855.html

[10] Parlamento Europeo (EPRS STU 2018-615637) — *Odometer manipulation in motor vehicles in the EU* (manipulación en el 5-12 % de ventas domésticas y 30-50 % transfronterizas; daño de 5,6-9,6 mil millones de euros anuales). https://www.europarl.europa.eu/RegData/etudes/STUD/2018/615637/EPRS_STU(2018615637_EN.pdf

Emisiones: el sensor que mentía antes que el papel

«Cuando puedes medir aquello de lo que hablas y expresarlo en números, sabes algo de ello; cuando no lo puedes medir, tu conocimiento es exiguo e insatisfactorio.»

— Lord Kelvin, «Electrical Units of Measurement» (1883)

El 18 de septiembre de 2015, la **Agencia de Protección Ambiental** de Estados Unidos (EPA) emitió contra **Volkswagen** un aviso de violación de la *Clean Air Act*. Sus turismos diésel TDI llevaban un **«dispositivo de desactivación»** (*defeat device*): un software del control del motor que reconocía el banco de pruebas del laboratorio —el volante quieto, la velocidad, la duración— y solo entonces activaba a fondo el control de óxidos de nitrógeno; en la carretera lo rebajaba y emitía NOx hasta **40 veces** el límite legal. Había unos **11 millones de vehículos** en el mundo (unos 590.000 en EE. UU., años 2009-2016), y a mediados de 2020 el escándalo ya había costado a VW más de **33.300 millones de dólares** en multas, recompras y acuerdos, incluida una sanción penal de 2.800 millones y una civil de 1.450 millones [1][2]. El guion se repitió: en enero de 2024, el fabricante de motores **Cummins** aceptó una sanción civil de **1.675 millones de dólares** —la más alta jamás impuesta bajo la *Clean Air Act*— por software de desactivación no declarado en más de **630.000** pick-ups diésel RAM 2500/3500 de los años 2013-2019 [3]. El hilo común es crudo: el dato de cumplimiento en el que el regulador confiaba parecía verídico, pero había sido **fabricado en el momento de la captura**. No se falseó el papel después; se engañó al sensor o a la prueba.

Este capítulo no habla de créditos de carbono ni de certificados de ahorro energético —eso es cosa de los capítulos 21-23, donde el activo es un título negociable y el riesgo es el doble cómputo o la reducción fantasma. Aquí el activo es otra cosa: el **dato de emisiones del sensor y del cumplimiento**, y el riesgo es la **medición manipulada o trucada**. La pregunta es precisa: ¿cómo fijamos que *esta* lectura salió de *este* analizador, en *este* lugar e instante, sin que nadie la pueda «sesgar» entre el sensor y la hoja de cálculo? La respuesta toca el corazón de la tesis del libro: cuando el dato ambiental vale dinero y decide sanciones, su **integridad** deja de ser un detalle técnico y pasa a ser la batalla.

Cuando se engaña el banco de pruebas

El caso Volkswagen reveló una forma de engaño que no deja huella en el papel porque nace antes del documento. El software detectaba que el coche estaba en un ensayo homologado y activaba un modo limpio que nunca se usaba en la carretera; la lectura del laboratorio era **auténtica**: allí el vehículo emitía poco, pero no circulaba realmente. Así, el fraude perduró años: cada certificado era técnicamente correcto e internamente coherente, y ninguna auditoría de documentos lo habría encontrado, porque el documento no mentía; mentía la realidad que describía.

El caso Cummins, ocho años después, demuestra que no se trataba de una anomalía de una sola marca. Como hemos visto, más de 630.000 camiones llevaban un software no declarado, una sanción civil récord y un acuerdo total superior a los 2.000 millones de dólares, con más de 325 millones para remedios y una llamada a revisar como mínimo el 85 % de los vehículos afectados en tres años [3]. En Europa, el **Tribunal de Justicia de la UE** ha cerrado la puerta jurídica al truco «elegante»: en julio de 2022 dictaminó que el software de **«ventana térmica»** —que solo garantiza el control de NOx entre 15 y 33 °C — es, en principio, un dispositivo de desactivación ilegal; una sentencia anterior, de diciembre de 2020, ya había declarado ilícito el software que reconoce el ciclo de prueba [8]. El mensaje es claro: engañar la prueba es engañar la ley, aunque la hoja salga limpia.

Cuando se trafica el sensor que vigila la chimenea

El truco del banco de pruebas tiene un hermano industrial aún más directo: manipular el monitor continuo de emisiones que vigila una chimenea. **Berkshire Power Company** y **Power Plant Management Services** se declararon culpables de delitos graves contra la *Clean Air Act* por sesgar intencionadamente el **sistema de monitorización continua de emisiones (CEMS)** de la central y subdeclarar el NOx entre enero de 2009 y marzo de 2011, como ya se ha mencionado. La maniobra era de una franqueza quirúrgica: introducían un ajuste fraudulento de unos **0,5 ppm**, lo **retiraban antes** de que llegaran los auditores independientes y lo **volvían a poner** cuando se marchaban. BPC pagó una

multa penal de 2,75 millones de dólares; en marzo de 2017 las partes debían unos 7,25 millones en multas y sanciones [4]. No había ningún documento falso: el CEMS registraba y transmitía, fielmente y en tiempo real, una cifra fabricada. El fraude vivía en la **ventana ciega** entre dos auditorías.

El mismo agujero existe a escala planetaria con el metano. El *Global Methane Tracker 2024* de la **AIE** estima cerca de **120 Mt** de metano del sector de los combustibles fósiles en 2023; pero las cifras que las empresas de petróleo y gas reportan a la **UNFCCC** son un 50 % más bajas que la estimación de la AIE, y las que reportan al OGMP 2.0 implican unos 5 Mt —un **95 %** más bajas [5]. El satélite **MethaneSAT** (lanzado el 4 de marzo de 2024, comunicación perdida el 20 de junio de 2025) encontró emisiones de metano de petróleo y gas de EE. UU. **más de cuatro veces** superiores a las estimaciones de la EPA, con una tasa de pérdida agregada del 1,6 % en doce cuencas —ocho veces el objetivo del 0,2 % de la industria [6]. La distancia entre lo que se declara y lo que se mide desde el aire es, ella misma, la prueba del problema.

Lo que la ley ya exige

La respuesta reguladora se ha endurecido a ambos lados del Atlántico. La *Clean Air Act* de EE. UU. prohíbe los dispositivos de desactivación y tipifica como delito falsear, manipular o **inutilizar a sabiendas** cualquier método de monitorización exigido —es el gancho legal tanto del *Dieselgate* como de la manipulación de CEMS. La **norma final de metano de la EPA** (firmada el 2 de diciembre de 2023, publicada el 8 de marzo de 2024), dentro de las *New Source Performance Standards* 40 CFR Part 60 subpartes OOOOb y OOOOc, crea un **Programa de superemisores**: un «evento de superemisión» es una liberación de **100 kg de metano por hora** o más, detectada por terceros certificados por la EPA mediante satélite, avión/dron o sensores móviles terrestres; el operador ha de empezar a investigar en **5 días** e informar a la EPA en **15 días** [4][6]. Se espera que la norma evite **58 millones de toneladas** de metano entre 2024 y 2038 (una reducción del ~80 %).

En la Unión Europea, el **Reglamento (UE) 2024/1787** sobre la reducción de las emisiones de metano en el sector de la energía impone un **MRV** (medición, informe y verificación) a escala de fuente con **verificación independiente de terceros**, un mecanismo de alerta rápida de superemisores basado en datos de satélite, y obligaciones equivalentes para los importadores a partir de 2027 [10]. Y la aplicación ya muerde: el 11 de julio de 2024, EPA y el Departamento de Justicia anunciaron un acuerdo de **241,5 millones de dólares** con **Marathon Oil** por infracciones de la *Clean Air Act* en casi 90 instalaciones de la reserva de Fort Berthold (Dakota del Norte) —64,5 millones de sanción civil, la más alta jamás aplicada a una fuente fija— que recorta unas 110.000 toneladas de COV y metano [7]. Con el *Waste Emissions Charge* de la *Inflation Reduction Act*, cada tonelada de metano declarada tiene un precio. Cuando el dato vale dinero, el incentivo a maquillarlo crece.

Por qué la norma por sí sola no salva

Hay que decirlo sin rodeos, porque aquí el autoengaño sería caro. Una norma que exige un CEMS acreditado, un MRV verificado y un informe puntual no impide, por sí sola, que el número que llega a él sea mentira desde el origen. Como hemos visto, la *Clean Air Act* prohibía los dispositivos de desactivación mucho antes de 2015; Volkswagen los instaló igualmente, y el sistema de homologación, basado en confiar en la prueba de laboratorio, no los detectó durante años. El caso Berkshire muestra el agujero aún más desnudo: todo el régimen de CEMS funcionaba sobre el papel —el sensor transmitía, el regulador recibía— mientras el operador metía y sacaba el sesgo alrededor de las visitas. Lo que falla no es el umbral legal ni el deber de informar; es que entre el sensor y la hoja de cálculo hay una **cadena de custodia que nadie sella**, y un número se puede sesgar, retrodatar o sustituir sin dejar huella. Un informe de cumplimiento es un PDF; nada impide retocar el dato antes de que se convierta en PDF.

La prueba de existencia aplicada

Es aquí donde **t2p** aporta el eslabón que falta, sobre el artefacto que importa: el **registro crudo de la medición en el instante de la captura**, antes de que se pueda «sesgar», trucar con el ciclo de prueba o editar en silencio. El CEMS, el analizador de metano o su sistema de adquisición —y también la carga de sensores de un dron o de un avión— calcula en el mismo dispositivo la **huella SHA-512** de cada lectura o bloque de datos crudos; el fichero original nunca sale. Acto seguido obtiene un **sello de tiempo RFC 3161/eIDAS** y **ancla la huella a la blockchain pública**, dentro de un contenedor **.asice** verificable

fuera de línea. En los vuelos de campo, se añade **GPS forense** para que la lectura de la pluma quede ligada de manera probable a un lugar y un momento. Igual vale para una prueba de certificación de un motor o para una notificación de superemisor: el técnico o la ONG **sella la traza del ensayo** —o el fotograma de detección del satélite— en el momento de producirlo. Cuando el operador presente el informe regulador, el auditor puede verificar que las cifras entregadas **coinciden con la captura cruda sellada** y que nada se ha cambiado entre el sensor y la hoja —cerrando exactamente el agujero que Berkshire explotaba metiendo y sacando el sesgo alrededor de las auditorías. No sustituye nada de la pila existente —certificación EPA/CARB, QA acreditado del CEMS, el programa OOOOb/c y de superemisores, el MRV del Reglamento 2024/1787, los contrastes por satélite (MethaneSAT, AIE, Copernicus)—: le añade una **cadena de custodia a prueba de manipulación** del sensor a la presentación. Es el complemento, sobre el dato ambiental, de lo que los capítulos 13 y 15 proponen para la procedencia C2PA del contenido.

Ahora el límite, con toda la crudeza. «Basura a la entrada, basura en la cadena»: el sello prueba origen, tiempo, autor e integridad de un registro de medición —que esta lectura salió de este aparato, en este lugar e instante, y que no se ha alterado desde entonces. **No prueba que la lectura sea cierta** en el punto de captura. Un dispositivo de desactivación que engaña el banco (VW, Cummins) produce un resultado «limpio» genuinamente sellado y, a la vez, vacío de sentido; un CEMS sesgado físicamente registrará, fielmente y de manera verificable, números bajos fabricados. El sello no detecta que un sensor se ha falseado, que se ha quitado una sonda, que se ha introducido aire de dilución o que el motor ha entrado en modo de reconocimiento de prueba; ni sabe si una instalación **nunca muestreó** un componente que perdía. No cuantifica emisiones ni juzga el cumplimiento. Es, por tanto, inútil contra el fraude central del *Dieselgate* si no se combina con comprobaciones independientes del mundo real —medición en la carretera con equipos portátiles (PEMS), auditorías por sorpresa, calibración acreditada y contraste por satélite y avión— y no sustituye nunca el juicio del regulador, la aplicación ni la inspección humana.

La promesa y el peligro

La promesa es cerrar el vacío entre el sensor y la presentación: una **cadena de custodia inalterable y datada** que haga imposible sesgar un número en la ventana ciega entre dos auditorías, como hizo Berkshire, y que dé al auditor honesto y al regulador una prueba de que los números reportados son los que el sensor produjo. En un mundo donde la tonelada de metano declarada tiene un precio, hacer el origen del dato a prueba de manipulación protege tanto al operador honesto como al público.

El peligro pide los matices de siempre. El primero, no confundir **integridad con verdad**: una medición falsa y sellada sigue siendo falsa, y ahora, además, inmutable —el sello podría dar una falsa tranquilidad («está anclado, luego es bueno») que no se corresponde con nada, sobre todo ante el fraude que vive en el sensor, no en el papel. El segundo, la **captura del custodio**: si quien sella es la misma parte que controla el sensor manipulado, el sello solo certifica con más solemnidad un número falso; por eso la verificación independiente y el contraste externo son innegociables. Y el tercero, la **concentración y el coste**: el sello ha de fortalecer el MRV, no expulsar a los operadores pequeños ni a los observadores independientes. La prueba de existencia es una capa de cadena de custodia, no un certificado de bondad ambiental.

Es hora de actuar

Para los **operadores industriales y fabricantes de motores** (Volkswagen, Cummins, centrales térmicas, petróleo y gas): sellar la lectura cruda del CEMS y del analizador, y la traza de cada ensayo de certificación en el momento de la captura, para que nadie —ni ellos mismos— la pueda sesgar después.

Para los **reguladores** (EPA, CARB, autoridades europeas del Reglamento 2024/1787): exigir la presentación con captura sellada y contrastarla siempre con medición real —PEMS en la carretera, satélite en la chimenea—, porque ningún sello puede sustituir la inspección.

Para los **verificadores de terceros y las ONG** del Programa de superemisores: sellar con GPS forense el fotograma de detección en el momento del vuelo, para que la notificación de 100 kg/h, como ya se ha indicado, sea inatacable.

Para los **operadores de satélite y la comunidad científica** (MethaneSAT, AIE, Copernicus): mantener el contraste externo que ningún sello puede dar, porque la integridad del dato y su **plausibilidad** son dos comprobaciones diferentes. Y para los **legisladores**: reconocer la captura sellada como cadena de custodia válida, y recordar que cierra el agujero de Berkshire, no el de Volkswagen.

El 18 de septiembre de 2015, un regulador descubrió que durante años había confiado en una prueba que el coche sabía reconocer. Dar a cada lectura de emisiones una prueba sellada de su origen y de su instante —sin olvidar nunca que el sello no hace cierta una medición trucada en el sensor— es, en este frente donde el dato ambiental vale dinero y decide sanciones, **time2act**.

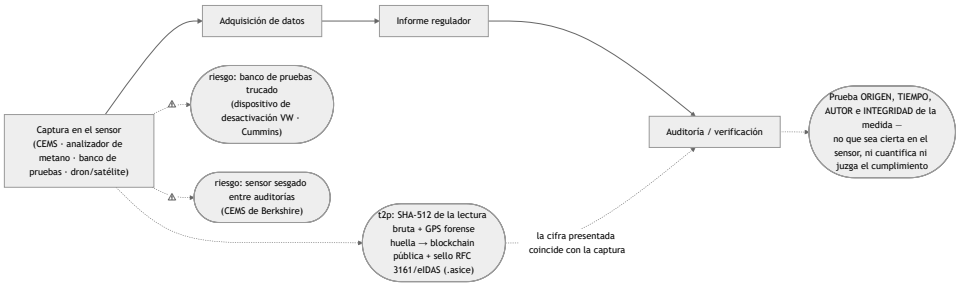


Figura 96.1 — La cadena de un dato de emisiones en cuatro eslabones: captura en el sensor (CEMS, analizador de metano, banco de pruebas, vuelo de dron/satélite) → adquisición → informe regulador → auditoría. t2p calcula en el dispositivo la huella SHA-512 de la lectura cruda, le añade sello de tiempo RFC 3161/eIDAS y, en campo, GPS forense, y la ancla a la blockchain pública (.asice); el auditor confronta la cifra presentada con la captura sellada. Dos puntos de riesgo: el banco de pruebas trucado (dispositivo de desactivación VW/Cummins) y el sensor sesgado alrededor de las auditorías (CEMS de Berkshire), que el sello NO detecta. Límite: el sello prueba origen, tiempo, autor e integridad de la medición; no prueba que la medición sea cierta en el punto de captura, ni cuantifica emisiones ni juzga el cumplimiento. Fuentes: EPA (VW, Cummins, Berkshire, Marathon, norma de metano); AIE; MethaneSAT; TJUE (ventana térmica).

---

[1] EPA — *Volkswagen Clean Air Act Civil Settlement* (acuerdos 2016-2017; sanción civil de 1.450 millones de dólares; fondo de mitigación; ~590.000 vehículos en EE. UU.; descripción del dispositivo de desactivación). https://www.epa.gov/enforcement/volkswagen-clean-air-act-civil-settlement ↩

[2] Wikipedia — *Volkswagen emissions scandal* (NOx hasta 40 veces el límite; ~11 millones de coches; ~33.000 millones de dólares de coste total; cronología global). https://en.wikipedia.org/wiki/Volkswagen_emissions_scandal ↩

[3] EPA — *United States and California Announce Diesel Engine Manufacturer Cummins Inc. Agrees to Pay Record $1.675 Billion Civil Penalty* (10 de enero de 2024; la sanción civil más alta bajo la Clean Air Act; 630.000+ camiones RAM; 325 M$ en remedios; condiciones de la revisión). https://www.epa.gov/newsreleases/united-states-and-california-announce-diesel-engine-manufacturer-cummins-inc-agrees ↩

[4] EPA — *Summary of Criminal Prosecutions: Berkshire Power* (sesgo intencionado del CEMS, 2009-2011; ajuste fraudulento retirado antes de las auditorías; multa penal de 2,75 M$ a BPC; ~7,25 M$ en total en marzo de 2017). https://cfpub.epa.gov/compliance/criminal_prosecution/index.cfm?action=3&prosecution_summary_id=2981 ↩

[5] AIE — *Global Methane Tracker 2024, Key Findings* (cerca de 120 Mt de metano fósil en 2023; UNFCCC ~50 % más bajo; OGMP 2.0 ~95 % más bajo; eventos de fuga por satélite +50 % interanual). https://www.iea.org/reports/global-methane-tracker-2024/key-findings ↩

[6] MethaneSAT (EDF) — *New Data Show US Oil and Gas Methane Emissions Over Four Times Higher Than EPA Estimates* (emisiones medidas >4 veces las estimaciones de la EPA; tasa de pérdida del 1,6 %, ocho veces el objetivo del 0,2 %; 30+ vuelos cubriendo ~70 % de la producción terrestre de EE. UU.). https://www.methanesat.org/project-updates/new-data-show-us-oil-and-gas-methane-emissions-over-four-times-higher-epa-estimates ↩

[7] EPA — *EPA and Justice Department Announce $241.5M Settlement with Marathon Oil* (11 de julio de 2024; 64,5 M$ de sanción civil, la más alta a una fuente fija; ~90 instalaciones; ~110.000 toneladas de COV/metano recortadas). https://www.epa.gov/newsreleases/epa-and-justice-department-announce-2415m-settlement-marathon-oil-reduce-climate-and ↩

[8] CJEU — *Press release on the July 2022 judgment that thermal-window defeat devices are in principle illegal* (PDF; definición legal del dispositivo de desactivación; sentencia previa de diciembre de 2020 sobre el reconocimiento del ciclo de prueba). https://curia.europa.eu/site/upload/docs/application/pdf/2022-07/cp220124en.pdf ↩

[9] EPA — *Key Things to Know About EPA's Final Methane Rule* (hoja informativa PDF; 58 millones de toneladas de metano evitadas 2024-2038; reducción del ~80 %; Programa de superemisores). https://www.epa.gov/system/files/documents/2023-12/key-things-to-know-about-epas-final-rule-for-oil-and-natural-gas-operations.fact-sheet.pdf

[10] Comisión Europea — *New EU Methane Regulation to reduce emissions from fossil fuels* (Reglamento (UE) 2024/1787; MRV a escala de fuente con verificación de terceros; alerta rápida de superemisores por satélite; equivalencia MRV para los importadores desde 2027). https://energy.ec.europa.eu/news/new-eu-methane-regulation-reduce-harmful-emissions-fossil-fuels-europe-and-abroad-2024-05-27_en ↩

Ciencia ciudadana ambiental: los sensores de abajo, con fecha cierta

«La obligación de soportarlo nos da el derecho de saber.»

— Jean Rostand, citado por Rachel Carson en Primavera silenciosa (1962)

Doñana, uno de los humedales más valiosos de Europa, se encogía en silencio mientras a su alrededor los invernaderos de fresas chupaban el acuífero con pozos, balsas y tuberías kilométricas que ningún registro oficial contaba. Las quejas a Bruselas se remontaban a 2009; el 24 de junio de 2021, el Tribunal de Justicia de la Unión Europea condenó a España por haber incumplido sus obligaciones: el Plan Hidrológico 2015-2021 no computaba las extracciones ilegales y no había medidas para evitar el deterioro de los hábitats protegidos [1]. La frase que lo resume hace daño: aquello que la administración no mide, jurídicamente no existe —aunque se esté bebiendo un parque nacional.

El capítulo 96 trató el sensor industrial vigilado desde arriba: la chimenea, el medidor oficial, el fraude del sensor que miente. Este capítulo mira en la dirección contraria: los sensores de abajo, los de la ciudadanía —el aparato de calidad del aire en el balcón, la foto del vertido, el diario del ruido, el ojo del voluntario sobre el acuífero. El testigo orbital está en el capítulo 104; la integridad del dato científico, en el capítulo 63. Pregunta clave: ¿cómo puede el dato de un ciudadano pesar lo suficiente para mover una inspección, un expediente o una sentencia? Respuesta: no pretendiendo ser lo que no es —un acta oficial—, sino siendo aquello que nadie más puede ser: una cronología densa, local y persistente, con fecha cierta e integridad inatacable gracias a **t2p** —la huella SHA-512 calculada en el origen, el anclaje de la huella en la blockchain pública y el sello de tiempo RFC 3161/eIDAS complementario, dentro de un contenedor .asice [5].

Lo que no se mide no existe

Vale la pena desgranar la paradoja de Doñana, porque es el patrón de todo el capítulo. La sentencia europea no castiga una contaminación: castiga un vacío de datos. El Estado no computaba las extracciones ilegales —la infraestructura de pozos y tuberías que drenaba el agua subterránea para regar fresas en invernaderos levantados sobre deforestaciones sistemáticas— y, al no computarlas, tampoco podía derivar medidas de protección [1]. Las entidades y la ciudadanía lo denunciaban desde 2009; hicieron falta doce años para que la justicia europea dijera lo que el territorio ya sabía [1].

La lección es estructural: la protección ambiental es, antes que nada, una cuestión de datos. Y cuando la administración no mide —por falta de medios, de voluntad o por captura de intereses—, el vacío solo lo puede llenar la ciudadanía organizada: plataformas vecinales, entidades de defensa del territorio, voluntariado científico. Pero este llenado choca siempre con el mismo muro: «¿y cómo sabemos que tus datos son de verdad?». La foto sin metadatos fiables, la hoja de cálculo del voluntario, la serie del sensor casero —todo es técnicamente impugnable, y quien contamina tiene abogados para impugnarlo.

La respuesta no es renunciar al dato ciudadano: es blindar lo que sí se puede blindar —cuándo se tomó, dónde, y que nadie lo ha tocado después [5]. La calidad metrológica se defiende con calibraciones y método; la integridad y la fecha, con criptografía. Separar estos dos planos —y no confundirlos nunca— es todo el secreto de este capítulo.

La laguna que se convirtió en persona

El Mar Menor cambió el marco entero. Después de décadas de degradación, una iniciativa legislativa popular reunió 639.826 firmas, y el resultado fue la Ley 19/2022, de 30 de septiembre: el reconocimiento de personalidad jurídica a la laguna y su cuenca —el primer ecosistema de Europa que se convierte en sujeto de derechos, con derecho a existir y evolucionar naturalmente, a la protección, la conservación y la restauración [2]. El Tribunal Constitucional confirmó su constitucionalidad, y el Real Decreto 90/2025 reguló su gobernanza: un comité de representantes de trece miembros, siete de ellos de la sociedad civil —inicialmente, del mismo grupo promotor de la iniciativa [2].

El significado para este libro va más allá del hito jurídico: la ciudadanía no solo vigiló el ecosistema —se convirtió en su voz legal. Y una persona jurídica, para defender sus derechos, necesita lo mismo que cualquier otra: pruebas. Quien hable por la laguna ante un tribunal tendrá que acreditar el estado del

agua, el episodio concreto, el vertido, la cronología del deterioro o de la recuperación. La ciencia ciudadana pasa del activismo al testimonio procesal —y un testigo necesita memoria infalible.

Aquí es donde la prueba de existencia cierra el círculo: cada muestra documentada, cada fotografía, cada serie de mediciones del voluntariado, con la huella SHA-512 generada en el origen, el sello de tiempo y el anclaje a la blockchain pública [5]. La personalidad jurídica da la legitimación; la prueba de existencia, la credibilidad. La una sin la otra es un derecho sin músculo, o un músculo sin derecho.

La red de los sensores de bajo coste

El músculo global de la ciencia ciudadana ya existe. Sensor.Community —nacida como luftdaten.info— es una red de sensores de calidad del aire montados por ciudadanos, con datos en tiempo real y presencia en más de 100 países [3]; en el ámbito hispanohablante, redes como AireCiudadano ofrecen monitores de partículas con mapa y API abiertos, y proyectos como CanAirIO miden PM2,5 con hardware abierto y un teléfono móvil [3].

La fuerza de estas redes es la que ninguna red oficial puede tener: densidad y proximidad. Un sensor en cada balcón, al lado de la escuela, delante de la fábrica —una malla tan fina que captura las variaciones locales que las grandes estaciones de referencia, por fuerza, promedian. Y un coste marginal casi cero, que convierte el mantenimiento en un acto colectivo.

La debilidad es doble, y hay que decirla sin rodeos. Primera, la calidad metrológica: un sensor de bajo coste no es una estación de referencia —deriva, se ensucia, le afecta la humedad. Segunda, la cadena de custodia: ¿quién garantiza que la serie no se ha retocado, que la fecha es la que dice, que el sensor estaba donde dice?

La división del trabajo correcta ataca cada debilidad con su arma. La primera se combate con método: calibraciones cruzadas con estaciones oficiales, protocolos documentados, transparencia del hardware [3]. La segunda, con prueba de existencia: cada lote de lecturas anclado en origen —huella, fecha cierta—, de manera que el retoque a posteriori se vuelve imposible y los vacíos de la serie quedan igualmente datados [5]. Un sensor humilde con la serie blindada vale más, ante un técnico o un juez, que un sensor excelente con una hoja de cálculo editable: la certeza del quién, qué y cuándo pesa tanto como la precisión.

El ruido: la prueba a dos voces

El caso de uso más cotidiano es también el más incomprendido. Cuando se denuncia un exceso de ruido, el ayuntamiento ha de hacer visita de inspección, y la medición la hacen técnicos municipales o la policía local con un sonómetro homologado y calibrado, levantando un acta con presunción de veracidad y pleno valor probatorio —fecha, hora, identidad del infractor, tipo de ruido y medición [4]. El dictamen de un perito acústico con equipamiento homologado es prueba contundente en el litigio [4]; los límites orientativos en interiores rondan los 35-45 decibelios de día y los 25-30 de noche [4]; y el Defensor del Pueblo ha tenido que recordar a las administraciones que habiliten medios para comprobar las denuncias [4].

El agujero del sistema es estructural: el ruido es intermitente y la inspección es puntual. El local que pincha música hasta la madrugada calla la noche que viene el técnico; la máquina que vibra cada madrugada descansa el día de la visita. El vecino que lo sufre tiene la información que el acta no puede capturar —la recurrencia— pero su grabación con el móvil no es un acta, ni lo será nunca.

La división del trabajo, otra vez: el ciudadano no sustituye el sonómetro oficial; aporta la cronología que lo hace llegar a tiempo. Un diario del ruido sellado —registros datados noche tras noche, con huella e integridad acreditadas [5]— no prueba decibelios, pero prueba persistencia: fechas, horas, duraciones, un patrón que ninguna inspección puntual puede negar y que permite programar la visita oficial cuando toca. La medición oficial hace la foto; el diario sellado hace la película. Y un expediente necesita las dos cosas.

La prueba de existencia aplicada

Un balcón, un sensor de treinta euros y una serie de datos que ningún abogado puede borrar.

1. La serie que nadie puede retocar

El sensor ciudadano de calidad del aire ancla cada lote de lecturas en origen: huella SHA-512, sello de tiempo, blockchain pública [5]. Cuando la plataforma vecinal presenta tres años de datos ante el ayuntamiento o el juzgado, la discusión sobre «datos retocados» se acaba antes de empezar: la serie es exactamente la que era, con sus vacíos datados incluidos. La crítica legítima queda circunscrita donde toca —la calibración, el método [3]—, que es exactamente la discusión que la ciencia ciudadana puede ganar con transparencia. Es el contrapeso del capítulo 96: allí, el sensor de la chimenea vigilado por el regulador; aquí, la ciudadanía que vigila al vigilante.

2. El vertido fotografiado

El purín en el torrente, el humo negro de madrugada, los escombros en el descampado: la denuncia ambiental vive o muere según la calidad de su rastro. Una serie de fotografías selladas al momento —huella, fecha cierta, ubicación— construye la progresión: no una imagen suelta que «podría ser de cualquier día», sino una cronología con integridad acreditada que la autoridad ambiental puede verificar antes de abrir expediente [5]. Y el mismo escudo protege al denunciado honesto: contra la foto vieja reciclada en una campaña de descrédito, la ausencia de sello coetáneo habla sola.

3. El diario del ruido

El vecino que sufre la máquina de cada madrugada registra, noche tras noche, el episodio: fecha, hora, duración, una grabación orientativa —todo sellado en su dispositivo [5]. Al cabo de tres meses, presenta al ayuntamiento una cronología con integridad acreditada que convierte su palabra en patrón verificable, y la inspección con sonómetro homologado —la única que levanta acta con valor probatorio [4]— se programa cuando el patrón dice que ocurrirá, no cuando el local lo espera. El diario sellado no mide decibelios: hace que la medición oficial llegue a la hora de la verdad.

4. La voz de la laguna

Los guardianes del Mar Menor —la sociedad civil que se sienta en el comité de representantes del ecosistema-persona [2]— pueden dar memoria criptográfica a su seguimiento: muestras de agua documentadas, episodios fotografiados, series de sensores comunitarios [3][5]. Cuando haya que defender ante un tribunal el derecho de la laguna «a existir y evolucionar naturalmente» [2], su voz legal llevará cronologías verificables, no recuerdos militantes. Y la misma lógica vale para Doñana: la cronología ciudadana de extracciones y secados, sellada año tras año, es el contrapeso permanente de aquel plan hidrológico que «no computaba» [1].

Los límites, con honestidad: el sello acredita cuándo y qué se registró, no que el sensor midiera bien —la calibración y el método siguen siendo la batalla científica [3]; el dato ciudadano no es un acta oficial ni un dictamen pericial, y no ha de pretender serlo [4]; y la vigilancia ambiental tiene una frontera ética: se documentan hechos, instalaciones y episodios —nunca la vida de los vecinos. Sin método, el sello blinda ruido; sin ética, blinda un asedio.

La promesa y el peligro

La promesa es una ciudadanía que ya no depende de que la administración quiera medir [1]: series de sensores blindadas [5], ecosistemas con voz legal y memoria [2], inspecciones oficiales que llegan a la hora [4] y expedientes que aguantan. La vigilancia ambiental democrática: medir, certificar, actuar.

Los peligros piden la misma claridad.

El primero es **el vecindario-policía**. La línea entre documentar la contaminación y vigilar a las personas es fina. La cámara apunta a la chimenea, no a la cocina del vecino; al torrente, no al paseo de quien va por él. Se documentan hechos ambientales; los rostros, las matrículas y las vidas ajenas no tienen lugar, y el diseño de solo-huellas no legitima ninguna difusión [5].

El segundo es **la falsa equivalencia**. Sellado no quiere decir exacto. Un dato mal calibrado con fecha cierta sigue siendo un dato malo —más peligroso todavía, porque parece sólido. Si la ciencia ciudadana vende el sello como certificado de calidad, perderá la credibilidad que busca: el sello acredita integridad y momento; la exactitud la acreditan la calibración y el método [3].

El tercero es **la instrumentalización**. También un interés industrial o político puede disfrazarse de «plataforma vecinal» e inundar el expediente de cronologías selladas sesgadas. El antídoto no es

criptográfico sino metodológico: transparencia sobre quién mide, con qué, cómo y con qué protocolo. El sello garantiza que nadie ha retocado los datos —no que los hayan recogido de buena fe.

Y el cuarto es **la excusa administrativa**. Si el dato ciudadano sirve para que la administración se desentienda —«ya miden los vecinos»—, habremos perdido. El TJUE condenó a España porque el Estado no computaba [1], y el Defensor del Pueblo reclama medios para inspeccionar [4]: la ciencia ciudadana es contrapeso y complemento del deber público de medir, nunca su sustituto.

Es hora de actuar

La naturaleza no puede declarar; quien la vigila, sí —si lleva las fechas a prueba de duda.

Para la ciudadanía y las entidades ambientales: montad sensores con protocolos documentados [3], sellad las series y las fotografías en origen [5], y pensad en cronologías largas —la persistencia es vuestra fuerza.

Para los ayuntamientos: abrid canales para recibir cronologías ciudadanas selladas y programad la inspección oficial —el acta con sonómetro homologado [4]— cuando el patrón lo indique; el Defensor del Pueblo ya os lo recuerda [4].

Para las confederaciones y agencias ambientales: computadlo todo —la lección de Doñana es que el vacío de datos se paga en Luxemburgo [1]— y tratad la serie ciudadana anclada como lo que es: un indicio cualificado que merece comprobación.

Para las plataformas de ciencia ciudadana: incorporad el anclaje por defecto [3][5]: es la diferencia entre un mapa bonito y un expediente que aguanta.

Para los guardianes de ecosistemas con derechos: dad memoria criptográfica a la voz del Mar Menor [2] —cada muestra y cada episodio, con fecha cierta.

Para los legisladores: reconoced la cronología ciudadana sellada como base suficiente para activar inspecciones, y financiad la red pública de medición —que el contrapeso no tenga que hacer de titular.

Doñana tardó doce años en tener sentencia porque las extracciones «no se computaban» [1]; el Mar Menor necesitó 639.826 firmas para tener voz [2]. Que la próxima laguna no tenga que esperar tanto: dadle testigos con fecha cierta. Por la tierra que no puede declarar, **time2act**.

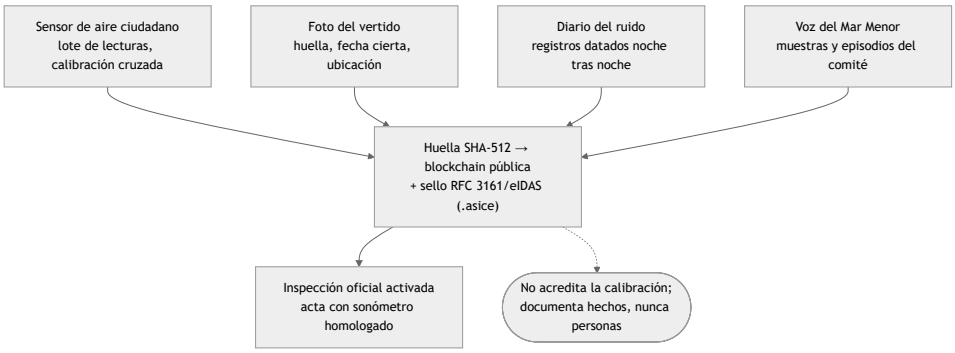


Figura 97.1 — La ciencia ciudadana con prueba de existencia: el sensor del balcón, la foto del vertido y el diario del ruido se anclan en origen (huella SHA-512, sello de tiempo RFC 3161/eIDAS, blockchain pública, .asice) y se convierten en cronologías con integridad acreditada que activan la inspección oficial (acta con sonómetro homologado, con presunción de veracidad), orientan al perito y dan memoria a la voz legal de los ecosistemas (Mar Menor, Ley 19/2022). Límites: el sello no acredita la calibración ni sustituye el acta oficial; se documentan hechos, no personas. Fuentes: TJUE (Doñana, 2021); BOE (Ley 19/2022); Sensor.Community; Defensor del Pueblo.

[1] El Ágora Diario — *Europa condena a España por no proteger el agua y hábitats de Doñana* (sentencia del TJUE de 24 de junio de 2021; extracciones ilegales no computadas en el Plan Hidrológico 2015-2021; quejas desde 2009); Greenpeace — *Doñana, agua sin ley* (pozos, balsas y tuberías; invernaderos de fresas; deforestaciones). https://www.elagoradiario.com/agua/tribunal-justicia-europa-condena-espana-agua-donana/ · https://es.greenpeace.org/es/en-profundidad/sos-acuiferos/donana-agua-sin-ley/ ↩

[2] BOE — *Ley 19/2022, de 30 de septiembre, para el reconocimiento de personalidad jurídica a la laguna del Mar Menor y su cuenca* (primer ecosistema de Europa; derechos a existir, evolucionar, protección, conservación y restauración; ILP con 639.826 firmas); Araoz & Rueda — *El TC reconoce la personalidad jurídica del Mar Menor*; BOE — *Real Decreto 90/2025* (comité de representantes: 13 miembros, 7 de la sociedad civil); Newtral — *Qué significa que el Mar Menor haya adquirido personalidad*

jurídica. https://www.boe.es/buscar/doc.php?id=BOE-A-2022-16019 · https://www.araozyrueda.com/el-tribunal-constitucional-reconoce-mar-menor-sujeto-de-derechos/ · https://www.boe.es/diario_boe/txt.php?id=BOE-A-2025-2577 · https://www.newtral.es/mar-menor-personalidad-juridica/20220923/ ↩

[3] Sensor.Community / World Air Quality Index — *Red de sensores de calidad del aire en tiempo real (antes luftdaten.info)* (más de 100 países; sensores ciudadanos de bajo coste); AireCiudadano — red abierta de monitores de partículas con mapa y API; SciStarter/CanAirIO — sensores abiertos de PM2,5. https://aqicn.org/network/luftdaten/es/ · https://aireciudadano.com/ · https://scistarter.org/crea-tu-propio-sensor-de-calidad-del-aire-con-cana ↩

[4] Perito Judicial — *Ruidos molestos y su reclamación: la clave está en la medición* (inspección municipal con sonómetro homologado y calibrado; actas con presunción de veracidad y pleno valor probatorio; límites interiores orientativos 35-45 dB día / 25-30 dB noche); COITTA — *La importancia de la prueba pericial acústica*; Defensor del Pueblo — *Comprobaciones ante las denuncias de ruidos molestos* (habilitar medios para comprobar las denuncias). https://peritojudicial.com/ruidos-molestos/ · https://www.aagit.org/la-importancia-de-la-prueba-pericial-acustica-y-la-proteccion-juridica-frente-al-ruido-como-agente-contaminante/ · https://www.defensordelpueblo.es/resoluciones/habilitar-los-medios-para-poder-realizar-comprobaciones-necesarias-cuando-se-denuncien-ruidos-molestos/ ↩

[5] t2p — manual de producto (huella SHA-512 en el origen —sensor o dispositivo—; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; series por lotes en tiempo real; vacíos datados; contenido en el dispositivo y revelación voluntaria). Véanse los capítulos 13 y 15; el sensor industrial, en el capítulo 96; el testigo orbital, en el capítulo 104. ↩

El pasaporte del producto: quién jura el contenido reciclado, y cuándo

«Si los nombres no son correctos, el lenguaje no concuerda con la verdad de las cosas.»

— Confucio, Analectas, XIII, 3

El 4 de junio de 2024, **Volvo Cars** presentó en su nuevo SUV eléctrico **EX90** lo que la marca y su socio **Circulor** llamaron «el primer pasaporte de batería del mundo», casi tres años antes de que el mandato europeo lo hiciera obligatorio. Construido durante cinco años con la empresa británica de cadena de bloques Circulor, a un coste aproximado de **10 dólares por vehículo** para quince años de seguimiento, el pasaporte permite al propietario escanear un **código QR** en el montante de la puerta del conductor —o abrir la aplicación de Volvo— y ver la química de la batería, el origen y el recorrido de producción de su cobalto, níquel, iones de litio y grafito, el **porcentaje de contenido reciclado** y la **huella de carbono** incorporada de todo el paquete. Circulor afirma haber recogido ya más de **20.000 millones de puntos de trazabilidad** a través de **150 millones de celdas**, trabajando con proveedores que representan aproximadamente el **52 % de la producción mundial** de celdas [5][6]. El caso es vívido precisamente porque expone la tensión de fondo del pasaporte digital de producto: el documento registra y data fielmente todo lo que la cadena de suministro declara, pero el linaje de prueba de concepto del propio EX90 —el piloto de la Global Battery Alliance de 2023 con Audi y Tesla— admitía abiertamente que «la calidad de los datos presentados no ha sido plenamente verificada y se ha complementado parcialmente con estimaciones razonables» [7]. Un pasaporte bellamente estructurado puede, pues, transportar una declaración de contenido reciclado inflada o sin verificar. Es exactamente el riesgo de *greenwashing* que el propio barrido de la UE de 2020 cuantificó: cerca del **42 % de las afirmaciones verdes** de las empresas europeas eran falsas o engañosas.

Este capítulo trata el **pasaporte de ciclo de vida de un objeto físico concreto** a lo largo de toda su vida, distinto del capítulo 29 —la cadena de suministro, que es la custodia y la procedencia de los inputs mientras las mercancías pasan de un actor a otro. Aquí el sujeto no es el flujo de materiales, sino **una sola batería**: su porcentaje de contenido reciclado, los datos de reparabilidad y desmontaje, el **estado de salud** en uso y el estatus de **segunda vida** y fin de vida —afirmaciones que persisten y se actualizan *después* de que el producto se ha vendido. La pregunta no es si se puede construir un pasaporte bonito —Volvo ya ha construido uno—, sino cómo hacer que cada cifra que contiene sea **demostrable** y no solo declarada.

El documento fiel a un dato que nadie ha comprobado

Un pasaporte digital es, en esencia, un contenedor de declaraciones: estructurado, legible por máquina y accesible con un QR. Su virtud —recogerlo todo en un solo lugar verificable— es también su talón de Aquiles, porque el documento es exactamente tan bueno como los datos que entran en él. El piloto de la **Global Battery Alliance**, presentado en Davos el 18 de enero de 2023 con Audi, BASF, CATL, Glencore, Tesla y Volkswagen, lo dijo con una franqueza rara: los datos «no han sido plenamente verificados» y se «complementaron parcialmente con estimaciones razonables» [7]. Esa frase, enterrada en una nota de prensa triunfal, es la clave del capítulo. El pasaporte no fabrica verdad; transporta lo que se le da.

Y lo que se le da son **cifras falsificables con consecuencias legales**. Desde el 18 de agosto de 2031, el Reglamento europeo de baterías impone umbrales mínimos de contenido reciclado —**cobalto 16 %**, **plomo 85 %**, **litio 6 %**, **níquel 6 %**—, que en un segundo escalón a partir de 2036 suben a **cobalto 26 %**, **litio 12 %**, **níquel 15 %** [2]. Son porcentajes precisos que el pasaporte ha de declarar, y cada uno es una tentación: un punto porcentual de cobalto reciclado «de más» abarata el cumplimiento y mejora la imagen. El cobalto virgen reetiquetado como reciclado en la fundición no deja ninguna huella visible en el documento; el pasaporte, dócil, lo registra como reciclado. Esta es la diferencia entre un sistema que **estructura** la información y uno que la **prueba**.

El estado de salud que sobrevive a la venta

Hay una segunda familia de declaraciones que hace el pasaporte de producto radicalmente diferente de la simple trazabilidad de la cadena: las que **se actualizan mientras el objeto vive**. Circulor anuncia quince años de **monitorización del estado de salud** (*state of health*) de la batería del EX90 [6]. Esta

cifra —la capacidad que conserva el paquete respecto de su valor nuevo— determinará el precio de un EX90 de segunda mano en 2032, si una batería es apta para una **segunda vida** como almacenamiento estacionario o si ha de ir al reciclaje. Es una afirmación que vive y cambia después de la venta, y su valor económico es inmenso.

Justamente por eso es manipulable. El estado de salud sale del sistema de gestión de la batería (el BMS); una exportación de diagnóstico es un fichero, y un fichero se puede retocar. Un vendedor sin escrúpulos tiene todos los incentivos para maquillar la capacidad de una batería gastada antes de revender el coche; un operador de segunda vida, para declarar apta una celda que no lo es. El pasaporte, de nuevo, registrará obedientemente la cifra que se le entregue. La promesa de un mercado de segunda mano y de segunda vida transparente —una de las grandes ganancias ambientales de toda la economía circular— depende de que estas lecturas sean **auténticas**, no solo **presentes** en el documento.

El marco regulador: el pasaporte como ley, no como favor

Europa ha convertido el pasaporte en obligación, no en gesto voluntario. El **Reglamento (UE) 2023/1542** de baterías, que deroga la directiva de 2006 y se aplica desde el 18 de febrero de 2024, hace **obligatorio el pasaporte de batería a partir del 18 de febrero de 2027** para toda batería de vehículo eléctrico, toda batería industrial de más de 2 kWh y toda batería de medios de transporte ligeros (LMT) colocada en el mercado europeo, accesible vía QR enlazado a un identificador único; las baterías puestas en el mercado después de esta fecha sin pasaporte registrado **no se pueden vender legalmente**, y las autoridades aduaneras reciben acceso directo al registro en la frontera [1][3]. La **declaración de huella de carbono** ya empezó para las baterías de vehículo eléctrico el 18 de febrero de 2025 y se extiende a las industriales de más de 2 kWh el 18 de febrero de 2026; sigue el método ISO 14040/44 y la PEF europea y **la ha de verificar un organismo notificado —no se puede autocertificar** [3].

Por encima, el **Reglamento de ecodiseño de productos sostenibles (UE) 2024/1781** (ESPR), en vigor desde el 18 de julio de 2024, eleva el pasaporte digital de producto a **herramienta horizontal** que se extenderá a textiles, hierro y acero, aluminio, mobiliario y neumáticos según el plan de trabajo 2025-2030, como hemos visto, adoptado el 16 de abril de 2025; la batería es su piloto legalmente vinculante [8]. El comité **CEN-CENELEC JTC 24** desarrolla los estándares horizontales (identificadores únicos, portadores de datos, enlace físico-digital, interoperabilidad, derechos de acceso), y los proyectos **CIRPASS / CIRPASS-2**, financiados por la Comisión, definen el modelo de datos transversal. Un detalle revela la prudencia del legislador: las obligaciones de **diligencia debida** de la cadena se aplazaron dos años, del 18 de agosto de 2025 al 18 de agosto de 2027, mediante el Reglamento (UE) 2025/1561, el ómnibus de «parar el reloj» [4]. La ley pide cifras precisas; todavía se está construyendo el sistema que las ha de hacer fiables.

Por qué el pasaporte por sí solo no salva

Hay que decirlo con crudeza. Un pasaporte digital de producto, por bien estructurado y lleno de QR que esté, **es tan fiable como la voluntad de quien vuelca los datos en él**. Un certificado de contenido reciclado colgado en el pasaporte es un PDF; nada impide que el porcentaje se haya inflado antes de entrar en él. Una exportación de estado de salud es un fichero; nada en el documento demuestra que refleje el paquete real y no una lectura del BMS retocada. Una declaración de huella de carbono puede seguir el método PEF al pie de la letra y a la vez alimentarse de datos de actividad falsos. Y la verificación del organismo notificado, aunque sea obligatoria para la huella de carbono, no se extiende a cada lectura de estado de salud ni a cada certificado de reciclado a lo largo de quince años de vida.

El pasaporte resuelve el problema de **tener** la información en un lugar accesible y estandarizado. No resuelve el problema de **acreditar** que la información era cierta y no se ha tocado. Falta una capa que fije, para cada artefacto probatorio subyacente —el certificado del reciclador, el informe del organismo notificado, la exportación del BMS—, **quién lo emitió, cuándo, y que no se ha alterado desde entonces**. Sin esta capa, el piloto de la GBA tenía razón: los datos del pasaporte a menudo están «estimados» y «no plenamente verificados», y el documento los bendice igualmente.

La prueba de existencia aplicada

Es aquí donde **t2p** aporta la pieza que falta, y lo hace sobre el **acto probatorio** detrás de cada afirmación, no sobre la entrada de la base de datos. En el momento en que un proveedor o un fabricante genera un artefacto primario —un certificado de lote del reciclador con el contenido de cobalto o iones de litio reciclado, un informe de verificación de huella de carbono de un organismo notificado, una exportación de diagnóstico de estado de salud del BMS al final de la primera vida, un acta de inspección de desmontaje o de segunda vida, o una foto de un lote de material en una mina o en una planta de triaje—, el dispositivo calcula localmente la **huella SHA-512** (el fichero **no sale nunca** del dispositivo), obtiene un **sello de tiempo RFC 3161 conforme a eIDAS**, la ancla a la cadena de bloques pública y la empaqueta en un contenedor **.asice** verificable fuera de línea. Para la captura de campo —una mina, una línea de reciclaje, una bahía de desguace— el **GPS forense** y una **prueba de vida** ligan el registro a un lugar real y a una persona real en un momento real.

El QR del pasaporte puede transportar, junto a la afirmación legible por humanos, un **enlace verificable** a aquel artefacto sellado. Cualquiera —un agente de aduanas en la frontera, el comprador de un EX90 usado que lee el estado de salud de segunda vida, un auditor que comprueba el umbral de contenido reciclado— puede confirmar **fuera de línea** que *este* certificado de reciclado o *esta* lectura de estado de salud existía, inalterado, en *esta* fecha y de *este* autor, antes de que se publicara la afirmación. Complementa la pila regulada —la verificación del organismo notificado del artículo 7, el libro de reglas de aseguramiento de datos de la GBA, los estándares de portadores de datos del JTC, la trazabilidad blockchain al estilo Circulor— dando a cada documento subyacente un rastro de procedencia a prueba de manipulación, sin sustituir nunca la verificación. Es, sobre el ciclo de vida del producto, el hermano de la marca C2PA y SynthID de los capítulos 13 y 15: aquellos sellan **lo que un modelo produce**; t2p sella **lo que un objeto ha vivido**.

Ahora el límite, con toda la crudeza. **«Basura a la entrada, basura en la cadena»**: el sello prueba el origen, el instante, el autor y la integridad de un artefacto de ciclo de vida; **no prueba que la afirmación que contiene sea cierta**. No confirma que el cobalto reciclado fuera realmente reciclado y no metal virgen reetiquetado en la fundición, ni que una exportación de estado de salud sellada refleje el paquete real y no un BMS manipulado, ni que un análisis de ciclo de vida usara datos de actividad honestos, ni que una batería de «segunda vida» sea realmente segura para redesplegar. Un certificado de contenido reciclado falsificado, una vez sellado, se convierte en un certificado falsificado **a prueba de manipulación**. t2p fija la procedencia y la inalterabilidad; no sustituye la evaluación de conformidad del organismo notificado, la auditoría de diligencia debida, el ensayo físico del material ni el juicio humano que deciden si el contenido sellado es legítimo.

La promesa y el peligro

La promesa es un mercado circular donde el linaje de un producto es verificable y no solo publicado: poder demostrar que este porcentaje de reciclado, esta huella de carbono y este estado de salud fueron declarados por este actor en aquella fecha, y que nadie los ha retocado desde entonces. Para el comprador de un EX90 usado, para el auditor —como hemos visto— y para el agente de aduanas, hacer el origen inalterable convierte una promesa de marketing en una afirmación con consecuencias.

El peligro pide los matices de siempre. El primero, no confundir integridad con verdad: un pasaporte lleno de artefactos bien sellados pero con datos inflados sigue siendo un pasaporte engañoso, ahora con una pátina de rigor tecnológico que puede adormecer al auditor —«está anclado, luego debe ser cierto»— cuando el sello no dice nada sobre la verdad del contenido. El segundo, la concentración: si sellar y pasaportar sale a cuenta solo a los grandes fabricantes —los 10 dólares por vehículo de Volvo escalan mal para un taller de reparación pequeño—, el estándar puede expulsar a los actores pequeños de la reparación y la segunda vida en lugar de fortalecerlos. Y el tercero, la privacidad y el secreto industrial: el pasaporte expone datos de la cadena que pueden ser sensibles, y hay que equilibrar la transparencia con el derecho legítimo a no revelarlo todo. La prueba de existencia es una capa de gobernanza del ciclo de vida, no un certificado de bondad ambiental.

Es hora de actuar

Para los **fabricantes y marcas** (Volvo, sus pares de la automoción y, pronto, los del textil y de la electrónica): sellar cada artefacto probatorio en el momento de generarlo —certificado de reciclado, informe de huella de carbono, lectura de estado de salud— y enlazarlo desde el QR del pasaporte, para que cada cifra tenga fecha cierta y autor. Para los **recicladores y organismos notificados**: sellar los

certificados de lote y los informes de verificación a la emisión, de manera que el auditor pueda confirmarlos fuera de línea sin depender de la buena fe del registro. Para los **reguladores y las autoridades aduaneras** (la Comisión bajo el ESPR, el JTC 24, las aduanas con acceso directo desde 2027): reconocer el artefacto sellado como evidencia de la procedencia que el pasaporte ya exige, y tratar la fecha cierta como la diferencia entre una declaración y una coartada fabricada posteriormente. Para los **proveedores de plataformas de pasaporte** (Circulor y sus competidores): anclar la huella de cada documento subyacente, no solo estructurar su contenido. Y para los **compradores y operadores de segunda vida**: exigir el enlace verificable al estado de salud sellado antes de pagar por una batería usada, para que la lectura sea auténtica y no solo presente.

En Gotemburgo, el 4 de junio de 2024, un coche salió de fábrica con el primer pasaporte de batería del mundo y una nota al pie que admitía que los datos no estaban «plenamente verificados». Dar a cada producto una prueba sellada de cada afirmación que hace a lo largo de su vida —sin olvidar nunca que el sello no hace verdadero el reciclado que alguien declara— es, en este frente donde un objeto ha de responder de lo que dice de sí mismo, time2act.

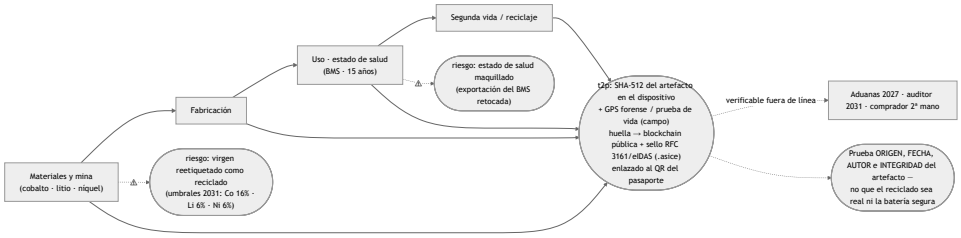


Figura 98.1 — El ciclo de vida de una batería en cuatro eslabones: materiales y mina → fabricación → uso y estado de salud → segunda vida / reciclaje. Cada eslabón genera un artefacto probatorio (certificado de reciclado, informe de huella de carbono del organismo notificado, exportación del BMS, acta de desmontaje); t2p calcula su huella SHA-512 en el dispositivo y la ancla en la blockchain pública, con sello RFC 3161/eIDAS complementario (.asice), con GPS forense y prueba de vida en captura de campo. El QR del pasaporte enlaza la afirmación con el artefacto sellado, verificable fuera de línea por aduanas, auditores y compradores de segunda mano. Límite: el sello prueba origen, fecha, autor e integridad del artefacto; no prueba que el contenido reciclado sea real, que el estado de salud no se haya maquillado ni que la batería sea segura. Fuentes: Volvo EX90 / Circulor; Global Battery Alliance; Reglamento (UE) 2023/1542; ESPR (UE) 2024/1781.

---

[1] EUR-Lex — *Sustainability rules for batteries and waste batteries (Regulation (EU) 2023/1542 summary)* (pasaporte desde 2027 vía QR e identificador único; objetivos de contenido reciclado desde el 18 de agosto de 2031: Co 16 %, Pb 85 %, Li 6 %, Ni 6 %; acceso aduanero al registro). https://eur-lex.europa.eu/EN/legal-content/summary/sustainability-rules-for-batteries-and-waste-batteries.html ↩

[2] DigiProdPass — *EU Battery Regulation: Recycled Content Targets (2031-2036)* (porcentajes de 2031 —Co 16/Pb 85/Li 6/Ni 6— y de 2036 —Co 26/Pb 85/Li 12/Ni 15—, las afirmaciones falsificables que el pasaporte transporta). https://digiprodpass.com/blogs/eu-battery-regulation-recycled-content-targets ↩

[3] Circularise — *EU battery passport regulation requirements* (calendario por fases: huella de carbono VE 18 feb 2025 / industrial 18 feb 2026; pasaporte 18 feb 2027; verificación por organismo notificado; ámbito VE/industrial >2 kWh/LMT). https://www.circularise.com/blogs/eu-battery-passport-regulation-requirements ↩

[4] Minespider — *EU Battery Due Diligence Obligations postponed* (diligencia debida aplazada del 18 ago 2025 al 18 ago 2027 vía Reglamento (UE) 2025/1561 «stop-the-clock»; guía ampliada hasta el 26 jul 2026). https://www.minespider.com/blog/eu-battery-due-diligence-postponed-what-it-means-for-companies ↩

[5] Electrek — *Volvo EX90 launches world's first EV battery passport* (4 jun 2024; cinco años de desarrollo con Circulor; ~10 $/vehículo por 15 años; QR en el montante de la puerta; traza materiales, contenido reciclado y huella de carbono). https://electrek.co/2024/06/04/volvo-ex90-launch-worlds-first-ev-battery-passport/ ↩

[6] IEEE Spectrum — *Volvo's Battery Passport Traces the Supply Chain* (más de 20.000 millones de puntos de datos en 150 millones de celdas; ~52 % de los fabricantes mundiales de celdas; 15 años de monitorización de estado de salud). https://spectrum.ieee.org/volvo-ex90-battery-passport ↩

[7] Global Battery Alliance — *World's First Battery Passport Proof of Concept* (Davos, 18 ene 2023; Audi/BASF/CATL/Glencore/Tesla/VW; los datos «no han sido plenamente verificados y se han complementado parcialmente con estimaciones razonables»). https://www.globalbattery.org/press-releases/global-battery-alliance-launches-world%E2%80%99s-first-battery-passport-proof-of-concept/ ↩

[8] Comisión Europea (Green Forum) — *Implementing the Ecodesign for Sustainable Products Regulation (ESPR)* (ESPR en vigor el 18 jul 2024; el pasaporte digital de producto como herramienta horizontal; plan de trabajo 2025-2030 adoptado el 16 abr 2025). https://green-forum.ec.europa.eu/implementing-ecodesign-sustainable-products-regulation_en ↩

[9] Hogan Lovells — *Digital Product Passports in the EU: expansion under ESPR and lessons from the Battery Passport pilot* (análisis jurídico que distingue el piloto de baterías del despliegue horizontal del ESPR; calendario de actos delegados). https://www.hoganlovells.com/en/publications/digital-product-passports-in-the-eu-comprehensive-expansion

[10] CIRPASS — *Standardisation gaps and roadmap (v1.2, July 2024)* (modelo de datos del DPP, identificadores únicos, portadores de datos y lagunas de estandarización del JTC 24 —la arquitectura donde se enchufa el sello). https://cirpassproject.eu/wp-content/uploads/2024/07/CIRPASS-standardisation-gaps-and-roadmap-V1.2.pdf

Residuos: adónde va de verdad el contenedor

«Adónde llevan cada día su carga los basureros, nadie se lo pregunta.»

— Italo Calvino, Las ciudades invisibles (1972), «Leonia»

Cada noche, en millones de cocinas, se repite la misma coreografía: enjuagar el bote de yogur, plegar la caja de cartón, y bajarlo todo —el amarillo de los envases, el azul del papel, el marrón de la orgánica. Es un gesto de confianza pura: ninguno de nosotros ha visto nunca qué pasa después. Confiamos en que aquel gesto tiene sentido, que el viaje acaba bien, que «se recicla» quiere decir que se recicla.

La pregunta de este capítulo es exactamente esa: ¿adónde va, de verdad, el contenedor? Y la urgencia no es retórica [1]: Europa exporta residuos a escala industrial —Turquía sola recibió el 39 % de las exportaciones europeas, 12,4 millones de toneladas en un año—, y la trayectoria de estos cargamentos ha sido lo bastante oscura como para que la Unión haya tenido que intervenir: el Reglamento (UE) 2024/1157 de traslados de residuos, aplicable de manera general desde el 21 de mayo de 2026, somete las exportaciones de todos los residuos plásticos a notificación y autorización previas por escrito, prohíbe exportar residuos para valorización a países de fuera de la OCDE e impone la tramitación electrónica de los traslados [1].

Entre tu contenedor y el «reciclado» final hay una cadena —recogida, transferencia, gestor, tratamiento, a menudo un camión o un barco— hecha de cambios de manos y papeles de parte. Cuando todo va bien, nadie lo mira; cuando no, lo descubrimos tarde: el «reciclaje» que era vertido, el certificado firmado sin tratamiento, la etiqueta verde sin nada debajo.

Este capítulo trata el acto de fe colectivo más grande de nuestro tiempo. El pasaporte del producto nuevo —su contenido reciclado, su segunda vida— está en el capítulo 98; las emisiones trucadas, en el capítulo 96; el origen de las mercancías, en el capítulo 29; la cadena de custodia del socorro —la misma lógica, invertida—, en el capítulo 50; la prueba ciudadana, en el capítulo 97. Pregunta clave: ¿cómo se sostiene un sistema que mueve millones de gestos y miles de millones en tasas sobre albaranes que nadie puede verificar? Respuesta: dando fecha cierta a cada cambio de manos con **t2p** —la cadena huella–hora–ancla del capítulo 13 [3]— de la báscula al certificado de tratamiento final. Las reglas nuevas del Reglamento [1] valen lo que valga el albarán que las documenta; la traza verificable es lo que las hace valer.

La cadena del residuo — y dónde se rompe

La cadena, tal como es: el productor —la fábrica, el comercio, el hogar— genera el residuo; la recogida lo lleva a una planta de transferencia, donde se consolidan flujos; el gestor autorizado lo encamina hacia el tratamiento —reciclaje, valorización o eliminación—; y a menudo hay un traslado por medio: un camión hacia otra comunidad, un contenedor hacia otro continente. La normativa ya exige documentos de identificación y seguimiento para cada paso, y el nuevo Reglamento europeo los quiere electrónicos y con autorización previa cuando cruzan fronteras [1].

Los puntos de rotura tienen nombres conocidos en el sector. La subcontratación en cascada: el gestor autorizado que delega en otro, que delega en un tercero —y los papeles se van diluyendo en cada escalón. El certificado de tratamiento final firmado lejos del tratamiento. El balance de masa que no cuadra: a la planta entran más toneladas de las que salen tratadas, y la diferencia se evapora en informes incompletos. La exportación que se declara «valorización» y acaba en un vertedero en la otra punta del mundo. Y, coronándolo todo, el greenwashing: el «100 % reciclable», el «cero vertido» —afirmaciones que ningún consumidor puede contrastar.

La clave probatoria es la de todo este libro: todos estos agujeros pasan entre albaranes de parte —modificables, extraviables, sin fecha cierta oponible. Las responsabilidades ampliadas del productor pagan por toneladas declaradas; las autoridades inspeccionan muestras; y el ciudadano, que sostiene el sistema con su gesto y sus tasas, no puede verificar nada de nada.

La prueba de existencia aplicada

La misma cadena, eslabón a eslabón —y cada cambio de manos con lugar, hora y peso ciertos [3].

1. El contenedor con lugar y hora

En cada cambio de manos —la carga del camión, la entrada a la planta de transferencia, la descarga en el gestor—, una foto con el GPS forense de t2p: fijo genuino, precisión de unos 50 metros, antigüedad máxima de unos 30 segundos; una ubicación simulada bloquea la certificación [3]. El contenedor que sale de un municipio y «aparece» donde no toca deja de ser una sospecha: es una cadena de capturas datadas con un agujero exactamente allí donde alguien lo ha desviado. Y el precintado del contenedor de exportación, filmado con la fecha y la hora sobreimpresas [3], viaja como evidencia con el barco.

2. El balance de masa sellado

Los registros de báscula —qué entra, qué sale, cuándo— certificados por lotes con huellas encadenadas: cada cierre, una huella que incorpora la anterior [3]. El balance de masa de una planta se convierte en una serie datada que nadie puede reescribir: si un mes entran mil toneladas y salen seiscientas de tratadas, la diferencia tiene fecha y exige explicación. Es la misma lógica que el Estado ya impone a las facturas: la cadena de huellas como normalidad contable.

3. El certificado de tratamiento final

El documento que cierra el círculo —«este residuo ha sido tratado así, aquí, este día»— escaneado y sellado con fecha cierta, ligado por huella a los albaranes y capturas de toda la cadena [3]. El productor que paga su responsabilidad ampliada sabe qué ha pagado; la autoridad que autoriza un traslado [1] puede exigir el certificado anclado del destino; y el gestor honesto —que es la mayoría— tiene en su propia traza la defensa contra la competencia desleal de quien hace ver que trata.

4. La afirmación verde, congelada

El «fabricado con 70 % de material reciclado», el «cero residuos a vertedero», la página de sostenibilidad corporativa: capturados con el navegador certificado de t2p —imagen completa y código fuente, con fecha [3]. El día que la realidad no cuadre con el eslogan, el eslogan de aquel día existe, exacto y datado. Y el puente con el capítulo 98: el pasaporte del producto declara contenido reciclado —la traza del residuo es la única manera de que aquella declaración tenga de dónde venir.

Y los límites, que también los hay: el sello acredita custodia —lugar, hora, peso, documento—, no la calidad del tratamiento: que el reciclaje sea reciclaje de verdad lo han de decir las inspecciones y los análisis. El balance de masa puede engañar si el primer pesaje ya es falso —la cadena vale desde donde empieza, y por eso ha de empezar en la báscula de entrada. Y la traza es de la carga y de los documentos, nunca de las personas: la proporcionalidad con los trabajadores de planta manda, como en todos los capítulos laborales de este libro.

La promesa y el peligro

La promesa: tasas de responsabilidad ampliada pagadas sobre toneladas verificadas, no declaradas; traslados internacionales [1] con expedientes que el regulador puede auditar sin viajar; gestores honestos que compiten con traza en lugar de sufrir la competencia del fraude; y el gesto del ciudadano —el contenedor de cada noche— correspondido, por fin, con una cadena que se puede enseñar.

Y los peligros, uno por uno.

El primero es **el sello como maquillaje**. Certificar albaranes falsos con fecha cierta solo hace el fraude más elegante. La traza vale lo que vale su primer eslabón: básculas calibradas, capturas al momento, inspecciones que contrastan físicamente. La criptografía documenta; no sustituye el control.

El segundo es **la carga sobre el pequeño gestor**. El punto limpio municipal y la pequeña planta no pueden absorber burocracia infinita. El gesto ha de ser el de siempre —la foto de diez segundos en la báscula [3]— y el grueso documental, automático; si la traza se convierte en barrera de entrada, solo quedarán los grandes.

El tercero es **la vigilancia de la planta**. Documentar cargas no puede convertirse en vigilar a los trabajadores. Se capturan básculas, contenedores y documentos; las personas, nunca —la línea de todos los capítulos laborales de este libro.

Y el cuarto es **el tecnosolucionismo del contenedor**. La mejor traza del mundo no reduce ni un gramo de residuo. La jerarquía es la de siempre: reducir, reutilizar —y solo después reciclar bien. La

prueba de existencia hace honesto el tercer escalón; los dos primeros son decisiones de producción y de consumo que ningún hash toma por nosotros.

Es hora de actuar

Que el gesto de millones tenga la traza que merece.

Para los ciudadanos: vuestro gesto merece traza —exigid a vuestros municipios y a los sistemas de envases datos verificables, no porcentajes de folleto [1].

Para los gestores y las plantas: la foto en la báscula y el balance por lotes [3] —vuestra honestidad, demostrable, es vuestro mejor contrato.

Para los productores y los sistemas de responsabilidad ampliada: pagad —y cobrad— sobre toneladas con fecha cierta; el certificado de tratamiento anclado como condición de pago.

Para las autoridades ambientales y la fiscalía: el nuevo Reglamento [1] os da la tramitación electrónica; pedidla anclada —el expediente verificable del traslado es la diferencia entre autorizar y bendecir.

Para los legisladores: que el despliegue español del Reglamento y el sistema de depósito y devolución de envases anunciado nazcan con fecha cierta neutral de serie —sería el primer sistema de residuos del mundo verificable de la báscula al certificado.

Que el bote de yogur de cada noche tenga el viaje que le prometimos —y que quien lo desvíe deje huellas. Por el gesto de millones que merece ser verdad, **time2act**.

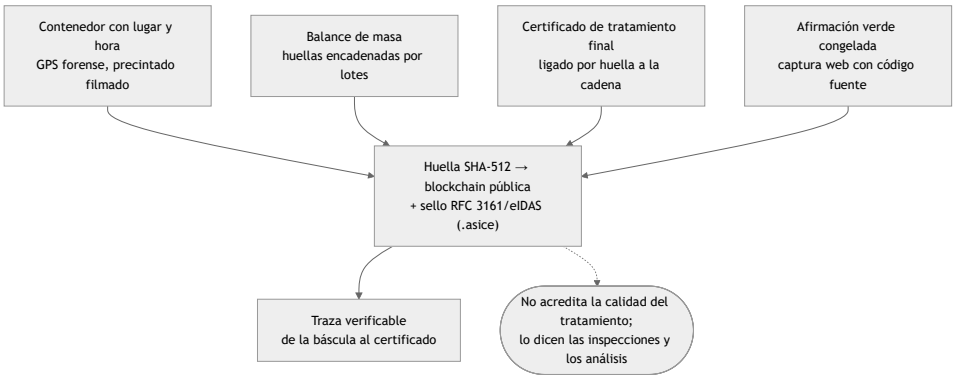


Figura 99.1 — La cadena del residuo con prueba de existencia (sellado con t2p — capítulo 13): el contenedor con lugar y hora en cada cambio de manos (GPS forense; precintado filmado con fecha sobreimpresa), el balance de masa sellado por lotes encadenados (entradas vs salidas datadas), el certificado de tratamiento final anclado y la afirmación verde congelada (captura web con código fuente). Contexto: Reglamento (UE) 2024/1157, aplicable desde el 21-5-2026 —notificación previa para todo residuo plástico exportado, prohibición hacia países no OCDE; Turquía recibía el 39 % de las exportaciones europeas (12,4 Mt). Límites: la traza acredita custodia, no calidad de tratamiento; primero reducir y reutilizar. Fuentes: DOUE/BOE; RETEMA.

[1] DOUE/BOE — *Reglamento (UE) 2024/1157, de 11 de abril de 2024, relativo a los traslados de residuos* (deroga el Reglamento 1013/2006; aplicable de manera general desde el 21 de mayo de 2026; exportaciones de todos los residuos plásticos a terceros países sujetas a notificación y autorización previas por escrito; prohibición de exportar residuos para valorización a países no OCDE; tramitación electrónica); RETEMA — *Nuevo Reglamento de traslados de residuos*; Residuos Profesional — *Análisis del Reglamento (UE) 2024/1157* (contexto: Turquía recibió el 39 % de las exportaciones europeas de residuos —12,4 millones de toneladas, datos 2022). https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-80606 · https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:32024R1157 · https://www.retema.es/blog/nuevo-reglamento-de-traslados-de-residuos-la-normativa-que-pone-en-jaque-la-industria-europea · https://www.residuosprofesional.com/reglamento-relativo-traslados-de-residuos/ ↩

[2] Marco general de residuos (documentos de identificación y seguimiento de los traslados; responsabilidad ampliada del productor; jerarquía de residuos). Véase el capítulo 98 para el pasaporte digital de producto y el capítulo 96 para las emisiones.

[3] t2p — manual de producto (foto con GPS forense —fijo genuino ~50 m / ≤30 s, la ubicación simulada bloquea la certificación; vídeo con fecha/hora sobreimpresa; escáner de documentos hasta 50 páginas; certificar cualquier fichero por lotes —solo la huella viaja; captura de página web con imagen completa + código fuente; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; el pasaporte de producto, en el capítulo 98; la ciencia ciudadana, en el capítulo 97. ↩

El campo y la PAC: el cuaderno verificable

«El suelo es el gran conector de vidas, origen y destino de todo. Es el sanador, el restaurador y el resucitador.»

— Wendell Berry, The Unsettling of America (1977)

El tractor parado en el margen, el móvil en la mano sucia de tierra —y una notificación de la administración: el satélite «no ha detectado actividad agraria» en la parcela declarada; hay que aportar una fotografía georreferenciada en un plazo, o la ayuda peligra. El agricultor mira el campo que sembró hace seis semanas —el campo que está ahí, con las líneas verdes del trigo recién nacido— y entiende lo que le acaba de pasar: ahora tiene que probar lo evidente a un algoritmo.

La escena se va haciendo cotidiana porque la política agraria común —el presupuesto más grande de la Unión Europea— ha cambiado de manera de vigilar [2]: de la inspección presencial por muestras, a la monitorización por satélite. Los Sentinel del programa Copernicus escanean cada parcela declarada, y los sistemas clasifican si aquello que se declaró —el cultivo, el pasto, el barbecho— se ve desde arriba; cuando no pueden concluir —nubes, parcelas pequeñas, cultivos tardíos—, la carga baja a tierra: una foto georreferenciada que el agricultor hace con el móvil [2].

Este capítulo trata la finca como sujeto de prueba. El testigo orbital y sus manipulaciones están en el capítulo 104; el fraude alimentario —qué hay de verdad en el plato—, en el capítulo 101; la geolocalización de parcelas contra la deforestación, en el capítulo 29; los sensores ciudadanos, en el capítulo 97; los residuos de la finca, en el capítulo 99. Pregunta clave: cuando el ojo que reparte las ayudas es un algoritmo orbital, ¿con qué se defiende el agricultor que sí sembró? Respuesta: con su propia cronología —el cuaderno sellado al momento y en el campo, la foto con fecha cierta neutral— mediante **t2p**: huella en el dispositivo y hora cierta anclada a la cadena (capítulo 13) [3]. La simetría del capítulo 104, mirada desde abajo.

El cuaderno que viene — y el satélite que ya está

La segunda pieza del tablero tiene calendario exacto [1]: el cuaderno digital de explotación —el CUE, el registro electrónico de las actuaciones de cada finca: tratamientos fitosanitarios, fertilización, riegos y otras prácticas— está disponible voluntariamente desde el 1 de enero de 2024 y, tras sucesivos aplazamientos, será obligatorio el 1 de enero de 2028 para las explotaciones más grandes: más de 30 hectáreas de cultivo, más de 5 de regadío o más de 0,1 de invernadero. Antes, un hito intermedio: el registro electrónico de los tratamientos fitosanitarios será obligatorio el 1 de enero de 2027 —el papel se acaba el 31 de diciembre de 2026 [1].

La lectura de este libro —y ya es la tercera vez que pasa: primero las facturas con VeriFactu, después el registro horario, ahora el campo: el Estado pide registros digitales de actuaciones, y vigila con ojos orbitales. La arquitectura de la prueba de existencia se impone a la agricultura… pero con una asimetría: el satélite es de la administración, las apps son de la administración, y el cuaderno vivirá en plataformas que la administración consulta. El agricultor pone los datos; la prueba, la custodian otros.

Y el matiz técnico que lo cambia todo: el satélite también se equivoca. Nubes persistentes, parcelas pequeñas, cultivos tardíos o atípicos, márgenes —el sistema que «no detecta actividad» puede estar mirando mal [2]. Cuando esto pasa, el agricultor honesto se encuentra en la posición más kafkiana de este libro: probar contra un algoritmo que su campo existe.

La prueba de existencia aplicada

El cuaderno y la foto, sí —pero sellados al momento, en el campo, y en manos del agricultor [3].

1. La entrada del cuaderno, al momento y en el campo

El tratamiento fitosanitario, el abonado, el riego —anotados cuando se hacen, donde se hacen: la entrada del cuaderno sellada con t2p con el GPS forense del campo —fijo genuino, precisión de unos 50 metros, antigüedad máxima de unos 30 segundos; una ubicación simulada bloquea la certificación [3]. La diferencia con el cuaderno «reconstruido el domingo en la mesa» es probatoria y es sanitaria: el registro hecho al momento es el que vale cuando llega la inspección, el residuo en el producto o la duda sobre

plazos de seguridad. Y cuando el CUE sea obligatorio [1], la versión sellada del agricultor será su contraste ante cualquier discrepancia de plataforma.

2. La foto que el satélite pide — con fecha cierta neutral

La fotografía georreferenciada que el sistema de monitorización reclama [2], hecha con t2p: lugar y hora ciertos, con el certificado y su código QR [3]. No es solo cumplir el trámite: es que la respuesta del agricultor tenga el mismo rango probatorio que la pregunta del algoritmo —una evidencia verificable por terceros, no una imagen más dentro de una app que hace lo que hace.

3. La defensa contra el ojo que se equivoca

La simetría decisiva: la serie de fotos datadas del cultivo —la siembra, el nacimiento, el crecimiento— hecha con cuatro gestos a lo largo de la campaña [3]. Cuando el satélite «no vea» lo que está ahí —las nubes, la parcela pequeña, el cultivo tardío [2]—, el agricultor no empieza de cero contra la notificación: tiene una cronología anclada que demuestra la actividad agraria antes de que nadie la cuestionara. Es el capítulo 104 mirado desde abajo: el testigo orbital es poderoso, pero no infalible —y quien trabaja la tierra merece poder contradecirlo con hechos.

4. El expediente de la ayuda

La solicitud, el cuaderno sellado, las fotos de campaña, las respuestas a los requerimientos —agrupados y exportables como paquete .asice verificable sin conexión [3]: para el recurso contra una reducción de ayuda, para la inspección presencial, para la trazabilidad que el comprador del grano o la cooperativa empiezan a pedir. Y el puente con los vecinos de parte: lo que el campo produce entra en la cadena del capítulo 101, y de ella salen los residuos del capítulo 99 —la finca verificable es el primer eslabón de ambas.

Los límites, dichos con claridad: el sello acredita actuaciones, lugares y fechas —no sustituye el cuaderno oficial ni las plataformas de la administración: las contrasta y las complementa [1]. No hace buenas las prácticas —los límites de fitosanitarios y las condiciones de las ayudas son los que son [2]. Y la brecha digital del campo es real: la herramienta ha de ser el gesto de diez segundos con el móvil que ya se lleva en el bolsillo, y las cooperativas y los técnicos, los aliados de quien no se aviene.

La promesa y el peligro

La promesa: agricultores que responden a los requerimientos del satélite con cronologías propias [2][3]; cuadernos que valen como prueba porque se escribieron al momento [1]; ayudas que se cobran y se defienden con hechos datados; y una trazabilidad de finca que el mercado empezará a pagar —el grano con pedigrí ya no es una utopía: es la continuación natural de los capítulos 29 y 101.

Los peligros, mirados de cara.

El primero es **el campo vigilado**. La monitorización orbital más el cuaderno digital pueden hacer del agricultor la profesión más fiscalizada del país. La respuesta es la de este libro: que la traza sirva a las dos direcciones —si la administración mira desde arriba, el agricultor ha de poder responder desde abajo con el mismo rango de prueba; vigilancia sin simetría es sumisión.

El segundo es **la burocracia que expulsa**. Cada requisito nuevo pesa más en la finca pequeña. El calendario del CUE ya lo reconoce —obligatorio solo para las grandes, de momento [1]—; la herramienta ha de restar trabajo, no añadirlo: la anotación al momento es más rápida que la reconstrucción del domingo.

El tercero es **el algoritmo como juez**. Si la notificación del satélite se trata como verdad por defecto, la presunción de inocencia agraria muere. El sistema de monitorización es un filtro, no un veredicto [2]; sus discrepancias se han de resolver con evidencia de tierra —y la carga de la prueba no puede ser toda del agricultor.

Queda el cuarto, el más tentador: creer que con esto basta. Ningún sello arregla los precios en origen, la sequía ni el relevo generacional. La prueba de existencia hace justas las ayudas y defendibles las fincas; la política agraria la hacen —y la han de hacer bien— las personas.

Es hora de actuar

Que el campo que está ahí se pueda demostrar desde allí.

Para agricultores y ganaderos: la anotación al momento con GPS forense [3] —el cuaderno que se hace en el campo vale el doble que el que se reconstruye; y la serie de fotos de campaña es vuestra póliza contra el ojo que se equivoca [2].

Para cooperativas y técnicos: sois la capa que hace posible todo esto para la finca pequeña —integrad el sellado en vuestros servicios de cuaderno y de solicitud [1][3].

Para la administración agraria: la monitorización os ahorra inspecciones [2]; devolved la simetría —aceptad la cronología anclada del agricultor como contraste cualificado de las discrepancias del satélite, y que vuestras apps emitan evidencia verificable, no cautiva.

Para los compradores y la industria: la finca con traza propia es el primer peldaño de vuestra cadena —los capítulos 29 y 101 son su continuación; pagadla como lo que vale.

Para los legisladores: el CUE llegará [1]; que llegue con la prueba en manos de quien la genera —el cuaderno sellado por el agricultor, con fecha cierta neutral, como registro con valor probatorio pleno.

Hace diez mil años que el campesinado alimenta el mundo sin que nadie le pidiera probarlo; ahora que se lo piden desde el espacio, que al menos tenga las herramientas. Por el campo que está ahí —y que se pueda demostrar—, **time2act**.

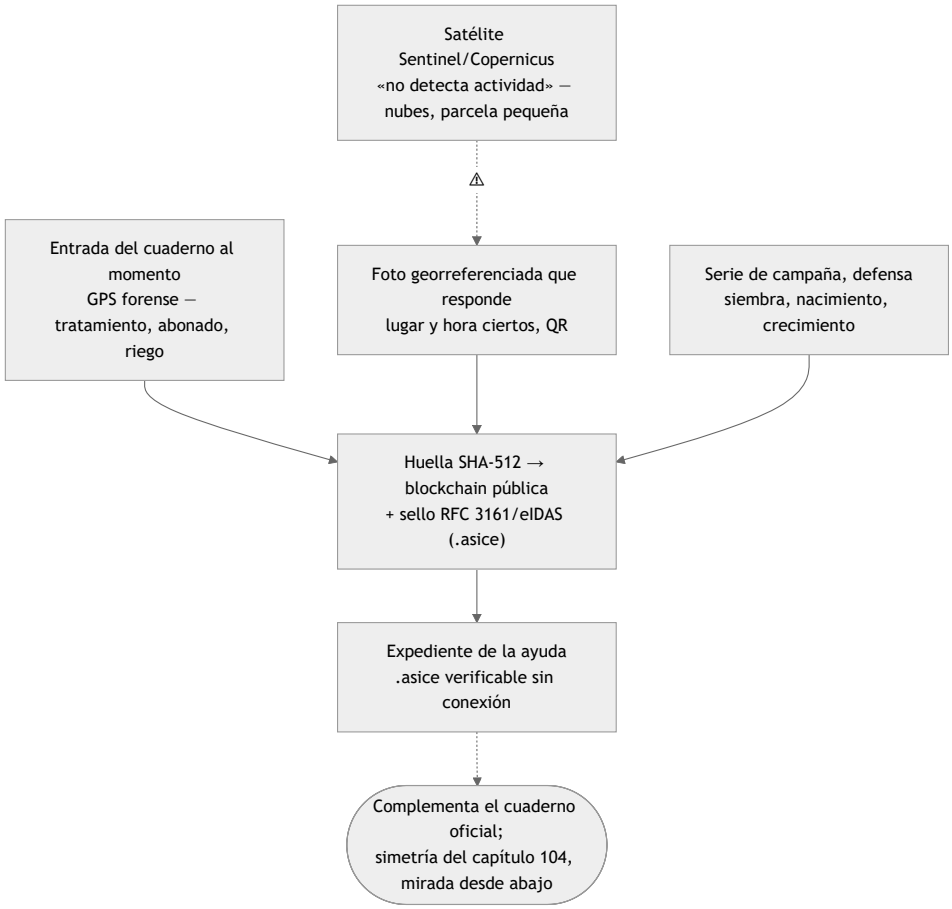


Figura 100.1 — El campo con prueba de existencia (sellado con t2p — capítulo 13): la entrada del cuaderno sellada al momento y en el campo (GPS forense), la foto georreferenciada que la monitorización pide —con fecha cierta neutral—, la serie de campaña como defensa contra el satélite que se equivoca (la simetría del capítulo 104, mirada desde abajo) y el expediente de la ayuda en .asice. Contexto: PAC vigilada por Sentinel/Copernicus; cuaderno digital (CUE) voluntario desde 2024, fitosanitarios electrónicos desde el 1-1-2027, CUE obligatorio el 1-1-2028 (>30 ha). Límites: complementa el cuaderno oficial, no lo sustituye; la brecha digital del campo exige cooperativas y técnicos como aliados. Fuentes: FEGA/normativa CUE; PAC 2023-2027.

[1] Agrodigital — *El cuaderno digital de explotación será obligatorio a partir del 1 de enero de 2028* (CUE voluntario desde el 1-1-2024; aplazamientos; obligatorio desde el 1-1-2028 para explotaciones >30 ha de cultivos, >5 ha de regadío o >0,1 ha de invernadero; registro electrónico de tratamientos fitosanitarios obligatorio desde el 1-1-2027 —papel hasta el 31-12-2026); FEGA/Agronews — aclaraciones de entrada en vigor; Gobierno de Aragón — *Cuaderno digital (CUE)* (contenido: actuaciones fitosanitarias, fertilización, riegos y otras prácticas). https://agrodigital.info/2025/01/23/el-cuaderno-digital-de-explotacion-sera-obligatorio-a-partir-del-1-de-enero-de-2028/ · https://www.agronewscastillayleon.com/el-fega-publica-aclara-la-entrada-en-vigor-del-cuaderno-de-explotacion-y-el-plan-de-abonado/ · https://www.aragon.es/pac-2026/cuaderno-digital-cue · https://www.fega.gob.es/sites/default/files/files/document/10.2023.03.15-12.45h_blq-04_inmaculada-bravo_cue.el-cue-y-el-riego.pdf ↩

[2] PAC 2023-2027 — sistema de seguimiento por monitorización (imágenes Sentinel/Copernicus sobre las parcelas declaradas en el SIGPAC; requerimientos de fotografías georreferenciadas al agricultor cuando el sistema no puede concluir). Marco general del FEGA y de la Comisión Europea. Véase el capítulo 104 para la integridad del testigo orbital. ↩

[3] t2p — manual de producto (foto con GPS forense —fijo genuino ~50 m / ≤30 s, la ubicación simulada bloquea la certificación; certificación en segundo plano —el campo sin cobertura; certificar cualquier fichero por lotes; escáner de documentos; proyectos para el expediente de una campaña; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; el satélite, en el capítulo 104; los alimentos, en el capítulo 101; los residuos, en el capítulo 99. ↩

Fraude alimentario: cuando la etiqueta miente sobre lo que te has comido

«Dime qué comes y te diré qué eres.»

— Jean Anthelme Brillat-Savarin, Fisiología del gusto (1825), aforismo IV

La noche del 8 al 9 de julio de 2024, el Comando de los Carabinieri para la Tutela de la Salud (NAS) de Italia, dentro del marco OPSON coordinado por Europol, registró dieciocho almacenes de la región de la Apulia y requisó unas **42 toneladas de aceite adulterado** ya envasado y etiquetado como «aceite de oliva virgen extra italiano», más unas 71 toneladas de una «sustancia oleosa», por cerca de un millón de dólares. El detalle que lo explica todo: los investigadores encontraron **623 litros de clorofila** que se añadían a aceites baratos para falsear el color verde del virgen extra auténtico, con etiquetas «virgen extra» falsificadas y **1.145 sellos de impuestos especiales** sospechosos de ser falsos. Siete personas fueron acusadas de asociación delictiva, adulteración de alimentos para la venta, fraude en suministros públicos y militares y adulteración para la exportación [3]. Todo procedía de la Operación Omegabad de noviembre de 2023 (Guardia Civil + Carabinieri + Europol), que requisó **260.000 litros** de aceite —«lampante» barato cortado y vendido como virgen extra en Ciudad Real, Sicilia y la Toscana—, detuvo a once sospechosos y confiscó 91.000 euros en efectivo [4]. La oleada seguía el precio récord del virgen extra al por mayor, unos 10,50 €/kg a comienzos de 2024, después de que la sequía andaluza redujera las cosechas a casi la mitad.

Este capítulo aborda una pregunta distinta de la de sus vecinos. El capítulo 29 cubre la cadena de suministro genérica —custodia, logística y procedencia de mercancías—; el capítulo 72, la extracción ilegal y el origen conflictivo de una materia prima. Aquí hablamos específicamente de la **autenticidad y el origen del alimento**: la adulteración (cortar el aceite con lampante o girasol, la miel con jarabe de azúcar), la sustitución de especie (caballo por ternera) y las **falsas alegaciones geográficas** de denominación protegida. La pregunta es simple y antigua: *¿es este producto lo que dice la etiqueta?* Y la tesis del libro encaja aquí: ante un fraude que vive del **papeleo falso** —etiquetas, certificados, sellos—, la prueba de existencia fija quién declaró qué, dónde y cuándo, sin poder antedatarlo.

Un negocio de unos 40.000 millones que vive de la prima del origen

El fraude alimentario afecta aproximadamente al 1 % de la industria mundial y supone un coste anual de entre 10.000 y 40.000 millones de dólares [7]. La Red de Fraude Agroalimentario de la UE registró 758 sospechas en 2023, un 26 % más que el año anterior, con la sustitución de carne, la adulteración de miel y el aceite mal etiquetado a la cabeza [7]. El valor de ventas anual de los productos con indicación geográfica de la UE era de 74.800 millones de euros en 2017, cerca del 7 % de las ventas de alimentos y bebidas, y un producto con denominación protegida se vende de media al doble del precio de uno comparable sin certificar [6]; cuanto más valiosa es la denominación, más tentador resulta falsificarla.

La **Operación OPSON XIII** (resultados anunciados en octubre de 2024) confiscó unas 22.000 toneladas de alimentos por unos 91 millones de euros, desmantelando once redes y denunciando a 278 personas; en Italia se encontraron 42 toneladas de falso virgen extra y 623 litros de clorofila, y en España 45.000 litros de aceite y 120.000 latas de atún [1]. La **Operación OPSON XIV** (anunciada en 2025) elevó la cifra a unos 95 millones de euros —11.566 toneladas de alimentos y 1,4 millones de litros de bebidas—, con 631 personas denunciadas y trece grupos de crimen organizado desarticulados en 31 países [2].

La miel que no es miel y el caballo que era ternera

El aceite no es el único frente. En la acción coordinada europea «From the Hives» (muestras de noviembre de 2021 a febrero de 2022, resultados publicados el 21 de marzo de 2023), **147 de 320 partidas de miel importada —el 46 %—** resultaron sospechosas de adulteración con jarabes de azúcar, un aumento enorme respecto al 14 % registrado en 2015-17. El cálculo es transparente: la miel real costaba de media unos 2,32 €/kg importada y el jarabe de arroz entre 0,40 y 0,60 €/kg; la UE importa unas **175.000 toneladas al año**, cerca del 40 % del consumo [5]. Así, una de cada dos partidas llegaba bajo sospecha de no ser miel verdadera.

Y ningún repaso está completo sin el episodio que sacudió Europa. En el escándalo de la carne de caballo de 2013, la lasaña de ternera de Findus contenía más del 60 % —hasta el 100 %— de carne de caballo. En el juicio de París del 16 de abril de 2019, el exresponsable de Spanghero, Jacques Poujol, recibió dos años (dieciocho meses en suspenso) y una multa de 100.000 euros; el comerciante neerlandés Jan Fasen, dos años y una prohibición permanente del sector cárnico, por la venta de más de **500 toneladas de carne de caballo** canalizadas a través de Comigel hacia 28 empresas de trece países [9]. Una etiqueta puede mentir a lo largo de media Europa antes de que nadie lo note.

La ley del origen: un registro reforzado, pero de papel

La respuesta normativa ha sido sustancial. El régimen de indicaciones geográficas de la UE se revisó con el **Reglamento (UE) 2024/1143**, en vigor desde el **13 de mayo de 2024**, que fusiona las reglas de DOP, IGP e IG para alimentos, vinos y bebidas espirituosas en un único marco de registro y refuerza la protección de las indicaciones usadas como ingrediente y vendidas en línea [8]. El **Reglamento (UE) 2017/625** de controles oficiales da base legal a los controles a lo largo de la cadena y a la **Red de Fraude Agroalimentario (FFN)** de la DG SANTE, conectada al sistema de alertas RASFF. Los estándares del aceite (Reg. 2022/2104 y 2022/2105) definen las categorías —virgen extra, virgen, lampante—, y la Directiva de la miel 2001/110/CE se reforzó en 2024 con la Directiva (UE) 2024/1438. En Estados Unidos, los controles preventivos de la **FSMA** obligan a protegerse contra la adulteración por motivos económicos (EMA); el ejemplo canónico es el aceite barato vendido como 100 % aceite de oliva [10]. Y OPSON aporta la fuerza operativa cada año.

El problema es que toda esta arquitectura descansa sobre **documentos**: certificados de conformidad, números de lote, informes de laboratorio, sellos de impuestos y etiquetas de denominación. Un documento, como hemos visto en la Apulia, se puede falsificar, clonar, reciclar o antedatar; el registro 2024/1143 indica qué denominación merece protección, pero no garantiza que ese certificado sea genuino ni que ese análisis cubra ese lote.

Por qué el certificado solo no salva

Hay que decirlo con crudeza. Un certificado de conformidad en PDF, un número de lote impreso o un informe de laboratorio firmado no demuestran nada si se pueden alterar sin dejar huella. Como hemos visto en la Apulia, los defraudadores crearon las etiquetas «virgen extra» y los sellos de impuestos para hacer pasar la mentira por los controles. Un certificado genuino de un lote pequeño puede servir para amparar un envío mucho mayor diluido después; un informe auténtico de un lote honesto se puede adjuntar, retocándole la fecha, a un lote adulterado; y si el sello de impuestos es falsificable, toda la cadena de garantías se resquebraja. Lo que falta no es más papel: hace falta un anclaje inalterable que fije quién emitió cada artefacto de autenticidad, sobre qué lote y en qué instante, de modo que no se pueda clonar ni antedatar.

La prueba de existencia aplicada

Aquí es donde **t2p** aporta la capa que falta, sobre el papeleo y el acto de campo, no sobre la química. Funciona en tres fases. Primero, al crear el lote, el productor captura fotos y vídeo geoetiquetados y con prueba de vida del olivar, de la colmena o de la línea de envasado; el dispositivo calcula la huella SHA-512 en el propio aparato —el archivo no sale nunca—, la ancla en la blockchain pública, añade un sello de tiempo complementario RFC 3161 conforme a eIDAS, y el GPS forense vincula el acto al territorio DOP/IGP reclamado, fijando dónde y cuándo se produjo el lote antes de que ninguna mezcla pueda pasar. Segundo, se sellan los artefactos de autenticidad: el informe del laboratorio acreditado (perfil NMR/IRMS, ratio isotópica, polen para la miel, ácidos grasos para el aceite), el certificado de conformidad, el número de lote, los documentos de impuestos y el arte de la etiqueta DOP/IGP, cada uno con su huella y sellado en un contenedor **.asice** verificable sin conexión y ligado a un identificador de lote. Tercero, cualquier inspector, importador o tribunal puede verificar, sin conexión, que el certificado, el informe y las fotos de origen existían entonces, los emitió aquel organismo y no se han alterado ni antedatado —desactivando etiquetas falsificadas, sellos clonados y certificados reciclados vistos en OPSON y Omegabad. Es el complemento, sobre la etiqueta y el documento, de lo que proponen los capítulos 13 y 15 con C2PA para la procedencia de la imagen y del certificado, y puede alimentar el pasaporte digital de producto del capítulo 98.

El límite es claro: «basura a la entrada, basura en la cadena». El sello prueba origen, tiempo, autor e integridad de un artefacto capturado; no comprueba que el contenido sellado sea verdad, legítimo ni seguro. No puede decir si el aceite de la botella es realmente virgen extra, si la miel está cortada con jarabe de arroz o si la alegación geográfica es químicamente cierta: eso solo lo determina el análisis de laboratorio (NMR, IRMS, ADN, polen). Un productor deshonesto todavía puede sellar una foto auténtica de un olivar equivocado, ponerle huella a un certificado genuino que cubre menos lote del que se expide o sellar papeleo correcto de un producto adulterado. No detiene la sustitución aguas abajo ni vale nada si el propio organismo certificador es corrupto; es una herramienta probatoria y antiantedatación sobre —nunca en lugar de— la autenticación de laboratorio, los controles oficiales, la certificación acreditada y el juicio humano.

La promesa y el peligro

La promesa es un ecosistema agroalimentario donde el origen y la garantía documental sean **verificables y no antedatables**: poder demostrar con fecha cierta que aquel certificado, aquel informe y aquellas fotos del olivar existían, los emitió el organismo legítimo y no se han tocado. En un sector donde la prima de la denominación se vende al doble y el fraude cuesta hasta 40.000 millones al año, **como hemos visto**, hacer el origen inalterable protege al productor honesto, al importador prudente y al consumidor.

El peligro pide los matices de siempre. Primero, no confundir **integridad con verdad**: un papeleo falso y sellado sigue siendo falso, y ahora, además, inmutable; el sello podría dar una falsa tranquilidad —«está anclado, luego es genuino»— sin correspondencia con la química real. Segundo, la **dependencia del organismo certificador**: si el consejo regulador o el laboratorio son cautivos o corruptos, el sello eterniza la mentira con apariencia de rigor. Y tercero, la **brecha digital**: imponer un sello avanzado podría expulsar al pequeño cooperativista o al productor del sur global sin laboratorio acreditado ni herramienta a su alcance, concentrando aún más el mercado de la calidad.

Es hora de actuar

Para los **consorcios y consejos reguladores de DOP/IGP**: sellar el número de lote, el arte de la etiqueta y el certificado al emitirlos, para que una etiqueta clonada como las de la Apulia falle la verificación. Para los **laboratorios acreditados y organismos de control**: anclar el informe analítico (NMR/IRMS, polen, ácidos grasos) y el certificado de conformidad en el momento de emisión, vinculándolos al identificador de lote. Para los **productores y cooperativas**: capturar la prueba de campo geoetiquetada con prueba de vida y GPS forense en la cosecha, en la colmena o en la línea de envasado, antes de cualquier mezcla. Para los **inspectores y aduanas** (NAS, Guardia Civil, OPSON, OLAF): verificar sin conexión la autenticidad y la fecha de los sellos y certificados, en lugar de fiarse de ellos a ojo. Y para los **reguladores y la DG SANTE**: reconocer el artefacto sellado como evidencia de la documentación exigida y alimentar con él la red de alertas —como hemos visto en el Reg. 2024/1143—.

En la Apulia, una noche de verano, siete personas llenaban botellas de aceite barato teñido con **623 litros** de clorofila y les pegaban etiquetas y sellos falsos para que pasaran por virgen extra italiano. Dar a cada lote honesto una prueba sellada de su origen, su fecha y su certificado —sin olvidar nunca que el sello no hace verdad lo que en él se declara— es, en este frente donde la etiqueta puede mentir sobre lo que nos comemos, time2act.

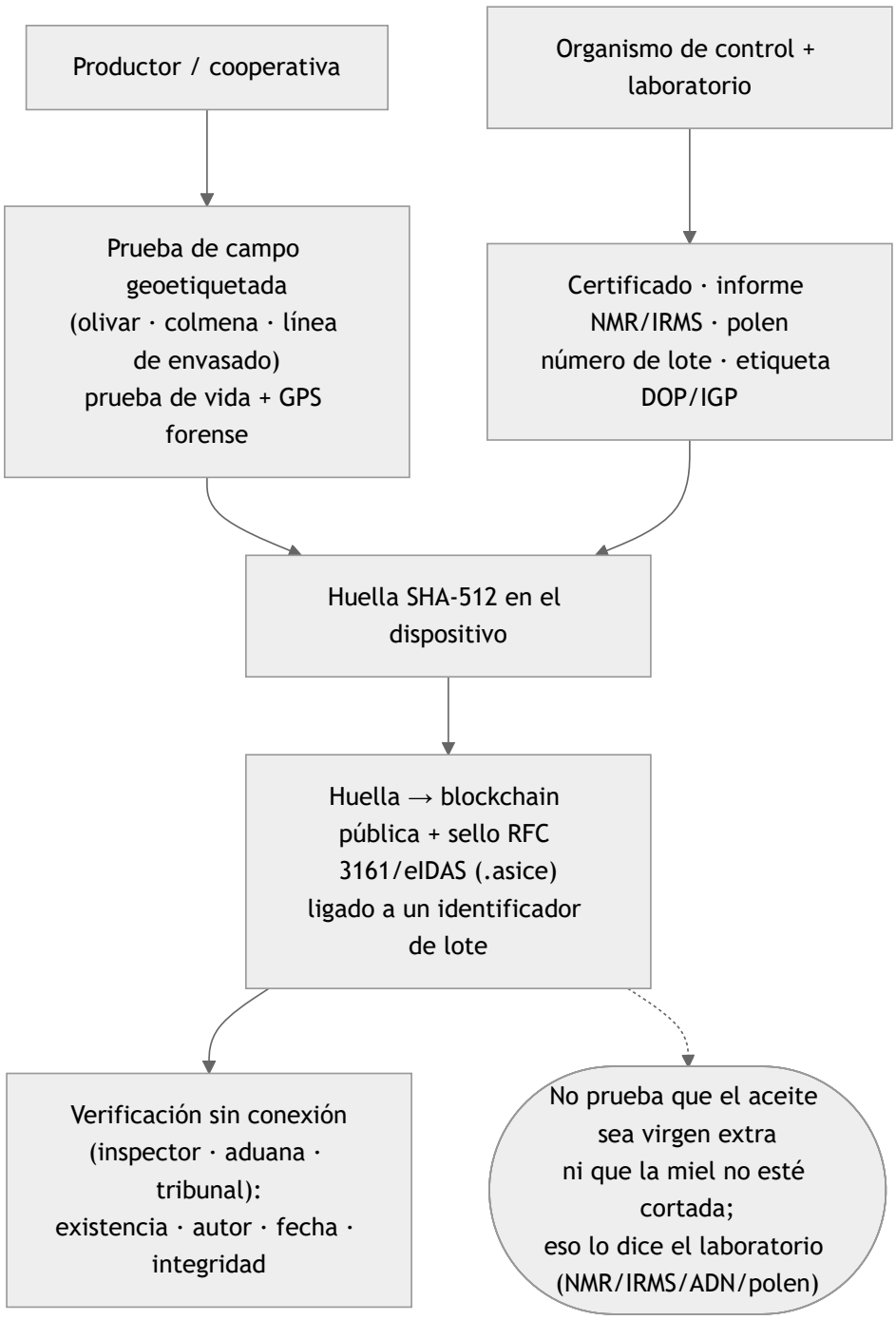


Figura 101.1 — El productor captura la prueba de campo geoetiquetada con prueba de vida y GPS forense (olivar, colmena, línea de envasado) y calcula su huella SHA-512 en el dispositivo; en paralelo, el organismo de control y el laboratorio sellan el certificado, el informe analítico, el número de lote y la etiqueta DOP/IGP. La huella del conjunto se ancla en la blockchain pública, con sello RFC 3161/eIDAS complementario (.asice), ligado a un identificador de lote. Cualquier inspector, aduana o tribunal lo verifica sin conexión: existencia, autor, fecha e integridad. Límite: el sello prueba el papel y el acto de campo, no que el aceite sea virgen extra ni que la miel no esté cortada —eso lo dice el laboratorio (NMR/IRMS/ADN/polen). Fuentes: OPSON XIII y XIV (Europol); caso Apulia; Operación Omegabad; «From the Hives»; Reg. (UE) 2024/1143.

---

[1] Europol — *EUR 91 million worth of counterfeit and substandard food seized in Europe-wide operation* (Operación OPSON XIII; 22.000 t de alimentos, 91 M€, 11 redes; Italia: virgen extra y clorofila; España: aceite y atún). https://www.europol.europa.eu/media-press/newsroom/news/eur-91-million-worth-of-counterfeit-and-substandard-food-seized-in-europe-wide-operation ↩

[2] Europol — *Counterfeit and substandard food worth EUR 95 million seized in global operation* (Operación OPSON XIV; 95 M€, 11.566 t, 631 denunciados, 13 grupos de crimen organizado, 31 países). https://www.europol.europa.eu/media-press/newsroom/news/counterfeit-and-substandard-food-worth-eur-95-million-seized-in-global-operation ↩

[3] CNN — *Italian authorities confiscate almost $1 million in fake olive oil* (11 de julio de 2024; registro de los Carabinieri en la Apulia, 42 t de falso virgen extra, 623 L de clorofila, 7 acusados, etiquetas y sellos falsos). https://www.cnn.com/2024/07/11/europe/italy-olive-oil-seizure-scli-intl/ ↩

[4] Food Safety News — *Spanish and Italian investigators uncover olive oil fraud* (diciembre de 2023; Operación Omegabad: 260.000 L requisados, 11 detenciones, lampante vendido como virgen extra, Ciudad Real/Sicilia/Toscana, 91.000 € en efectivo). https://www.foodsafetynews.com/2023/12/spanish-and-italian-investigators-uncover-olive-oil-fraud/ ↩

[5] Comisión Europea (DG SANTE) — *EU coordinated action on honey ('From the Hives')* (muestras 2021-2022; 46 % de 320 partidas sospechosas de adulteración con jarabe de azúcar; metodología y países participantes). https://food.ec.europa.eu/food-safety/eu-agri-food-fraud-network/eu-coordinated-actions/honey-2021-2022_en ↩

[6] FoodNavigator — *Geographical Indications worth a mouth-watering €75 billion, study finds* (valor de las IG de la UE: 74.800 M€ en 2017; prima de precio de unas 2 veces para los productos protegidos). https://www.foodnavigator.com/Article/2020/04/22/Geographical-Indications-worth-a-mouth-watering-75-billion-study/ ↩

[7] Comisión Europea — *EU Agri-Food Fraud Network: reports and publications* (el fraude afecta a ~1 % de la industria y cuesta 10.000-40.000 M$/año; 758 sospechas en 2023, +26 %; carne, miel y aceite a la cabeza). https://food.ec.europa.eu/food-safety/eu-agri-food-fraud-network/reports-and-publications_en ↩

[8] EUR-Lex — *Regulation (EU) 2024/1143 on geographical indications* (en vigor el 13 de mayo de 2024; marco único de DOP/IGP/IG y ETG; protección como ingrediente y en línea). https://eur-lex.europa.eu/eli/reg/2024/1143/oj/eng ↩

[9] Food Safety News — *Four sentenced in France for roles in horse meat scandal* (juicio de 2019; Poujol (Spanghero) 2 años + 100.000 € de multa, Fasen 2 años + prohibición permanente; Comigel, 500+ t hacia 13 países). https://www.foodsafetynews.com/2019/04/four-sentenced-in-france-for-roles-in-horse-meat-scandal/ ↩

[10] FDA — *Economically Motivated Adulteration (Food Fraud)* (definición de EMA, p. ej. aceite barato vendido como 100 % aceite de oliva; deber de controles preventivos de la FSMA). https://www.fda.gov/food/compliance-enforcement-food/economically-motivated-adulteration-food-fraud ↩

[11] Sensors (MDPI) — *Blockchain and IoT for food traceability in olive oil supply chains* (2024; estado del arte en sellado/anclaje de la procedencia del aceite y en autenticación analítica NMR/IRMS). https://www.mdpi.com/1424-8220/24/24/8189

Quién lo hizo, y en qué condiciones: la diligencia debida en la mano de obra

«Considerad si es un hombre / quien trabaja en el fango, / quien no conoce la paz, / quien lucha por medio pan, / quien muere por un sí o por un no.»

— Primo Levi, «Shemà», Si esto es un hombre (1947)

A finales de enero y durante febrero de 2024, la aduana de Estados Unidos retuvo miles de coches de lujo del **grupo Volkswagen** —modelos **Porsche, Bentley y Audi**— en los puertos estadounidenses. El motivo no era el motor, ni la carrocería, ni el acero alemán: era una **pieza electrónica diminuta**, escondida en la profundidad de la cadena, con material rastreable hasta **Xinjiang**, la región donde la *Uyghur Forced Labor Prevention Act* presume que todo bien se fabrica con trabajo forzoso. Volkswagen declaró que no había sabido el origen del componente en el noroeste de China hasta que un proveedor lo avisó a mediados de enero de 2024, después de que las autoridades estadounidenses ya lo hubieran marcado en diciembre de 2023; prometió sustituir la pieza en todos los coches vendidos en todo el mundo y trabajó para liberar los vehículos [4]. El episodio es la dimensión laboral en estado puro: los coches y su acero eran «de Alemania», pero la pregunta que los detuvo en el muelle era **quién había hecho una pieza minúscula muy abajo en la cadena, y en qué condiciones**.

Este capítulo es distinto del capítulo 29 —la integridad de la cadena de suministro—, que sella **de dónde** viene un bien y su custodia física: el origen del objeto. Aquí hablamos de la capa **social** que se le superpone: quién lo fabricó y bajo qué condiciones laborales, el registro de diligencia debida en derechos humanos y el testimonio de los trabajadores, no la geografía del material. La pregunta del capítulo es: cómo se fija, con fecha cierta y de modo que no se pueda antedatar ni desestimar como deepfake, **la prueba de lo que sabíamos y de lo que hicimos** sobre las personas que hay al final de la cadena. El episodio de Volkswagen lo cristaliza: una multinacional puede quedar ciega ante un proveedor de cuarto o quinto nivel que no ve.

Una lacra de 28 millones de personas y 236.000 millones de dólares

La magnitud es aplastante. La **OIT** estima que **27,6 millones de personas** estaban en trabajo forzoso un día cualquiera de 2021, 2,7 millones más que en 2016; **17,3 millones** son explotadas en la economía privada y los **trabajadores migrantes** corren un riesgo **tres veces** mayor [1]. El trabajo forzoso genera **236.000 millones de dólares** de beneficios ilegales al año —64.000 millones más (un 37 %) que en 2014—, con los beneficios más altos en Europa y Asia Central (**84.000 millones**) [2]. Como hemos visto, no es un problema de países lejanos: es un modelo de negocio global y una parte del dinero se hace en casa.

El episodio de Volkswagen no salió de la nada. En febrero de 2024, **Human Rights Watch** publicó el informe *Asleep at the Wheel*, que documentaba la exposición de los fabricantes de automóviles —VW, BMW, Mercedes-Benz, GM y otros— al trabajo forzoso uigur en la cadena del aluminio y los componentes [5]. En junio de 2023, el **ECCHR** había presentado una denuncia ante la **BAFA** alemana, alegando que Volkswagen, BMW y Mercedes-Benz habían incumplido la Ley alemana de cadenas de suministro por sus vínculos con Xinjiang. El riesgo no era invisible: ya estaba documentado y denunciado antes de que la aduana actuara.

El riesgo migra de la ropa al coche

Durante años, el trabajo forzoso se asoció al textil; ya no. Entre junio de 2022 y julio de 2025, la aduana estadounidense (**CBP**) retuvo **16.755 envíos** valorados en **3.690 millones de dólares** bajo la UFLPA; solo en 2024 retuvo mercancía por **1.340 millones**, y casi el **48 %** de las retenciones de aquel año acabaron con la entrada denegada [3]. La cifra que lo dice todo: las retenciones en el sector del **automóvil y el aeroespacial** crecieron casi un **1.600 %** en 2024 respecto a 2023 —de 59 a 991 envíos entre enero y noviembre—, una prueba de que el riesgo de trabajo forzoso ha emigrado de la ropa a los bienes manufacturados complejos [3].

Y la presión crece. El **14 de enero de 2025**, el **DHS** hizo su ampliación mayor de la *Entity List* de la UFLPA, añadiendo **37 empresas** chinas de energía y textil y llevando la lista negra de presunción

refutable a **144 entidades** [3] —como hemos visto anteriormente—. Cada nombre añadido convierte una cadena hasta entonces tranquila en un campo de minas documental: el comprador debe demostrar, con pruebas «claras y convincentes», que su producto no contiene ninguno.

La ley ya exige vigilar toda la cadena

El marco normativo se ha endurecido en ambas orillas del Atlántico. En **EE. UU.**, la **UFLPA** (vigente desde el 21 de junio de 2022) presume que todo bien hecho total o parcialmente en Xinjiang, o por una entidad de la lista, es producto de trabajo forzoso y queda vetado, salvo que pruebas «claras y convincentes» lo refuten. En la **UE**, la **Directiva de diligencia debida en sostenibilidad corporativa (CSDDD, Directiva 2024/1760)** entró en vigor el **25 de julio de 2024**, cubriendo las empresas con 5.000 empleados y 1.500 millones de euros de facturación (y las de fuera con 1.500 millones de facturación en la UE); tras las enmiendas Ómnibus, la transposición se aplaza hasta el **26 de julio de 2028** y la aplicación al **26 de julio de 2029** [6]. El **Reglamento europeo de trabajo forzoso**, vigente desde el **13 de diciembre de 2024** y aplicable a partir del **14 de diciembre de 2027**, prohíbe cualquier producto hecho con trabajo forzoso, pero sin presunción geográfica —la carga de la prueba recae en las autoridades, a diferencia de la UFLPA [7]. En **Alemania**, la **LkSG** se aplica a las empresas de 1.000 empleados desde el 1 de enero de 2024; la BAFA puede imponer multas de hasta **800.000 euros o el 2 % de la facturación mundial**, y en 2023 hizo **486 auditorías** [8]. Bajo todo ello está el marco internacional: los convenios 29 y 105 de la OIT y los Principios Rectores de la ONU sobre empresas y derechos humanos.

Por qué la auditoría social sola no salva

Hay que decirlo con crudeza, porque aquí la complacencia mata literalmente. La herramienta que la industria dice que vigila la mano de obra —la auditoría social y los certificados como SA8000, BSCI o SMETA— falla repetidamente en aquello mismo para lo que existe. La fábrica del Rana Plaza, auditada bajo BSCI, se derrumbó el 24 de abril de 2013 y mató a 1.131 personas; la fábrica de Ali Enterprises en Pakistán, certificada SA8000, se incendió en 2012 y mató a más de 250 trabajadores. Ambas habían pasado la inspección poco antes del desastre [9]. No son casos aislados: el informe de Human Rights Watch de noviembre de 2022 documentó cómo las auditorías se amañan de manera rutinaria —consultorías que enseñan a los trabajadores a mentir, dobles libros de cuentas, nóminas falsas y niños escondidos durante la inspección [10].

Y hay un vacío más fundamental, anterior al fraude: el certificado solo verifica el cumplimiento de un mínimo legal que a menudo es miseria. Como hemos visto, los salarios legales están muy por debajo de un salario digno en todos los grandes centros textiles —alrededor del 31 % en la India, el 37 % en China y Bangladés, el 33 % en Camboya y el 13 % en Sri Lanka [11]. Un PDF de conformidad puede decir «todo correcto» sobre una fábrica donde nadie cobra lo suficiente para vivir. El documento, solo, no salva: es tan fiable como la voluntad de quien lo firma y tan honesto como la inspección que lo emitió.

La prueba de existencia aplicada

Aquí es donde **t2p** aporta la capa que falta, y lo hace sobre la **prueba contemporánea y contextualizada** de las condiciones y de las personas, no sobre el producto —como hemos visto en el capítulo 29—. En el momento de la captura, un trabajador, un representante sindical, un auditor de campo sin aviso previo o una ONG local de confianza graba con su dispositivo una foto o un vídeo corto del taller, de un dormitorio, de una salida de emergencia encadenada, de una nómina o de una hoja de turnos. La aplicación calcula en el dispositivo la **huella SHA-512** del archivo —que nunca sale del teléfono—, obtiene un **sello de tiempo RFC 3161/eIDAS** y ancla la huella en la blockchain pública, produciendo un contenedor **.asice** verificable sin conexión. Para las capturas de campo de una persona o un lugar se añade un **GPS forense** (que demuestra que la foto se hizo dentro de aquella fábrica o aquel dormitorio de reclutamiento) y una **prueba de vida** (que demuestra que fue un trabajador real, no un testigo deepfake aleccionado, quien dio el relato en aquel momento).

El mismo mecanismo sella la cara corporativa de la cadena: la **declaración del proveedor** y la atestación de custodia que una marca recopila para refutar la presunción de la UFLPA, el **registro de diligencia debida** de la LkSG o la CSDDD, la **queja de un trabajador** presentada por una aplicación tipo WOVO, o los **hallazgos en bruto de un auditor** sin aviso previo antes de que ninguna fábrica haya

tenido tiempo de «prepararse». Complementa el sistema existente atacando los dos agujeros documentados por reguladores y HRW: las auditorías se amañan con trabajadores aleccionados y documentos fabricados, y una marca que combate una retención de la CBP debe demostrar **cuándo** supo realmente las cosas y cuándo actuó. Una queja o un hallazgo sellados con fecha, GPS y prueba de vida son mucho más difíciles de antedatar, editar o desestimar como deepfake que un informe en PDF —y esto refuerza el testimonio del trabajador, el rastro de quejas y el expediente que una empresa presenta a la CBP, la BAFA o una autoridad competente de la UE.

Ahora el límite, con toda la crudeza, porque aquí engañarse haría daño. «Basura a la entrada, basura en la cadena»: el sello prueba **el acto** —que esta persona, en este lugar y momento verificados, grabó esta imagen o firmó esta declaración, y que nada se ha alterado desde entonces. **No prueba que las condiciones sean buenas** ni que el salario sea digno; una foto sellada y geolocalizada de un taller ordenado y montado para la inspección sigue siendo una puesta en escena. No confirma que la declaración de un proveedor sea veraz, ni que la fábrica de tercer nivel que aparece sea realmente la que hace la pieza, ni que el testimonio de un trabajador se haya dado libremente y no bajo coacción —la prueba de vida derrota una cara sintética, no una asustada. No verifica que los bienes estén libres de contenido de Xinjiang ni que satisfagan la UFLPA o las obligaciones de la CSDDD y la LkSG; todo eso todavía exige investigación, rastreo documental, visitas sin aviso y juicio humano. El sello hace la prueba inalterable y fechada; nunca sustituye la auditoría, al regulador ni la credibilidad del propio trabajador. Es el complemento laboral de lo que los capítulos 13 y 15 proponen con el C2PA y la procedencia del contenido.

La promesa y el peligro

La promesa es convertir el testimonio más frágil de la cadena —la voz de un trabajador, a menudo atemorizado y sin poder— en una **prueba fechada, geolocalizada y admisible** que ninguna fábrica puede borrar y ningún abogado puede desestimar como fabricada después. La marca honesta gana un expediente de diligencia debida que aguanta ante la CBP y la BAFA; el trabajador gana que su palabra deje de ser «su palabra contra la de la empresa».

El peligro pide los matices más estrictos. El primero, y de vida o muerte: la **seguridad del testigo**. Un trabajador que sella una prueba contra su empleador se expone a represalias; el sistema debe proteger su identidad, no exponerla. El segundo, no confundir **integridad con verdad**: una declaración de proveedor falsa y sellada sigue siendo falsa, y ahora, además, inmutable; el sello podría dar una falsa tranquilidad —«está anclado, luego cumple»— que no se corresponde con nada. Y el tercero, la **concentración**: si solo las grandes marcas pueden sellar y documentar, el estándar puede volverse una barrera que expulsa al pequeño proveedor honesto en lugar de fortalecer al trabajador. La prueba de existencia es una herramienta de dignidad y de rendición de cuentas, no un certificado de bondad.

Es hora de actuar

Para los **trabajadores y los sindicatos**: poder sellar en el dispositivo una queja, una nómina o una imagen del taller como prueba fechada y geolocalizada, sin que la foto salga del teléfono y con la identidad protegida. Para las **marcas y los compradores** (Volkswagen, BMW, Mercedes-Benz y el resto): sellar la declaración del proveedor y el registro de diligencia debida en el momento de recopilarlos, para que el expediente presentado a la CBP o la BAFA tenga fecha cierta y no parezca fabricado posteriormente. Para los **auditores de campo y las ONG**: anclar los hallazgos en bruto antes de que ninguna fábrica se «prepare», convirtiendo la inspección sin aviso en prueba inalterable. Para los **reguladores** (CBP, BAFA, autoridades de la UE bajo el Reglamento de trabajo forzoso): reconocer la prueba sellada con sello de tiempo como evidencia válida de lo que una empresa sabía y cuándo, y tratar la fecha cierta como diferencia entre diligencia y coartada. Y para los **legisladores** (UFLPA, CSDDD, LkSG): exigir que el rastro de diligencia debida sea verificable y anclado, no un PDF que se pueda retocar mañana.

En los puertos estadounidenses, miles de coches de lujo se detuvieron por una pieza que nadie en la sede sabía que existía. Dar a cada trabajador del final de la cadena una prueba sellada de lo que vivió y a cada marca honesta una prueba de lo que sabía y cuándo actuó —sin olvidar nunca que el sello no hace dignas las condiciones— es, en este frente, el momento de actuar: time2act.

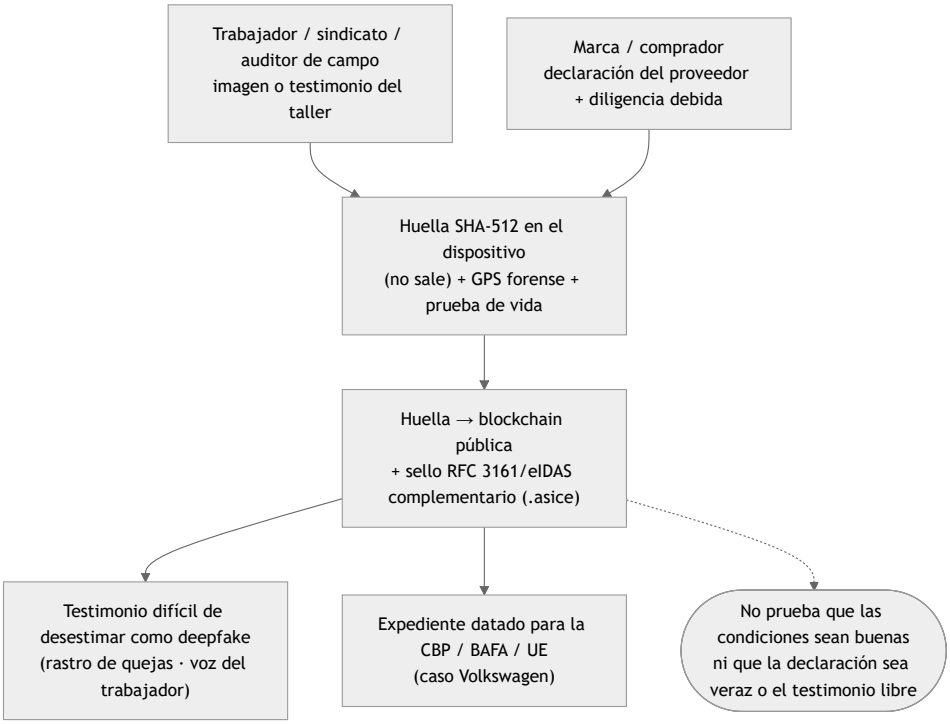


Figura 102.1 — Dos fuentes de prueba: el trabajador, el sindicato o el auditor de campo capturan en el dispositivo una imagen o un testimonio del taller (huella SHA-512 que no sale del teléfono, GPS forense, prueba de vida); la marca sella la declaración del proveedor y el registro de diligencia debida. La huella del conjunto se ancla en la blockchain pública, con sello de tiempo RFC 3161/eIDAS complementario (.asice). Resultados: testimonio del trabajador más difícil de desestimar como deepfake, y expediente fechado para la CBP, la BAFA o la autoridad de la UE. Límite: el sello prueba el acto, el lugar y la fecha; no prueba que las condiciones sean buenas, que la declaración sea veraz ni que el testimonio fuera libre. Fuentes: caso Volkswagen/CBP; OIT; Miller & Chevalier (UFLPA); HRW (auditorías y automóvil); ECCHR (certificados).

---

[1] OIT — *Data and research on forced labour (Global Estimates 2022)* (27,6 millones de personas en trabajo forzoso en 2021; 17,3 millones en la economía privada; los migrantes triplican el riesgo). https://www.ilo.org/topics/forced-labour-modern-slavery-and-trafficking-persons/data-and-research-forced-labour ↩

[2] OIT — *Annual profits from forced labour amount to US$236 billion* (marzo de 2024; +37 % desde 2014; 84.000 millones en Europa y Asia Central). https://www.ilo.org/resource/news/annual-profits-forced-labour-amount-us-236-billion-ilo-report-finds ↩

[3] Miller & Chevalier — *UFLPA Enforcement 2024 Year in Review* (16.755 envíos y 3.690 M$ retenidos; 1.340 M$ en 2024; 48 % de entradas denegadas; +1.600 % en el automóvil; *Entity List* a 144). https://www.millerchevalier.com/publication/trade-compliance-flash-uflpa-enforcement-2024-year-review ↩

[4] Business & Human Rights Resource Centre — *Volkswagen cars held up at US ports over part linked to allegations of forced labour in Xinjiang* (marcas, subcomponente, cronología diciembre 2023 – mediados de enero 2024). https://www.business-humanrights.org/en/latest-news/volkswagen-cars-held-up-at-us-ports-over-part-linked-to-allegations-of-forced-labour-in-xinjiang/ ↩

[5] Human Rights Watch — *Asleep at the Wheel: Car Companies' Complicity in Forced Labor in China* (febrero de 2024; VW, BMW, Mercedes, GM y la cadena del aluminio). https://www.hrw.org/report/2024/02/01/asleep-wheel/car-companies-complicity-forced-labor-china ↩

[6] Comisión Europea — *Corporate Sustainability Due Diligence (CSDDD)* (Directiva 2024/1760, en vigor el 25 de julio de 2024; transposición hasta el 26 de julio de 2028, aplicación desde el 26 de julio de 2029 tras el Ómnibus). https://commission.europa.eu/business-economy-euro/doing-business-eu/sustainability-due-diligence-responsible-business/corporate-sustainability-due-diligence_en ↩

[7] Covington — *EU Forced Labour Regulation Enters Into Force* (diciembre de 2024; en vigor el 13 de diciembre de 2024, aplicación el 14 de diciembre de 2027; modelo de investigación sin presunción geográfica). https://www.cov.com/en/news-and-insights/insights/2024/12/eu-forced-labour-regulation-enters-into-force ↩

[8] BAFA — *Supply Chain Act (LkSG): Overview* (aplicación a empresas de 1.000 empleados desde el 1 de enero de 2024; multas hasta el 2 % de la facturación mundial; 486 auditorías en 2023). https://www.bafa.de/EN/Supply_Chain_Act/Overview/overview_node.html ↩

[9] ECCHR — *More for show than safety: Certificates in the textile industry* (Rana Plaza, 1.131 muertos, BSCI; Ali Enterprises, más de 250 muertos, SA8000; ambas habían pasado la inspección). https://www.ecchr.eu/en/case/more-for-show-than-safety-certificates-in-the-textile-industry/ ↩

[10] Human Rights Watch — *Obsessed with Audit Tools, Missing the Goal: Why Social Audits Can't Fix Labor Rights Abuses* (noviembre de 2022; trabajadores aleccionados, dobles libros, nóminas falsas, niños escondidos). https://www.hrw.org/report/2022/11/15/obsessed-audit-tools-missing-goal/why-social-audits-cant-fix-labor-rights-abuses ↩

[11] COSH — *Living wages for EU garment workers* (el salario mínimo legal es el 31 % de un salario digno en la India, el 37 % en China y Bangladés, el 33 % en Camboya, el 13 % en Sri Lanka). https://cosh.eco/en/articles/living-wages-eu-garment-workers ↩

Integridad marítima: dónde está de verdad ese barco, y ¿es quien dice ser?

«El mar nunca ha sido amigo del hombre. A lo sumo, ha sido el cómplice de la inquietud humana.»

— Joseph Conrad, El espejo del mar (1906)

El 29 de abril de 2026, la empresa de inteligencia marítima **Windward** destapó un esquema de contrabando de crudo iraní valorado en unos **800 millones de dólares**. Cuatro superpetroleros VLCC sancionados por Estados Unidos —**Alicia** (IMO 9281695), **RHN** (IMO 9208215), **Star Forest** (IMO 9237632) y **Aqua** (IMO 9248473)—, cada uno con unos **2 millones de barriles** a bordo, emitían mensajes AIS de destino falsos y trazados erráticos para parecer fondeados frente a Basra y cargando en el puerto iraquí de **Khor al Zubair**. En realidad, se escabullían hacia terminales iraníes, cargaban crudo iraní y fabricaban una **coartada digital** de origen iraquí legítimo. Windward rastreó una decena de petroleros sancionados falseando posiciones frente a Irak, y más de veinte buques al oeste del estrecho de Ormuz con señales delatoras de spoofing: trazados circulares en forma de «círculos de cosecha», escalas portuarias inventadas [2].

Este capítulo es distinto del capítulo 54 —el fraude documental del comercio internacional, que sella albaranes y cartas de crédito— y del capítulo 72 —la pesca ilegal, que mira si una captura se hizo donde y como tocaba. Aquí el objeto sellado no es ningún papel ni ninguna captura: es el **hecho físico de dónde está un buque y quién es**, aguas arriba de cualquier documento. En el mar, la posición y la identidad declaradas son **aserciones de radio autoinformadas** que se pueden fabricar al por mayor. La pregunta del capítulo es cómo hacer que un buque pueda **probar de manera no repudiable** dónde estaba y quién era en un instante dado —y, sobre todo, cómo hacer que un buque sancionado **no pueda** fabricar a posteriori un rastro que lo sitúe en Khor al Zubair cuando nunca estuvo allí.

La señal que se puede inventar

El AIS —el sistema de identificación automática— nace para la seguridad: que los buques se vean entre sí. Pero lo que un buque emite (posición, rumbo, identidad MMSI, destino) es lo que **él mismo decide** emitir. Aquí está el fraude. Entre enero de 2024 y julio de 2025, **Kpler** identificó **261 buques** que falsearon su AIS antes de ser sancionados —la categoría de práctica engañosa más numerosa—, incluidos pequeños gaseros que inventaban escalas en Khor al Zubair para fabricar historias de viaje plausibles [3]. La firma británica **Lloyd's List Intelligence** documenta la mecánica del *blanqueo de identidad*: el fraude del número IMO, el salto de bandera, la manipulación del «apretón de manos» AIS para que dos cascos intercambien identidades en el mar [11]. La otra cara es el apagado deliberado: en diciembre de 2024, la OFAC designó a los operadores del **MS ENOLA**, que «seguía empleando prácticas engañosas, incluido el apagado del AIS» para ocultar transferencias ilícitas de petróleo iraní bajo la orden ejecutiva 13902 [9].

La flota fantasma y el mapa que miente

La escala es industrial. La **flota fantasma rusa** cuenta con más de **1.000 petroleros** envejecidos e infraasegurados —alrededor del **17 %** de la flota petrolera mundial—; el catálogo de inteligencia ucraniano listaba **1.337** en febrero de 2026, y en 2024 la flota generó unos **9.400 millones de dólares** de ingresos rusos adicionales esquivando el techo de precio [6]. Viven del falseamiento: posiciones inventadas, identidades prestadas, transbordos buque a buque (STS) lejos de toda mirada. Y no es solo petróleo: el 25 de diciembre de 2024 el petrolero **Eagle S**, con bandera de las Islas Cook y parte de la flota fantasma, arrastró el ancla y dañó el cable submarino Estlink 2 entre Finlandia y Estonia, reforzando una dimensión de **seguridad híbrida** [10].

Por encima del fraude deliberado está el **ruido de fondo** que lo hace indistinguible: la interferencia masiva del GNSS. En el segundo trimestre de 2025, más de **10.000 buques** sufrieron oficialmente interferencia de GPS —ocho veces más que los unos 1.250 del primer trimestre—, con casi **3.000 buques** afectados en el golfo Pérsico y Ormuz durante el pico de junio de 2025 [4]. Durante la guerra Israel-Irán de aquel mes, el spoofing en Ormuz —por donde pasa el **20 %** del petróleo mundial— ponía las pantallas de los superpetroleros «sobre tierra firme» y a través de una central nuclear; el profesor Todd Humphreys, de la Universidad de Texas, lo decía sin rodeos: «Estoy bien seguro de que son los iraníes quienes hacen

este spoofing» [1]. El 1 de marzo de 2026, más de **1.100 buques** del golfo sufrieron interferencia en 24 horas, con 21 nuevos núcleos que situaban buques dentro de la central nuclear de Barakah; los tránsitos por Ormuz cayeron una tercera parte [5]. El mapa global de seguimiento se ha convertido él mismo en una **falsificación**.

La ley pide trazabilidad; el fraude la ridiculiza

El marco existe. El **convenio SOLAS, capítulo V, regla 19**, de la OMI, obliga a llevar AIS en todos los buques de 300 GT o más en viajes internacionales y a mantenerlo «en funcionamiento en todo momento» salvo que la seguridad justifique apagarlo —lo que convierte la navegación «a oscuras» y el spoofing deliberado en una **infracción de seguridad**. Las sanciones de la **OFAC**, bajo la orden 13902, y el régimen del techo de precio ruso citan explícitamente la manipulación del AIS, la navegación oscura y el blanqueo de identidad como prácticas engañosas [9]. La UE listó más de **444 buques** de la flota fantasma hacia diciembre de 2025 (añadió 41 el 18 de diciembre) [7], y el 18.º paquete, del 18 de julio de 2025, rebajó el techo del crudo ruso de 60 a **47,60 dólares** con un mecanismo dinámico que lo mantiene un 15 % por debajo del mercado [8]. El Comité Jurídico de la OMI trabaja contra la **matriculación fraudulenta**: el LEG 111 (abril de 2024) y el LEG 112 (marzo de 2025) publicaron directrices sobre registro de buques, previstas para 2027, para frenar el salto de bandera y el fraude del número IMO. La ley pide trazabilidad; el problema es que descansa sobre una señal que el propio infractor controla.

Por qué el mandato del AIS solo no salva

Hay que decirlo con crudeza. Que SOLAS obligue a llevar el AIS encendido no impide ni el apagado ni el spoofing; solo los convierte, sobre el papel, en infracción. El problema de fondo es que el AIS es **autoinformado**: el buque indica dónde está y quién es, y el receptor se lo cree. Una posición AIS sin anclaje independiente no distingue el buque honesto del que fabrica un trazado; un fallo de AIS puede ser una avería o una tapadera; y cuando el fraude se esconde dentro de un mar de **numerosos** buques con interferencia real, la maniobra dolosa se vuelve indistinguible del ruido legítimo. Detectar la anomalía —cosa que Windward, Kpler o Pole Star hacen muy bien— no es lo mismo que **probarla ante un tribunal**, ni impide que un operador sancionado alegue que su rastro sospechoso era una víctima más de la interferencia. Falta una capa que convierta «este trazado parece anómalo» en «esta posición verificada es criptográficamente probable, y la ausencia de sello es en sí misma una bandera roja».

La prueba de existencia aplicada

Aquí es donde **t2p** cierra el agujero de integridad de la posición y de la identidad autoinformadas. Cuando se toma una fijación, una unidad de a bordo resistente a la manipulación —como un inspector de confianza de la guardia costera o del puerto, o una aplicación de escala o de aprovisionamiento de combustible— captura el **registro de navegación**: la fijación GNSS con hora, IMO y MMSI, el calado y la trama AIS tal como se emite. En el propio dispositivo se calcula la **huella SHA-512** del registro —el rastro en bruto no debe salir del buque—, se le añade un **sello de tiempo RFC 3161** conforme a eIDAS y se ancla en la blockchain pública, dentro de un contenedor **.asice** verificable sin conexión. Cuando un inspector comprueba físicamente el casco, el nombre y la placa IMO en una escala o un transbordo STS, se incorpora una **fijación GPS forense** y una **prueba de vida** del inspector y de la escena.

El resultado es un **libro mayor de posición e identidad**, continuo y anclado independientemente: un buque puede demostrar posteriormente dónde y quién era, y —como hemos visto— un buque sancionado **no puede** fabricar a posteriori un rastro sellado que lo sitúe en Khor al Zubair cuando no existe ningún sello contemporáneo. Esto **complementa** los sistemas existentes (AIS, LRIT, detección por RF y SAR de satélite, cribado OFAC y UE) añadiendo un ancla fechada, no repudiable y de grado judicial. Como los capítulos 13 y 15 hacen con la procedencia C2PA de lo que un dispositivo **produce**, aquí se sella lo que un buque **hace y es**.

El sello prueba el origen, la hora, el autor y la integridad de un registro de posición —**no que la señal GNSS subyacente fuera genuina**. Si el receptor recibe una señal de satélite falseada, un sello válido anclará una posición falsa: la criptografía certifica «este dispositivo registró esta fijación en este instante», no que la fijación fuera real. Por tanto, sin receptores multiconstelación y análisis forense, el sello no distingue una ubicación honesta de una falseada; solo la ausencia de sello se convierte en prueba.

Complementa la procedencia C2PA/SynthID pero **nunca sustituye** la auditoría de bandera, el control del puerto ni el juicio humano.

La promesa y el peligro

La promesa es convertir el océano en un espacio con **memoria verificable**: que un buque honesto pueda demostrar su posición e identidad con un anclaje que ningún operador puede retocar, y que el silencio —la falta de sello— pase a ser un dato acusatorio. En un sector donde un casco cambia de nombre, de bandera y de número IMO sin dejar recibo, hacer el origen inalterable protege tanto a la naviera limpia como a la aseguradora y al estado costero.

El peligro pide los matices de siempre. El primero, no confundir **integridad con verdad**: una posición falseada pero sellada sigue siendo falsa, y ahora, además, inmutable; el sello podría dar una falsa tranquilidad —«está anclado, luego es real»— que no se corresponde con nada. El segundo, la **voluntariedad**: ningún régimen puede obligar a un petrolero fantasma a sellar su posición, de modo que el sistema protege sobre todo a los honestos y deja la prueba en la ausencia. Y el tercero, la **gobernanza** de quien opera las unidades de a bordo y las claves: si las controla quien tiene incentivos para mentir, el sello pierde el sentido. La prueba de existencia es una capa de integridad de la señal, no un certificado de legalidad ni un sustituto del ojo humano que sabe leer un mar.

Es hora de actuar

Para los **estados de bandera y la OMI**: incorporar el sello de posición e identidad a las directrices de registro de 2027 y al régimen SOLAS, de modo que un vacío de AIS sin sello contemporáneo pese como indicio. Para las **autoridades de control del estado del puerto y las guardias costeras**: sellar con GPS forense y prueba de vida cada inspección de casco, nombre y placa IMO en escalas y transbordos STS. Para los **reguladores de sanciones** (OFAC, Consejo de la UE): reconocer la ausencia de rastro sellado como señal de riesgo en el cribado, y el sello como evidencia de grado judicial. Para las **aseguradoras y los clubes P&I**: exigir el libro mayor de posición anclado como condición de cobertura, para que el petrolero infraasegurado de la flota fantasma quede fuera del mercado. Y para las **firmas de inteligencia marítima** (Windward, Kpler, Pole Star): conectar su detección de anomalías con el ancla sellada, para que «parece spoofing» pase a ser «probablemente no estaba donde decía».

Como hemos visto el 29 de abril de 2026, cuatro superpetroleros pintaron en el mapa una geografía que no existía para esconder 800 millones de dólares de crudo iraní. Dar a cada buque honesto una prueba sellada de dónde estaba y quién era —y convertir el silencio del defraudador en su propia acusación—, sin olvidar nunca que el sello no hace real una señal manipulada; es, en este frente donde el propio océano se ha vuelto falsificable, time2act.

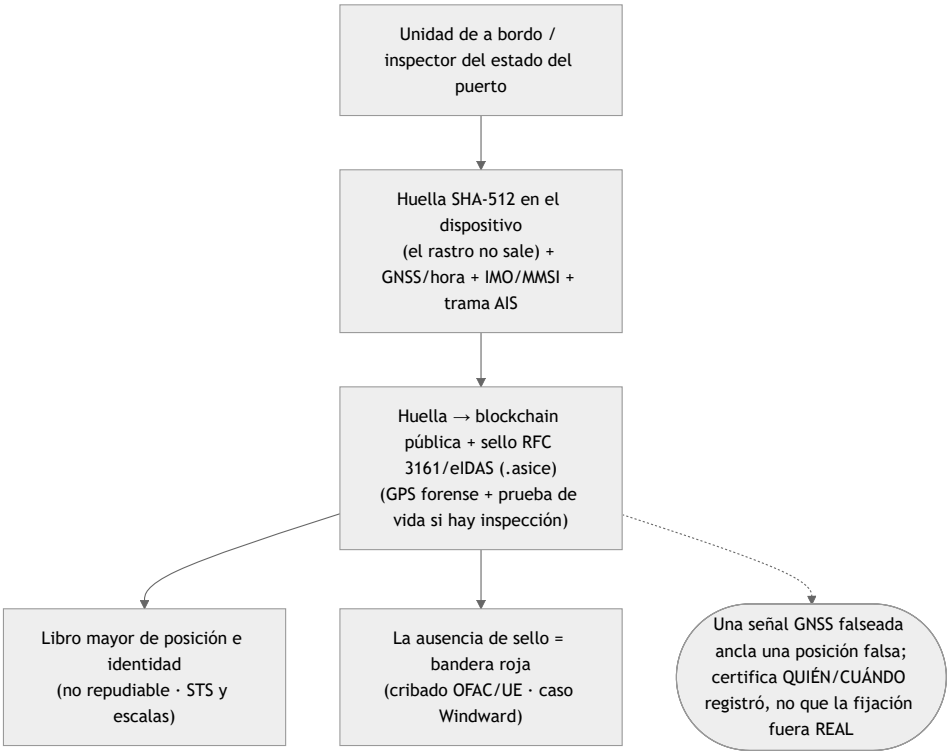


Figura 103.1 — Al tomar una fijación, una unidad de a bordo o un inspector del estado del puerto captura el registro de navegación (GNSS + hora, IMO/MMSI, calado, trama AIS) y calcula su huella SHA-512 en el dispositivo; la huella del conjunto se ancla en la blockchain pública, con sello RFC 3161/eIDAS complementario (.asice), con GPS forense y prueba de vida cuando hay inspección física. Dos resultados: a la izquierda, un libro mayor de posición e identidad no repudiable; a la derecha, la ausencia de sello se convierte en una bandera roja para el cribado de la OFAC/UE. Límite: el sello certifica que el dispositivo registró esta fijación en este instante, no que la señal GNSS fuera genuina; una señal falseada ancla una posición falsa. Fuentes: caso Windward (esquema de 800 M$); Kpler (261 buques); GPSPATRON (10.000+ buques); Scientific American (Ormuz); OFAC (MS ENOLA).

---

[1] GPS spoofing is scrambling ships in the Strait of Hormuz — *Scientific American* (spoofing en Ormuz durante la guerra Israel-Irán de 2025; buques sobre tierra y centrales nucleares; atribución de Humphreys a Irán; ~20 % del petróleo mundial por el estrecho). https://www.scientificamerican.com/article/gps-spoofing-is-scrambling-ships-in-the-strait-of-hormuz/ ↩

[2] Iran's $800M oil-smuggling scheme uses tankers posing as Iraqi ships — *Fox News* (revelación de Windward, 29 de abril de 2026; VLCC con números IMO; escalas falsas en Khor al Zubair). https://www.foxnews.com/world/irans-800m-oil-smuggling-scheme-uses-tankers-posing-iraqi-ships-dodge-blockade-.amp ↩

[3] AIS spoofing: the fast track to sanctions — *Kpler* (261 buques falsearon el AIS antes de ser sancionados, enero 2024-julio 2025; escalas falsas en Khor al Zubair). https://www.kpler.com/blog/ais-spoofing-fast-track-to-sanctions ↩

[4] Maritime GNSS Interference Worldwide: A Cumulative Analysis 2025 — *GPSPATRON* (10.000+ buques afectados en el 2T 2025, ocho veces más que el 1T; puntos calientes regionales). https://gpspatron.com/maritime-gnss-interference-worldwide-a-cumulative-analysis-2025/ ↩

[5] Widespread GPS jamming hits 1,000-plus ships in the Middle East Gulf — *Windward* (1 de marzo de 2026: 1.100+ buques en 24 h, 21+ núcleos; fijaciones falsas en Barakah y Al Hamra; Ormuz un tercio a la baja). https://windward.ai/blog/gps-jamming-disrupts-1100-ships-in-the-middle-east-gulf/ ↩

[6] Russian Shadow Fleet Tracker — *Kyiv School of Economics (KSE) Institute* (tamaño de la flota; ~17 % de la flota petrolera mundial; 9.400 M$ de ingresos extra en 2024; peso creciente de la bandera rusa). https://kse.ua/about-the-school/news/russian-shadow-fleet-tracker-march-2026-share-of-russian-flagged-shadow-tankers-jumps-from-3-to-21-in-nine-months/ ↩

[7] Council sanctions 41 vessels of the Russian shadow fleet — *Consejo de la UE (Consilium)* (18 de diciembre de 2025: el total de la UE llega a 444+ buques; prohibiciones de acceso a puerto y de servicios). https://www.consilium.europa.eu/en/press/press-releases/2025/12/18/russia-s-war-of-aggression-against-ukraine-council-sanctions-41-vessels-of-the-russian-shadow-fleet/ ↩

[8] EU adopts 18th package of economic and individual measures — *Consejo de la UE (Consilium)* (18 de julio de 2025: techo del crudo rebajado de 60 a 47,60 $ con mecanismo dinámico 15 % por debajo del mercado).

https://www.consilium.europa.eu/en/press/press-releases/2025/07/18/russia-s-war-of-aggression-against-ukraine-eu-adopts-18th-package-of-economic-and-individual-measures/ ↩

[9] Treasury Maintains Pressure on Iranian Shadow Fleet (MS ENOLA) — *U.S. Department of the Treasury / Iran Primer* (diciembre de 2024; acción de la OFAC bajo la E.O. 13902 citando el MS ENOLA «apagando el AIS»). https://iranprimer.usip.org/blog/2024/dec/19/us-sanctions-more-irans-dark-fleet ↩

[10] Estlink 2 incident / Eagle S shadow-fleet tanker — *NPR* (petrolero Eagle S de bandera de las Islas Cook, 25 de diciembre de 2024, daño al cable submarino del Báltico; dimensión de amenaza híbrida). https://www.npr.org/2024/12/31/nx-s1-5243302/finland-russia-severed-undersea-cable-shadow-fleet ↩

[11] AIS spoofing: vessel-identity manipulation typologies — *Lloyd's List Intelligence* (blanqueo de identidad, fraude del número IMO, apretón de manos AIS y mecánica del spoofing de posición). https://www.lloydslistintelligence.com/resources/blog/the-secret-lives-of-the-shadow-fleet-ais-spoofing-vessel-identity-manipulation ↩

Observación de la Tierra: el testigo orbital que también puede falsificarse

«Mirad de nuevo ese punto. Eso es aquí. Eso es nuestro hogar. Eso somos nosotros.»

— Carl Sagan, Un punto azul pálido (1994)

En abril de 2022, después de que las fuerzas rusas se retiraran de **Bucha**, en Ucrania, el Kremlin afirmó que las imágenes de cuerpos esparcidos por las calles se habían «escenificado» una vez que sus soldados se habían marchado. Pero los satélites **WorldView** de **Maxar Technologies** ya habían fotografiado aquellas calles: imágenes de alta resolución del 18, el 19 y el 31 de marzo de 2022 mostraban cadáveres tendidos en la calle Yablónska y una fosa común recién excavada —una zanja de unos 14 metros junto a una iglesia de cúpula dorada—, todas fechadas en semanas en que las tropas rusas aún ocupaban la ciudad. *The New York Times* geolocalizó los cuerpos de los fotogramas orbitales hasta la posición exacta que luego se vería en los vídeos a pie de calle, refutando de manera demostrable la negación de Moscú y alimentando las investigaciones por crímenes de guerra [2][3]. Y sin embargo, ese mismo «testigo» en órbita es hoy un objetivo de falsificación: en 2021, el geógrafo **Bo Zhao**, de la Universidad de Washington, acuñó el término «geografía deepfake» y demostró, en *Cartography and Geographic Information Science*, que la IA podía injertar las texturas de Pekín sobre un mapa de Tacoma para fabricar escenas de satélite falsas y convincentes [1].

Este capítulo es transversal y toca a tres vecinos sin confundirse con ellos. El capítulo 20 usa la imagen de satélite como **prueba judicial** de un crimen de guerra; el capítulo 22 la usa para **medir el carbono** (biomasa, deforestación); el capítulo 96 para **vigilar emisiones**. Los tres tratan la imagen como una *fuente* de prueba sobre otra cosa. Aquí el sujeto es la imagen misma: la **integridad del fotograma orbital**, a la vez testigo y objetivo de falsificación. La pregunta es incómoda: si el ojo en el cielo puede ahora mentir tan bien como cualquier deepfake, ¿cómo fijamos que este píxel, de este sensor, existió en este instante —antes de que nadie lo discutiera? Es la tesis del libro aplicada al lugar más inesperado: la fotografía de la Tierra desde arriba.

Cuando la imagen orbital es el único testigo

La imagen de satélite se ha convertido en prueba de primera línea precisamente donde a pie de tierra no llega nadie. En 2020, el equipo de **BuzzFeed News** —la serie *Built to Last*, después ganadora de un Pulitzer— combinó imágenes de **Planet** y de otros satélites con los recuadros en blanco que la censura china dejaba sobre sus propios mapas para identificar **268 campos de detención** recién construidos en Xinjiang, y **428 emplazamientos sospechosos** en total [4]. Sin un solo periodista sobre el terreno, la órbita documentó un sistema de internamiento masivo. En Bucha, el patrón se repite a la inversa: la órbita había fechado el crimen semanas antes de que el negador pudiera inventarse una coartada. En ambos casos, la imagen no era una ilustración: era *la evidencia*, y toda la cadena —tribunal, Naciones Unidas, opinión pública— descansaba en ella.

Esta dependencia es, a la vez, su vulnerabilidad. Cuando todo un edificio de prueba reposa sobre un fotograma, quien pueda falsificarlo —o solo sembrar la duda de que se puede falsificar— derriba el edificio entero. Y aquí es donde 2021 cambió las reglas.

El testigo que ahora se puede fabricar

Bo Zhao no habló en hipotético. Su estudio construyó un conjunto de detección de **8.064 imágenes de satélite** —la mitad auténticas de Seattle, Tacoma y Pekín; la otra mitad deepfakes de Tacoma con texturas injertadas de Pekín y de Seattle— y advirtió que la imagen falsificada por IA es una **amenaza para la seguridad nacional** [1]. Cuatro años después, el peligro ya es operativo, no teórico. En noviembre de 2025, un estudio de detección probaba clasificadores contra imágenes aéreas forjadas con **StyleGAN2** y **Stable Diffusion** sobre más de **130.000 imágenes** etiquetadas, y encontraba que los *Vision Transformers* las detectan mucho mejor que las redes convolucionales: **95,11 % frente al 87,02 %** de acierto; las falsificaciones GAN dejan distorsiones de alta frecuencia, mientras que las de difusión muestran «disonancia semántica» —terreno repetido, carreteras que se acaban de golpe, sombras mal emparejadas [5].

El riesgo sube cuando el objetivo es estratégico. En 2024, investigadores de verificación nuclear (Nguyen, Glaser y Biessmann, de Princeton) demostraron que los modelos de texto a imagen pueden generar imágenes de satélite **fotorrealistas de instalaciones concretas** —centrales nucleares incluidas—, «difíciles de distinguir de los datos reales», con implicaciones directas para el control de armamento y la verificación [6]. La propia **NGA** —la agencia de inteligencia geoespacial de EE. UU.— ha advertido que la imagen manipulada con GAN podría desviar convoyes ante puentes o carreteras que no existen. El ojo en el cielo, durante décadas el patrón oro de la prueba incontestable, ha entrado en la era en que hay que preguntarle, también a él, «¿cómo sé que eres real?».

La carrera institucional: autenticar la señal y la imagen

La respuesta institucional avanza en dos frentes. El primero es la geolocalización: el 24 de julio de 2025 el servicio OSNMA de Galileo entra en operación, convirtiéndose en el primer GNSS mundial que emite una firma digital criptográfica (protocolo TESLA) para que los receptores rechacen señales de posicionamiento falsificadas [7]. Es la columna vertebral del dónde y del cuándo de una captura —aunque no detiene la interferencia (jamming). El segundo frente es el reconocimiento automático: como hemos visto, en 2024 la NGA lanza el programa Sequoia de etiquetado de datos, valorado hasta 708 millones de dólares en siete años —su contrato de datos mayor de la historia— para entrenar la visión por computador (Maven) sobre imágenes de satélite [8]. Cuanto más dependen las decisiones automáticas de la imagen, más caro es que esta mienta.

El tercer frente es el estándar de confianza. La UE ha levantado su Programa Espacial (Reglamento 2021/696, 14.800 millones de euros para 2021-2027) y la agencia EUSPA, encargada de la seguridad de Copernicus, Galileo y EGNOS. El Open Geospatial Consortium publicó en abril de 2025 una iniciativa anual de Integridad, Procedencia y Confianza (IPT) que define la integridad (el manejo a lo largo del ciclo de vida), la procedencia (el origen y quién ha modificado los datos) y la confianza (bien documentada, consistente, inalterable) para los datos geoespaciales [9]. Es el marco conceptual que faltaba, pero tiene un vacío decisivo.

Por qué el marco IPT solo no salva

Hay que decirlo con crudeza. La iniciativa IPT del OGC define magníficamente qué queremos decir con integridad y procedencia, pero se basa en estándares de metadatos, no en firma criptográfica ni cadena de bloques [9]. Un metadato es tan fiable como el sistema que lo custodia: un campo de procedencia en un archivo se puede reescribir, antedatar o suavizar después de una disputa, sin dejar ninguna huella independiente. Lo mismo pasa con las otras capas: el C2PA —las Content Credentials que la guía conjunta de la NSA, la ODNI y la CISA del 29 de enero de 2025 recomienda para la integridad de la imagen— firma la procedencia si se aplica en el momento de la captura, pero no dice nada si el forjador sella su propia falsificación. Y los detectores de Vision Transformer, por buenos que sean, dan una probabilidad, no una prueba fechada: su 95 % de acierto quiere decir que uno de cada veinte forjados pasa, y que cada nueva generación de difusión los obliga a reentrenarse. Ninguna de estas capas fija, de manera inalterable e independiente, quién entregó qué píxeles y cuándo. Falta la cadena de custodia.

La prueba de existencia aplicada

Aquí es donde **t2p** aporta la capa que falta, y lo hace sobre el artefacto digital —la escena— en el punto más temprano defendible de la cadena. El artefacto sellado es **la escena de satélite cruda o de nivel L1** más los metadatos portadores (identificador de sensor, órbita/efemérides, hora de recepción en la estación de tierra, proyección y parámetros de procesamiento). Hay dos anclajes complementarios. **Primero**, en el *ingest* de la estación de tierra: el operador (Maxar, Planet, el segmento de tierra de Copernicus de la ESA) calcula la **huella SHA-512** de la escena entregada sobre el sistema receptor —el archivo no sale de allí—, obtiene un **sello de tiempo RFC 3161** conforme a eIDAS, ancla la huella en la cadena pública y emite un contenedor **.asice** verificable sin conexión que viaja con cada tesela e informe derivados. **Segundo**, en el extremo del analista, periodista o investigador —un equipo OSINT geolocalizando los fotogramas de Bucha o de Xinjiang—: el recorte concreto, la capa de anotación y las coordenadas GPS y la hora de adquisición afirmadas se vuelven a sellar, con **GPS forense** ligando cualquier captura de campo que lo corrobore y una **prueba de vida** cuando una persona verifica un lugar sobre el terreno.

El sello fija qué píxeles existieron, de qué sensor, en qué instante UTC, atribuidos a qué operador o analista. Así, una escena forjada o generada por difusión más tarde no se puede hacer pasar por la original, y un tribunal —o un auditor de carbono MRV— puede demostrar que la imagen entró en el registro antes de cualquier disputa. Complementa, no sustituye: la procedencia del IPT del OGC, la autenticación de posición de Galileo OSNMA, las Content Credentials del C2PA de los capítulos 13 y 15, y los detectores de deepfake de Vision Transformer —aportando la capa de custodia a prueba de manipulación que todos ellos no tienen.

Ahora el límite, con toda la crudeza. «Basura a la entrada, basura en la cadena»: el sello prueba el origen, el instante exacto, la autoría y la integridad bit a bit de una escena; no prueba que la escena muestre lo que se afirma, que el sensor estuviera bien calibrado, que la nube, la sombra, el ángulo fuera de nadir o la resolución no engañen, ni que la geolocalización sea correcta. Si un forjador genera una central nuclear falsa con Stable Diffusion —o una escena de deforestación adulterada— y sella eso, el sello fechará fielmente una mentira: solo fija que esa imagen exacta existió en ese momento, firmada por ese firmante, no que sea observación auténtica de la Tierra. No puede autenticar de manera retroactiva una imagen sellada solo después de manipularla, no detiene la interferencia del GNSS, ni dictamina si un puente, una fosa común o un bosque arrasado son reales. Detectar píxeles sintéticos sigue exigiendo clasificadores forenses y juicio experto; el carbono MRV, inventarios a pie de tierra; el uso para crímenes de guerra, corroboración sobre el terreno y evaluación judicial. El sello refuerza la cadena de custodia; nunca sustituye la verificación de la verdad del contenido.

La promesa y el peligro

La promesa es un registro de la observación de la Tierra donde cada escena arrastra un **recibo inalterable** de su origen, hora y autor —de modo que el negador de Bucha ya no pueda alegar «escenificación» sobre una imagen fechada criptográficamente semanas antes, y el auditor de carbono o el fiscal puedan demostrar que la prueba es anterior a la disputa. En un mundo donde el ojo en el cielo puede mentir, hacer el origen inalterable protege tanto a la víctima como al verificador honesto.

El peligro pide los matices de siempre. El primero, no confundir **integridad con verdad**: una escena forjada y sellada en el momento de forjarla sigue siendo falsa, y ahora, además, lleva un sello que puede dar una falsa tranquilidad —«está anclado, luego es real»— que no se corresponde con nada. El segundo, la **concentración de poder**: si solo un puñado de operadores comerciales y agencias estatales pueden sellar en la estación de tierra, el estándar puede consolidar quién controla la verdad orbital y dejar fuera al investigador independiente. Y el tercero, el uso **autoritario**: la misma cadena que da peso probatorio a la imagen de Xinjiang puede dar peso a la vigilancia; la integridad de la imagen no juzga su uso legítimo. La prueba de existencia es una capa de custodia, no un certificado de autenticidad ni un sustituto del juicio experto que sabe leer un fotograma.

Es hora de actuar

Para los **operadores de satélite** (Maxar, Planet, el segmento de tierra de la ESA Copernicus): sellar la escena cruda o L1 en el ingest de la estación de tierra —huella SHA-512, sello eIDAS, anclaje en la blockchain pública, contenedor .asice— para que cada tesela derivada arrastre una procedencia inalterable desde el minuto cero. Para los **investigadores OSINT, periodistas y ONG de derechos humanos** (quienes geolocalizaron Bucha y Xinjiang): volver a sellar el recorte, la anotación y las coordenadas afirmadas, con GPS forense y prueba de vida cuando haya captura de campo. Para los **organismos de estándares** (OGC, dentro de la iniciativa IPT): añadir la firma criptográfica y el anclaje inalterable a la capa de metadatos, llenando el vacío que hoy deja el IPT. Para los **estados y agencias** (EUSPA, NGA, el programa Galileo OSNMA): combinar la autenticación de la señal de posición con el sellado de la imagen, para que el cuándo y el dónde y los píxeles se defiendan juntos. Y para los **tribunales y auditores de MRV** (la CPI, los verificadores de carbono): reconocer el sello fechado como la cadena de custodia que distingue una prueba anterior a la disputa de una imagen presentada después —sin olvidar nunca que el sello no decide si lo que se ve es real.

En Bucha, el ojo en el cielo había fechado el crimen semanas antes de que el negador pudiera inventarse la coartada. Dar a cada escena de satélite una prueba sellada de su origen, hora y autor —sin olvidar que el sello fija la existencia, no la verdad de lo que muestra— es, en este frente donde el testigo orbital es a la vez nuestra mejor prueba y un nuevo objetivo de falsificación, time2act.

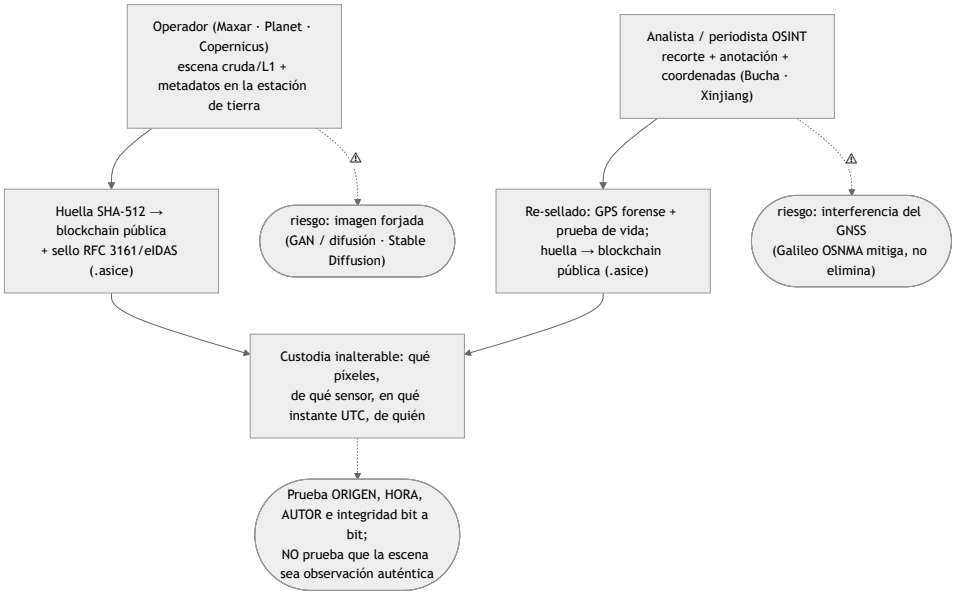


Figura 104.1 — La cadena de la observación de la Tierra en dos eslabones de sellado. En el origen, el operador (Maxar, Planet, Copernicus) calcula la huella SHA-512 de la escena cruda/L1 más los metadatos en el ingest de la estación de tierra, con sello RFC 3161/eIDAS anclado en la blockchain pública (.asice). En el otro extremo, el analista o periodista OSINT vuelve a sellar el recorte, la anotación y las coordenadas, con GPS forense y prueba de vida. Puntos de riesgo: imagen forjada con GAN/difusión (Stable Diffusion, StyleGAN2) e interferencia del GNSS, que la firma de Galileo OSNMA y los detectores de Vision Transformer mitigan pero no eliminan. Límite: el sello prueba origen, hora, autor e integridad bit a bit; no prueba que la escena sea observación auténtica ni que la interpretación sea correcta. Fuentes: caso Bucha (Maxar); Bo Zhao (geografía deepfake); Xinjiang (BuzzFeed); arXiv 2511.17766; Galileo OSNMA; OGC IPT.

---

[1] University of Washington — *A growing problem of 'deepfake geography': How AI falsifies satellite images* (21 de abril de 2021; Bo Zhao acuña «geografía deepfake» en *Cartography and Geographic Information Science*; conjunto de 8.064 imágenes; amenaza para la seguridad nacional). https://www.washington.edu/news/2021/04/21/a-growing-problem-of-deepfake-geography-how-ai-falsifies-satellite-images/ ↩

[2] The Moscow Times — *Satellite Images Show Bodies in Bucha for Weeks, Rebutting Moscow Claim* (5 de abril de 2022; nueve imágenes de Maxar del 18/19/31 de marzo; cuerpos en la calle Yablónska; fosa común de 14 metros). https://www.themoscowtimes.com/2022/04/05/satellite-images-show-bodies-in-bucha-for-weeks-rebutting-moscow-claim-a77211 ↩

[3] Aerospace America / AIAA — *Maxar describes its role in Bucha revelations* (captura del WorldView-3; Daniel Jablonsky sobre la recogida intensiva de Maxar; uso del New York Times el 4 de abril de 2022). https://aerospaceamerica.aiaa.org/maxar-bucha-insights/ ↩

[4] BuzzFeed News — *Blanked-Out Spots On China's Maps Helped Us Uncover Xinjiang's Camps* (método ganador de un Pulitzer; imagen de Planet y teselas censuradas; 268 campos nuevos y 428 emplazamientos sospechosos). https://www.buzzfeednews.com/article/alison_killing/satellite-images-investigation-xinjiang-detention-camps ↩

[5] *Deepfake Geography: Detecting AI-Generated Satellite Images* (arXiv 2511.17766, noviembre de 2025; ViT 95,11 % frente a CNN 87,02 % sobre más de 130.000 imágenes; artefactos GAN frente a difusión). https://arxiv.org/abs/2511.17766 ↩

[6] *Generating Synthetic Satellite Imagery With Deep-Learning Text-to-Image Models* (arXiv 2404.07754, abril de 2024; Nguyen, Glaser y Biessmann; imagen sintética fotorrealista de instalaciones incluidas centrales nucleares; control de armamento). https://arxiv.org/abs/2404.07754 ↩

[7] Comisión Europea — *Observer: How Galileo OSNMA helps counter GNSS spoofing* (OSNMA operativo el 24 de julio de 2025; primera autenticación mundial de la señal del Servicio Abierto de un GNSS vía firmas criptográficas TESLA). https://defence-industry-space.ec.europa.eu/observer-how-galileo-osnma-helps-counter-gnss-spoofing-2025-09-08_en ↩

[8] SpaceNews — *NGA to launch $700 million program to help AI make sense of satellite images* (contrato de etiquetado Sequoia de hasta 708 M$ en 7 años, 2024; alimenta la visión por computador Maven; el contrato de datos mayor de la agencia). https://spacenews.com/nga-to-launch-700-million-program-to-help-ai-make-sense-of-satellite-images/ ↩

[9] Open Geospatial Consortium — *Navigating Synthetic Imagery Trust in Geospatial Data* (iniciativa Integridad, Procedencia y Confianza, abril de 2025; define integridad/procedencia/confianza, pero sin firma criptográfica ni cadena de bloques). https://www.ogc.org/blog-article/navigating-synthetic-imagery-trust-geospatial-data/ ↩

[10] NSA/ODNI/CISA — *Content Credentials: Strengthening Multimedia Integrity in the Generative AI Era* (29 de enero de 2025; guía conjunta que apoya la firma de procedencia C2PA para la integridad de la imagen, aplicable a la observación de la Tierra). https://media.defense.gov/2025/Jan/29/2003634788/-1/-1/0/CSI-CONTENT-CREDENTIALS.PDF

Protección civil y emergencias: quién sabía qué, y cuándo

«Pero si el centinela ve venir la espada y no toca la trompeta, y el pueblo no es advertido [...] demandaré cuentas de su sangre a la mano del centinela.»

— Ezequiel 33,6

La tarde del 29 de octubre de 2024, la estación de aforo de la rambla del Poyo, al suroeste de Valencia, envió sus últimos datos. A las 16:13, un correo de la Confederación Hidrográfica del Júcar (CHJ) a Emergencias informaba de un caudal de 28,7 metros cúbicos por segundo: parecía que aquello remitía [5]. A las 17:00, el caudal era ya de 325,52; a las 17:40, la propia CHJ registraba en el Poyo un caudal cinco veces superior al del Ebro [6]; a las 18:00, la serie marcaba 1.725,89 [5]. A las 18:43, otro correo avisaba: 1.686 metros cúbicos por segundo y riesgo elevado [5]. A las 18:55, el sensor marcó 2.282. Hacia las 19:00, la fuerza del agua arrastró y destruyó la propia estación [5]. Y la alerta ES-Alert no sonó en los móviles hasta las 20:11, cuando los barrancos ya se habían llevado calles enteras [1]. El balance: 229 muertos en la provincia de Valencia y 237 en toda España, más de 2.600 heridos, unos 141.000 vehículos y 11.242 viviendas afectadas, 800 kilómetros de carreteras dañadas [4], unas pérdidas estimadas de 17.800 millones de euros [3].

Este capítulo aborda la protección civil y las emergencias: riadas, incendios, aludes, el estado de las carreteras y las alertas a la población. La verdad de las comunicaciones oficiales en general se trata en el capítulo 86; el testigo orbital de los satélites, en el capítulo 104; los sensores industriales, en el capítulo 96; la reclamación de seguros ordinaria, en el capítulo 28. La pregunta que vertebra las páginas siguientes es otra: ¿cómo se reconstruye, de modo que nadie la pueda discutir, la cronología de una emergencia? Porque después de cada catástrofe empieza una segunda batalla —judicial, política y aseguradora— que siempre gira sobre lo mismo: quién sabía qué, y cuándo. La respuesta de este libro es sellar cada dato en origen con **t2p**: la huella SHA-512 calculada en el dispositivo o en la fuente, el sello de tiempo RFC 3161/eIDAS y el anclaje en la blockchain pública, dentro de un contenedor .asice, tal como hemos visto en los capítulos 13 y 15 [23]. Una prueba de existencia así es neutral por construcción: puede exculpar a una administración o incriminarla, blindar al ciudadano ante la aseguradora y desarmar bulos. No tiene bando. Por eso sirve.

La cronología como campo de batalla

Reconstruyamos las cinco horas decisivas con lo que se sabe. El CECOPI —el órgano que coordina la emergencia— se convocó a las 15:00 y se reunió a las 17:00; pasadas las 18:00, el presidente de la Confederación planteó la posibilidad de enviar alertas masivas a los móviles [2]. La primera ES-Alert salió a las 20:11, y una segunda, a las 21:03; en una emergencia de nivel 2, la gestión y la petición de envío corresponden a la comunidad autónoma [1]. Entre la propuesta y el sonido en los teléfonos pasaron unas dos horas; entre el correo del riesgo elevado y la alerta, casi una hora y media. Sobre esos minutos se ha construido desde entonces una batalla de versiones que ha ocupado portadas, comparecencias y declaraciones cruzadas.

Y una instrucción judicial. Desde el 10 de marzo de 2025, el Juzgado de Instrucción número 3 de Catarroja, con la jueza Nuria Ruiz Tobarra al frente, investiga a la exconsellera Salomé Pradas y al exsecretario autonómico de Emergencias Emilio Argüeso por presuntas omisiones graves en la gestión de aquella tarde [9]. La Audiencia de Valencia confirmó la imputación de Argüeso; el Tribunal Superior de Justicia valenciano rechazó investigar al expresidente Mazón; en marzo de 2026, la causa aún «afrontaba la recta final» [10]. Más de quinientos días para fijar una cronología de cinco horas.

La ironía central del caso merece detenerse en ella. La jueza tuvo que requerir a À Punt «todas las grabaciones de imagen y sonido» de la reunión del CECOPI, y reclamar los vídeos originales a la productora —contratada, precisamente, por la propia secretaría de Emergencias— para poder «determinar la hora exacta de cada vídeo» [11]. Un año después de la riada, el instrumento central de la instrucción era un puñado de archivos cuya fecha nadie podía acreditar. Este es exactamente el problema que resuelve la prueba de existencia: si cada acta, cada vídeo y cada orden se hubiera sellado en el momento de crearse, la cronología sería hoy un hecho verificable en cuestión de horas, no una hipótesis procesal que consume años. Y conviene subrayarlo: el sello no prejuzga nada ni señala a nadie por adelantado. Solo fija el reloj —para todos.

Datos que desaparecen cuando más importan

El sensor del Poyo murió trabajando: según el comunicado de la CHJ del 4 de noviembre, la fuerza del agua arrastró los sistemas de medida hacia las 19:00, después de dos horas reflejando la crecida [5]. Hasta aquí, la fragilidad física. Lo que pasó después ilustra una fragilidad peor: la del propio dato. A primeros de noviembre, en medio de la batalla de versiones, los datos del Poyo desaparecieron de la web pública de la CHJ, y reaparecieron días más tarde; la prensa lo llamó «el apagón informativo» [7]. Y las revelaciones posteriores añadieron inquietud: barrancos clave que no formaban parte de la red de control y un medidor en Massanassa que no se mostraba públicamente [8].

No hace falta ninguna conspiración para que un dato crítico se desvanezca. Basta con un servidor que se reinicia, una web «en mantenimiento» o un funcionario asustado. Pero el efecto es siempre el mismo: la ciudadanía pierde la capacidad de distinguir entre el error, la negligencia y la ocultación, y el vacío lo llena la sospecha. En plena crisis, cuando la confianza es el único recurso que no se puede improvisar, cada dato que desaparece erosiona todos los que quedan.

La solución estructural es anclar la telemetría en origen. Si cada lectura del Sistema Automático de Información Hidrológica (SAIH) se convierte, al nacer, en una huella SHA-512 con sello de tiempo anclado en la blockchain pública [23], borrarla de la web ya no la hace desaparecer: la existencia y el contenido quedan acreditados para siempre, y cualquier ciudadano puede verificar que la serie publicada coincide con la sellada. Incluso los huecos se vuelven probables: lo que no se midió tampoco se puede maquillar a posteriori, porque la ausencia de huellas fechadas es, en sí misma, un hecho demostrable [8]. La confianza deja de depender de la buena fe del organismo y pasa a depender de la matemática. El sensor del Poyo murió enviando datos; el registro de lo que envió no debería poder morir nunca.

La mentira durante la emergencia

Los días posteriores a la riada, el aparcamiento inundado del centro comercial Bonaire, en Aldaia, se convirtió en el epicentro de una teoría de la conspiración: «nos ocultan los muertos». Vídeos de otros aparcamientos presentados como si fueran de Bonaire; camiones frigoríficos y coches fúnebres descontextualizados como presuntos traslados de cadáveres; una falsa acta municipal que hablaba de «más de 220 cadáveres» sacados el primer día; documentos falsos que elevaban el total por encima de las 800 víctimas. Cuando la investigación oficial terminó, la conclusión fue rotunda: ninguna víctima mortal en el aparcamiento [12]. Daba igual: la maquinaria ya giraba. Newtral desmintió más de 60 bulos sobre la DANA solo durante el primer mes [13], con la IA generativa como principal facilitador —imágenes y vídeos verosímiles a partir de un texto, voces clonadas con pocos segundos de audio—; y aquella marea de falsedades llegó a generar problemas de orden público y a interferir en las tareas de los equipos de emergencia [14].

En una emergencia, la duda mata dos veces: cuando el ciudadano no cree la alerta oficial, y cuando cree el bulo. La crisis de la verdad que describimos en el capítulo 10 tiene aquí su versión más letal, porque el tiempo de reacción se mide en minutos y no hay margen para la verificación artesanal.

La prueba de existencia no detecta mentiras —no es un detector de bulos— pero permite la estrategia inversa: que toda pieza oficial nazca sellada. Fotos de drones, comunicados, órdenes de evacuación, balances: si cada elemento lleva la huella y la fecha ancladas desde el origen, cualquier persona, medio o verificador puede comprobar su autenticidad sin depender de nadie, y lo que circula sin sello queda automáticamente bajo sospecha. El «dividendo del mentiroso» —despachar la prueba incómoda como falsa— se desactiva cuando la prueba lleva anclaje criptográfico: el responsable que querría negar un retraso ya no puede decir que el registro es un montaje, y el conspiracionista que agita un «acta» apócrifa choca con un ecosistema donde los documentos auténticos se reconocen por la huella. La verdad oficial se vuelve comprobable; la mentira, huérfana de sello.

Fuegos, nieve y asfalto: el patrón se repite

En agosto de 2025, España vivió la peor oleada de incendios forestales en más de treinta años: cerca de 400.000 hectáreas quemadas hasta el 19 de agosto, con una veintena de grandes incendios declarados en dos semanas [17][18]. Ourense, con unas 150.000 hectáreas —una séptima parte de la provincia—, León y Zamora concentraron cerca de la mitad de la superficie quemada; el fuego de Uña de Quintana arrasó unas 40.000 hectáreas y el de A Rúa, más de 38.000; en Molezuelas de la Carballeda, más de 700

personas tuvieron que ser evacuadas, y el Gobierno desplegó 500 militares adicionales de la UME sobre los más de 1.400 ya activos [17]. Cuando el humo se disipó, empezó la pregunta de siempre, la misma de la DANA pero con fuego: ¿se avisó a tiempo a aquel pueblo? Cada orden de evacuación, cada corte de carretera y cada parte de medios desplegados es un documento fechado que después se discutirá.

La nieve repite el patrón en silencio. El Centro de Lauegi de Arán publica cada día el boletín de peligro de aludes a partir de salidas al terreno y tests del manto, complementado con la cartografía ATES de exposición del terreno, y advierte que esta información «no sustituye la formación, la experiencia y el buen juicio» [19]; el ICGC cubre el Pirineo catalán y la AEMET, el resto de macizos [20]. Cuando hay un accidente, la pregunta —de aseguradoras, familias y, si procede, juzgados— es siempre la misma: ¿qué nivel de peligro estaba publicado cuando el grupo salió? Un boletín sellado al publicarse hace la respuesta indiscutible, y protege a todos a la vez: el predictor puede acreditar qué publicó y cuándo; la víctima y los suyos, sobre qué información se tomó la decisión.

Y el asfalto. El artículo 106.2 de la Constitución y la Ley 40/2015 obligan a la Administración a indemnizar los daños causados por el funcionamiento de los servicios públicos: un accidente por mal estado de la vía es indemnizable si hay nexo causal y no interviene fuerza mayor, el atestado de la Guardia Civil es la pieza probatoria central, y el silencio administrativo de seis meses aboca al ciudadano al contencioso [22]. Registros de mantenimiento, inspecciones y cortes de carretera sellados en origen zanjan la discusión por los dos lados: la Administración diligente puede probar que actuó; el conductor, que el bache estaba allí. En los tres escenarios —fuegos, nieve, asfalto— la constante es la misma que en Valencia: la segunda batalla se gana o se pierde según quién pueda acreditar sus fechas.

La prueba de existencia aplicada

Imaginemos un centro de coordinación de emergencias, el próximo octubre. Nada ha cambiado a la vista: las mismas pantallas, las mismas llamadas. Pero cada acta, cada correo del SAIH, cada orden y cada alerta se va sellando a medida que se produce, sin ningún esfuerzo añadido para los operadores: la huella SHA-512 se calcula en la fuente, recibe el sello de tiempo RFC 3161/eIDAS y se ancla en la blockchain pública dentro de un contenedor .asice [23]. La cadena de custodia se construye sola, mientras todos hacen su trabajo.

1. El registro de la decisión

El órgano de coordinación de una emergencia —el CECOPI valenciano o cualquier otro— produce actas, vídeos y órdenes que dirigen la respuesta. Sellados en el momento de crearse, se convierten en una cronología no repudiable: si el envío de una alerta se plantea pasadas las 18:00 y se ejecuta a las 20:11 [1] [2], el registro lo acredita sin requerimientos judiciales a televisiones ni a productoras [11], y una instrucción que hoy consume años [9][10] se reduce en buena parte a verificar huellas. La neutralidad es la clave de bóveda: el mismo sello que puede evidenciar la lentitud de un responsable acredita la diligencia de quien actuó bien. Las autoridades pueden demostrar que decidieron a tiempo; la ciudadanía dispone de una base verificable para exigir responsabilidades cuando no fue así.

2. El sensor que no puede desaparecer

Las lecturas del SAIH —como la secuencia del Poyo: 28,7, 325,52, 1.725,89, 2.282 metros cúbicos por segundo [5]— se anclan en origen, por lotes y en tiempo real. Ni un «apagón informativo» en la web [7] ni la destrucción física de la estación [5] borran el registro: la huella acredita qué se midió y cuándo, y los huecos de la serie quedan igualmente fechados. La red de control se vuelve auditable desde fuera [8]: cualquier persona con el archivo de datos puede comprobar que coincide, bit a bit, con lo que se selló aquel día. La discusión sobre «qué datos había» se acaba antes de empezar.

3. La foto del ciudadano

El Consorcio de Compensación de Seguros ha pagado por la DANA 212.237 siniestros por un importe de 4.378 millones de euros, con un coste total estimado de unos 4.800 millones (datos de marzo de 2026) [15][16]. Cada expediente empieza con el mismo material frágil: fotos y vídeos del coche sumergido, del bajo inundado, de la cosecha perdida. Una foto sellada en el dispositivo en el momento de hacerla —la huella con la fecha, sin que la imagen tenga que salir del teléfono [23]— acelera el peritaje, blinda al ciudadano honesto ante la sospecha y deja sin margen el fraude de quien recicla fotos de otra riada: sin sello coherente con la fecha del siniestro, la imagen reciclada no se sostiene. La escala lo hace decisivo:

251.249 expedientes de golpe [16], un alud administrativo que distingue la emergencia del flujo ordinario de seguros que hemos visto en el capítulo 28.

4. El boletín y la carretera

El boletín de peligro de aludes [19][20], la orden de evacuación de un pueblo amenazado por el fuego [17], el corte preventivo de una vía o el registro de mantenimiento de una carretera [22] comparten una misma naturaleza: son documentos públicos cuyo valor probatorio depende de que nadie pueda discutir su hora de publicación. Sellados al publicarse, protegen a la vez al técnico que avisó, al conductor que reclama y a la familia que quiere saber si el aviso llegó a tiempo. La fecha cierta no tiene bando: es de quien la necesita.

Hay que decir con la misma claridad lo que el sello no hace: no predice riadas, no apaga fuegos, no hace sonar ninguna sirena; no detecta bulos ni impide crearlos. Solo hace indiscutible qué existía y cuándo. Es infraestructura de prueba, no sustituto de la inversión en prevención.

La promesa y el peligro

La promesa es una emergencia con todos los datos críticos sellados en origen: sensores, actas, alertas, órdenes, fotos. La reconstrucción posterior se haría en horas y no en años [9][10][11]; el Consorcio podría tramitar los aludes de expedientes sobre pruebas no repudiables, con peritajes más cortos y menos fraude [16]; y el bulo perdería fuerza porque todo lo oficial sería verificable por cualquiera [12][13]. La segunda batalla —la de las versiones— quedaría desactivada antes de empezar.

Los peligros exigen la misma franqueza.

El primero es la **vigilancia**. Sellar la recepción de alertas o las fotos de los ciudadanos no puede convertirse nunca en un rastro centralizado de dónde estaba cada uno. El diseño debe ser el del libro: las huellas se generan y se custodian en el dispositivo de cada persona; ningún contenido ni ninguna ubicación viaja a ningún registro central, y el sistema no puede servir para desanonimizar a nadie [23].

El segundo es la **administración defensiva**. Si el sello se convierte en escudo burocrático, el funcionario puede acabar dedicando más energía a «quedar cubierto» que a decidir bien. La cultura del paraguas ya existe; la criptografía no debe amplificarla. El sello documenta la acción: no la sustituye ni la exime.

El tercero es la **revocabilidad**. Las huellas de las fotos personales de daños deben poder invalidarse a petición del ciudadano. La inmutabilidad es para el dato público —el caudal, el acta, la orden—, no para la vida privada de las víctimas, que conservan el derecho al olvido.

Y el cuarto es el **tecnosolucionismo**. Ninguna cadena de bloques salva vidas. Salvan vidas las sirenas, los planes de emergencia ensayados, los barrancos limpios, la cultura de autoprotección y, sobre todo, la decisión tomada a tiempo [2]. El sello garantiza solo que, después, la verdad sea indestructible. Pero eso, bien entendido, también es prevención: quien sabe que su inacción quedará acreditada para siempre tiene un incentivo poderoso para actuar.

Es hora de actuar

La DANA de Valencia dejó 229 muertos [4], una instrucción judicial que cuenta los días por centenares [10] y una lección que ningún país debería necesitar aprender dos veces: la verdad de una emergencia es demasiado importante para confiarla a la memoria de las reuniones, a las webs que «se mantienen» y a los vídeos sin hora.

Para las administraciones de protección civil y los centros 112: sellad en origen actas, órdenes y alertas. El ES-Alert —nacido del artículo 110 de la Directiva europea 2018/1972, transpuesta por la Ley 11/2022, y operativo desde 2022-2023 [21]— ya llega a todos los móviles; haced que la cronología de la próxima emergencia sea un hecho verificable desde el primer minuto, y no una investigación de años [9] [10].

Para las confederaciones hidrográficas y los operadores de sensores: anclad cada lectura del SAIH en tiempo real, que ningún «apagón informativo» [7] vuelva a ser posible y que incluso los huecos de medida queden acreditados [8].

Para las aseguradoras y el Consorcio: aceptad y priorizad la foto sellada en el dispositivo. Ante 251.249 expedientes de golpe [16], la prueba no repudiable es peritaje más rápido, menos fraude y más respeto por el asegurado honesto.

Para los medios y los verificadores: exigid y comprobad el sello del material oficial de emergencia, y tratad con cautela por defecto lo que circule sin anclaje [12][13].

Para ti, ciudadano: documenta los daños con la huella en el dispositivo, y recuerda que el sello no sustituye la alerta: cuando suene el móvil [1], deja el coche y sube al piso de arriba.

Para los legisladores: reconoced valor probatorio pleno al registro sellado de emergencias e imponedlo como estándar de la Red de Alerta Nacional [21].

El sensor del Poyo murió a las 19:00 enviando la verdad [5]. Que nunca más ninguna verdad de emergencia dependa de la supervivencia de un aparato ni de la memoria de una reunión. En este frente, time2act.

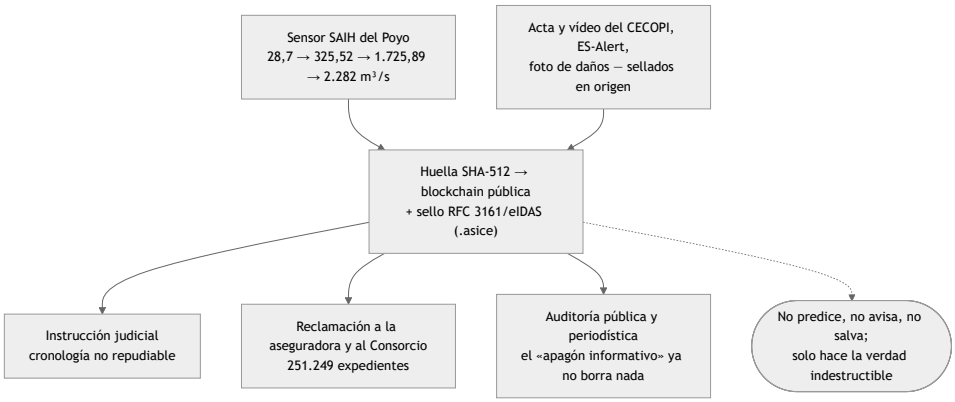


Figura 105.1 — El dato de emergencia se sella en origen: la lectura del sensor (SAIH/Poyo), el acta y el vídeo del órgano de coordinación (CECOPI), la alerta (ES-Alert), la orden de evacuación y la foto de daños del ciudadano reciben la huella SHA-512 en el dispositivo o en la fuente, el sello de tiempo RFC 3161/eIDAS y el anclaje en la blockchain pública (.asice). Tres salidas: la instrucción judicial (cronología no repudiable), la reclamación a la aseguradora y al Consorcio, y la auditoría pública y periodística. Límite: el sello no predice, no avisa y no salva; solo hace la verdad indestructible. Fuentes: Maldita.es; CHJ/SAIH; Consorcio de Compensación de Seguros; Lauegi.

---

[1] Maldita.es — *Quién envió la alerta de las 20:11 horas en Valencia, qué dice el protocolo* (31 de octubre de 2024; ES-Alert a las 20:11 y 21:03; en nivel 2 la petición corresponde a la comunidad autónoma). https://maldita.es/malditateexplica/20241031/generalitat-valenciana-responsable-alerta-movil/ ↩

[2] elDiario.es — *El envío de la alerta masiva a móviles se planteó en la reunión clave de la DANA pasadas las 18.00, dos horas antes* (CECOPI convocado a las 15:00, reunido a las 17:00; propuesta de alerta masiva pasadas las 18:00). https://www.eldiario.es/comunitat-valenciana/reunion-clave-dana-debatio-enviar-alerta-masiva-moviles-pasadas-18-00-horas_1_11802363.html ↩

[3] France 24 — *En cifras: 229 muertos y 17.800 millones de euros en pérdidas, a un año de la DANA* (28 de octubre de 2025). https://www.france24.com/es/europa/20251028-en-cifras-229-muertos-y-17-800-millones-de-euros-en-p%C3%A9rdidas-a-un-a%C3%B1o-de-la-dana ↩

[4] Wikipedia — *Inundaciones de la DANA de 2024 en España* (237 muertos en total: 229 en la provincia de Valencia, 7 en Castilla-La Mancha, 1 en Málaga; más de 2.600 heridos; 11.242 viviendas; ≈141.000 vehículos; 800 km de carreteras). https://es.wikipedia.org/wiki/Inundaciones_de_la_DANA_de_2024_en_Espa%C3%B1a ↩

[5] Maldita.es — *Qué sabemos de los datos de la riada en la Rambla del Poyo durante la DANA* (7 de noviembre de 2024; correos de la CHJ de las 13:42, 15:04, 16:13 y 18:43; caudales de las 17:00 y las 18:00; 2.282 m³/s a las 18:55; la estación de aforo, destruida por el agua hacia las 19:00, según el comunicado de la CHJ del 4 de noviembre). https://maldita.es/clima/20241107/datos-rambla-poyo-dana-valencia/ ↩

[6] El Debate — *«A las 17.40 del día de la dana la CHJ registró que el caudal del barranco del Poyo era cinco veces superior al del Ebro»* (24 de febrero de 2026). https://www.eldebate.com/espana/comunidad-valenciana/20260224/1740-dia-dana-chj-registro-caudal-barranco-poyo-cinco-veces-superior-ebro_388667.html ↩

[7] El Debate — *La Confederación del Júcar borra datos críticos del caudal del Poyo en plena crisis de la DANA* (5 de noviembre de 2024); esDiario — *Desaparecen y reaparecen los datos del barranco del Poyo de la web de la CHJ*. https://www.eldebate.com/espana/comunidad-valenciana/20241105/confederacion-jucar-borra-datos-criticos-caudal-poyo-plena-crisis-dana-valencia_242165.html · https://www.esdiario.com/comunidad-valenciana/241105/146265/desparecen-aparecen-datos-barranco-poyo-web-chj.html ↩

[8] Actualidad Valencia — *La CHJ omitió barrancos clave en su red de control y ocultó un medidor en Massanassa, según revela el SAIH*. https://actualidadvalencia.com/control-caudal-chj-barrancos-horteta-gallego-massanassa/ ↩

[9] ORM — *La jueza de Catarroja llama a declarar como investigados en la causa por la DANA a Salomé Pradas y Emilio Argüeso* (instrucción abierta el 10 de marzo de 2025; Juzgado de Instrucción n.º 3 de Catarroja, jueza Nuria Ruiz Tobarra). https://www.orm.es/informativos/la-jueza-de-catarroja-llama-a-declarar-como-investigados-en-la-causa-por-la-dana-a-salome-pradas-y-emilio-arg-eso/ ↩

[10] El Independiente — *La causa de la DANA afronta su recta final tras el varapalo del TSJ a la jueza de Catarroja* (17 de marzo de 2026; el TSJ rechaza investigar a Mazón). https://www.elindependiente.com/espana/2026/03/17/causa-dana-afronta-recta-final-varapalo-tsj-jueza-catarroja/ ↩

[11] The Objective — *La jueza de la dana une a la causa los vídeos del Cecopi y pide a À Punt la hora de cada uno* (2 de octubre de 2025); El Español — *La jueza requiere a À Punt «todas las grabaciones de imagen y sonido» de la reunión del Cecopi* (los vídeos, de una productora contratada por la secretaría de Emergencias; se piden los originales para fijar la hora exacta de cada uno). https://theobjective.com/espana/tribunales/2025-10-02/jueza-dana-videos-cecopi-punt-hora/ · https://www.elespanol.com/valencia/20250919/jueza-dana-requiere-punt-todas-grabaciones-imagen-sonido-reunion-cecopi-octubre/1003743931870_0.amp.html ↩

[12] Maldita.es — *«Nos están ocultando los muertos» del parking de Bonaire (Aldaia): un año después, cómo funcionó la maquinaria de la desinformación* (29 de octubre de 2025; falsa acta municipal de «más de 220 cadáveres»; documentos falsos con más de 800 víctimas; ninguna víctima mortal en el aparcamiento). https://maldita.es/malditobulo/20251029/teoria-conspiracion-muertos-bonaire/ ↩

[13] Newtral — *Un mes y más de 60 bulos desmentidos: la desinformación surgida a raíz de la dana* (29 de noviembre de 2024). https://www.newtral.es/desinformacion-dana/20241129/ ↩

[14] COPE — *Quién está detrás de la creación de bulos de la DANA y qué herramientas digitales han usado* (la IA generativa como principal facilitador); elDiario.es — *Los bulos y falsedades sobre la DANA de València* (interferencia en las tareas de emergencia). https://www.cope.es/programas/la-linterna/audios/detras-creacion-bulos-dana-valencia-herramientas-digitales-han-usado-20241117_3046424.html · https://www.eldiario.es/comunitat-valenciana/bulos-falsedades-dana-valencia-cientos-cadaveres-bonaire-demolicion-pantanos_1_11791455.html ↩

[15] La Moncloa — *El Consorcio de Compensación de Seguros supera los 4.000 millones en pagos por indemnizaciones a afectados por la DANA* (26 de noviembre de 2025; 210.106 indemnizaciones). https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/economia-comercio-empresa/paginas/2025/261125-indemnizacion-dana.aspx ↩

[16] SegurosNews — *El Consorcio ya ha pagado 4.378 millones por la DANA de Valencia* (27 de marzo de 2026; 212.237 siniestros pagados; 251.249 expedientes; el 99,3 % tramitados; coste total estimado ≈4.800 M€). https://segurosnews.com/news/el-consorcio-ya-ha-pagado-4-378-millones-por-la-dana-de-valencia ↩

[17] Wikipedia — *Incendios forestales de España de 2025* (≈400.000 ha hasta el 19 de agosto; Ourense ≈150.000 ha; Uña de Quintana ≈40.000 ha; A Rúa >38.000 ha; Molezuelas de la Carballeda, más de 700 evacuados; 500 militares adicionales de la UME sobre más de 1.400). https://es.wikipedia.org/wiki/Incendios_forestales_de_Espa%C3%B1a_de_2025 ↩

[18] Vallfirest — *La oleada de incendios forestales de agosto de 2025* (una veintena de grandes incendios en dos semanas, más de 300.000 ha; la peor temporada en más de 30 años). https://www.vallfirest.com/noticias/oleada-incendios-forestales-2025 ↩

[19] Centro de Lauegi de Arán (Conselh Generau d'Aran) — *Butlletí de perill d'allaus i cartografia ATES* (boletín diario; «la información no sustituye la formación, la experiencia y el buen juicio»). https://lauegi.conselharan.org/ates/?lang=en ↩

[20] ICGC — *Butlletí de Perill d'Allaus (BPA)* (Pirineo catalán); AEMET — *Boletín de peligro de aludes* (resto de macizos). https://www.icgc.cat/en/Thematic-areas/Risks-and-emergencies/Avalanches/Avalanche-Danger-Bulletin-BPA · https://www.aemet.es/en/eltiempo/prediccion/montana/boletin_peligro_aludes ↩

[21] Protección Civil (España) — *Public Warning System / ES-Alert* (art. 110 de la Directiva (UE) 2018/1972, transpuesto por la Ley 11/2022 General de Telecomunicaciones; sistema operativo desde junio de 2022 y a disposición de los 112 autonómicos desde 2023; tecnología cell broadcast). https://www.proteccioncivil.es/coordinacion/redes/ran/public-warning-system · https://www.vademecumlegal.es/legislacion/articulo-110-codigo-europeo-comunicaciones-electronicas ↩

[22] esPúblico — *Responsabilidad patrimonial por daños por el estado de la calzada* (art. 106.2 CE; Ley 40/2015; nexo causal; el atestado de la Guardia Civil como prueba central; silencio administrativo de 6 meses). https://www.administracionpublica.com/responsabilidad-patrimonial-por-danos-por-el-estado-de-la-calzada/ ↩

[23] t2p — manual de producto (huella SHA-512 en el dispositivo o en el origen del dato; sello de tiempo RFC 3161/eIDAS; anclaje en la blockchain pública; contenedor .asice). Véanse los capítulos 13 y 15. ↩

Elecciones verificables: del «dividendo del mentiroso» a la evidencia anclada

«Si todos te mienten siempre, la consecuencia no es que te creas las mentiras, sino que ya nadie cree nada.»

— Hannah Arendt, entrevista con Roger Errera (1973)

El **28 de septiembre de 2023**, dos días antes de las elecciones parlamentarias eslovacas, empezó a circular por Telegram y Facebook una grabación de audio en la que el líder del partido Eslovaquia Progresista, **Michal Šimečka**, y la periodista del diario Denník N **Monika Tódová** parecían discutir cómo amañar las elecciones: comprando votos de la minoría gitana, manipulando el recuento y sobornando a periodistas. El audio era una falsificación generada con IA; ambos lo negaron inmediatamente y los verificadores de la AFP encontraron en él las señales de la manipulación. Pero llegó en el peor momento posible: dentro de la **moratoria electoral de 48 horas**, cuando ni los medios ni los políticos podían desmentirlo con detalle; y, al ser audio y no vídeo, esquivó el agujero de la política de «medios manipulados» de Meta, que entonces solo cubría el vídeo. Superó las **100.000 visualizaciones** en Facebook y las **30.000** en Instagram, y corrió por cadenas de correo con la transcripción incluida. El partido de Šimečka perdió ante el Smer de Robert Fico; los analistas aún debaten cuánto influyó el audio, pero el caso se ha convertido en el primer estudio de caso de una mentira que llega cuando ya no queda tiempo para desmentirla [12].

Cuatro meses después, en Nuevo Hampshire, una voz clonada de **Joe Biden** pedía por teléfono a los votantes que no fueran a las primarias —el caso que hemos analizado en el capítulo 68—, y la FCC acabó sancionando al responsable [1]. El problema de fondo es el mismo en ambas orillas del Atlántico: cuando la falsificación llega más deprisa que el desmentido, la confianza electoral queda sin ancla. Esta es la cuestión de este capítulo.

Estas escenas se convierten en la ilustración de una paradoja profunda: la amenaza más fundamental no es que nos engañen con una mentira, sino que abandonemos la fe en cualquier verdad. Beth Noveck, en *Reboot*, describe este fenómeno como el «liar's dividend», donde la posibilidad de crear falsas narrativas permite descartar las realidades incómodas como engaños deliberados [2]. Así, una simple grabación de audio puede desencadenar un efecto dominó que merma la credibilidad del proceso democrático entero.

El impacto de incidentes como estos se mide mejor en la escala de las elecciones de 2024: el año electoral más grande de la historia, con más de cuatro mil millones de personas llamadas a votar en más de cuarenta países [3]. En un contexto donde cada voto cuenta y una amplia fracción de la población depende de un proceso transparente, la erosión de la confianza se convierte en una crisis sistémica. Las tecnologías emergentes —IA para la generación de contenido sintético y plataformas sociales que amplifican su alcance— han transformado las mentiras en herramientas de presión política, creando un entorno donde la verdad necesita una defensa más robusta que la simple detección de lo falso.

La respuesta que propone este capítulo, y que constituye el hilo conductor de la Parte XII, no es solo afinar los filtros contra deepfakes o reforzar las leyes como la SB 131 de Utah, que obliga a etiquetar medios sintéticos con procedencia tamper-evident [4]. El verdadero golpe de timón se encuentra en una prueba de existencia anclada en la blockchain: el t2p descrito en el capítulo 13. Esta ancla neutral e inmutable ofrece un registro verificable que no depende de terceros de confianza ni de la integridad del creador original; es, por tanto, una evidencia de autenticidad inalterable que puede consultarse independientemente del contenido visual o sonoro. La integridad del proceso mismo —el censo, la urna, el recuento visto desde dentro— la hemos tratado en el capítulo 48; el frente de este capítulo es la evidencia pública que rodea la elección.

En lugar de centrarnos exclusivamente en detectar falsos —una carrera a menudo perdida, como demuestra el capítulo 15— nuestra misión es demostrar qué es real con una prueba inmutable. Solo así podemos contrarrestar el «dividendo del mentiroso» y restaurar la confianza que sustenta las elecciones democráticas. En este escenario, la blockchain se convierte no solo en una infraestructura tecnológica, sino en el fundamento de una nueva era de transparencia electoral.

El dividendo del mentiroso

Cuando la tecnología crea imágenes y audios tan perfectos que nadie puede discernir lo verdadero del engaño, la simple existencia de un deepfake se convierte en un arma poderosa contra la verdad. No solo el falso engaña; la **posibilidad** de que cualquier prueba pueda ser un montaje generado por IA genera una duda universal: «quizá todo esto es una manipulación». Este escenario, llamado por Beth Noveck *dividendo del mentiroso*, transforma cada fragmento de la evidencia electoral —desde una fotografía del colegio hasta el registro digital de un voto— en una posible ficción. Cuando ninguna imagen, audio o acta puede creerse con certeza, el voto pierde su anclaje en la realidad compartida y se convierte en un gesto aislado, desprovisto de confianza colectiva.

Esta erosión del fundamento democrático no es una mera hipótesis. Como hemos visto, 2024 fue el año electoral más grande de la historia, con más de **4.000 millones** de personas llamadas a las urnas en más de cuarenta países [3]. En este contexto masivo, cualquier incertidumbre sobre la validez de los resultados puede desencadenar crisis políticas que atraviesan fronteras. La detección de deepfakes, aunque avanzada, se convierte en una carrera armamentística: cada nuevo algoritmo capaz de identificar manipulaciones es evaluado y superado por técnicas de engaño más sofisticadas, como recortes o compresiones que alteran la señal original. Como indica el capítulo 15, confiar exclusivamente en la detección es una **carrera perdida**; los defensores de lo verdadero se ven constantemente superados por la evolución de las técnicas falsas.

La solución no es perseguir lo falso con más celo. Lo que hace falta es un fundamento positivo, una **ancla neutral e inmutable** que pueda demostrar, sin duda, que algo auténtico existió y no ha sido alterado. Aquí entra la prueba de existencia basada en blockchain: el t2p que ya hemos mencionado en el capítulo 13. Esta tecnología ofrece una marca de tiempo criptográfica verificable por cualquier actor, sin necesidad de un tercero de confianza ni dependiendo de credenciales que puedan ser revocadas o falsificadas. En lugar de buscar lo falso, se demuestra lo **verdadero**: cada acta electoral, cada registro de voto y cada transmisión en vivo puede ser «anclado» en la cadena, asegurando que no ha sufrido ninguna alteración posterior.

Las marcas de agua y los estándares de procedencia, pese a su importancia como complemento —como muestra el *Tech Accord* de 2024 [5]— son insuficientes si se consideran por separado. Noveck insiste en que «las marcas de agua y los estándares de procedencia solas no resolverán el problema»; hay que combinarlas con una infraestructura inmutable que proporcione **confianza verificable** en todo momento [10]. Así, la IA deja de ser un instrumento para crear duda y se convierte en una herramienta para reforzar la verdad, etiquetando cada fragmento de evidencia con una prueba inalterable.

En resumen, el dividendo del mentiroso no es solo un efecto colateral de los deepfakes; es una amenaza estructural que desestabiliza la confianza en las elecciones. La respuesta no se encuentra en una guerra interminable contra los falsos, sino en establecer una base neutra e inmutable —la blockchain como testigo inmutable del hecho real— que permita a cada votante confiar en que su voto se cuenta tal como fue emitido, sin la sombra de un posible engaño. Esta es la verdadera clave para restaurar la credibilidad democrática en una era de manipulación digital.

El complemento: ley e industria (necesarios, insuficientes)

En la primavera de 2024 el estado de Utah aprobó la SB 131, una norma que obliga a cualquier anuncio político que contenga «medios sintéticos» a incluir una cadena de procedencia tamper-evident: debe quedar claro quién es el autor original, qué editores han intervenido y si se ha usado IA generativa. La sanción prevista —1.000 dólares por infracción— pretende crear un desincentivo económico para que los actores políticos no puedan esconder la verdad detrás de una imagen o una voz manipulada [4]. Esta ley reconoce, de manera explícita, que la clave para combatir los deepfakes es rastrear el origen del contenido. No obstante, su enfoque se basa en un modelo de confianza dependiente del creador y de los intermediarios: si el autor no registra correctamente la información o si una plataforma decide no aplicarla, el mecanismo queda desactivado.

Al mismo tiempo, en febrero de 2024 se firmó el *Tech Accord to Combat Deceptive Use of AI in Elections* durante la Conferencia de Seguridad de Múnich. Veinte empresas líderes —Adobe, Amazon, Google, IBM, Meta, Microsoft, OpenAI y otras— se comprometieron voluntariamente a desarrollar herramientas para detectar contenido electoral engañoso y a «rastrear el origen» de este material [5]. El acuerdo no comporta sanciones legales ni ningún mecanismo de verificación externa; se apoya únicamente en la buena fe de los participantes. Esto significa que, si una empresa decide ignorar sus propias directrices o si un nuevo proveedor entra en el mercado sin adherirse al acuerdo, el vacío de confianza persiste —como hemos visto.

Beth Noveck, autora de *Reboot* (2026), pone el punto final a este dibujo incompleto: «las marcas de agua y los estándares de procedencia solas no resolverán el problema», porque dependen de la cooperación del creador y de la plataforma [10]. En sus palabras, estas soluciones son solo un «complemento menor» ante una crisis que requiere un ancla independiente. La IA puede ayudar a clasificar y filtrar contenido, pero sin una fuente inmutable que no pueda ser alterada por ninguna parte, la confianza sigue siendo frágil.

—Es aquí donde el anclaje en blockchain entra como protagonista indiscutible. A diferencia de las credenciales de contenido descritas en el capítulo 13 —como hemos visto—, que se basan en un talón de Aquiles y dependen de una autoridad central para validarse, la prueba de existencia ofrece una verdad inmutable. Una vez que el votante o el registro electoral queda grabado en una cadena de bloques con hash SHA-512 y árbol de Merkle, cualquier intento posterior de modificarlo se vuelve detectable instantáneamente y, más importante aún, imposible sin dejar huella. Esta neutralidad total elimina la necesidad de confiar ni en quien creó el contenido ni en qué plataforma se aloja.

—En resumen, las iniciativas legislativas como la SB 131 de Utah —como hemos visto— son pasos imprescindibles para establecer un marco normativo y cultural que reconozca la importancia de la procedencia. Sin embargo, sin una capa adicional que proporcione una prueba de existencia inalterable, estas medidas se quedan cortas. La verdadera solución a la crisis de confianza electoral no es solo rastrear el origen; es crear un testigo inmutable que pueda ser consultado por cualquier ciudadano, sin depender de terceros. Esto es lo que ofrece t2p: un anclaje neutral e independiente que convierte la verdad electoral en un bien público, inmutable y verificable para todos.

El ancla neutral: probar lo auténtico

En un mundo donde el «dividendo del mentiroso» se ha convertido en un arma política –«la capacidad de desestimar hechos verdaderos pero incómodos como falsos»[2]– la confianza en las elecciones se encuentra al borde de un precipicio. La solución no es solo rastrear el origen del contenido, sino crear un testigo inmutable que cualquier ciudadano pueda consultar sin depender de ningún tercero de confianza; como hemos visto, t2p ofrece una prueba de existencia en blockchain que actúa como anclaje neutral e independiente, convirtiendo la evidencia electoral en un bien público verificable.

El anclaje se fundamenta en tres principios. Primero, la cadena no toma partido; cada bloque es generado por una red distribuida donde ninguna entidad única controla el consenso. Segundo, no es necesario que el creador conserve ninguna credencial o clave secreta: una vez que la evidencia se ha inscrito, su hash se convierte en una huella digital irreversible que cualquiera puede validar contra la cadena pública. Tercero, esta neutralidad permite que partidos, observadores independientes, medios de comunicación y ciudadanos puedan utilizar el mismo mecanismo sin temer manipulaciones internas.

Un ejemplo vivo de esta aplicación se encuentra en el proyecto Voto Libre de Perú y América Latina. Allí, la IA clasifica las imágenes fotográficas recogidas durante las fases de recuento y, junto con blockchain, genera un informe «seguro, transparente y en tiempo real»[6]. Cuando el gobierno peruano aprobó la ley 32270 para el voto digital con blockchain al año siguiente, se estableció que cada prueba fotográfica de fraude debería estar anclada en la cadena, garantizando que nadie pueda alterarla sin dejar rastro. Así, las imágenes se convierten en testigos verificables por cualquier ciudadano u organización internacional.

En Taiwán, la exministra digital Audrey Tang impulsó una campaña de «prebunking» donde los electores grababan su propio colegio electoral y subían esos metrajes a una plataforma basada en blockchain[7]. Cada vídeo se registra con un hash único; cuando se consulta, cualquiera puede comprobar que el contenido coincide exactamente con el estado original del archivo. Este proceso ha transformado las grabaciones personales en pruebas verificables de lo que realmente pasó en las urnas, contrarrestando las teorías conspirativas y reforzando la legitimidad del resultado.

Como hemos visto en el capítulo 13, un anclaje neutral puede aplicarse a todo tipo de actuación electoral: recuentos de votos, comunicados oficiales de la junta electoral, vídeos ciudadanos de los colegios o incluso declaraciones públicas de los candidatos. Una vez registrado en la cadena, cada elemento adquiere una capa de confianza que no depende del dispositivo de votación (el «frontend») sino de su registro posterior (el «backend»). Esto quiere decir que, aunque la infraestructura de voto electrónico sea vulnerable, la prueba de existencia mantiene la integridad de la evidencia y permite a cualquiera revisitar el proceso con una verdad inmutable.

Beth Noveck advierte que las marcas de agua y los estándares de procedencia «solas no resolverán el problema»[10]; hay que combinarlas con mecanismos como la prueba de existencia para crear un

ecosistema donde la educación mediática y las instituciones sólidas puedan apoyar una confianza real. En este sentido, t2p ofrece la pieza clave que falta: una cadena neutral que convierta cada fragmento de la verdad electoral en un testigo público, inmutable y verificable para todos. (Véase el capítulo 13 para el detalle técnico de la prueba de existencia.)

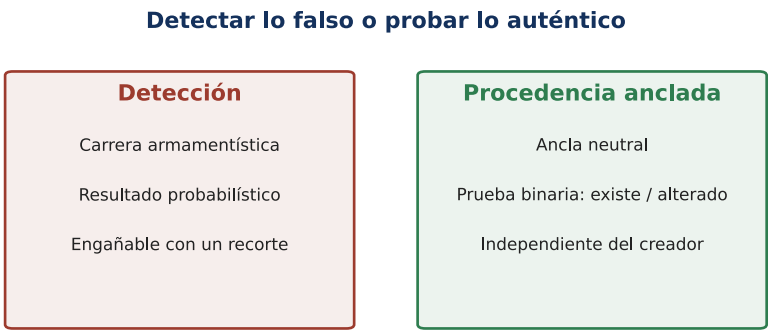


Figura 106.1 — Ante la carrera a menudo perdida de la detección, el anclaje neutral demuestra que algo auténtico existió y no se ha alterado.

Cuando el candidato es un avatar

En la primavera de 2024, mientras se recogían votos en Wyoming, una figura inesperada apareció en el pleno del ayuntamiento: **VIC**, el Virtual Integrated Citizen. El chatbot, programado como «títere de carne» de su creador, se presentó como candidato a alcalde y, sorprendentemente, obtuvo **327 votos**[8]. En las Islas Samoa Americana, otro avatar —**PalmerAI**, con la voz y la imagen de Jason Palmer— se proclamó vencedor del caucus demócrata con **51-40** puntos de votación[8]. Y en Albania, septiembre de 2025 ha marcado la llegada de **Diella**, la primera ministra de IA del mundo, encargada de las compras públicas y autorizada por un visto bueno humano final[8].

Estos casos hacen desaparecer la pregunta tradicional: «¿Es real este vídeo?» La respuesta ya no es relevante. Lo que ahora preocupa a votantes, periodistas y reguladores es **cualquier declaración proveniente de una entidad digital que puede reproducirse infinitamente**. Cuando un avatar dice «prometo reducir los impuestos para las pequeñas empresas», la verdad del enunciado depende tanto del contenido como de quién —o qué— ha generado aquel mensaje. La **procedencia verificable**, que la prueba de existencia en blockchain garantiza, pasa a ser el criterio clave para autorizar o desautorizar una réplica digital.

Esta nueva frontera se encuentra en el corazón del dividendo del mentiroso que describe Beth Noveck: «la capacidad de descartar como falsos los hechos verdaderos pero incómodos»[2]. Los avatares de IA amplifican este fenómeno; su habilidad para generar discursos coherentes y persuasivos facilita que los humanos deleguen la voz a una entidad sin cara. En el momento en que **el votante no puede distinguir si el mensaje viene del candidato real o de su avatar**, la elección se convierte en un campo de batalla de autenticidad digital más que de políticas.

Es aquí donde la prueba de existencia (t2p) entra en juego. Registrando cada declaración oficial —texto, audio y vídeo— con una huella criptográfica inmutable en una cadena **neutral**, se crea un testigo público inalterable de quién ha hablado y de qué se ha dicho. Este anclaje no depende de un tercero de confianza; su neutralidad total elimina la necesidad de que el creador mantenga credenciales o de que las marcas de agua sean consideradas suficientes[10]. Como hemos visto, iniciativas como el *Tech Accord* y la legislación de Utah sobre medios sintéticos reconocen que las marcas de procedencia son solo un complemento menor, sin capacidad para resolver la crisis de confianza por sí solas[5][4].

No obstante, la solución todavía es parcial. El capítulo 81 detalla los **derechos de réplica digital**, que permiten a una persona exigir la eliminación o la corrección de un contenido difundido sin su consentimiento. Cuando un avatar de IA repite una declaración errónea, la víctima puede invocar ese derecho, pero solo si dispone de una prueba inequívoca de la fuente original. Sin la **prueba de existencia**, la cadena de responsabilidad se rompe y el debate se desvía hacia litigios interminables.

Así, la pregunta que queda abierta es cómo integrar esta capa de verificación en los procesos electorales sin engañar a la ciudadanía con una nueva forma de burocracia digital. La respuesta pasa por **convertir cada mensaje electoral en un registro inmutable** y, al mismo tiempo, establecer mecanismos legales que reconozcan ese registro como prueba vinculante ante las autoridades. Solo entonces podremos decir que la democracia ha encontrado una herramienta para hacer gobernable el reto del avatar político, manteniendo viva la confianza en la verdad electoral mientras se conserva la libertad de expresión digital.

La promesa y el peligro

En una jornada de elecciones en la capital peruana, una observadora grabó con su teléfono una mesa de votación donde aparecía claramente la papeleta de la urna y el número del colegio electoral. Unos minutos más tarde, aquella imagen se subió a las redes sociales y, sin ninguna marca de agua ni etiqueta que certificara su origen, algunos grupos políticos empezaron a cuestionarla como «fotomontaje». La misma escena, reproducida con una IA generativa, podría haber sido desmentida en pocos segundos si la prueba de existencia registrada en la blockchain hubiera podido demostrar que aquel instante había quedado fijado de manera inmutable y neutral. Esta es la promesa central del t2p: convertir el «no puedes probar nada» en «esto existía y no se ha alterado», ofreciendo un ancla independiente que no depende de un tercero de confianza ni de credenciales que puedan ser revocadas.

El impacto de este anclaje es inmediato. Cuando la verdad se puede corroborar con un hash inmutable, el «dividendo del mentiroso» —el poder de desestimar hechos incómodos alegando que son falsos— pierde fuerza ([2]). En lugar de una carrera infructuosa por detectar deepfakes, las elecciones pasan a ser una prueba verificable: la simple existencia del registro es suficiente para desactivar el argumento de «quizá no pasó». Esto no solo refuerza la confianza de los votantes, sino que ofrece a los medios y a las autoridades un punto de inicio sólido para cualquier investigación posterior. La neutralidad total de la blockchain —sin ninguna entidad central que pueda manipular el registro— asegura que la prueba sea aceptada tanto en tribunales como en procesos electorales internacionales.

Pero esta promesa viene acompañada de un peligro inevitable. Primero, las marcas de agua y los estándares de procedencia, tan bien intencionados como son, no pueden resolver el problema solos ([10]). Sin una alfabetización mediática robusta —como demuestra el estudio coreano que ha reducido la intención de compartir información falsa ([11])—, la población sigue vulnerable a las narrativas manipuladas. La tecnología solo puede proporcionar evidencia; no puede sustituir el juicio humano ni la confianza colectiva en instituciones sólidas.

Segundo, el tecnosolucionismo puede engañar con la idea de que un ancla inmutable garantiza la verdad del contenido. El t2p solo certifica que un documento o una imagen existieron y no han sido alterados posteriormente; no evalúa si las declaraciones contenidas son veraces o no. Así, un acta electoral podría estar perfectamente anclada pero llena de errores de conteo o manipulación humana anterior a su captura. La tecnología debe ser complementaria a procesos de verificación y auditorías independientes, no un sustituto.

Finalmente, ¿quién controla la cadena? El capítulo crítico 112 alerta de que la infraestructura que garantiza la verdad puede convertirse en una herramienta de vigilancia si se deja sin gobernanza democrática. Sin mecanismos claros de auditoría y participación ciudadana, la propia blockchain podría ser utilizada por entidades autoritarias o corporativas para registrar y monitorizar comportamientos políticos, consolidando un nuevo tipo de poder centralizado. Esto subraya la necesidad de un marco legal que reconozca el registro como prueba vinculante pero también limite el abuso.

En resumen, el ancla neutral del t2p es una herramienta indispensable para restablecer la confianza electoral en un entorno donde los deepfakes erosionan constantemente la verdad. No obstante, su eficacia depende de una alfabetización mediática sólida, de procesos humanos que verifiquen el contenido y de un gobierno democrático sobre la infraestructura blockchain. Solo así podremos decir que la herramienta es necesaria —y no solo suficiente.

Es hora de actuar

Las autoridades electorales son las primeras guardianas de la confianza ciudadana. Deben anclar cada acto oficial —acta de voto, recuento preliminar y comunicado de resultados— con una prueba de existencia en blockchain (t2p) y publicar su hash verificable en el portal electoral. Esto convierte cualquier intento de

manipulación en un cambio imposible sin dejar rastro, y permite que cualquier observador contraste la integridad del documento con una sola consulta a la cadena.

Los medios deben adoptar el mismo rigor. Cada informe que incluya material sensible —vídeos de debate, declaraciones grabadas o documentos filtrados— debe ser sellado con un sello de existencia y publicar su identificador al final del artículo. Esto ofrece a los lectores una prueba inmutable de que el contenido no se ha alterado desde el momento en que se subió a la red, y los capacita para verificarlo sin depender de un tercero de confianza. Los periodistas también deben formar a sus redacciones en el uso de las herramientas de comprobación basadas en IA que integran blockchain, tal como demuestra el proyecto Voto Libre en Perú [6], donde la combinación ha permitido un reportaje «seguro, transparente y en tiempo real».

La ciudadanía, por su parte, se convierte en la última línea de defensa. Ante un vídeo «explosivo» que circula por las redes durante una campaña, el votante debe pedir su prueba de existencia antes de compartirlo. Si no existe ningún hash verificable, el contenido debe tratarse como potencial deepfake y se recomienda notificar a las plataformas correspondientes. Además, cualquier testimonio directo —una grabación de su colegio electoral o una foto del tablero de votación— debe ir inmediatamente a una red pública de blockchain, tal como hizo Taiwán con la iniciativa Cofact liderada por Audrey Tang [7]. Esto convierte el acto individual en un ancla neutra que refuerza el tejido colectivo de la verdad.

Los reguladores deben establecer marcos legales que garanticen la interoperabilidad y la procedencia verificable del contenido electoral, inspirándose en el ejemplo de Utah con la Ley SB 131, que exige etiquetas «tamper-evident» para medios sintéticos [4]. No obstante, esta regulación no debe delegar todo el control en la tecnología; hay que combinarla con programas de alfabetización mediática y de formación en IA, tal como recomienda Beth Noveck: las marcas de agua por sí solas no resuelven el problema [10].

En resumen, la cadena de confianza se construye paso a paso: autoridades que anclan datos oficiales, medios que publican con sello inmutable, ciudadanos que verifican antes de difundir y reguladores que imponen estándares sin abdicar del control democrático.

Las elecciones no se piden; se comprueban. Es time2act.

---

[1] FCC — *Robocalls de voz clonada y elecciones (caso New Hampshire, 2024)*. https://www.fcc.gov/document/fcc-makes-ai-generated-voice-robocalls-illegal ↩

[2] Beth Simone Noveck — *Reboot: AI and the Race to Save Democracy* (Yale University Press, 2026), cap. 3 («Ballots and Bots»). ↩

[3] Munich Security Conference — *AI Elections Accord* (2024). https://securityconference.org/en/aielectionsaccord/ ↩

[4] Utah State Legislature — *SB 131, Synthetic Media / disclosure of synthetic media* (2024). https://le.utah.gov/~2024/bills/sbillenr/SB0131.pdf ↩

[5] Microsoft / MSC — *Tech Accord to Combat Deceptive Use of AI in 2024 Elections* (16-02-2024). https://blogs.microsoft.com/on-the-issues/2024/02/16/ai-deepfakes-elections-munich-tech-accord/ ↩

[6] Infobae — *Blockchain y elecciones 2026 en Perú* (06-06-2025). https://www.infobae.com/peru/2025/06/06/blockchain-y-elecciones-2026-como-se-desarrollara-en-peru-el-voto-digital-obligatorio-para-militares-y-ciudadanos-en-el-extranjero/ ; y *Reboot*, cap. 3 (Voto Libre). ↩

[7] Beth Simone Noveck — *Reboot* (2026), cap. 3 (Taiwán, Audrey Tang, Cofact). ↩

[8] The Washington Post — *AI mayoral candidate VIC, Cheyenne* (2024) https://www.washingtonpost.com/technology/2024/08/19/artificial-intelligence-mayor-cheyenne-vic/ ; Wikipedia — *Jason Palmer (politician)* https://en.wikipedia.org/wiki/Jason_Palmer_(politician ; TIME — *Albania's AI minister Diella* (2025) https://time.com/7324934/albania-ai-minister-diella/ ↩

[9] The Markup — *1 in 6 Congresswomen Targeted by AI-Generated Sexually Explicit Deepfakes* (11-12-2024). https://themarkup.org/artificial-intelligence/2024/12/11/1-in-6-congresswomen-targeted-by-ai-generated-sexually-explicit-deepfakes

[10] Beth Simone Noveck — *Reboot* (2026), introducción y cap. 3 («possibilist, not Pollyanna»; la procedencia «alone will not solve the problem»). ↩

[11] Beth Simone Noveck — *Reboot* (2026), cap. 3 (ensayo coreano sobre alfabetización mediática y deepfakes). ↩

[12] IPI / VSquare / HKS Misinformation Review — *el deepfake de audio Šimečka–Tódová en Eslovaquia* (28-09-2023; moratoria de 48 horas; agujero de la política de audio de Meta; el debate sobre la influencia real en el resultado). https://ipi.media/slovakia-deepfake-audio-of-dennik-n-journalist-offers-worrying-example-of-ai-abuse/ · https://vsquare.org/slovak-election-targeted-by-pro-kremlin-deepfake-hoax/ · https://misinforeview.hks.harvard.edu/article/beyond-the-deepfake-hype-ai-democracy-and-the-slovak-case/ ↩

IA pública auditable: el registro que se puede comprobar

«Los modelos son opiniones incrustadas en matemáticas.»

— Cathy O'Neil, Armas de destrucción matemática (2016)

Era una tarde fría de octubre en Londres cuando James Whitaker, subdirector de la oficina regional de Correos del Reino Unido, recibió la notificación oficial que cambiaría su vida. Un correo electrónico, enviado desde el departamento legal de la corporación, le anunciaba una acusación de fraude por parte de un programa llamado Horizon, desarrollado por Fujitsu e implementado en el servicio de gestión de transacciones postales. Whitaker, que había dedicado más de tres décadas a la logística postal y gozaba de una reputación impecable entre colegas y ciudadanos, se encontraba ahora ante un delito que nunca había cometido.

El programa Horizon, según su diseño, registraba cada movimiento de dinero en sus 600 sucursales. Pero una serie de errores informáticos creó «descubiertos» inexistentes: transacciones ficticias que sumaban millones de libras. Sin ningún registro independiente que pudiera ser consultado o verificado por un tercero, la sola declaración del software se convirtió en prueba abrumadora. Whitaker y más de 900 subdirectores de oficina fueron condenados injustamente, perdiendo sus hogares, su reputación y, en algunos casos, la vida misma; el caso se ha vinculado a al menos trece suicidios [1].

La investigación pública presidida por Sir Wyn Williams, concluida en diciembre de 2024, reveló que la ausencia de un registro auditable había permitido que el sistema fuera manipulado sin ningún rastro visible. No se trataba solo de un fallo técnico, sino de una falta estructural: nadie –ni los funcionarios del gobierno ni la propia agencia postal– podía reconstruir paso a paso cómo se habían generado aquellos supuestos errores. El resultado fue una catástrofe de confianza y responsabilidad que sacudió al sector público británico.

En este contexto, la voz de Noveck en *Reboot* resuena con claridad: «Hay que comprar la IA como infraestructura cívica — verificable, auditable y responsable para las personas a las que afecta» [1]. La lección no es evitar la inteligencia artificial, sino exigir que cada decisión asistida por una máquina se pueda rastrear y comprobar de manera independiente. Un registro tamper-evident, anclado con prueba de existencia (t2p), sería el fundamento mínimo para cualquier auditoría futura; sin él, las decisiones automatizadas permanecen en la oscuridad, inaccesibles a la revisión ciudadana y vulnerables a la impunidad.

Así, la escena de Whitaker, un hombre honrado convertido en víctima de un algoritmo invisible, ilustra el peligro más insidioso de delegar decisiones públicas a una IA sin un marco de responsabilidad claro: la irresponsabilidad. No es solo que el programa fuera sesgado; es que no había ningún mecanismo para comprobar qué había pasado realmente y quién era responsable. La propuesta de Noveck —exportación de registros para revisión independiente, escrows de terceros o acceso restringido de evaluadores— se convierte, pues, en una necesidad urgente para restaurar la confianza pública en las tecnologías gubernamentales [2].

En las secciones que siguen veremos cómo un registro inmutable basado en blockchain puede garantizar neutralidad y no repudiabilidad, convirtiendo cada acción de la IA pública en un acontecimiento verificable y auditable, y abriendo la puerta a una democracia realmente responsable ante las nuevas formas de automatización.

Lo que está en juego: del sesgo a la irresponsabilidad

Los gobiernos ya confían en sistemas de inteligencia artificial para asignar prestaciones sociales, adjudicar contratos públicos y definir las prioridades de políticas urbanas. En los debates públicos el foco a menudo recae en el sesgo de los algoritmos: si una IA aprende de datos históricos sesgados, puede perpetuar discriminaciones invisibles. Pero la verdadera llamada de alerta es más profunda. Cuando las decisiones son tomadas por una máquina y nadie puede reconstruir el camino que ha conducido a ellas, desaparece la esencia misma de la rendición de cuentas. Como dice Noveck, hay que evitar una «accountability in name only»: un teatro democrático donde las explicaciones son solo narrativas plausibles, pero no verificables [9].

Esta irresponsabilidad se vuelve especialmente peligrosa en el ámbito de la contratación pública, que es la palanca más potente para modelar la economía y la confianza ciudadana. Noveck insiste en que la compra de IA debe exigir «exportación de registros para revisión independiente» y, cuando el sistema sea cerrado, la creación de un escrow o un acceso restringido para auditores externos, de modo que cualquier resultado pueda ser reproducido y verificado [2]. Sin estos mecanismos, los reglamentos se convierten en simples formalidades: los proveedores pueden almacenar logs en servidores propietarios, y las administraciones pueden modificar o suprimir datos sin dejar rastro.

Es aquí donde entra el protagonismo del registro inmutable basado en blockchain. Un bloque encadenado actúa como testigo neutral, imposible de ser alterado ni por la administración ni por el proveedor. Cada acción de la IA —desde la selección de una oferta hasta el cálculo de una prestación— queda anotada con una prueba de existencia (t2p) que fija el qué y el cuándo, sin revelar el cómo. Esta mínima información es, por sí sola, el fundamento indispensable para cualquier auditoría: comprobar que el acontecimiento existió, pero no necesariamente conocer la lógica interna del modelo. Así se garantiza la neutralidad y la no repudiabilidad, mientras se mantiene la confidencialidad de las propiedades intelectuales y de los datos sensibles.

Los registros algorítmicos públicos que surgieron en Helsinki y Ámsterdam en 2020 —y que posteriormente se han replicado en Canadá y España— ya demuestran cómo una catalogación transparente de algoritmos puede reforzar la confianza ciudadana [4]. No obstante, sin un mecanismo inmutable, estos inventarios son vulnerables: pueden ser editados o borrados, y su valor queda limitado a una declaración de buena fe. La integración con blockchain transforma este registro en una evidencia forense fiable, que puede consultarse por parte de auditores independientes, tribunales y ciudadanos interesados.

En resumen, la transición del enfoque del sesgo hacia la responsabilidad implica tres pasos clave: (1) exigir la exportación y auditabilidad de los logs como condición de compra; (2) establecer escrows o acceso restringido para auditores externos cuando los sistemas sean cerrados; y (3) anclar estos registros en una infraestructura inmutable que garantice neutralidad y no repudiabilidad. Solo así la IA pública puede dejar de ser un instrumento de opacidad y convertirse en una infraestructura cívica verificable, tal como propone Noveck: «verificable, auditable y responsable para las personas a las que afecta» [1]. Esta es la base sobre la que podemos construir una democracia realmente responsable ante la automatización creciente.

El registro que se puede comprobar

En el laboratorio del GovLab en Washington, la primera versión de **Policy Synth** se desplegó en el verano de 2024 como una herramienta abierta para decisiones automatizadas en ámbitos tan diversos como las licitaciones públicas y el diseño de políticas urbanas. Cada acción de un agente de IA queda registrada en un «log» detallado que indica quién ha actuado, qué decisión se ha tomado, cuándo y qué fuentes de datos la han alimentado; además, cada entrada viene acompañada de una citación automática de los datos utilizados, tal como describe Noveck: «guarda un registro detallado de las acciones de sus agentes, que permite a los responsables políticos auditar y explicar las decisiones; todas las salidas están referenciadas y citadas» [3].

Lo que convierte este registro en una verdadera **infraestructura cívica** es el anclaje con la prueba de existencia descrita en el capítulo 13. Cuando cada entrada se «sella con marca de tiempo» a través de una cadena de bloques inmutable, el registro pasa de ser un simple archivo digital a convertirse en una evidencia **no repudiable**: nadie —ni la agencia que ha desplegado la IA, ni los proveedores del modelo— puede modificar retroactivamente la información registrada. Esto elimina el peligro de una responsabilidad difusa y la sustituye por una trazabilidad clara y verificable.

Esta neutralidad es clave porque, como señala Noveck, el verdadero reto no son los sesgos del modelo sino la **irresponsabilidad**: «¿quién asume la responsabilidad cuando un agente de IA autónomo recomienda una acción que acaba en un resultado perjudicial?» [3]. Un registro inmutable responde directamente a esta pregunta. Si una decisión de contratación pública ha conducido a un sobrecoste o a la selección de un proveedor corrupto, el log mostrado por Policy Synth indica exactamente qué agente recomendó la acción, qué datos la respaldaron y en qué momento se generó. Un auditor —o incluso un tribunal— puede reproducir este escenario sin depender de la buena fe de una parte o de la disponibilidad de código fuente.

Como hemos visto en Helsinki, el registro municipal de algoritmos de 2020 se enlazó con una capa de prueba de existencia para garantizar que las decisiones sobre asignación de viviendas sociales fueran

totalmente verificables [4]. En Ámsterdam, el registro de las políticas de vigilancia urbana sigue el mismo patrón: cada alerta generada por un modelo predictivo lleva marca de tiempo y queda anclada en la cadena, lo que permite a los ciudadanos solicitar una explicación completa e inmutable. Estas experiencias demuestran cómo la **neutralidad** del registro —la cadena no juzga el contenido, solo fija el hecho— se convierte en el elemento fundamental para una auditoría real.

En resumen, anclar el log de Policy Synth con prueba de existencia transforma un simple historial operativo en una fuente de verdad indiscutible. La pregunta de Noveck sobre la responsabilidad deja de ser abstracta y se convierte en una respuesta concreta: el registro indica **quién**, **qué**, **cuándo** y **con qué datos**. Esto ofrece a las instituciones públicas un mecanismo de autocontrol que no depende de la autosuficiencia del proveedor, sino de una infraestructura pública verificable y auditable —exactamente lo que Noveck defiende como «verificable, auditable y responsable para las personas a las que afecta» [1]. La democracia, así, puede avanzar hacia una era donde la confianza se basa en pruebas inalterables, no solo en promesas.



Figura 107.1 — La decisión de IA pública deja un registro citado que, anclado con prueba de existencia, se convierte en una auditoría independiente y no repudiable.

Registros y procedencia: del catálogo a la prueba

En el verano de 2020, Helsinki y Ámsterdam publicaron los primeros inventarios algorítmicos municipales, documentos que enumeraban cada sistema de IA desplegado en servicios públicos, desde la gestión de basuras hasta el control de tráfico. Aquellos catálogos no eran simples listados; incluían las finalidades del modelo, los conjuntos de datos de entrenamiento y las medidas de supervisión humana aplicadas. El objetivo era claro: transformar la «confianza en la web de la ciudad» en una confianza fundamentada en pruebas verificables [4]. Cuando estas entradas se anclaron con la prueba de existencia descrita en el capítulo 13, cualquier ciudadano o auditor externo podía demostrar que un registro había sido creado en un momento determinado y no se había modificado posteriormente. Esto elimina la opción de «editar a propósito» los logs después de una decisión controvertida y ofrece una base neutra para la revisión.

Los esfuerzos europeos inspiraron iniciativas similares en Canadá, con el proyecto Tracking Automated Government, y en España, donde el Observatorio Algorítmico ha consolidado un repositorio nacional que recoge las IA utilizadas en áreas como las compras públicas y la seguridad ciudadana. Estas plataformas se convierten en puntos de partida para auditorías independientes: los auditores pueden descargar el registro, comprobar su hora con la prueba de existencia y compararlo con las decisiones efectivas del sistema. La combinación de inventarios públicos y anclaje criptográfico crea una capa de transparencia que supera la simple «doble opacidad» descrita por Noveck, donde el conocimiento científico y comercial se mantiene separado y oculto [5].

A escala de procedencia del modelo, el concepto de AI-BOM (Bill of Materials) ha ganado tracción gracias a las directrices de Noveck, que insisten en incluir no solo los pesos del modelo sino también los datos de entrenamiento y la configuración completa de la infraestructura [8]. DeepSeek R1, lanzado en enero de 2025 con pesos abiertos bajo licencia MIT y un coste de desarrollo de 5,6 millones de dólares, ha

demostrado que es posible publicar toda la cadena de suministro de una IA avanzada sin comprometer la propiedad intelectual esencial [7]. Cuando este AI-BOM se registra mediante la prueba de existencia, cualquier entidad puede verificar que los datos declarados son exactos y que no se han añadido ni suprimido elementos posteriores al entrenamiento. Esto ofrece el fundamento mínimo sobre el que una auditoría externa puede construirse: se conocen tanto los ingredientes como el momento en que fueron combinados.

El marco regulador californiano, con la SB 53 y la creación de CalCompute, ya obliga a grandes proveedores a publicar informes de seguridad estandarizados y a mantener una nube pública donde las ejecuciones se registran de forma inmutable [6]. Esta infraestructura pública proporciona el «escrow» que Noveck pide para sistemas cerrados: los logs del núcleo de ejecución son accesibles a auditores independientes, garantizando la trazabilidad completa desde el momento en que se ha generado una recomendación hasta su despliegue final.

En resumen, la llamada «doble opacidad» no es un obstáculo insalvable si se combina un catálogo algorítmico público con la prueba de existencia y un AI-BOM completo. El registro pasa de ser una simple declaración a una evidencia inalterable que permite tanto al ciudadano como a la institución verificar qué existió y cuándo, abriendo el camino para auditorías reales y responsabilidad efectiva. Esta es la clave para que la IA pública se convierta en infraestructura cívica verificable, auditable y, finalmente, responsable.

La promesa y el peligro

Imagina una ciudad donde cada licitación, cada decisión de políticas sociales o cada alerta policial generada por un algoritmo se registra en una cadena de bloques inmutable. Un funcionario puede abrir la aplicación, ver la transacción con su hash, comprobar que el modelo de IA existió y cuándo, y consultar los metadatos que indican qué pesos y datos fueron utilizados. Esto transforma la confianza ciega en una verificación directa: «confía en la administración» se convierte en «compruébalo tú mismo». La prueba de existencia (t2p) ofrece, como ya se ha visto en el capítulo 13, el fundamento mínimo para cualquier auditoría independiente; la simple declaración pasa a ser una evidencia inalterable que puede ser revisada por ciudadanos y entidades externas.

Esta capacidad de hacer auditable cada acción asistida por IA es la promesa central del registro tamper-evident. La iniciativa Policy Synth, desarrollada por el GovLab de Noveck, ya demuestra cómo un log detallado permite a los responsables políticos rastrear y explicar las decisiones de un agente autónomo, con todas las salidas citadas y vinculadas a fuentes verificables[3]. Además, la normativa californiana (SB 53) obliga a los proveedores de modelos «frontera» a publicar informes de seguridad y a poner a disposición del público registros de uso, creando un ecosistema donde el control puede ejercerse desde fuera de las empresas creadoras[6].

Sin embargo, la misma infraestructura que garantiza la transparencia puede engendrar peligros graves si no se acompaña de una auditoría externa y de supervisión humana. La simple existencia del registro no explica la procedencia ni la justicia del modelo: el problema de la «doble opacidad», donde la ciencia es incomprensible y el comercio se mantiene cerrado, persiste aunque cada transacción sea inmutable[5]. Sin mecanismos de auditoría independiente, el registro puede convertirse en una mera «accountability in name only», un teatro democrático donde las explicaciones son plausibles pero no verdaderas[9].

Otro peligro se manifiesta cuando la confianza en la información registrada se confunde con la legitimidad de la decisión. El caso Diella, primera ministra de IA de Albania que promovió compras públicas «100 % libres de corrupción» con un visto bueno humano en cada fase, ilustra cómo una cadena impecable puede esconder decisiones injustas si el criterio subyacente del modelo es defectuoso[10]. Un registro inmutable no puede corregir una política que ya se basa en un sesgo o un error de programación; solo puede demostrar que la decisión fue tomada y cuándo.

Finalmente, la cuestión de quién controla la cadena y los nodos es fundamental. El capítulo 112 detalla cómo el mismo registro inmutable que hace responsable al gobierno puede, si se gestiona inadecuadamente, convertirse en una herramienta de vigilancia masiva sobre los ciudadanos, rastreando cada interacción con la IA y potencialmente restringiendo derechos digitales. Por tanto, la infraestructura es necesaria pero no suficiente: hay que establecer gobiernos de datos, mecanismos de escrow para terceros y un marco legal que asegure que el control del registro se mantiene en manos neutras y democráticas[2].

En resumen, el anclaje de las decisiones públicas en una prueba de existencia ofrece la clave para auditorías reales y responsabilidad efectiva. Pero esta promesa solo se alcanza si se complementa con auditoría externa, supervisión humana y una gobernanza clara del propio registro; de lo contrario, el riesgo de teatro democrático y vigilancia excesiva puede eclipsar cualquier beneficio esperado.

Es hora de actuar

La confianza de la que depende la democracia no puede quedarse en una promesa abstracta; debe ser verificable y, sobre todo, reproducible. Por eso cada actor del sector público debe tomar medidas concretas que transformen la IA pública en una infraestructura cívica realmente auditable.

Compradores públicos —tanto las administraciones centrales como las entidades locales— deben hacer obligatoria, en los contratos, la inclusión de un registro anclado en blockchain y probado por *t2p*. Este registro debe ser exportable para una revisión independiente y, cuando el sistema sea cerrado, se debe establecer un «escrow» de terceros o un acceso restringido de evaluadores tal como recomienda Noveck: «exportación de registros para revisión independiente» y «escrow de terceros o acceso de evaluador restringido» son condiciones imprescindibles para garantizar que ninguna decisión se pierda en una caja negra irreproducible[2]. La cláusula contractual debe prever sanciones si el proveedor no cumple con estos requisitos, evitando así el escenario del caso Horizon, donde datos erróneos condujeron a condenas injustas y hasta trece suicidios[1].

Administraciones —como propietarias de estas plataformas— deben publicar inventarios algorítmicos que incluyan cada entrada anclada al registro inmutable. Los ejemplos pioneros de Helsinki y Ámsterdam, lanzados en 2020, demuestran que es posible detallar datos de entrenamiento, uso, supervisión humana y evaluación de sesgo en un catálogo público accesible[4]. Estos inventarios deben nombrar explícitamente la procedencia de los modelos (AI-BOM) y los datos utilizados, tal como se describe en el capítulo 79, para que cualquier auditor pueda rastrear el origen y el momento exacto en que una decisión fue generada.

Auditores y tribunales —como guardianes de la responsabilidad— deben exigir la huella anclada como base mínima de revisión. La prueba de existencia no solo certifica que una acción ha existido, sino que establece el momento exacto en que se puede reproducir el proceso decisional, convirtiendo la inspección en una tarea factible y evitando la «accountability in name only», donde las explicaciones son meramente escenificadas sin fundamento real[9].

Ciudadanía —debe tener reconocido el derecho a reconstruir e impugnar cualquier decisión algorítmica que le afecte. Este derecho se materializa solo si los registros son públicos, no manipulables y accesibles para revisión independiente. La legitimidad de una política pública no se autodeclara; se comprueba con el registro que muestra qué pasos se siguieron y cuándo se ejecutaron.

En resumen, la combinación de **neutralidad** (un registro inmutable que nadie puede alterar) y **auditabilidad** (capacidad de acceder, exportar y revisar los registros) convierte la IA pública en una herramienta responsable. Esta promesa solo se materializa si cada actor asume sus obligaciones: contratos con cláusulas de exportación y escrow para compradores; inventarios anclados para administraciones; exigencia de la huella para auditores; y derecho de reconstrucción para ciudadanos. La legitimidad no se proclama, se comprueba. Es time2act.

---

[1] Beth Simone Noveck — *Reboot: AI and the Race to Save Democracy* (Yale University Press, 2026), cap. 8 ; y *Post Office Horizon Inquiry* (Sir Wyn Williams, 2024). https://en.wikipedia.org/wiki/British_Post_Office_scandal ↩

[2] Beth Simone Noveck — *Reboot* (2026), cap. 8 («Using procurement power»). ↩

[3] Beth Simone Noveck — *Reboot* (2026), cap. 6 (Policy Synth, runtime guardrails) ; The GovLab. https://thegovlab.org/ ↩

[4] VentureBeat — *Amsterdam and Helsinki launch algorithm registries* (2020) https://venturebeat.com/ai/amsterdam-and-helsinki-launch-algorithm-registries-to-bring-transparency-to-public-deployments-of-ai ; y *Reboot* (2026), cap. 8 (Canadá, España). ↩

[5] Beth Simone Noveck — *Reboot* (2026), cap. 8 («double opacity»; auditorías externas). ↩

[6] Gobierno de California — *Transparency in Frontier Artificial Intelligence Act (SB 53)* (29-09-2025). https://www.gov.ca.gov/2025/09/29/governor-newsom-signs-sb-53-advancing-californias-world-leading-artificial-intelligence-industry/ ↩

[7] DeepSeek — *DeepSeek-R1 release* (20-01-2025). https://api-docs.deepseek.com/news/news250120 ↩

[8] Beth Simone Noveck — *Reboot* (2026), cap. 8 (código abierto: los cinco elementos; registro de consultas y entrenamientos). ↩

[9] Beth Simone Noveck — *Reboot* (2026), introducción y cap. 6 («accountability in name only»; la IA como objeto). ↩

[10] TIME — *Albania's AI minister Diella* (2025). https://time.com/7324934/albania-ai-minister-diella/ ↩

Participación auténtica: una persona, una voz, sin vigilancia

«No decimos que quien no se interesa por la política sea alguien que se ocupa de sus propios asuntos; decimos que aquí no tiene nada que hacer.»

— Pericles, oración fúnebre (Tucídides, II, 40)

Era el verano de 2017 cuando la Federal Communications Commission (FCC) lanzó una consulta pública sobre la neutralidad de la red. El formulario en línea se llenó con más de **22 millones** de comentarios; el ruido que inundaba la plataforma era tan intenso que, unos meses después, un informe de la FCC reveló que **18 millones** de esos mensajes eran falsos y **9,3 millones** contenían identidades inventadas o robadas. La mayoría de esas intervenciones provenían de un solo joven de 19 años que había programado un bot para inundar el debate, mientras que cerca de **500.000** comentarios llegaban desde direcciones rusas vinculadas a una campaña secreta financiada por la industria de banda ancha[1].

Aquel escenario, tan concreto como emblemático, mostraba la paradoja que ahora se repite en cada ámbito digital: cuando el ruido supera a la señal y no podemos distinguir una voz humana de un algoritmo, la participación ciudadana se transforma en un **teatro de vacíos**. Las plataformas democráticas, que deberían ser escenarios para la expresión auténtica, acaban convirtiéndose en espacios donde la «opinión» es solo una capa superficial de información fabricada. La confianza se desintegra; la voz del ciudadano, sin ninguna prueba verificable que la respalde, pierde todo valor y se convierte en un murmullo que nadie escucha.

En este contexto, la necesidad de una **prueba de personalidad** —una persona, una voz— se hace imperiosa. No solo hay que garantizar que cada voto o apoyo a una iniciativa proviene de un individuo real; también se debe evitar que esa garantía dependa de una base biométrica centralizada, que podría convertirse en un instrumento de vigilancia masiva. La solución debe estar basada en la **prueba de existencia** y la **prueba de vida en el dispositivo**, como se describe en el capítulo 13: una firma digital que combina un vídeo-selfie con verificación biométrica realizada íntegramente dentro del propio teléfono, sin que ninguna entidad externa tenga acceso o almacene los datos biológicos[7].

A diferencia de sistemas como Worldcoin, que escanea el iris para «probar que eres humano» y ha sido objeto de prohibiciones y multas en más de nueve jurisdicciones, incluyendo la declaración de inconstitucionalidad en Kenia y la destrucción obligada de los datos recogidos en Colombia[4], esta aproximación descentralizada garantiza que la prueba de personalidad sea **neutral** y **no centralizada**, evitando que ninguna empresa o gobierno pueda utilizarla como punto de entrada para la vigilancia.

Así pues, el reto que plantea Noveck —escala, acción e institucionalización de la participación digital— solo puede abordarse si superamos el obstáculo fundamental del **ruido indistinguible**. Solo con una prueba de personalidad verificable, sin depender de una infraestructura biométrica centralizada, podremos transformar la participación digital de un simulacro a una fuerza real que decida y no solo que grite. Este es el primer paso hacia una democracia en la que cada ciudadano tenga una voz auténtica, reconocida y respetada.

Los dos fracasos de la participación

En los últimos años, las plataformas digitales han convertido el voto ciudadano en un espectáculo: encuestas masivas que recogen miles de voces pero nunca llegan a transformar ninguna decisión política. Este fenómeno, que Noveck describe como «participación sin integración», se convierte en un teatro donde la democracia actúa solo como escenario de una representación vacía [6]. Las consultas abiertas, las peticiones en línea y los referéndums digitales son a menudo recogidos por entidades que no disponen de ningún mecanismo para canalizar esos inputs hacia el poder legislativo o ejecutivo. El resultado es una acumulación de ruido que se difumina entre la multitud y desaparece sin dejar huella ni impacto real.

A este primer fracaso se añade otro, más insidioso: la escalada de identidades falsas y bots que ahogan el debate. Un informe de la FCC indica que, de más de 22 millones de comentarios enviados a través de las redes neutras, unos 18 millones eran falsos [1]; la Fiscalía General de Nueva York confirma que 9,3 millones de esos mensajes provenían de identidades ficticias controladas por un solo chaval de 19 años con software automatizado y una red de casi 500.000 direcciones rusas [1]. Como hemos visto, esta inundación de falsedades distorsiona la percepción del consenso ciudadano y desincentiva la participación

auténtica: los usuarios reales se ven obligados a luchar contra una marea de información engañosa y, finalmente, abandonan el proceso.

El peligro no reside solo en la abundancia de ruido; es la falta de confianza que esta práctica genera. Un estudio citado por Noveck indica que el 51 % de los europeos encuestados estarían dispuestos a sustituir a algunos políticos por inteligencia artificial, una cifra que denuncia un profundo agotamiento de la fe en las instituciones democráticas [8]. Esta estadística no es solo un barómetro de insatisfacción; es una señal clara de que el modelo actual de participación digital ha perdido legitimidad. Más ruido, más plataformas abiertas y más consultas sin consecuencias solo empeoran la percepción de que las voces individuales son irrelevantes.

Para salir de este bucle hay que redefinir dos requisitos básicos. En primer lugar, la participación debe decidir: los inputs ciudadanos deben estar conectados directamente a procesos de decisión real, como demuestra el portal e-Cidadania del Senado brasileño, donde una «Idea Legislativa» que llegue a 20.000 apoyos pasa a ser examinada por la Comisión de Derechos Humanos y puede convertirse en ley —ejemplo reciente es la «Ley Joca», aprobada en abril de 2025 tras un movimiento popular masivo [2]. En segundo lugar, esa decisión debe provenir exclusivamente de personas reales. La prueba de personalidad verificada por t2p ofrece una solución: un certificado que combina vídeo-selfie y verificación biométrica en el dispositivo sin que ninguna tercera parte almacene los datos [7]. A diferencia del modelo centralizado de iris de Worldcoin, prohibido y multado en nueve jurisdicciones por vulnerar la privacidad [4], esta prueba mantiene la integridad de la identidad a escala local, evitando el control masivo y garantizando que cada voz sea auténtica.

En resumen, el fracaso actual de la participación digital se debe tanto al hecho de que no decide como al hecho de que se hunde en una masa de identidades artificiales. La solución pasa por dos pilares imprescindibles: una conexión directa con las estructuras de poder y una verificación descentralizada que asegure que cada contribución proviene de una persona real. Solo así podremos transformar el ruido indistinguible en una fuerza democrática capaz de decidir, y no solo de gritar.

Participación que decide

En el Senado brasileño, el portal e-Cidadania ha transformado la voz del ciudadano en una obligación parlamentaria siempre que una propuesta llega a un umbral de veinte mil apoyos [2]. Esto no es solo una pequeña muestra de interés: el caso conocido como «Ley Joca», nacido de una denuncia popular sobre un perro muerto por error de una aerolínea, —como hemos visto— se convirtió en ley en abril de 2025 [2]. Hoy el sistema registra más de ciento veinte mil ideas legislativas y decenas de millones de apoyos, convirtiendo la masa de comentarios digitales en una fuerza normativa concreta.

En Taiwán, el modelo vTaiwan combina deliberación abierta con decisiones vinculantes. Las «tecnologías plurales» descritas por Tang y Weyl conectan los debates ciudadanos con las instituciones, de modo que las propuestas apoyadas al superar un umbral preestablecido pasan a ser consideradas oficialmente por el ejecutivo [3]. No se trata solo de una plataforma donde la gente comenta; es una infraestructura que traduce el consenso digital en acción legislativa real.

Estos dos ejemplos ilustran una regla fundamental: la tecnología solo puede potenciar la democracia cuando hay un marco institucional claro y un compromiso firme de respuesta. Sin ese marco, incluso las herramientas más sofisticadas se convierten en simples escenarios de entretenimiento, donde las voces no tienen ningún peso real. El peligro es que, a medida que la participación digital se expande, el ruido generado por identidades falsas y bots amenaza con desvirtuar este proceso.

Los datos recientes muestran cómo esta vulnerabilidad se materializa: **como hemos visto**, más del 80 % de los comentarios de aquella consulta de la FCC resultaron falsos o manipulados [1]. Cuando una iniciativa depende de un número mínimo de apoyos para avanzar, el efecto de las identidades artificiales se traduce directamente en decisiones políticas. Un grupo organizado puede crear miles de cuentas ficticias, inflar artificialmente el apoyo a una propuesta y, sin una verificación fiable, hacer que los legisladores tomen medidas basadas en un consenso inventado.

Esta fragilidad es la puerta de entrada para el siguiente paso: garantizar que cada apoyo proviene de una persona real y presente. La prueba de existencia de **t2p** ofrece exactamente eso —una firma vinculada a un vídeo-selfie y una verificación biométrica realizada exclusivamente en el dispositivo, sin que ninguna entidad externa acceda a la información [7]. A diferencia del modelo centralizado de iris de **Worldcoin**,

prohibido y multado en diversas jurisdicciones por vulnerar la privacidad [4], el mecanismo descentralizado de **t2p** mantiene la identidad segura e invisible para terceros.

Así, mientras Brasil y Taiwán demuestran cómo la tecnología puede canalizar la participación hacia resultados tangibles, su efectividad depende de un componente esencial: una verificación fiable que impida que los bots sustituyan las voces auténticas. Solo con esta capa de confianza podremos transformar el ruido digital en una fuerza democrática capaz de decidir realmente, y no simplemente de gritar.

Una persona, una voz, sin vigilancia

En un café de São Paulo, junto a una pantalla que mostraba en tiempo real las firmas digitales del portal e-Cidadania, una joven activista llamada Lúcia observaba cómo el número de apoyos a la «Ley Joca» superaba los 20.000 y, de golpe, se convertía en propuesta legislativa. El momento era electrizante: un ciudadano había conseguido transformar una pequeña queja en una iniciativa nacional solo porque su voto, su apoyo, estaba vinculado a una identidad verificable y única. Pero este éxito no sería posible sin una capa fundamental de confianza que garantice que detrás de cada firma hay una persona real y presente, y no un bot o una identidad falsa.

La crisis actual de la participación digital se manifiesta en dos dimensiones. Por un lado, muchos espacios en línea son meramente escenarios donde las voces se alzan sin ninguna capacidad de influir: un «teatro» de comentarios que nunca llegan a las decisiones políticas [6]. Por el otro, la proliferación de identidades falsas y bots ha inundado las plataformas con apoyos artificiales; como hemos visto, la FCC constató que casi todos los comentarios recibidos en una consulta pública de 2017 eran falsos [1]. Este doble problema paraliza la democracia digital y alimenta la desconfianza ciudadana.

Una solución aparente ha sido el proyecto Worldcoin, que pretende demostrar que un usuario es humano escaneando el iris y centralizando esa biometría en una cadena de bloques. Como hemos visto, este modelo se ha revelado peligroso: entre 2024 y 2025 fue prohibido y multado en más de nueve jurisdicciones; Kenia lo declaró inconstitucional y ordenó la destrucción total de los datos recogidos [4]. La centralización de una característica tan sensible como el iris genera una pesadilla de vigilancia, donde una entidad —pública o privada— controla información biológica que podría ser explotada con fines autoritarios o comerciales.

La vía neutral ofrece la prueba de existencia y de vida desarrollada por t2p. Esta tecnología combina un vídeo-selfie con verificación biométrica completamente en el dispositivo, sin que ningún tercero vea ni almacene la imagen o los datos biométricos [7]. Cuando el usuario captura su rostro y voz, se genera una firma criptográfica única que vincula el acto (voto, comentario, apoyo) a una persona presente. La prueba no depende de ninguna base de datos centralizada; la confianza reside en la integridad del propio dispositivo, garantizando que la identidad es auténtica pero sin revelarla.

Además, las «APIs personales» propuestas por Noveck permiten al ciudadano controlar su propia identidad y datos en línea [5]. En lugar de ser producto de una plataforma, el individuo se convierte en gestor de su perfil digital, decidiendo qué información compartir y con quién. Esta arquitectura refuerza la distinción crucial entre prueba de personalidad –el hecho de ser una persona única– e identificación –quién eres exactamente–. La primera asegura que solo personas reales pueden participar; la segunda se mantiene reservada y no es necesaria para la actuación cívica.

Como hemos visto, la prueba de existencia con vida en el dispositivo ofrece una respuesta directa al problema de las voces falsas sin crear un centro de vigilancia. Es la misma neutralidad que ha sostenido el éxito de plataformas como e-Cidadania o vTaiwan: ningún tercero controla la clave de la confianza, y cada voto se convierte en una declaración auténtica de una sola voz humana. Esta arquitectura es el fundamento sobre el que podemos transformar el ruido digital en decisión real y democrática.

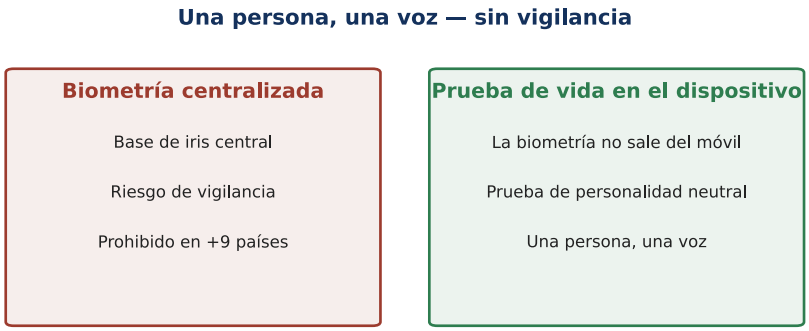


Figura 108.1 — La prueba de personalidad se puede hacer en el dispositivo, sin bases biométricas centralizadas: una persona, una voz, sin vigilancia.

La promesa y el peligro

Imaginemos una jornada electoral digital donde cada voto se registra con la misma seguridad de una huella física, pero sin que ninguna entidad pueda acceder a los datos biométricos que lo han generado. Esta es la visión que ofrece la prueba de personalidad neutral de **t2p**: una firma digital basada en un vídeo-selfie y una verificación biométrica completamente **en el dispositivo**, que vincula cada acto a una persona real y presente sin que ningún tercero vea ni guarde aquella información sensible [7]. En teoría, este mecanismo puede transformar el ruido de miles de identidades ficticias en decisiones auténticas, convirtiendo la participación masiva en un verdadero ejercicio democrático. La promesa es clara: una única voz humana por cada voto, sin el estallido de bots ni la manipulación de perfiles falsos que ha paralizado las iniciativas digitales de la última década.

No obstante, el camino hacia esa confianza plena está lleno de riesgos que no podemos ignorar. En primer lugar, cualquier sistema de prueba de personalidad corre el peligro de convertirse en una **arquitectura de vigilancia** si la biometría se centraliza. El ejemplo de Worldcoin ilustra este escenario: la propuesta de escanear el iris para demostrar que un usuario es humano ha sido prohibida, multada u obligada a borrar datos en más de nueve jurisdicciones, y tanto Kenia como Colombia han declarado inconstitucional su modelo por su dependencia de una base de iris centralizada [4]. Esta experiencia demuestra que una idea bien intencionada puede convertirse en un instrumento de control masivo cuando los datos biométricos se convierten en activos gestionados por entidades externas. La línea roja, por tanto, es clara: **nunca** bases biométricas centralizadas.

En segundo lugar, la prueba de personalidad solo es emancipadora si se integra en el poder institucional. Noveck recuerda que la participación digital se encuentra atrapada en tres retos recurrentes —escala, acción e institucionalización—; sin una conexión efectiva con las estructuras de decisión, el resultado sigue siendo un **teatro** donde los ciudadanos hablan pero no deciden [6]. Las experiencias exitosas de Brasil (e-Cidadania) y Taiwán (vTaiwan/Pol.is) muestran que la clave es una arquitectura neutral donde ningún tercero controla las claves de confianza, permitiendo que cada voto se convierta en una declaración auténtica de una sola voz humana [2][3]. Pero esta integración requiere un marco regulador que garantice que las firmas digitales sean reconocidas y valoradas por las instituciones legislativas.

Finalmente, la cuestión de **quién controla la cadena** donde se registran estas pruebas es fundamental. Si la infraestructura subyacente fuera gestionada por entidades privadas o por estados con intereses políticos, el potencial emancipador podría ser usurpado como instrumento de hegemonía digital. El capítulo 112 detalla las limitaciones del modelo de Worldcoin y la necesidad de una gobernanza abierta y democrática sobre cualquier cadena que almacene pruebas de personalidad.

En conclusión, la prueba de personalidad neutral ofrece una oportunidad única para una participación ciudadana auténtica —una persona, una voz— pero solo si se mantiene **descentralizada**, se integra en el poder real y está sometida a una gobernanza transparente. Sin estas garantías, el riesgo es que la tecnología, en vez de liberar, se convierta en una nueva capa de vigilancia que domestique la democracia que pretende reforzar. La decisión final recae en nosotros: diseñar y defender un sistema donde la confianza sea **neutral**, no una moneda para el control.

Es hora de actuar

Los parlamentos y ayuntamientos deben abandonar las consultas que solo recogen voces sin poder decidir. Hay que establecer umbrales obligatorios, como el modelo del portal e-Cidadania del Senado brasileño, donde una iniciativa que llegue a 20.000 apoyos pasa a la Comisión de Derechos Humanos y se convierte en proyecto de ley [2]. De manera similar, Taiwán ha integrado las tecnologías plurales de vTaiwan/Pol.is para transformar cada aportación ciudadana en un paso concreto hacia la acción legislativa [3]. La adopción de estos marcos debería ir acompañada de una prueba de personalidad en el dispositivo: una firma con vídeo-selfie y verificación biométrica que se realiza íntegramente dentro del teléfono, sin que ninguna entidad externa acceda ni almacene el dato biométrico [7]. Este mecanismo elimina los bots y las identidades falsas detectadas en la consulta de la FCC de 2017, donde 9,3 millones de comentarios eran ficticios —incluyendo un solo joven de 19 años— y cerca de medio millón provenían de Rusia [1].

Los diseñadores cívicos deben reconocer que la prueba de personalidad no es sinónimo de identificación. El objetivo es garantizar que cada voto o propuesta proviene de una persona real y presente, pero sin crear una base centralizada de información biométrica como la que intentó imponer Worldcoin con el escaneo de iris —un proyecto prohibido y multado en nueve jurisdicciones por vulnerar derechos fundamentales [4]. La lección es clara: las soluciones deben ser descentralizadas, mínimas y totalmente controladas por el dispositivo del usuario. Cualquier arquitectura que requiera repositorios biométricos centrales debe estar prohibida por la normativa, tal como prevé el marco regulador europeo sobre datos sensibles.

La ciudadanía debe exigir una participación que decida y herramientas que le permitan ser participante, no producto. Las «APIs personales» propuestas por Noveck ofrecen un panel de control donde cada individuo gestiona su propia identidad digital sin cederla a terceros [5]; así la voz ciudadana se convierte en una fuerza real de influencia y rompe el círculo vicioso de «participación sin integración» que reducía la democracia a un simulacro [6].

Finalmente, los reguladores deben proteger la prueba de personalidad descentralizada y vetar cualquier forma de repositorio biométrico central. Esto implica legislar contra el almacenamiento masivo de iris o huellas fuera del dispositivo y establecer sanciones para las empresas que intenten crear «capas de vigilancia» bajo la capa de confianza. La normativa debe estar alineada con el principio de neutralidad: la tecnología debe ser un instrumento que refuerza la confianza, no una moneda para el control.

En resumen, una democracia que escucha a las personas —sin tener que vigilarlas— puede transformar la participación digital en auténtica acción cívica adoptando umbrales decisorios, implementando pruebas de personalidad en el dispositivo y garantizando marcos reguladores estrictos. Es el momento de aplicar estas medidas concretas: time2act.

---

[1] Fiscalía General del Estado de Nueva York — *Report on fake comments in the FCC net neutrality proceeding* (2021). https://ag.ny.gov/press-release/2021/attorney-general-james-issues-report-detailing-millions-fake-comments-revealing ↩

[2] Senado Federal de Brasil — *Portal e-Cidadania / Ley Joca* (2024-2025) https://www12.senado.leg.br/ecidadania/ ; y *Reboot* (Noveck, 2026), cap. 7. ↩

[3] Audrey Tang y E. Glen Weyl — *Plurality: The Future of Collaborative Technology and Democracy* (2024) ; y *Reboot* (2026), cap. 7. ↩

[4] Biometric Update / ICLG — *Worldcoin/World ID: prohibiciones y órdenes de supresión (Kenia inconstitucional; Colombia)* (2024-2025). https://www.biometricupdate.com/202510/colombia-orders-world-shut-down-citing-biometrics-compliance-failures ↩

[5] Beth Simone Noveck — *Reboot* (2026), cap. 3 (APIs personales). ↩

[6] Beth Simone Noveck — *Reboot* (2026), cap. 7 (escala, acción, institucionalización; «participation without integration»). ↩

[7] time2act — capítulo 13 (t2p: firma con vídeo-selfie y prueba de vida en el dispositivo) ; T2P-Manual (v1.0, 2026). ↩

[8] Beth Simone Noveck — *Reboot* (2026), cap. 3 (encuesta Univ. de Madrid: 51% sustituirían políticos por IA). ↩

Manifestaciones: la prueba simétrica en la calle

«La injusticia en cualquier lugar es una amenaza para la justicia en todas partes.»

— Martin Luther King Jr., «Carta desde la cárcel de Birmingham» (1963)

Minneapolis, 25 de mayo de 2020. Al anochecer, ante una tienda de barrio, una chica de diecisiete años que pasaba por allí levanta el teléfono y graba. Se llama Darnella Frazier, y su vídeo contradice la versión inicial de los hechos y se convierte en prueba central en el juicio contra el agente Derek Chauvin por el asesinato de George Floyd [2]. El 11 de junio de 2021, el jurado del Premio Pulitzer le concede una mención especial por «informar con coraje del asesinato de George Floyd, un vídeo que espoleó protestas contra la brutalidad policial en todo el mundo, subrayando el papel crucial de la ciudadanía en la búsqueda de la verdad y la justicia por parte de los periodistas» [1]. Una adolescente con un teléfono cambió la historia porque su vídeo fue creído. Y esta es exactamente la pregunta que vertebra este capítulo: en la era del deepfake, ¿qué pasará el día en que un vídeo así se pueda despachar con dos palabras — «es falso»?

Este capítulo aborda el derecho de manifestación y el orden público: la documentación de la calle, en las dos direcciones. La prueba en conflictos armados y derechos humanos está en el capítulo 20; el fotoperiodismo, en el capítulo 17; las elecciones y el «dividendo del mentiroso», en el capítulo 106; la participación cívica, en el capítulo 108. La pregunta clave: ¿cómo se reconstruye una carga policial, un altercado o una detención sin que gane, simplemente, la versión del más fuerte? La respuesta de este libro es simétrica por construcción: evidencia anclada en captura por ambas partes — **t2p**: la huella SHA-512 calculada en el dispositivo mientras se graba, el sello de tiempo RFC 3161/eIDAS y el anclaje en la blockchain pública dentro de un contenedor .asice [14]. Ni el manifestante ni el agente pueden reescribir lo que quedó sellado. La prueba no tiene bando: esta es su fuerza democrática.

El vídeo contra el atestado

El caso español que lo condensa ocurrió a raíz de una protesta del movimiento «Rodea el Congreso», en Madrid. Tres agentes antidisturbios acusaron a una manifestante de haberles dado patadas y puñetazos; el atestado inicial, sin embargo, solo recogía insultos, y las acusaciones fueron creciendo durante la instrucción y el juicio — hasta que aparecieron los vídeos, que no mostraban ninguna agresión. La frase de la crónica judicial lo dice todo: «Ella no está condenada porque había un vídeo» [3]. El epílogo es incómodo: los agentes que la habían acusado acabaron absueltos — el tribunal reconoció que no había pruebas de las agresiones que ellos afirmaban con rotundidad, pero no vio delito en ello [4]. Sin el vídeo, una condena probable para ella. Con el vídeo, ninguna consecuencia para nadie.

Conviene entender el terreno procesal, sin épica. El atestado policial no es una sentencia anticipada: si los agentes que lo redactaron no lo ratifican en el juicio, bajo publicidad y contradicción, no tiene eficacia probatoria por sí solo [5]. Pero en la práctica la palabra del agente pesa, y en el ámbito administrativo — el de las multas — la presunción de veracidad de la autoridad deja al ciudadano casi indefenso si no dispone de imágenes. Aquel día, el vídeo niveló el campo. Por pura casualidad: alguien grababa.

La lección del caso no es contra nadie; es contra la casualidad. La verdad de una plaza no puede depender de que alguien tuviera el móvil en la mano, ni de que el archivo sobreviva, ni de que el juez se lo crea cuando la otra parte insinúe que está editado. Y la lección simétrica vale igual: ¿qué protege al agente honesto acusado en falso de una brutalidad que no cometió? La misma respuesta: evidencia anclada en el momento de la captura, de serie, para todos [14].

Grabar a la policía: un derecho con multa

En España, el derecho a documentar la calle ha vivido una década de zona gris. El artículo 36.23 de la Ley de Seguridad Ciudadana — la «ley mordaza», de 2015 — sanciona el uso de imágenes de agentes en intervenciones policiales; el Tribunal Constitucional anuló el término «no autorizado», cerrando la puerta a la censura previa, y, según las crónicas, los cuerpos policiales ya no aplican la infracción en su forma original [6]. PSOE y Sumar pactaron en 2024 una reforma para que el riesgo para los agentes al difundir imágenes tenga que ser «constatable» y reflejarse motivadamente [6]. El contexto más amplio explica la desconfianza: a los diez años de la ley, en marzo de 2025, se habían impuesto más de 400.000 multas — del conjunto de la ley, no solo de este artículo — y el tercer intento de reforma seguía en trámite [7];

Amnistía Internacional habla de «diez años de vulneraciones de derechos humanos y promesas incumplidas» [8].

Grabar a la policía en el ejercicio de funciones públicas, de buena fe y sin poner a nadie en peligro, es una garantía democrática: lo demostró Frazier en Minneapolis [1] y lo demostró el vídeo de «Rodea el Congreso» en Madrid [3]. Pero quien graba se expone todavía a la incertidumbre sancionadora, y el material que capta es frágil: un móvil confiscado o roto, un archivo borrado, y la prueba muere con él.

La respuesta de t2p es doble. Primero, el anclaje en captura: si la huella de cada segmento se ancla mientras se graba [14], ni la destrucción del dispositivo borra la existencia fechada del material — lo que se grabó queda acreditado, aunque haya que recuperar una copia más tarde. Segundo, la protección de quien graba: el diseño de solo-huellas no publica nada, no identifica a nadie y no difunde ninguna imagen; fija que aquello existía, y basta. Documentar deja de ser un acto de riesgo con prueba frágil para ser un acto discreto con prueba indestructible.

La cámara corporal: la mirada del otro lado

La simetría empieza por los cuerpos policiales, y el despliegue ya es un hecho. Los Mossos d'Esquadra han extendido las cámaras corporales Axon Body 3 al 98 % del territorio, con 800 unidades y 300 más previstas; 5.000 agentes han recibido la formación necesaria y se han habilitado horas de autorización para 7.000 policías, con 1.500 más en camino; el reglamento de uso se está actualizando, y los sindicatos reclaman su generalización [9][10]. La Policía Nacional extiende gradualmente su «Dispositivo de Grabación Unipersonal» (modelo AB3) entre los agentes de seguridad ciudadana, y está previsto que llegue también a la Guardia Civil; el objetivo declarado es doble: proteger a la ciudadanía y proteger a los agentes ante acusaciones falsas [11].

Pero el despliegue no resuelve el punto crítico: la custodia. ¿Quién guarda las imágenes? ¿Quién decide qué fragmento se publica, cuál «se pierde», cuál acompaña el comunicado de prensa? Una cámara corporal sin integridad verificable es, en esencia, la memoria de una sola parte: puede documentar la agresión al agente, y puede desaparecer cuando documenta el exceso. La confianza que genera depende, toda, de la confianza en quien la custodia.

Aquí es donde la propuesta de este libro completa lo que las cámaras han empezado: una cadena de huellas continua, anclada en captura [14]. Cada segmento de vídeo se sella al nacer, de modo que cualquier corte, hueco o edición posterior se vuelve matemáticamente detectable. El agente honesto gana el primero: nadie podrá decir que su vídeo exculpatorio es un montaje. Y el ciudadano gana a la vez: ninguna supresión selectiva pasará desapercibida, y el mando que publique un fragmento tendrá que asumir que el contexto existe, está fechado y es exigible judicialmente. La cámara corporal con anclaje deja de ser la memoria del más fuerte para ser la memoria de todos.

«Esto es IA»: el dividendo del mentiroso llega a la calle

En agosto de 2024, Donald Trump afirmó falsamente que la fotografía de la multitud que esperaba a Kamala Harris en el aeropuerto de Detroit era «generada por IA». La foto la había hecho un miembro del equipo de campaña y no estaba manipulada; había unas 15.000 personas, y periodistas de Associated Press y de otros medios, presentes en la misma pista, habían documentado la multitud desde todos los ángulos; los verificadores lo desmintieron en cadena [12][13]. La lección es de hielo: si una multitud fotografiada por decenas de profesionales se puede negar con dos palabras, ¿qué no se podrá negar de un vídeo incómodo de diez segundos grabado por un manifestante anónimo — o por una cámara corporal?

El «dividendo del mentiroso» — el concepto que introdujimos en el capítulo 106: la capacidad de despachar como falsa la prueba auténtica pero incómoda — corta en dos direcciones cuando llega a la calle. En una, el poder puede negar el vídeo real de un exceso policial: «montaje», «IA», «descontextualizado». En la otra, un grupo violento puede negar el vídeo real de sus altercados — o, peor, fabricar uno falso para criminalizar una protesta pacífica, con las mismas herramientas de síntesis que ya hemos visto aplicadas a voces e imágenes en capítulos anteriores.

En ambos escenarios, la salida estructural es la misma: que el material auténtico lleve fecha y huella ancladas desde el primer segundo [14], y que el material sin anclaje valga cada día menos ante un tribunal y ante la opinión pública. La verdad de la calle no se puede defender a gritos; se defiende con matemática.

La prueba de existencia aplicada

Una plaza llena, y dos relojes que graban: el móvil de una manifestante y la cámara corporal de un agente. Ninguno de los dos relatos podrá ser reescrito.

1. El manifestante que documenta

Una manifestante graba una intervención policial. Mientras graba, el dispositivo calcula por segmentos la huella SHA-512 y la ancla con el sello de tiempo RFC 3161/eIDAS [14]. No publica nada: el anclaje no revela ni contenido ni identidad. Si el móvil se pierde, se rompe o le es confiscado, la existencia y la fecha del material quedan acreditadas. Si la acusan de haber agredido a alguien — como en «Rodea el Congreso» [3][4] —, el vídeo íntegro aparece con una autenticidad que ninguna impugnación genérica puede tumbar. Si alguien grita «esto es IA» [12], la huella anterior al desmentido lo desmiente. Y si la agresión la cometió ella, el mismo sello servirá a la acusación: la prueba no tiene bando.

2. El agente con la cámara anclada

La cámara corporal del agente [9][11] genera una cadena continua de huellas: cada segmento, sellado en captura [14]. Ante una queja falsa por brutalidad, su vídeo es inatacable. Ante una sospecha de supresión selectiva, la cadena muestra si hay huecos, y los auditores — internos, judiciales o parlamentarios — pueden inspeccionar la secuencia entera. El cuerpo policial que publica un fragmento lo hace sabiendo que el contexto es fechado y exigible. La transparencia deja de depender de la buena voluntad del momento.

3. El observador y el periodista

Los observadores de derechos humanos y los fotoperiodistas que cubren la manifestación (capítulos 17 y 20) trabajan con equipos que sellan en captura: su material se convierte en un paquete probatorio con cadena de custodia desde la calle hasta la sala de vistas [14]. Y pueden hacerlo sin exponer sus fuentes: primero la huella; la publicación, solo si hace falta y cuando sea seguro — el mismo modelo de evidencia verificable que el libro ha mostrado para los conflictos armados en el capítulo 20.

4. La reconstrucción simétrica

El juzgado recibe las dos corrientes ancladas — móviles ciudadanos y cámaras corporales — y, en lugar de palabra contra palabra, obtiene una línea de tiempo fusionada y verificable: qué pasó primero, quién respondió qué, con qué proporcionalidad. El atestado, que por sí solo necesita ratificación [5], llega acompañado de material cuya fecha e integridad no admiten discusión. Las instrucciones se acortan; las sentencias se asientan sobre hechos.

Los límites, dichos con la misma claridad: el sello no otorga ningún derecho a grabarlo todo en toda circunstancia — la reforma de la ley de seguridad ciudadana sigue pendiente [6][7], y la intimidad de terceros cuenta; no valora la proporcionalidad de una carga ni la legalidad de una detención, que corresponden al juez; no sustituye testigos ni periciales; y un clip auténtico puede seguir siendo engañoso si se recorta el contexto. El anclaje acredita existencia e integridad; no acredita completitud.

La promesa y el peligro

La promesa: que nunca más la verdad de una plaza dependa de la casualidad de que alguien grabara [1][3], ni de la custodia unilateral de unas imágenes [9], ni de la credulidad ante el «esto es IA» [12]. Evidencia simétrica, anclada y neutral: la infraestructura probatoria de una democracia que se manifiesta. Los peligros, sin embargo, son serios, y hay que mirarlos de cara.

El primero es la **inversión vigilante**. Las herramientas para documentar el poder no pueden acabar identificando a quienes protestan. Anclar un vídeo no debe implicar ningún registro de quién estaba en la plaza: el diseño de solo-huellas no revela contenido ni identidad, y el reconocimiento facial sobre material de manifestaciones es una línea que una democracia no debe cruzar (véase el capítulo 108: participación sin vigilancia). Ningún registro central, ninguna desanonimización.

El segundo es **el auténtico descontextualizado**. El sello acredita que un clip existía; no acredita qué pasó fuera de plano. Un fragmento verídico recortado con malicia es la desinformación más difícil de combatir. Las mitigaciones: cadenas continuas en lugar de clips sueltos, metadatos de secuencia y una cultura del contexto — el sello nunca puede ser un argumento de autoridad total.

El tercero es **el hielo sobre la calle**. Si manifestarse implica saberse grabado por todas partes y para siempre, el miedo puede vaciar las plazas — el mismo efecto amortiguador que las sanciones de la ley mordaza han proyectado sobre fotógrafos y activistas durante una década [7][8]. Por eso la revocabilidad y la caducidad de las huellas personales, y la publicación siempre voluntaria, no son extras técnicos: son condiciones democráticas del sistema.

Y el cuarto es **la coartada tecnológica**. Ninguna cámara sustituye la reforma legal pendiente [6][7], ni la formación policial, ni los mecanismos independientes de rendición de cuentas. El sello hace la verdad recuperable; la justicia, la deben hacer las instituciones.

Es hora de actuar

La plaza es de todos, y su verdad también debe serlo.

Para manifestantes y ciudadanía: graba de buena fe cuando haga falta, sella en captura [14] y no publiques rostros de terceros sin necesidad; conoce el marco legal vigente [6] y recuerda que la huella te protege aunque no publiques nunca nada.

Para los cuerpos policiales: desplegad las cámaras corporales con cadena de huellas anclada [9][11][14] y publicad las políticas de custodia y conservación. El agente honesto es el primer beneficiario de una prueba que nadie puede poner en duda.

Para jueces y fiscales: exigid integridad anclada al material de ambas partes; una línea de tiempo verificable vale más que cien ratificaciones de atestado [5].

Para los legisladores: culminad la reforma del artículo 36.23 con un derecho explícito a documentar de buena fe [6][7]; reconoced presunción de autenticidad a la evidencia sellada en captura; y prohibid el reconocimiento facial masivo sobre material de protestas.

Para los medios y los observadores de derechos humanos: incorporad el sello en captura a vuestros equipos de serie (capítulos 17 y 20), verificad el anclaje antes de publicar material de terceros y tratad el material sin huella con la cautela que merece [12][13].

Darnella Frazier tenía diecisiete años y un teléfono, y el mundo la creyó [1][2]. La próxima Darnella quizá no sea creída — salvo que su vídeo lleve una fecha que ningún poderoso pueda borrar. Para que la plaza siga diciendo la verdad, time2act.

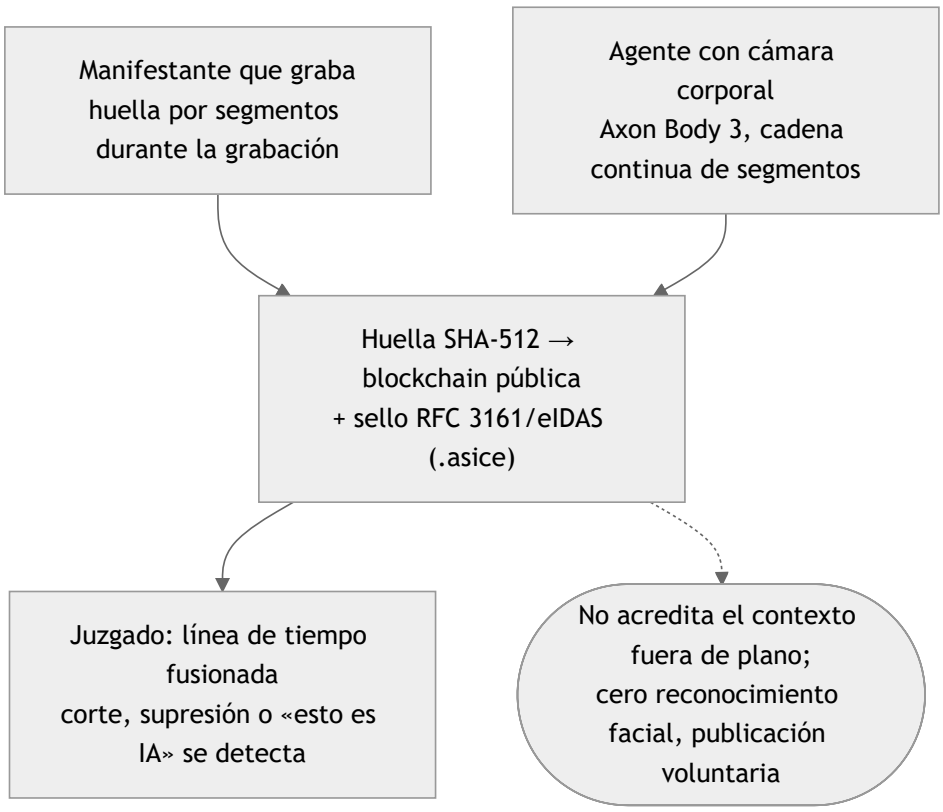


Figura 109.1 — La prueba simétrica en la calle: el vídeo del manifestante y la cámara corporal del agente se sellan en captura, por segmentos (huella SHA-512 en el dispositivo, sello de tiempo RFC 3161/eIDAS, anclaje en la blockchain pública, .asice), sin publicar nada ni identificar a nadie. En el juzgado, las dos cadenas se fusionan en una línea de tiempo verificable; cualquier corte o supresión se detecta. Límites: el sello no acredita el contexto fuera de plano, no valora la proporcionalidad y exige revocabilidad, publicación voluntaria y cero reconocimiento facial. Fuentes: Pulitzer/Frazier; elDiario.es («Rodea el Congreso»); SME/USPAC (Axon Body 3); Telemundo/Univision (Detroit).

---

[1] NPR — *Pulitzer Board Recognizes Darnella Frazier For Recording George Floyd's Murder* (11 de junio de 2021; mención especial; cita literal del jurado). https://www.npr.org/2021/06/11/1005601724/darnella-frazier-teen-who-filmed-george-floyds-murder-wins-pulitzer-prize-citati ↩

[2] Wikipedia — *Darnella Frazier* (17 años al grabar; el vídeo como prueba en el juicio de Derek Chauvin). https://en.wikipedia.org/wiki/Darnella_Frazier ↩

[3] elDiario.es — *Juicio a tres policías por acusar en falso a una manifestante de agresión: «Ella no está condenada porque había un vídeo»* (caso «Rodea el Congreso»; el atestado inicial solo recogía insultos). https://www.eldiario.es/politica/juicio-tres-policias-acusar-falso-manifestante-si-no-llegamos-encontrar-video-hubieran-condenado_1_10922988.html ↩

[4] elDiario.es — *Absueltos los antidisturbios acusados de mentir en un juicio contra una manifestante del 'Rodea el Congreso'* (absolución; el tribunal no ve delito pese a la ausencia de pruebas de la agresión). https://www.eldiario.es/politica/absueltos-antidisturbios-acusados-mentir-juicio-manifestante-rodea-congreso_1_10979336.html ↩

[5] Togas.biz — *Si el atestado policial no ha sido ratificado en el plenario… las manifestaciones en él contenidas no tienen eficacia probatoria* (doctrina sobre la eficacia probatoria del atestado). https://togas.biz/articulos/articulo-profesionales--si-el-atestado-policial-no-ha-sido-ratificado-en-el-acto-del-plenario-por-los-agentes-de-la-autoridad-que-lo-confeccionaron-sometiendose-al-principio-de-publicidad-y-contradicci-n-las-manifestaciones-en-l-contenidas-no-tiene-la-eficacia-probatoria/ ↩

[6] Infobae — *El artículo de la 'ley mordaza' que derogarán PSOE y Sumar fue declarado inconstitucional y los policías ya no lo aplican* (17 de julio de 2024; art. 36.23; el TC anula el término «no autorizado»; reforma pactada: riesgo «constatable» y motivado). https://www.infobae.com/espana/2024/07/17/el-articulo-de-la-ley-mordaza-que-derogaran-psoe-y-sumar-fue-declarado-inconstitucional-y-los-policias-ya-no-lo-aplican/ ↩

[7] Infobae — *Más de 400.000 multas y un tercer intento de reforma: la ley mordaza cumple 10 años* (31 de marzo de 2025; multas del conjunto de la ley). https://www.infobae.com/espana/2025/03/31/mas-de-400000-multas-y-un-tercer-intento-de-reforma-la-ley-mordaza-cumple-10-anos-en-medio-de-las-criticas-sobre-su-impacto-en-derechos-y-libertades/ ↩

[8] Amnistía Internacional España — *Ley Mordaza: diez años de vulneraciones de derechos humanos y promesas incumplidas* (2025). https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/ley-mordaza-diez-anos-de-vulneraciones-de-derechos-humanos-y-promesas-incumplidas/ ↩

[9] SME — Sindicat de Mossos d'Esquadra — *Consell de la Policia de 6 de febrer del 2025* (Axon Body 3 al 98 % del territorio con 800 cámaras; 5.000 agentes formados; autorización para 7.000 y 1.500 más; reglamento en actualización). https://sme-mossos.cat/consell-de-la-policia-de-6-de-febrer-del-2025/ ↩

[10] USPAC — *Resum reunió subcomissió de materials, 27 de novembre de 2024* (300 cámaras más previstas; peticiones de generalización). https://uspac.cat/resums-reunions/resum-reunio-subcomissio-de-materials-27-novembre-2024/ ↩

[11] Cámaras de Vigilancia IP — *Cámaras unipersonales de la Policía: funcionamiento y normativa* (DGU modelo AB3; extensión gradual; previsto para la Guardia Civil; objetivo: proteger ciudadanía y agentes). https://camarasdevigilanciaip.es/camaras-unipersonales-policia/ ↩

[12] Telemundo — *Trump afirma falsamente que una foto de la multitud en un mitin de Harris en Detroit fue creada con inteligencia artificial* (agosto de 2024; foto de un miembro del equipo, sin manipular; periodistas de AP en la pista; 15.000 asistentes). https://www.telemundo.com/noticias/noticias-telemundo/elecciones-estados-unidos-2024/trump-afirma-falsamente-que-una-foto-de-la-multitud-en-un-mitin-de-har-rcna166423 ↩

[13] Univision — *Esas fotografías de eventos de campaña de Kamala Harris no fueron creadas con IA, como afirman Trump y en redes* (verificación). https://www.univision.com/noticias/fotografias-eventos-campana-kamala-harris-no-ia-como-afirman-trump-y-redes ↩

[14] t2p — manual de producto (huella SHA-512 en el dispositivo, por segmentos durante la grabación; sello de tiempo RFC 3161/eIDAS; anclaje en la blockchain pública; contenedor .asice; cadena de huellas continua para cámaras corporales; publicación opcional). Véanse los capítulos 13 y 15. ↩

Clavar los talones: el coste de no hacer nada

«Odio a los indiferentes. Creo que vivir quiere decir tomar partido. [...] La indiferencia es el peso muerto de la historia.»

— Antonio Gramsci, «Indifferenti», La città futura (1917)

En 2050, en la primera tarde de un julio que parece no acabarse nunca, el sol se alza como un disco incandescente sobre una llanura deshabitada al sur del Sahel. Las dunas, ahora recubiertas por capas de polvo fino que reflejan la luz en tonos de gris metálico, son el único rastro visible de una civilización que decidió clavar los talones ante el cambio climático. En la frontera entre lo que queda de Malí y lo que antes era una ciudad costera, un grupo de refugiados —hombres y mujeres con sus posesiones más preciadas envueltas en trapos desgastados— se reúne alrededor de un pozo de arena que aún conserva agua. No es solo agua; es el último recurso que puede salvarlos de una muerte segura por deshidratación. En este mundo, las aseguradoras hace tiempo que se retiraron de regiones que antes consideraban de «riesgo moderado», y la cobertura ante los desastres climáticos se ha convertido en un lujo inalcanzable para la mayoría.

Esta escena no es una predicción: es uno de los futuros que aún podemos escoger o evitar. Y lo que la hace estremecedora es que en 2026 ya sabíamos lo suficiente para impedirla. Los informes del IPCC mostraban que mantener el calentamiento global por debajo de los 2 °C requeriría una transición energética decidida e inversiones del 1-2 % del PIB mundial[3]. Pero las políticas de la década anterior fallaron a la hora de aplicar estas medidas, y dejaron que las emisiones siguieran su camino ascendente. En aquel futuro, el calentamiento ha superado los 3 °C respecto al nivel preindustrial, tal como advertían las proyecciones para las políticas vigentes[1]. A este nivel, los modelos económicos indican que el PIB per cápita mundial podría caer más del 50 % hacia el año 2100 si llegamos a 2 °C por encima del nivel actual[1]; y a 3 °C, la producción acumulada disminuye entre un 15 % y un 34 % respecto a lo que se esperaba[1].

Los efectos se dejan sentir en cada rincón del planeta. Las olas de calor se alargan durante semanas, tensan los sistemas sanitarios y disparan su gasto cuando se les suman las enfermedades relacionadas con la exposición prolongada al calor y la desnutrición. El coste neto de la inacción llega a representar entre un 11 % y un 27 % del producto acumulado mundial —tres veces el gasto sanitario global proyectado hasta 2100—, una carga que ninguna economía puede soportar sin consecuencias[2]. Y los puntos de inflexión del sistema climático, una vez traspasados, pueden costar hasta 2,4 billones de euros al año[2]. Las migraciones masivas se han convertido en una realidad cotidiana; ciudades costeras enteras se encuentran inundadas y abandonadas.

Así, aquel 2050 no es solo un año más avanzado en la cronología; es el reflejo de una decisión colectiva que habría preferido la comodidad de la inacción a la energía de la transformación. El precio de la procrastinación se mide en vidas perdidas, economías desintegradas y una confianza global erosionada — un doble peligro, climático y de credibilidad, que se alimenta mutuamente. La pregunta que queda pendiente, y que resuena entre las dunas y las ciudades abandonadas, es simple pero profunda: ¿qué cantidad de futuro estamos dispuestos a sacrificar por mantenernos quietos?

Hacia dónde vamos

Los números no mienten: las políticas vigentes nos arrastran hacia un escenario de **más de 3 °C de calentamiento global**, y esto ya es una realidad documentada [1]. La distancia entre las promesas que se hacen en las cumbres de las COP y la realidad del terreno, descrita en el capítulo 6, no es solo un tema de diplomacia; se paga en grados. Cada décima perdida representa vidas que se desvanecen, sectores económicos que colapsan y una confianza global que se rompe como el vidrio bajo presión.

Como hemos visto, las proyecciones indican una caída del PIB per cápita superior al 50 % y pérdidas entre el 15 % y el 34 % de la producción mundial hasta 2100, con costes que podrían llegar hasta **2,4 billones de euros anuales** [2]; estas cifras reflejan una economía que se derrumba ante fenómenos climáticos cada vez más intensos —sequías prolongadas, inundaciones devastadoras e incendios forestales que arrasan infraestructuras clave.

En contraposición, la inversión necesaria para limitar el calentamiento por debajo de los 2 °C es sorprendentemente modesta: **entre el 1 % y el 2 % del PIB mundial** [3]. Esta cifra representa solo una fracción de lo que costaría mantenernos en el estado de pasividad actual, sin contar las oportunidades

perdidas de un crecimiento sostenible basado en tecnologías limpias. Por tanto, asumir que actuar implica costes prohibitivos es un error económico y moral; el verdadero coste es la abstención.

Además, el doble peligro —climático y de confianza— se retroalimenta. Cada grado adicional empeora las condiciones ambientales y alimenta la desconfianza en las instituciones y los procesos democráticos, ya que la población percibe una incapacidad de actuar ante la crisis. Esta erosión de credibilidad reduce la capacidad colectiva para movilizar recursos y apoyo político necesario para medidas ambiciosas, generando un círculo vicioso cada vez más difícil de escapar.

Como hemos visto, las políticas actuales nos llevan directamente hacia una temperatura que supera los 3 °C, traduciéndose en pérdidas económicas masivas y un aumento del gasto sanitario. La inversión para frenar este camino es relativamente pequeña comparada con el coste de no hacer nada; ahora hay que romper esta inercia, reconocer que cada grado perdido es una advertencia y actuar inmediatamente, ya que solo así se puede preservar tanto el planeta como la confianza en nuestras instituciones.

El precio de no hacer nada

Imagina una escala que mide el bienestar económico mundial como un termómetro: cada grado adicional de calentamiento global recorta el PIB per cápita y la diferencia es brutal. Como hemos visto, un aumento de 2 °C podría reducir este indicador más del 50 % hacia el final del siglo, mientras que superar los 3 °C provocaría una caída entre el 15 % y el 34 % de la producción acumulada hasta 2100 [1]. Este descenso no es solo una cifra abstracta; significa que buena parte de las personas del planeta verían reducida a la mitad su capacidad de compra, de ahorro y de inversión, y se traduciría en menos recursos para educación, salud e innovación.

Pero el coste económico directo no es el único factor que pesa sobre esta balanza. El coste neto de la inacción —la diferencia entre los gastos adicionales generados por el cambio climático y los beneficios de una política de adaptación o mitigación— se sitúa entre el 11 % y el 27 % de la producción acumulada [2]; como hemos visto, esta franja equivale a tres veces el gasto sanitario global proyectado hasta 2100, revelando cómo las consecuencias del cambio climático se extenderán a todos los ámbitos de la vida humana: desde el aumento de enfermedades relacionadas con el calor hasta la aparición de epidemias emergentes por la migración de vectores.

Además, hay puntos de inflexión que amenazan con romper el sistema en momentos críticos. Las estimaciones indican que estos cambios estructurales pueden costar hasta 2,4 billones de euros al año [2]. Estas cifras no son meramente costes adicionales; representan la necesidad urgente de invertir en infraestructura resiliente, tecnologías limpias y sistemas de gobernanza capaces de gestionar el aumento de los riesgos. Cada año que pasa sin una respuesta coordinada acumula este coste oculto y lo convierte en una carga cada vez más pesada para las generaciones futuras.

En resumen, la inacción no es un estado neutro: es una apuesta económica y social que cuesta mucho más de lo que cualquier inversión preventiva podría pedir. Las cifras muestran claramente que el precio de quedarnos quietos supera de manera significativa el de actuar ahora, tanto en términos de pérdida de bienestar material como de deterioro de la confianza institucional. La clave para evitar este escenario desolador es reconocer que cada grado perdido incrementa los costes y reducir inmediatamente las emisiones para mantener el calentamiento por debajo de los 2 °C, una tarea que supone solo el 1-2 % del PIB mundial [3]. Es un compromiso asequible comparado con la factura colosal de la inacción.

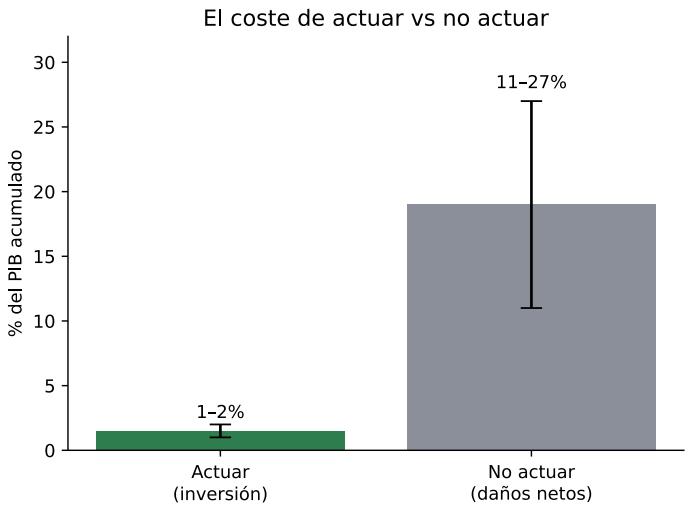


Figura 110.1 — Cuanto más sube la temperatura, más cae la economía: el coste de no actuar se dispara con cada décima de grado.

El riesgo sistémico doble

En el corazón de una crisis que se bifurca entre verdad y clima, las dos se enredan en una espiral de retroalimentación que amplifica cada vulnerabilidad. La incertidumbre alimentada por *deepfakes* sofisticados, informes de *greenwashing* y narrativas manipuladas erosiona la confianza institucional e impide una gobernanza eficaz de la transición energética; sin datos fiables, las políticas climáticas se convierten en proyectos en el aire, vulnerables a presiones económicas y a desinformación que diluye el consenso científico. Cada retraso incrementa los costes climáticos.

A la inversa, un escenario más cálido genera una crisis de verdad aún más profunda: fenómenos extremos —inundaciones, incendios forestales y sequías prolongadas— producen flujos de información caótica que a menudo se traducen en noticias sensacionalistas o falsificadas por intereses particulares. Cuando las comunidades sufren daños reales, la percepción pública se fragmenta; algunos buscan explicaciones científicas y otros adoptan narrativas conspirativas que minimizan la responsabilidad humana, dificultando la aplicación de medidas de adaptación o mitigación por parte de los gobiernos.

Los datos muestran claramente cómo esta doble crisis multiplica el riesgo global; si las políticas actuales siguen su trayectoria, el calentamiento mundial superará los 3 °C y el PIB per cápita caerá drásticamente —como hemos visto—. El coste neto de la inacción equivale a una parte importante de la producción acumulada global, superando tres veces el gasto sanitario previsto hasta el final del siglo, y los puntos de inflexión podrían llegar hasta 2,4 billones de euros al año si no se toman medidas urgentes [1][2].

En contraste, contener el calentamiento por debajo de los 2 °C solo requiere una inversión modestísima —entre el 1 y el 2 % del PIB mundial [3]—, una cifra asequible comparada con la factura colosal de la inacción. Esta disparidad demuestra que el verdadero peligro no reside tanto en las tecnologías o los costes iniciales, sino en el estallido de una crisis de confianza que paraliza la respuesta colectiva; reforzar instituciones fiables y sistemas de verificación transparente es tan urgente como cualquier política climática.

Así, el doble riesgo sistémico —clima y verdad— no son fenómenos independientes, sino dos caras de una misma moneda. La incapacidad de confiar en los datos impide gobernar la transición; la falta de gobierno eficaz empeora el clima, que a su vez genera más incertidumbre y desinformación. Romper este círculo vicioso es el objetivo central de time2act: demostrar que, con inteligencia artificial y cadena de bloques para garantizar la integridad de la información, podemos restaurar la confianza e impulsar acciones climáticas decisivas antes de que los costes se vuelvan insostenibles.

El coste de la mentira, cara a cara

El coste de no actuar no se mide solo en grados. Hay una segunda factura, más silenciosa, que ya se está pagando: la de la confianza que se derrumba. Y, como la climática, crece con cada año de retraso. Recorrámosla por los cinco frentes que este libro ha examinado.

En las **finanzas**, una sola videollamada falsificada costó unos 25,6 millones de dólares a la ingeniería Arup en 2024 [4]; y la consultora Deloitte proyecta que el fraude impulsado por la inteligencia artificial podría llegar a los 40.000 millones de dólares anuales en Estados Unidos en 2027 [5]. Cada estafa erosiona un poco más la confianza que engrasa el comercio.

En la **sanidad**, una imagen médica manipulada —un tumor inyectado o borrado— no cuesta dinero: cuesta diagnósticos acertados, tratamientos a tiempo y, en última instancia, vidas. En la **educación**, los títulos falsos y la autoría imposible de verificar deprecian el mérito de toda una generación. Y en la **democracia y la defensa**, los deepfakes electorales y la desinformación de guerra hacen añicos la base de hechos compartida sin la cual ninguna sociedad puede ponerse de acuerdo para actuar —ni siquiera sobre el clima.

Y estos cinco frentes solo son el principio. A lo largo del libro, la misma factura de la desconfianza ha ido apareciendo en cada rincón de la vida colectiva: en el **clima**, donde los créditos de carbono inflados y el greenwashing vacían de sentido cada tonelada ahorrada; en la **economía real**, desde el seguro y la cadena de suministro hasta los inmuebles, la tokenización de activos, la propiedad intelectual y las licitaciones públicas; y, en este último tramo, en el tejido mismo de la sociedad: la **identidad** de quienes no tienen documento para probar que existen, la **integridad electoral** de las actas y el escrutinio, la **ayuda humanitaria** que debe llegar a la persona real, los **testamentos**, el **comercio internacional**, la **auditoría** de las cuentas, el **fraude publicitario**, los **registros de ciberseguridad**, el **patrimonio artístico** y la protección de los **denunciantes** que se juegan la libertad. Y aún más allá, en las nuevas fronteras: la **ciencia**, donde un dato fabricado corrompe el conocimiento; el **cuerpo**, desde las pensiones y el dopaje hasta el dato genético que también es de tu familia; las **máquinas**, que deciden accidentes y guardan su propia caja negra; los **mercados** especializados de la música, el hardware y las materias primas; y la **justicia misma**, donde una grabación auténtica se puede negar como falsa. En cada frente, el mecanismo del daño es el mismo —una prueba que se puede fabricar o negar— y la defensa también: una prueba de existencia que nadie pueda alterar impunemente.

Porque aquí los dos costes convergen. Una sociedad que no se pone de acuerdo sobre qué es real no se pondrá de acuerdo sobre qué hay que hacer ante los 3 °C. El «dividendo del mentiroso» —la posibilidad de descartar cualquier prueba incómoda tachándola de falsa— paraliza la acción climática tanto como la desinformación directa. La crisis de la verdad y la crisis del clima no son dos emergencias separadas; son la misma emergencia vista desde dos ángulos, y se alimentan mutuamente [6].

La conclusión vuelve a ser la misma, y por eso es tan poderosa: el seguro más barato contra ambas facturas es la verdad verificable. Anclar los datos —climáticos, financieros, médicos, educativos, probatorios— para que nadie los pueda alterar impunemente no es un gasto técnico; es la condición previa para que cualquier otra inversión tenga sentido. Sin una base de hechos fiable, incluso el 1-2 % del PIB que hace falta para frenar el calentamiento se gastaría en medio del ruido y la sospecha. Con ella, cada euro cuenta. El coste de la mentira, como el del carbono, solo sube mientras no actuamos.

La apuesta racional

Imaginemos una sala de reuniones llena de altos cargos que observan un gráfico de líneas ascendentes: cada grado adicional de calentamiento se acumula como una carga invisible sobre las economías del mundo. En aquel momento, una voz rompe el silencio y, como hemos visto, señala que solo una pequeña fracción del PIB mundial invertida en la transición podría mantener el calentamiento por debajo de los 2 °C. Esta es la promesa de las políticas climáticas con respaldo científico, y el coste de no actuar es una bomba de relojería que late más fuerte a cada instante.

Las proyecciones actuales muestran que las políticas insuficientes nos llevan hacia un escenario de calentamiento superior a los 3 °C antes del fin del siglo [1]. En este contexto, el impacto económico es devastador: como hemos visto, si el planeta llega a una temperatura de 2 °C por encima del nivel actual, el producto interior bruto per cápita podría caer más del 50 % en 2100, y a 3 °C la producción acumulada mundial se reduciría entre un 15 % y un 34 % [1]. Paralelamente, el coste neto de la inacción se estima entre el 11 % y el 27 % de la producción acumulada —equivalente a tres veces el gasto sanitario global hasta 2100— con puntos de inflexión que podrían llegar a 2,4 billones de euros al año [2].

En contraste, destinar entre el 1 % y el 2 % del PIB a financiar la transición hacia fuentes de energía renovable, mejorar la eficiencia energética y desplegar sistemas que garanticen la transparencia de los datos climáticos representa un gasto comparativamente pequeño [3]. Esta inversión no es un coste adicional, sino un seguro económico sin precedentes: el retorno se mide en reducción de riesgos y

preservación del crecimiento a largo plazo. Cada euro invertido ahora evita décadas de pérdidas masivas, desde inundaciones que devastan infraestructuras hasta crisis sanitarias alimentadas por el aumento de las temperaturas.

Además, la inversión en inteligencia artificial y cadena de bloques ofrece una doble capa de protección. Por un lado, la IA puede optimizar los procesos de generación y distribución de energía, reducir el consumo innecesario y aumentar la resiliencia del sistema; por otro, la cadena de bloques asegura que los datos climáticos sean verificables y difíciles de alterar, contrarrestando la oleada de desinformación y deepfakes que minan la confianza pública. Esta combinación aspira a crear un ecosistema donde la información fiable alimente decisiones políticas acertadas, rompiendo el círculo vicioso entre incertidumbre climática y pérdida de credibilidad.

En definitiva, la apuesta racional consiste en reconocer que el coste de actuar es una fracción diminuta del producto mundial, mientras que el precio de la inacción se extiende durante décadas y afecta a todos los sectores de la sociedad. La decisión no es entre pagar o no pagar; es entre invertir en un futuro sostenible o dejar que las consecuencias económicas y sociales nos sobrepasen. Como ciudadanos, empresarios y líderes, tenemos la oportunidad —y la responsabilidad— de aportar este 1-2 % del PIB mundial, y asegurar así una economía más robusta y un planeta habitable para las generaciones futuras. La pregunta que queda es: ¿estamos dispuestos a hacer esta pequeña apuesta para garantizar nuestro bienestar colectivo?

La promesa y el peligro

Al borde del límite climático, las herramientas que hace unos años parecían fantasías de ciencia ficción son ahora recursos tangibles y económicamente viables. Las fuentes de energía renovable —solar fotovoltaica, eólica marina e hidrógeno verde— han abaratado sus costes de manera espectacular y, en buena parte de los mercados, ya son más baratas que las fósiles. Así, la transición se convierte tanto en una necesidad ambiental como en una oportunidad para reducir los costes operativos empresariales.

Esta nueva abundancia energética se ve potenciada por la inteligencia artificial, capaz de optimizar el balance entre oferta y demanda en tiempo real, minimizando pérdidas y maximizando el aprovechamiento de los recursos intermitentes. Los algoritmos de predicción meteorológica, cada vez más precisos, se integran en las redes inteligentes, reduciendo la necesidad de reservas costosas y aumentando la fiabilidad del suministro. Paralelamente, la cadena de bloques ofrece transparencia y trazabilidad que contrarresta la opacidad de los mercados energéticos tradicionales; los contratos inteligentes pueden automatizar el pago de energía verde y asegurar que cada kilovatio-hora proviene realmente de una fuente limpia, minimizando el riesgo de greenwashing.

Como hemos visto, invertir solo entre uno y dos por ciento del PIB mundial permitiría mantener el calentamiento global por debajo de los 2 °C, el umbral establecido por el pacto de París [3]. Se trata de un gasto modesto comparado con la reducción de pérdidas por desastres climáticos y con el incremento de productividad que conlleva.

Sin embargo, el peligro se presenta como una fuerza invisible pero potente: la inercia institucional y la resistencia cultural al cambio. La desinformación —alimentada por redes sociales e intereses económicos — distorsiona los datos reales y hace que el público perciba las soluciones como costosas o arriesgadas cuando, en realidad, son más baratas que el coste de la inacción; **como hemos visto** [1].

Además, los costes ocultos de la inacción ya empiezan a hacerse sentir: el coste neto estimado de no actuar se eleva hasta un 11 %-27 % de la producción global acumulada hasta 2100, equivale a tres veces el gasto sanitario mundial de aquel período y podría llegar a 2,4 billones de euros al año [2]. Este impacto no solo afecta a la economía; erosiona la confianza social e institucional y genera un círculo vicioso donde la incertidumbre alimenta más inacción.

Como hemos visto, disponemos de una caja de herramientas tecnológicas ya demostradas como eficientes y económicas. El reto no es encontrar soluciones, sino superar las barreras psicológicas y políticas que nos empujan hacia el camino más caro: la inacción. Si elegimos este último, el coste acumulado será muy superior al de cualquier inversión responsable hoy. La decisión se convierte, por tanto, en una cuestión de visión: ¿preferimos invertir un pequeño porcentaje de nuestro producto interior bruto para garantizar un futuro sostenible y fiable, o dejaremos que la inercia y la desinformación nos lleven a un coste mucho más alto e irreversible?

Las dos curvas

Imaginemos una sala de control donde se proyectan dos gráficos simultáneos: por un lado, la curva aparentemente ascendente del PIB mundial si las políticas actuales continúan tal como son; por el otro, el descenso abrupto del producto interior bruto cuando el calentamiento supera los 3 °C. La primera muestra un crecimiento aparente, pero a largo plazo revela una caída de la producción acumulada de entre el 15 % y el 34 % si llegamos a este umbral crítico [1]; la segunda indica que el coste neto de la inacción podría absorber entre el 11 % y el 27 % del producto global, el equivalente a tres veces el gasto sanitario mundial hasta 2100, con puntos de inflexión que llegan a 2,4 billones de euros al año [2] —como hemos visto.

En contraste, la inversión necesaria para mantener el calentamiento por debajo de los 2 °C se sitúa entre el 1 % y el 2 % del PIB mundial [3]. Esta cifra, comparada con los porcentajes de producción que se perderán si no hacemos nada, es poco más que un ajuste de presupuesto. Es, por tanto, una decisión de escala humana: destinar una pequeña parte de nuestro producto interior bruto a la transición energética y a las infraestructuras digitales que garanticen transparencia y trazabilidad.

El plan debe ser tan claro como el mapa de una ruta marítima. Primero, establecer hitos intermedios con plazos cortos y financiar proyectos piloto que combinen la inteligencia artificial para optimizar el uso energético y la cadena de bloques para certificar la procedencia limpia de los recursos. Segundo, crear mecanismos de rendición de cuentas basados en contratos inteligentes: si una empresa supera los objetivos establecidos, recibe incentivos; si falla, se derivan consecuencias verificables. Tercero, movilizar capital privado mediante bonos verdes y fondos de impacto que sean auditables en tiempo real gracias a la cadena de bloques.

Esta hoja de ruta no es una mera lista de medidas —es un contrato colectivo entre gobiernos, empresas y ciudadanos. Cada acción debe ser medible, verificable y, sobre todo, ajustable si los resultados no coinciden con las expectativas. La confianza se reconstruye cuando el público puede ver, en tiempo real, cómo se invierte el dinero y qué impacto tangible genera. Así, la doble amenaza —climática y de confianza — se desactiva simultáneamente: una reducción efectiva de emisiones disminuye las presiones ambientales que alimentan la incertidumbre social, y una infraestructura transparente refuerza la credibilidad institucional.

En última instancia, el reto es tan político como tecnológico. Es necesario que los líderes adopten una visión a largo plazo y reconozcan que el coste de una inacción prolongada supera con mucho los gastos inmediatos de un plan de transición. El momento es ahora; la ruta está dibujada y solo queda decidir si avanzamos con pasos firmes o nos quedamos atrapados en el estancamiento, dejando que la historia registre una oportunidad perdida y un futuro empobrecido.

---

[1] Oxford Economics, *The global economic costs of climate inaction*. https://www.oxfordeconomics.com/resource/the-global-economic-costs-of-climate-inaction/ ↩

[2] Climate Policy Initiative, *The Cost of Inaction*. https://www.climatepolicyinitiative.org/the-cost-of-inaction/ ↩

[3] (síntesis de modelización climática-económica) Earth.org. https://earth.org/have-economists-been-underestimating-the-cost-of-climate-change/ ↩

[4] World Economic Forum — *Cybercrime: lessons from a $25m deepfake attack* (caso Arup). https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/ ↩

[5] Deloitte — *Generative AI is expected to magnify the risk of deepfakes and other fraud in banking*. https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html ↩

[6] Sumsub — *Global deepfake incidents surge tenfold from 2022 to 2023*. https://sumsub.com/newsroom/sumsub-research-global-deepfake-incidents-surge-tenfold-from-2022-to-2023/ ↩

¿Cómo llegamos? Una hoja de ruta

«Caminante, no hay camino, / se hace camino al andar.»

— Antonio Machado, «Proverbios y cantares», XXIX (1912)

En 2035 la ciudad de Barcelona se alza como testigo vivo de una decisión tomada diez años atrás: en 2026, los gobiernos y las empresas decidieron actuar. Desde el primer momento en que se aprobó el marco regulador para la prueba de existencia basada en IA y blockchain, las infraestructuras de confianza empezaron a proliferar como filamentos de una red neuronal colectiva. Hoy, en el paseo de la Rambla, los turistas no solo consultan mapas digitales; escanean códigos QR que, con un simple gesto, verifican el origen y la integridad de cada producto —desde el vino de la DO Penedès hasta las piezas de arte fabricadas por impresión 3D. Cada etiqueta lleva una pequeña cadena de bloques que registra, en tiempo real, los pasos de producción, transporte y consumo, todo sin consumir apenas energía: la blockchain moderna, tras el Merge, ha reducido su coste energético cerca de un 99,95 % respecto al modelo anterior, de modo que anclar la verdad ya no malgasta el planeta [2].

En las fachadas de los edificios se proyectan datos verificables de impacto climático: gráficos que muestran cómo los sistemas urbanos han optimizado el consumo gracias a la inteligencia artificial. Estas plataformas inteligentes ajustan el consumo de electricidad de los edificios en función de la demanda real y la disponibilidad de energía renovable, minimizando los residuos y maximizando la eficiencia. La inversión necesaria para este cambio se estimó entre el 1 y el 2 % del PIB mundial —una cifra que muchos críticos consideraron demasiado alta en aquel momento, pero mucho más barata que el coste de no hacer nada— y la recuperación de estos costes ha sido rápida, impulsada por el ahorro operativo y la nueva confianza del mercado [1].

En las escuelas, los estudiantes aprenden a usar herramientas de IA que ayudan a verificar documentos y noticias, dificultando la propagación de deepfakes. En un centro de investigación, una joven investigadora muestra cómo un sistema entrenado para reconocer manipulaciones digitales puede contrastar en milisegundos una imagen viral contra su origen, enviando inmediatamente el resultado a una cadena de bloques pública. Este proceso —la prueba de existencia, el corazón de *t2p*— se ha convertido en un pilar de la confianza digital: cada dato que circula por la red es rastreable hasta el momento en que fue sellado, y cualquier alteración queda al descubierto.

En el mercado laboral, las empresas ya no dependen únicamente de auditorías anuales para validar certificaciones; muchas credenciales se emiten y se verifican al instante a través de contratos inteligentes. Un ingeniero informático puede demostrar, con una sola transacción, que ha completado un proyecto de código abierto, y su historial queda registrado de manera verificable para futuros colaboradores.

Este escenario no es una utopía; es la culminación posible de una serie de decisiones concretas tomadas a lo largo de una década. Cada actor —gobierno, empresa, ciudadano— puede adoptar un conjunto de principios claros, que van desde el compromiso con la estandarización de la prueba de existencia hasta la elección de protocolos de consenso de bajo consumo energético. El resultado es una sociedad donde la confianza se construye sobre datos verificables, y donde las tecnologías emergentes trabajan como infraestructura para un futuro sostenible y justo.

Los tres actores

Gobernantes — liderar el marco de confianza. El primer paso de un gobierno responsable es establecer un precio al carbono que refleje el coste real del daño climático e incentive la descarbonización a todos los niveles de la economía. Este precio debe estar respaldado por estándares internacionales de verificación y monitorización (MRV) basados en la prueba de existencia. La blockchain moderna, tras el Merge, consume mucha menos energía que las cadenas de bloques tradicionales, como hemos visto, y puede convertirse así en la columna vertebral de un registro inmutable y verificable de datos de emisiones [2]. Los gobiernos pueden financiar redes de verificación a escala nacional y regional, apoyar la investigación de protocolos de consenso ultraeficientes y establecer legislación que oriente a las empresas hacia informes ESG certificados de manera comprobable. De esta forma se crea una cadena de confianza donde cada declaración de impacto puede auditarse casi en tiempo real, reduciendo el riesgo de greenwashing y aumentando la credibilidad ante inversores y ciudadanos.

Empresas — transformar los datos en activos sostenibles. Para las organizaciones, la clave es invertir en una infraestructura limpia que garantice la trazabilidad de sus procesos productivos. Esto implica desplegar soluciones de blockchain para anclar datos ESG y utilizar pruebas de existencia para validar cada paso del ciclo de vida del producto, desde la extracción de materias primas hasta el reciclaje final. Las empresas que adoptan este modelo no solo cumplen la normativa emergente, sino que también ganan una ventaja competitiva: los consumidores y los inversores prefieren marcas que ofrecen transparencia verificable. Además, la adopción de estas tecnologías reduce los costes asociados a auditorías externas y certificaciones tradicionales, liberando recursos para la innovación y el crecimiento sostenible. El principio es sencillo: invertir en limpio, anclar los datos y no hacer greenwashing.

Ciudadanía — ser vigilante y activa. Cada individuo dispone de pequeñas pero potentes palancas: optimizar el consumo energético en el hogar, adoptar movilidad eléctrica y verificar las declaraciones antes de compartirlas. Las herramientas basadas en blockchain permiten que cualquier usuario compruebe la trazabilidad de una información con solo unos clics, evitando la propagación de desinformación y reforzando la confianza colectiva. Además, la participación ciudadana en programas de monitorización distribuida —como las redes de sensores para la calidad del aire o los contadores inteligentes de energía— alimenta datos accesibles públicamente y sirve de fundamento para políticas locales más efectivas. La combinación de acción personal con herramientas de verificación descentralizada crea un ecosistema donde la responsabilidad se distribuye, aumentando la presión sobre gobiernos y empresas para que actúen con integridad.

Como hemos visto, los **gobernantes** deben establecer precios al carbono y marcos reguladores robustos; las **empresas** deben convertir sus datos ESG en activos inmutables y transparentes; y la **ciudadanía** debe ejercer una vigilancia activa, aprovechando las herramientas de prueba de existencia para validar la información. Esta sinergia multiplica el impacto de cada palanca, convirtiendo el desafío global en una oportunidad colectiva. Es hora de ponernos en marcha: **time2act**.

La infraestructura de confianza

La transición hacia una economía limpia y resiliente se fundamenta en una única premisa: sin datos fiables no hay acción efectiva. Durante todo *time2act* hemos mostrado cómo las tecnologías emergentes pueden transformar la incertidumbre en seguridad, y ahora es el momento de consolidar este hilo conductor. La inteligencia artificial (IA) y la blockchain forman una sinergia que permite generar, validar y compartir información con un grado de integridad hasta ahora difícil de alcanzar. En este ecosistema, la prueba de existencia —el concepto central de *t2p*— actúa como anclaje inmutable para todo tipo de evidencias: desde las emisiones de carbono de una fábrica hasta los certificados de energía verde de un microgrid comunitario.

1. Datos inmutables, decisiones ágiles

La blockchain garantiza que cada registro de emisión o certificado ESG se mantenga inalterable y verificable para cualquier parte interesada. Esto reduce la necesidad de procesos de auditoría costosos y prolongados, acortando el tiempo de validación de semanas a minutos. Esta eficiencia no solo impulsa la competitividad, sino que crea una base sólida para políticas públicas fundamentadas en evidencias reales.

2. La IA como motor de análisis y predicción

Los algoritmos de IA procesan grandes volúmenes de datos en tiempo real, identificando patrones ocultos y proyectando escenarios futuros con una precisión cada vez más alta. Cuando estas predicciones se apoyan en registros inmutables, su credibilidad aumenta: los resultados dejan de ser solo estimaciones difíciles de contrastar y pasan a estar anclados en una capa de confianza verificable. Esto permite a gobiernos y empresas tomar medidas proactivas —como ajustar la producción de energía renovable o reorientar inversiones— sin la parálisis de la duda sobre la veracidad de los datos.

3. Prueba de existencia: el sello de la verdad

t2p ofrece una solución técnica para cualquier información que requiera autenticación. Mediante un hash criptográfico y el registro en una cadena de bloques pública, se genera una prueba de existencia que puede ser consultada por cualquier actor —desde el consumidor hasta el regulador— sin necesidad de intermediarios. Esta capacidad es crucial en la era de los deepfakes y la desinformación: cada declaración,

certificación o reclamación puede contrastarse con una prueba inmutable, reforzando la confianza social y mercantil.

4. Gobernanza descentralizada y participación ciudadana

La blockchain no solo almacena datos; también habilita mecanismos de gobernanza transparente. Mediante contratos inteligentes, las organizaciones pueden establecer reglas claras para la gestión de activos digitales, recompensar comportamientos sostenibles y penalizar infracciones de manera automática. Además, los ciudadanos disponen de herramientas de verificación que les permiten ejercer una vigilancia activa sobre las políticas públicas y las prácticas corporativas, convirtiendo la supervisión en un proceso colectivo y continuo.

5. Ruta hacia la acción: principios para todos los actores

1. **Adoptar plataformas blockchain de bajo consumo energético** — el Merge ha reducido el consumo de energía de las cadenas modernas cerca de un 99,95 % [2].
2. **Integrar la IA para el procesamiento y el análisis de datos ESG**, asegurando que cada modelo se nutra de registros verificados.
3. **Implementar la prueba de existencia como estándar de validación** en certificados, informes y declaraciones públicas.
4. **Fomentar la participación ciudadana mediante portales abiertos**, donde cualquier usuario pueda consultar y validar los datos con un clic.
5. **Establecer marcos reguladores que reconozcan la cadena de bloques como fuente de verificación**, simplificando los procesos de auditoría.

Como hemos visto, la confianza es el puente entre la visión de un futuro sostenible y la realidad operativa actual. La combinación de IA y blockchain, reforzada por *t2p*, crea una infraestructura que convierte datos en verdad y verdad en acción. El reto ya no es tecnológico sino colectivo; depende de cada empresa, gobierno y ciudadano ponerse en marcha. Es hora de actuar con decisión y convicciones claras: **time2act**.

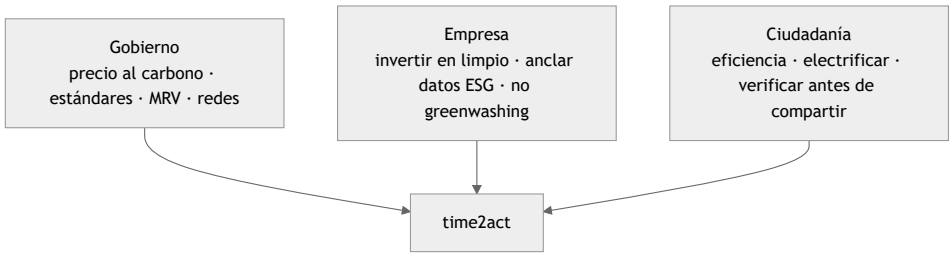


Figura 111.1 — Cada actor —gobierno, empresa y ciudadanía— tiene acciones concretas a corto, medio y largo plazo.

Los principios de la acción

1. Electrificarlo todo lo posible. La transición energética ya no es una opción, sino la base sobre la que se construye cualquier modelo sostenible. Cada equipamiento industrial, cada flota de transporte y cada infraestructura urbana debería estar alimentada por electricidad, preferentemente generada a partir de fuentes renovables. La clave es establecer un calendario de migración escalable: identificar los puntos críticos, sustituir los equipos por motores de alta eficiencia y aprovechar las oportunidades de carga inteligente para equilibrar la demanda.

2. Hacerlo con energía limpia y firme. No basta con electrificar si la electricidad proviene de origen fósil. La combinación de IA para optimizar el gasto energético y de blockchain para registrar en tiempo real la procedencia de la corriente ayuda a garantizar una cadena de suministro verdaderamente limpia. Cuando cada kilovatio-hora se puede certificar mediante un contrato inteligente, la energía limpia deja de ser solo una aspiración ambiental y se convierte también en una palanca de competitividad y de confianza para el consumidor.

3. Medir y verificar de manera incorruptible. La verdad de los datos se convierte en el nuevo activo más valioso. Mediante *t2p*, cada registro de energía consumida, de emisiones o de resultados operativos se puede codificar en una cadena de bloques inmutable, dificultando las manipulaciones y facilitando auditorías mucho más rápidas. La medición precisa y la verificabilidad instantánea son, por tanto, los pilares que sustentan cualquier estrategia de impacto real.

4. Alinear incentivos. El precio del carbono debe reflejar su coste social. Aplicar un precio a las emisiones y eliminar las subvenciones a los combustibles fósiles crea un marco económico donde las decisiones verdes son también las más rentables. Este alineamiento incentiva comportamientos responsables y orienta la inversión hacia las tecnologías limpias, sin necesidad de intervenciones reguladoras excesivas.

5. Proteger la verdad como bien público. En una era de deepfakes y desinformación, la confianza se convierte en un recurso escaso. La infraestructura basada en blockchain, reforzada por *t2p*, hace que la información crítica sobre energía, emisiones e impacto social sea inmutable y accesible a todos los interesados. Las políticas públicas deben reconocer la verdad como un bien común, estableciendo marcos legales que protejan los datos certificados y disuadan las manipulaciones. Así, cada ciudadano, empresa o gobierno puede confiar en una fuente verificable para tomar decisiones informadas.

Estos cinco principios no son solo recomendaciones teóricas; son pasos concretos que cualquier actor —desde la start-up más ágil hasta el gobierno nacional— puede empezar a implementar hoy mismo. Al seguirlos, convertimos el potencial de la IA y la blockchain en una infraestructura de confianza capaz de transformar datos en verdad y verdad en acción. **time2act**.

El horizonte regulador

Ninguna hoja de ruta estaría completa sin mirar el marco legal que se acerca, porque la regulación recompensará a quienes se adelanten. En Europa, el artículo 50 del Reglamento de Inteligencia Artificial (la EU AI Act) obligará a marcar en formato legible por máquina el contenido generado por IA y a etiquetar las *deepfakes*; sus obligaciones se aplican a partir del 2 de agosto de 2026 [3]. En paralelo, el reglamento eIDAS 2.0 despliega la cartera de identidad digital europea e introduce figuras nuevas —los registros electrónicos cualificados y el archivo electrónico cualificado— que dan reconocimiento legal al modelo de traza de auditoría inmutable que este libro defiende [4].

Al otro lado del Atlántico, Estados Unidos ha aprobado la TAKE IT DOWN Act (firmada en mayo de 2025), que penaliza la imagen íntima no consentida —incluidas las generadas por IA— y obliga a las plataformas a retirarla en 48 horas; y la DEFIANCE Act, aprobada por el Senado en enero de 2026, añade una vía civil para que las víctimas puedan reclamar [5].

El mensaje para gobiernos y empresas es inequívoco: la expectativa legal ya no es solo «guardar» la información, sino poder DEMOSTRAR su origen y su integridad. Las organizaciones que hoy adoptan la prueba de existencia —anclar el hash de cada dato crítico antes de compartirlo— no cumplirán la norma a regañadientes y a última hora, sino que llegarán preparadas, porque ya habrán convertido la verificabilidad en un hábito. La regulación no es, pues, una carga añadida a la transición: es el mismo camino, señalizado.

La promesa y el peligro (síntesis)

Por primera vez en la historia contemporánea disponemos de un diagnóstico claro, de herramientas probadas y de una infraestructura capaz de proteger la verdad que sustenta nuestras decisiones. La inteligencia artificial, alimentada por grandes volúmenes de datos limpios y verificados, puede transformar información dispersa en conocimiento accionable con una precisión que hace décadas era imposible. Paralelamente, la blockchain —en su forma más eficiente tras el Merge, que ha reducido el consumo energético cerca de un 99,95 %— ofrece una capa de imparcialidad e inmutabilidad que convierte cada transacción, cada registro de propiedad intelectual o cada certificación climática en una prueba de existencia difícil de falsear [2]. Esta combinación crea una infraestructura de confianza donde la verdad no solo se detecta, sino que se mantiene intacta ante intentos de manipulación, como los deepfakes y las campañas de desinformación masiva.

No obstante, el relato de la oportunidad está inevitablemente entrelazado con un peligro inminente. Actuar tiene un coste —entre el 1 y el 2 % del PIB mundial para mantener el calentamiento por debajo de los 2 °C—, pero es mucho más barato que el coste de no actuar, que crece con cada año de retraso [1]. Además, la tecnología, aun siendo poderosa, no es una panacea. La blockchain puede garantizar la integridad de los registros, pero sin una voluntad política y empresarial decidida a adoptarla, estos registros permanecen inactivos, como archivos en un depósito cerrado. De manera similar, los modelos de IA pueden ofrecer predicciones útiles, solo si se dispone de datos fiables y de procesos de gobernanza que aseguren su utilización ética y transparente.

La ventana para aprovechar esta sinergia es limitada. Cada año que pasa sin una acción coordinada aumenta el coste económico y complica el camino tecnológico, porque las infraestructuras legales y reguladoras se quedan atrás respecto al ritmo de innovación. Las barreras de adopción —desde la falta de talento especializado hasta la oposición de intereses establecidos— se hunden cuando el momento clave desaparece. Por eso, hace falta una voluntad colectiva que impulse políticas públicas, inversiones estratégicas y colaboraciones intersectoriales para desplegar esta infraestructura de confianza a escala global.

Disponemos de herramientas y del marco conceptual necesarios para que la verdad sea el fundamento de cada decisión; pero si no actuamos ahora, la puerta se cerrará, los costes aumentarán y nuestra capacidad de actuar con información fiable quedará comprometida. La clave es combinar la potencia tecnológica con una voluntad decidida a transformar esta promesa en realidad concreta. Es el momento de decir **time2act**.

Esta visión se ve reforzada por Beth Noveck, quien tras el escándalo Horizon —donde más de 900 condenas injustas condujeron a al menos trece suicidios— propone que la inteligencia artificial sea una infraestructura cívica, **verificable, auditable y responsable ante las personas a las que impacta** [6]. Su marco de contratación obliga a gobiernos y empresas a exigir registros anclados en blockchain neutral e independientes del creador, asegurando que cada modelo de IA pueda ser revisado y reproducido sin cajas negras. Este requisito convierte la prueba de existencia en una condición mínima para cualquier licitación pública, transformando datos y algoritmos en activos abiertos que se pueden validar en tiempo real, y completa nuestra hoja de ruta: no solo protegemos la verdad, sino que hacemos obligatoria su transparencia desde el primer momento de adquisición.

Es time2act

Hace veinte años, Paul Roberts, en *The End of Oil* (2004), pintó el cuadro de un mundo que se quedaba sin energía fácil, con una geopolítica fragmentada y un clima que mostraba las primeras fisuras irreversibles. Su diagnóstico, tan preciso como alarmante, aún resuena en cada sala de consejos directivos y en cada aula universitaria. Pero el panorama ha cambiado: hoy disponemos no solo del conocimiento de los riesgos, sino también de una infraestructura tecnológica capaz de restablecer la confianza que la crisis ha erosionado.

Principio 1 — Verdad como base operativa. La prueba de existencia convierte cualquier dato —desde certificados de origen energético hasta resultados de auditorías climáticas— en un registro inmutable y verificable. Esto reduce la incertidumbre que alimenta los deepfakes y las manipulaciones de mercado, y permite decisiones basadas en hechos contrastables.

Principio 2 — Eficiencia energética como requisito. Como hemos visto, la blockchain moderna consume mucha menos energía que las primeras iteraciones [2]. Esto significa que la infraestructura de confianza no se convierte en una nueva fuente de demanda desbocada, sino en una herramienta que puede convivir con los sistemas ya existentes.

Principio 3 — Coste de adopción sostenible. Mantener el calentamiento por debajo de los 2 °C requiere invertir entre el 1 y el 2 % del PIB mundial, una cifra que se paga con creces si se compara con el coste de la inacción: incremento de desastres climáticos, pérdida de confianza en los mercados y aumento del precio de las materias primas [1]. La transición no es gratuita, pero es mucho más barata que su contrario.

Principio 4 — Escalabilidad para todos los actores. Desde gobiernos nacionales hasta start-ups de energía renovable, la combinación de IA para el procesamiento de datos y blockchain para su certificación crea una capa que se puede adoptar progresivamente. Cada entidad puede iniciar un piloto local —por ejemplo, validar el origen de la energía en una zona industrial— y escalar hacia cadenas de suministro más amplias.

Principio 5 — Gobernanza participativa. La transparencia inherente a estos sistemas permite incluir a ciudadanos, académicos y ONG en procesos de verificación y auditoría, reforzando el contrato social y generando un ecosistema donde la confianza no es una concesión sino una consecuencia natural.

El camino que se abre ante nosotros es claro: integrar IA y blockchain como pilares de una nueva arquitectura de confianza, desplegando la prueba de existencia para garantizar que cada decisión se fundamente en datos auténticos. No solo hay que implantar tecnología; hay que transformar

mentalidades, establecer marcos reguladores ágiles y crear colaboraciones intersectoriales que catalicen el cambio.

Así pues, la llamada no es a más diagnósticos ni a promesas vacías, sino a poner en marcha las herramientas que ya tenemos. El momento de hablar ha pasado; ahora toca actuar con decisión y precisión. **Es time2act**.

---

[1] (coste de actuar 1-2% del PIB) Oxford Economics / CPI. https://www.climatepolicyinitiative.org/the-cost-of-inaction/ ↩

[2] ethereum.org, *The Merge*. https://ethereum.org/roadmap/merge/ ↩

[3] EU AI Act, artículo 50 (transparencia del contenido generado por IA; aplica 2-ago-2026). https://artificialintelligenceact.eu/article/50/ ↩

[4] Signaturit — *eIDAS 2.0: registros y archivo electrónicos cualificados*. https://www.signaturit.com/blog/eidas-2-regulation/ ↩

[5] Orrick — *TAKE IT DOWN Act becomes law*; DEFIANCE Act (Senado, ene-2026). https://www.orrick.com/en/Insights/2025/05/TAKE-IT-DOWN-Act-Becomes-Law ↩

[6] Beth Simone Noveck — *Reboot* (Yale UP, 2026), cap. 8; Post Office Horizon Inquiry (Sir Wyn Williams, 2024). ↩

El sello y la cadena: quién controla la prueba, y quién queda atrapado

«El poder tiende a corromper, y el poder absoluto corrompe absolutamente.»

— Lord Acton, carta a Mandell Creighton (1887)

A la entrada de un laboratorio improvisado en Nairobi, una fila de personas esperaba para ser inspeccionada. Entre ellas, jóvenes estudiantes, vendedores ambulantes y familias con niños pequeños se alineaban bajo un póster que anunciaba «World ID — Demuestra que eres humano». Un equipo de ingenieros, con mascarillas de protección y una cámara de alta resolución, escaneaba el iris de cada persona mientras un monitor mostraba números que parecían confirmar su identidad. En menos de dos minutos, el sistema registraba una «prueba» inmutable en una cadena de bloques pública, asignándole un crédito criptográfico como recompensa por participar.

Esta escena, que podría aparecer en cualquier reportaje optimista sobre la lucha contra bots y deepfakes, es exactamente lo que *time2act* ha defendido: un mecanismo fiable para demostrar que detrás de un avatar hay una persona real. No obstante, la ironía se vuelve palpable cuando, solo dos años después, el mismo proyecto Worldcoin/World ID se enfrenta a prohibiciones y multas en más de nueve jurisdicciones. Kenia lo declaró inconstitucional, y tanto Kenia como Colombia ordenaron la destrucción total de los datos biométricos recogidos. Lo que había empezado como una solución para reforzar la confianza digital se transforma en un ejemplo claro del peligro que esconde cualquier infraestructura inmutable [1].

Esta paradoja es el punto de arranque de este capítulo. La infraestructura que permite t2p —biometría, registro inmutable y cadena de bloques— puede ser, simultáneamente, la arquitectura de la vigilancia masiva. No se trata de un rechazo del concepto; el mecanismo es necesario para combatir la falsificación digital. Lo que sí hay que reconocer, tal como establece Snowden, es que «el credo del sistema de vigilancia masiva era 'recógelo todo, procésalo todo, aprovéchalo todo, asócialo todo'», y que este patrón ya ha dejado una huella indeleble en nuestra historia reciente [20].

Este capítulo se presenta como el contrapeso honesto del libro. Siguiendo el mandato de *time2act* —«la promesa y el peligro»— recoge, en un solo lugar, las críticas que hasta ahora habían estado dispersas entre informes de ética, análisis legales y testimonios de whistleblowers. La tesis central es clara: la descentralización técnica no garantiza una gobernanza democrática; el verdadero problema son las relaciones de poder que se establecen en torno al control de la prueba. ¿Quién define las reglas de entrada a este registro? ¿Quién puede eliminar o modificar los datos sin rendición de cuentas? ¿Qué intereses se benefician cuando una sola entidad controla tanto el acceso como la verificación?

En el contexto actual, donde los grandes L2 de Ethereum operan con un único secuenciador corporativo y el 42 % de los bloques son censurados según las listas OFAC [5], la pregunta que queda abierta es quién verifica al verificador. La cadena de bloques puede decir «no confíes, verifica», pero sin una auditoría independiente y transparente, esta verificación se convierte en una forma sutil de control, como recuerda Dominic Frisby: «el lema de la cadena de bloques es «no confíes, verifica»; pero la pregunta que queda abierta es quién verifica al verificador» [32].

Así, este capítulo de apertura pone de relieve que, pese a las promesas de confianza restaurada, la misma tecnología puede ser utilizada para consolidar poder e imponer una vigilancia que limita la libertad individual. La respuesta no es desestimar la biometría ni la cadena inmutable, sino construir marcos de gobernanza democrática que aseguren que el «sello» sirva para protegernos y no para atraparnos. El próximo paso del lector será confrontar estas tensiones y considerar cómo garantizar que el control de la prueba se mantenga al servicio de la sociedad, y no en manos de una élite tecnológica.

La neutralidad que no existe

Al atardecer de 2026, la infraestructura que sostiene la red Ethereum se ve dominada por una sola entidad: un secuenciador corporativo gestionado por Coinbase a través de Base. No es solo una cuestión de rendimiento; este único nodo decide qué bloque se incluye y en qué cadena de confirmación pasa, ejerciendo una forma de censura que afecta al 42 % de los bloques de Ethereum vía relays que aplican las listas OFAC. Además, la capa segunda de validación que t2p usa hoy ha concentrado la producción de bloques en un grupo reducido de validadores elegidos tras la actualización «Rio» (2025) [5].

Esta concentración contradice el mito popular de que la blockchain es inherentemente descentralizada y neutral. La verdad es que quien programa y opera los nodos determina qué registros se guardan y quién tiene acceso a ellos. Como señala Cathy O'Neil, los modelos matemáticos que sostienen estas infraestructuras son «opacos e invisibles para todos excepto para los grandes sacerdotes del sector: los matemáticos y los ingenieros informáticos» [4]. Su observación revela que la confianza no recae en el código, sino en las personas que lo escriben y lo mantienen.

Marc Goodman lo resume con claridad: «quien controle el código controlará el mundo, para bien y para mal» [3]. Esto no es una hipérbole; la capacidad de definir las reglas de una cadena inmutable se traduce en poder sobre la identidad digital, los derechos de propiedad intelectual e incluso la capacidad de excluir a actores políticos o sociales. Edward Snowden confirma esta dinámica: «estas máquinas hacen lo que hacen porque alguien se lo ordena, de una manera muy concreta y minuciosa; y ese alguien puede ser incluso un niño de siete años» [2].

En la mesa donde se redactan las reglas del juego, el margen para saltárselas es enorme. Jack Watling observa que «estar en la mesa donde se establecen las reglas del juego aumenta el margen de un estado para saltarse esas mismas reglas en beneficio propio» [6]. Este poder no se limita a los estados; infraestructuras privadas como Starlink, controladas por corporaciones sin rendición de cuentas democrática, se han convertido en activos estratégicos que modelan la comunicación global y, por tanto, la capacidad de vigilancia y control [7].

El paralelismo histórico es revelador. Dominic Frisby recuerda cómo Isaac Newton, como único responsable de la ceca real (Master of the Mint), concentró el control de la validación de la moneda y persiguió a los falsificadores con una rigurosidad implacable [8]. La centralización del poder de verificación no es un fenómeno nuevo; solo ha cambiado de metal a bits.

Sin una gobernanza democrática explícita que regule quién puede ser validador, cuáles son sus obligaciones y cómo se supervisan las decisiones, la prueba de existencia (t2p) corre el riesgo de transferir el poder de los intermediarios tradicionales —bancos, notarios, autoridades públicas— a una élite técnica que opera en la sombra; como hemos visto. La infraestructura inmutable se convierte así en un nuevo tipo de intermediario: invisible pero decisivamente influyente, y sin mecanismos de rendición de cuentas que garanticen su neutralidad.

El consentimiento cristalizado

En el marco del «consentimiento verificado» que sustenta la prueba de existencia, el libro ha presentado este sello como garantía de transparencia y responsabilidad. Sin embargo, la mera existencia de una aceptación registrada no asegura que sea autónoma ni libre. Carissa Véliz recuerda que «no tienes margen para negociar los términos y las condiciones, que, además, pueden cambiar en cualquier momento sin aviso previo»[9]; y la opinión del Comité Europeo de Protección de Datos subraya que el modelo «consentir o pagar» no constituye un consentimiento «libremente prestado»[10]. Esto quiere decir que, cuando la cadena blockchain sella permanentemente aquel «acepto», transforma una posible elección voluntaria en un hecho inmutable y, por tanto, ineludible.

Dos ejemplos concretos ilustran cómo esta dinámica se materializa en infraestructuras de registro. En la Casa de Contratación de Sevilla, el registro de obligaciones se imponía mediante juramentos obligatorios y sanciones que llegaban hasta doscientos azotes por incumplimiento[11]. Aquel «registro inmutable» servía como herramienta de coacción: el acto de firmar no era una manifestación libre, sino un requisito legal que, si se rechazaba, comportaba penas económicas y personales severas. En este contexto, la blockchain podría consolidar la memoria de aquellos juramentos, convirtiéndolos en testigos eternos de una presión institucional.

Otro vector de coerción proviene de la dependencia energética que sostiene las redes descentralizadas. Jack Watling describe esta situación como un «dedo puesto sobre la garganta»[12], una condición que invalida la autonomía del consentimiento porque los operadores no pueden disociarse de la infraestructura crítica sin comprometer su funcionamiento. La necesidad de un suministro energético constante para nodos y validadores crea una vulnerabilidad estructural: el «clic» que da fe del consentimiento se convierte en un acto forzado, motivado por el temor a perder acceso a recursos esenciales.

Estos casos revelan una contradicción fundamental en la propuesta de t2p. Si la tecnología registra y verifica cualquier aceptación sin discernir entre voluntad e imposición, el resultado es una forma de

autoritarismo digital que refuerza las jerarquías de poder existentes. La solución no consiste solo en añadir más capas de seguridad criptográfica; hay que introducir mecanismos de gobernanza que puedan validar la legitimidad del propio consentimiento. Esto implica, por ejemplo, establecer protocolos de auditoría independiente que revisen las condiciones contractuales y aseguren que el registro no se convierta en una herramienta de coacción estructural.

En definitiva, la cadena puede ser un testigo fiable solo si su testimonio es genuino. Distinciones claras entre consentimiento real y forzado deben ser incorporadas al diseño de t2p; de lo contrario, el «clic» eterno que se registra podría acabar por perpetuar las formas de control que pretende combatir. El reto, pues, no es solo tecnológico sino institucional: hay que garantizar que la verificación del consentimiento vaya acompañada de un marco democrático que proteja la autonomía de los individuos e impida que el sello se convierta en una cadena de vigilancia.

La plusvalía de la prueba

Cuando tokenizamos la experiencia humana como «prueba de existencia», lo que aparentemente es una herramienta para restablecer la confianza se convierte, en realidad, en un activo negociable. Shoshana Zuboff describe este fenómeno como el capitalismo de la vigilancia: «la experiencia humana [es] materia prima gratuita» que las plataformas extraen, predicen y venden [13]. Cada vez que una huella biométrica o un sello temporal se registra en una cadena inmutable, se añade una nueva unidad de valor a la base de datos que alimenta el mercado de la información personal. La propia Zuboff recuerda que «los acaparados somos nosotros; nuestra experiencia es el objeto de extracción» [14], subrayando que el control del flujo de datos se traduce en poder económico y político.

Esta dinámica no es solo teórica. En 2024, la Federal Trade Commission de Estados Unidos prohibió por primera vez a corredores de datos la venta de localizaciones sensibles y multó a Avast con 16,5 millones de dólares [15]. El mismo año, la Autoridad de Protección de Datos neerlandesa (DPA) impuso una sanción de 30,5 millones de euros a Clearview AI por haber creado una base biométrica de treinta mil millones de fotografías extraídas sin consentimiento. Estas acciones demuestran que la mercantilización del registro inmutable ya ha generado un modelo de ingresos basado en la explotación de las pruebas de identidad, y que los mecanismos reguladores todavía luchan por mantener el paso.

El aviso histórico de Dominic Frisby sobre la degradación silenciosa de los estándares ofrece una perspectiva de largo plazo. El denario romano, según Frisby, pasó del 95-98 % de plata a menos de un 1 % sin que nadie se diera cuenta [16]. Este declive se produjo porque no había una auditoría independiente y continua que vigilara la calidad y la integridad del sistema monetario. De manera paralela, las tecnologías de registro inmutable pueden sufrir una erosión similar si su funcionamiento queda sometido a intereses privados sin supervisión pública. La falta de una auditoría permanente deja abierta la puerta a manipulaciones sutiles: cambios en los algoritmos de consenso, inserción de nodos controlados por entidades corporativas y, finalmente, una concentración del poder que contradice el ideal descentralizado.

Por tanto, hay que establecer salvaguardas concretas contra la mercantilización de los datos registrados. Primero, el protocolo debe incluir mecanismos de verificación externa, con auditores independientes acreditados por instituciones democráticas y no por empresas que sacan provecho de ellos. Segundo, se debe instaurar un marco legal que obligue a la transparencia del propietario de los sellos y de las cadenas asociadas, garantizando que cualquier transferencia de valor sea pública y reversible. Finalmente, hace falta un sistema de gobernanza participativa donde los usuarios puedan ejercer control sobre las políticas de uso y las tarifas aplicadas a su propia prueba.

Solo con estas medidas se puede evitar que el «sello» se convierta en una «cadena» de explotación. La plusvalía de la prueba no reside únicamente en su capacidad técnica para validar la autenticidad, sino en el modo en que la sociedad regula quién obtiene beneficios de ella y qué límites impone a su uso. Sin una auditoría permanente y una gobernanza democrática, el riesgo es que, tal como ha pasado con las monedas antiguas, los estándares técnicos se degraden silenciosamente hasta perder completamente su función protectora.

El derecho al olvido eliminado

En el momento en que una información se graba en una cadena inmutable, su existencia deja de estar sujeta al capricho de las instituciones ni al paso del tiempo. La inmutabilidad, celebrada como garantía de confianza, se convierte simultáneamente en el anclaje de un rastreo permanente que impide cualquier

posibilidad de olvido. Edward Snowden describe este fenómeno con una precisión inquietante: «me resultaba atroz estar tan inextricable y tecnológicamente ligado a un pasado del que me arrepentía del todo, pero que apenas recordaba»[20]. No es solo una reflexión personal; es la realidad de un sistema diseñado para «recogerlo todo, procesarlo todo, aprovecharlo todo, asociarlo todo» y en el que, en el centro de sus operaciones, el centro de datos de Bluffdale se construyó para almacenar «el patrón de vida del planeta entero»[17].

Estos procesos van más allá de una simple acumulación de datos: la red ha impuesto una «fidelidad a la memoria, la uniformidad identitaria y, por tanto, la conformidad ideológica»[18]. Cuando el registro es inmutable, cualquier error, dato obsoleto o información que en un futuro pueda resultar perjudicial para el sujeto se convierte en una herida permanente. No hay mecanismo de supresión ni de anulación; la memoria digital se mantiene viva y accesible indefinidamente.

Como ya se ha señalado en 2026, este poder de rastreo se ha materializado en el uso masivo de herramientas de análisis de cadena por parte de agencias federales estadounidenses. ICE, IRS y FBI han adquirido soluciones como Chainalysis o TRM Labs con el objetivo explícito de desanonimizar el registro inmutable, vinculando direcciones digitales a personas concretas[19]. Estas tecnologías permiten seguir el flujo de activos digitales, identificar transacciones y, finalmente, rastrear a los individuos hasta su origen biológico o geográfico. El resultado es una forma de vigilancia que trasciende las fronteras tradicionales del control estatal: la información ya no depende solo del consentimiento de un usuario, sino que se convierte en un testigo inmutable de cada acción.

Frisby destaca que incluso el oro, considerado el «único dinero que no es una promesa», se vuelve vulnerable cuando su propiedad y ubicación son totalmente transparentes: «un objetivo fácil de confiscación o de impuestos»[21]. De manera análoga, un registro inmutable se convierte en un activo que cualquier autoridad puede aprovechar para imponer sanciones, confiscar bienes o limitar derechos civiles. La imposibilidad de eliminar o revocar datos erróneos significa que los ciudadanos no disponen de ningún recurso efectivo ante decisiones injustas basadas en información inexacta.

Esta situación plantea una contradicción fundamental: la inmutabilidad, que el libro ha celebrado como pilar de confianza, se convierte también en el instrumento que elimina cualquier posibilidad de olvido y, por tanto, impide la rectificación o la supresión de datos perjudiciales. Sin una auditoría permanente y una gobernanza democrática, este registro inmutable gira contra el ciudadano, convirtiéndose en una herramienta de coerción más que en una garantía de transparencia. El reto, pues, no es solo tecnológico sino político: hay que establecer mecanismos de revocabilidad y de caducidad para registros erróneos o transitorios, asegurando que la inmutabilidad no se traduzca en un estigma de injusticia permanente.

Algoritmos inapelables

En el momento en que una entidad decide sellar la procedencia de un dato, el criterio que sustenta ese sello queda oculto detrás de un muro de código y de matemáticas incomprensibles para la mayoría. Como advierte Cathy O'Neil, los veredictos emitidos por estos modelos son «inapelables» y, a la vez, «opiniones incrustadas en matemáticas» que solo los grandes sacerdotes del sector –ingenieros y científicos de datos– pueden leer y cuestionar [22]. Esta opacidad convierte el sello en una autoridad incontestable y crea un poder que supera cualquier control democrático.

Carissa Véliz refuerza esta perspectiva: predecir el comportamiento humano equivale a intentar controlarlo, una dinámica que conduce inevitablemente hacia el autoritarismo cuando las predicciones se utilizan para regular o restringir libertades [23]. El modelo que garantiza la «veracidad» de un registro inmutable puede ser empleado para imponer límites al individuo sin que este tenga conocimiento de ello ni capacidad de impugnarlo. Edward Snowden añade: «la predictibilidad es manipulación». Cuando un sistema anticipa las acciones futuras, no solo ofrece información; crea un mecanismo sutil de coacción que condiciona las decisiones presentes para ajustarlas al patrón preestablecido [24]. Así, el sello deja de ser una simple garantía de procedencia y se convierte en un instrumento de conformidad.

Esta concentración de poder algorítmico se ve reforzada por el hecho de que quien establece las reglas del juego tiene margen para romperlas. Jack Watling señala que «quien hace las reglas tiene margen para saltarse esas mismas reglas en beneficio propio» [6]. En un ecosistema donde la infraestructura de cadena de bloques y el registro inmutable son controlados por unos pocos actores corporativos, esta capacidad se traduce en una vulnerabilidad estructural: el sello puede ser modificado o ignorado según los intereses de aquellos que lo han creado.

Como hemos visto, el marco legal de 2026 retrocede ante estas amenazas; el aplazamiento de las obligaciones para la IA de alto riesgo dentro del paquete «Digital Omnibus» y la derogación de la ley de IA de Colorado dejan un vacío regulador que facilita la expansión indiscriminada de los sistemas de sellado [25]. Sin una normativa clara que imponga transparencia y revisión independiente, los algoritmos inapelables pueden operar sin ningún freno ni contrapeso.

La fragilidad del sello queda evidente también en el campo de la geolocalización. Durante la guerra de Ucrania, la interferencia electrónica engañó las señales GPS, demostrando que ni el tiempo ni la posición son invulnerables a manipulaciones deliberadas [26]. Esto revela una verdad fundamental: la fuerza vinculante del sello solo es tan segura como la fiabilidad de las infraestructuras subyacentes. Si estas pueden ser falsificadas, hay que desarrollar mecanismos de explicabilidad verificable y de rectificación que tengan la misma robustez legal que el registro inmutable original.

En resumen, la concentración del poder algorítmico convierte el sello en un arma potencial de control. La solución no reside solo en mejorar la tecnología, sino en establecer una gobernanza democrática capaz de imponer transparencia, revisión independiente y mecanismos de rectificación que impidan que el «código» se convierta en el único guardián del futuro.

La autocensura del registro permanente

En la primavera de 2024, una joven escritora catalana retiró un ensayo sobre las prácticas de inteligencia artificial en el período electoral, temerosa de que el simple hecho de publicarlo pudiera atraer la vigilancia estatal. Este comportamiento no es anecdótico; según Carissa Véliz, entre un tercio y dos tercios de los escritores evitan ciertos temas por miedo a la vigilancia gubernamental [27]. La causa profunda reside en lo que los estudiosos llaman *mission creep*: una infraestructura diseñada para un propósito —como la prueba de existencia t2p— se extiende progresivamente hacia usos no previstos, transformándose en un arma de control social.

El registro inmutable, el elemento central de cualquier cadena de bloques que pretende garantizar integridad y trazabilidad, se convierte así en un «sello» que puede ser aprovechado para imponer límites funcionales y temporales a la libertad de expresión. Un ejemplo reciente es Eurodac, el sistema europeo de huellas digitales para procesos de asilo. En 2024 se ha rebajado la edad mínima de recogida biométrica de doce a seis años, abriendo la base a un acceso policial ampliado y facilitando una vigilancia precoz sobre menores [28]. Esta expansión no es meramente técnica; es una decisión política que transforma una herramienta de gestión migratoria en una fuente de información para el control social.

La proliferación del registro permanente también alimenta efectos disuasorios más sutiles pero igualmente devastadores. En Siria, durante la guerra, la desinformación orquestada por actores rusos creó una incertidumbre fabricada que paralizó las respuestas internacionales y locales [29]. Cuando el conocimiento se vuelve incierto, la capacidad de actuar de manera autónoma se desvanece: la población empieza a autocensurarse para evitar ser objeto de posibles sanciones o persecuciones. Este fenómeno se refleja en la observación de Shoshana Zuboff de que el poder fundamental del sistema es determinar «quién sabe, quién decide y quién decide quién decide» [30]. En este escenario, el registro inmutable deja de ser una garantía de transparencia para convertirse en un mecanismo que consolida la información al servicio de unas pocas autoridades.

La legitimidad de este poder se cuestiona cuando las plataformas se convierten en «los árbitros reales de lo que la gente puede decir», como señala Véliz: hay que preguntarse si disponen del tipo adecuado de legitimidad para ejercer este control [31]. El «proteger» datos biométricos o transacciones digitales a menudo se presenta como eufemismo de «controlar» el comportamiento y las identidades de los individuos. La consecuencia directa es una autocensura que se extiende más allá del discurso, limitando la iniciativa creativa, inhibiendo la investigación crítica y alentando la autoexclusión de temas incómodos.

Para evitar que una herramienta de un fin se convierta en infraestructura de otro, hay que establecer límites explícitos tanto funcionales como temporales. Esto implica definir claramente qué datos pueden ser registrados, durante cuánto tiempo y bajo qué supervisión independiente. Solo con mecanismos de revisión transparente y la participación democrática se puede garantizar que el sello digital no se convierta en una cadena de opresión. En este equilibrio delicado entre confianza y vigilancia, el peligro real reside no tanto en la tecnología misma sino en quién la controla y cómo se permite la expansión de su alcance.

El contraargumento que t2p debe sobrevivir

En el largo viaje de este libro hemos mostrado cómo la prueba de existencia puede restaurar la confianza en un mundo saturado de deepfakes y falsificaciones digitales. Ahora nos encontramos ante el reflejo más incómodo: la misma infraestructura —biometría, registro inmutable y cadena de bloques— es el esqueleto de una arquitectura de vigilancia que podría convertir el sello digital en una cadena de opresión. La clave para no perdernos en un escenario de tecnoutopismo es reconocer que **la descentralización técnica no equivale a gobernanza democrática**; el problema fundamental son las relaciones de poder que se configuran en torno al control y la supervisión.

El lema de la cadena, «no confíes, verifica», se ha convertido en un axioma universal para la seguridad distribuida. No obstante, como señala Dominic Frisby, la pregunta abierta es **¿quién verifica al verificador?** [32] Si el proceso de verificación se mantiene dentro de una caja negra operada por unos pocos actores, lo que debería ser una garantía de transparencia se transforma en un instrumento de coacción. **Como hemos visto, en 2026 el 42 % de los bloques se construyen a través de relays que aplican censura OFAC**; la cadena que t2p usa hoy concentra la producción de bloques en un grupo reducido de validadores elegidos. [5] Esta concentración revela cómo, pese a una arquitectura descentralizada al nivel del protocolo, el control efectivo recae en manos corporativas y estatales.

Para que **t2p** pueda cumplir con su misión sin convertirse en un instrumento de vigilancia, hay que establecer cuatro exigencias imprescindibles:

1. **Gobernanza democrática de los nodos** — Quien opera, valida y audita los nodos debe estar sometido a procesos abiertos y participativos, evitando la concentración observada en las cadenas L2. La supervisión debe provenir de entidades independientes y representativas, no solo de grandes plataformas financieras.
2. **Auditoría transparente de los algoritmos** — Los métodos de verificación deben estar sujetos a revisiones periódicas por parte de expertos externos, con resultados publicados en formatos accesibles. Así se contrarresta la opacidad descrita por Cathy O'Neil, según la cual los modelos son «opiniones incrustadas en matemáticas», legibles solo para los «grandes sacerdotes del sector». [4]
3. **Mecanismo de revocabilidad y corrección** — Cuando un registro inmutable contiene errores o datos recogidos sin consentimiento (como Eurodac, que ha reducido la edad biométrica a seis años y permite acceso policial), se debe incluir una vía segura para la rectificación o supresión, garantizando el derecho al olvido y evitando el uso coercitivo de datos erróneos. [28]
4. **Control de la plusvalía de los datos** — Hay que definir claramente quién captura y comercializa la información derivada del registro; sin este control, se perpetúa una economía de vigilancia donde la información personal se convierte en bienes de altos rendimientos para corporaciones y estados. [15]

En resumen, **la cadena sella probabilidades, no verdades**; un sello inmutable puede anclar la coacción tan eficazmente como la autenticidad. Reconocer esta dualidad no debilita el mensaje de *time2act*, sino que lo blinda: solo confrontando las limitaciones del poder y estableciendo reglas estrictas de gobernanza podemos garantizar que la prueba de existencia sea una herramienta de confianza y no un instrumento de opresión.

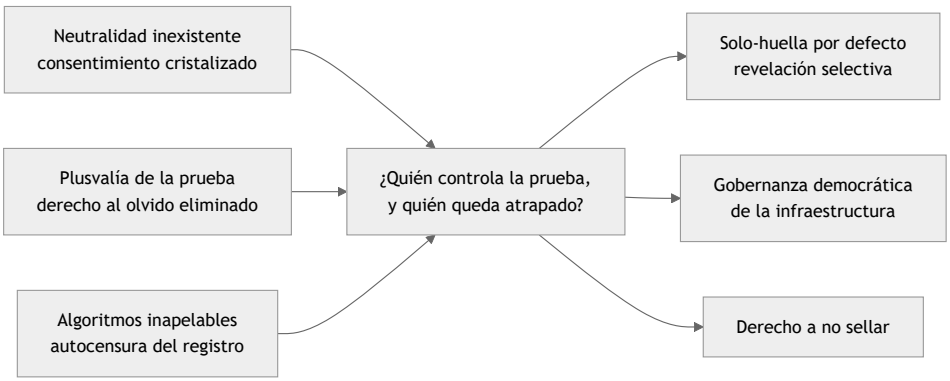


Figura 112.1 — El sello y la cadena: quién controla la prueba, y quién queda atrapado. Los riesgos que el capítulo desgrana — la neutralidad que no existe, el consentimiento cristalizado, la plusvalía de la prueba, el derecho al olvido eliminado, los algoritmos inapelables y la autocensura del registro permanente— y los contrapesos que reclama: solo-huella por defecto, revelación selectiva, gobernanza democrática de la infraestructura y el derecho a no sellar.

Es hora de actuar

La prueba de existencia que hemos construido a lo largo de *time2act* es, como cualquier sello, una doble herramienta: autentica la verdad y, simultáneamente, puede convertirse en el anclaje de una nueva forma de coerción. Para que este instrumento se mantenga al servicio de la confianza y no del control, hay que establecer cinco principios de diseño que guíen su gobernanza.

1. Gobernanza de nodos transparente y distribuida. La descentralización técnica no garantiza por sí sola una democracia digital; el poder sigue concentrado en quien controla los puntos de entrada. Como hemos visto, en 2026 el 42 % de los bloques de Ethereum se construyen a través de relays que imponen censura OFAC y las redes L2 operan con un único secuenciador corporativo como Base de Coinbase [5]. Por tanto, los nodos que registran la prueba deben estar sujetos a una auditoría pública continuada y a una selección basada en criterios abiertos (competencia técnica, diversidad geográfica y compromiso con valores democráticos). La transparencia debe ser verificada por entidades independientes, tal como recuerda Frisby: «no confíes, verifica», pero la pregunta clave es *quién* verifica al verificador [32].

2. Derecho a la revocación y a la caducidad. Un registro inmutable no puede ser eterno si pretende respetar los derechos fundamentales de las personas. La legislación europea ha avanzado hacia el modelo «consentir o pagar», pero sin un mecanismo que permita retirar el consentimiento, este modelo se convierte en una forma de cautiverio [10]. Hay que establecer protocolos que posibiliten la revocación del certificado de identidad y la caducidad automática de los registros biométricos cuando dejen de estar necesarios o sean vulnerables al abuso.

3. Minimización biométrica real. La centralización de bases biométricas, como el proyecto Eurodac, que ha rebajado la edad de recogida a seis años y la comparte con fuerzas policiales [28], demuestra cómo una infraestructura pensada para la seguridad puede ser convertida en herramienta de vigilancia masiva. La solución pasa por evitar bases centralizadas y, en su lugar, utilizar pruebas descentralizadas basadas en técnicas de «zero-knowledge» que no revelan datos sensibles pero permiten validar la existencia de un individuo.

4. Auditoría algorítmica independiente. Los modelos matemáticos que sustentan las decisiones automatizadas son, según O'Neil, opacos y accesibles solo para «los grandes sacerdotes del sector» [4]. Para garantizar que la prueba no se convierta en un instrumento de injusticia, hay que instituir comisiones independientes con poder legal para revisar y validar los algoritmos que procesan los datos biométricos y blockchain.

5. Cifrado de extremo a extremo como defensa real. Snowden afirma que el cifrado de extremo a extremo es la única protección efectiva contra la vigilancia, ya que convierte los datos interceptados en ruido incomprensible sin las claves [34]. Toda transmisión de pruebas debe estar protegida por este nivel de cifrado, y las claves deben ser gestionadas de manera descentralizada, evitando puntos únicos de fallo.

Estos principios establecen límites funcionales contra el *mission creep* que, como advierte Zuboff, transforma la experiencia humana en materia prima gratuita para la extracción y la venta [13]. Solo si se instalan controles democráticos —auditorías independientes, revocación de consentimiento y una arquitectura transparente— la prueba de existencia puede mantenerse como herramienta emancipadora y no como instrumento de captura. **El sello puede garantizar la verdad; la cadena debe impedir que esa verdad se convierta en una jaula**.

---

[1] Biometric Update / ICLG — *Worldcoin/World ID: prohibiciones y órdenes de supresión (Kenia inconstitucional; Colombia)* (2024-2025). https://www.biometricupdate.com/202510/colombia-orders-world-shut-down-citing-biometrics-compliance-failures ↩

[2] Edward Snowden — *Vigilancia permanente* (Planeta, 2019). ↩

[3] Marc Goodman — *Delitos del futuro* (Ariel, 2015). ↩

[4] Cathy O'Neil — *Armas de destrucción matemática* (Capitán Swing, 2018). ↩

[5] L2BEAT — *Estado de descentralización de los L2 de Ethereum (secuenciadores)* (2026). https://l2beat.com/scaling/summary — y MEV Watch, *bloques con censura OFAC* (2026). https://www.mevwatch.info/ ↩

[6] Jack Watling — *Statecraft: The New Rules of Power in a Divided World* (2023). ↩

[7] Jack Watling — *Statecraft: The New Rules of Power in a Divided World* (2023). ↩

[8] Dominic Frisby — *The Secret History of Gold* (2024). ↩

[9] Carissa Véliz — *Privacidad es poder* (Debate, 2021). ↩

[10] EDPB — *Opinion 08/2024 on «consent or pay»* (17-04-2024). https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en ↩

[11] Dominic Frisby — *The Secret History of Gold* (2024). ↩

[12] Jack Watling — *Statecraft: The New Rules of Power in a Divided World* (2023). ↩

[13] Shoshana Zuboff — *La era del capitalismo de la vigilancia* (Paidós, 2020). ↩

[14] Shoshana Zuboff — *La era del capitalismo de la vigilancia* (Paidós, 2020). ↩

[15] FTC — *Acciones contra data brokers (X-Mode/Outlogic) y Avast* (2024). https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data — y Autoriteit Persoonsgegevens (NL), *multa de 30,5 M€ a Clearview AI* (2024). https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en ↩

[16] Dominic Frisby — *The Secret History of Gold* (2024). ↩

[17] Edward Snowden — *Vigilancia permanente* (Planeta, 2019). ↩

[18] Edward Snowden — *Vigilancia permanente* (Planeta, 2019). ↩

[19] FedScoop — *Agencias federales de EE. UU. y la analítica de blockchain (Chainalysis, TRM Labs)* (2024-2025). https://fedscoop.com/ice-wants-more-blockchain-analytics-tech/ ↩

[20] Edward Snowden — *Vigilancia permanente* (Planeta, 2019). ↩

[21] Dominic Frisby — *The Secret History of Gold* (2024). ↩

[22] Cathy O'Neil — *Armas de destrucción matemática* (Capitán Swing, 2018). ↩

[23] Carissa Véliz — *Prophecy: Prediction, Power, and the Fight for the Future* (2025). ↩

[24] Edward Snowden — *Vigilancia permanente* (Planeta, 2019). ↩

[25] Consejo de la UE / Pinsent Masons — *«Digital Omnibus»: aplazamiento de las reglas de IA de alto riesgo* (mayo 2026). https://www.pinsentmasons.com/out-law/news/rules-high-risk-ai-delayed-under-eu-omnibus-deal — y Colorado General Assembly, *SB 26-189* (2026). https://leg.colorado.gov/bills/sb26-189 ↩

[26] Jack Watling — *Statecraft: The New Rules of Power in a Divided World* (2023). ↩

[27] Carissa Véliz — *The Ethics of Privacy and Surveillance* (Oxford University Press, 2024). ↩

[28] European Policy Centre — *Expansión de Eurodac (edad 12→6; acceso policial), Pacto de Migración 2024.* https://www.epc.eu/publication/managing-migration-through-data-the-expansion-and-integration-of-eurodac/ ↩

[29] Jack Watling — *Statecraft: The New Rules of Power in a Divided World* (2023). ↩

[30] Shoshana Zuboff — *La era del capitalismo de la vigilancia* (Paidós, 2020). ↩

[31] Carissa Véliz (ed.) — *The Oxford Handbook of Digital Ethics* (Oxford University Press, 2022). ↩

[32] Dominic Frisby — *The Secret History of Gold* (2024). ↩

[33] time2act — *Guía de estilo (STYLE.md): «la promesa y el peligro»; «nada de tecno-utopía sin evidencia».*

[34] Edward Snowden — *Vigilancia permanente* (Planeta, 2019). ↩

El asedio a la verdad: el testigo que no se puede silenciar

«Nuestra misión es informar de estos horrores de la guerra con exactitud y sin prejuicios.»

— Marie Colvin, «Truth at all costs», St Bride's, Londres (2010)

Hacia las diez de la mañana del 25 de agosto de 2025, la cámara de Reuters instalada en lo alto de una escalera exterior del hospital Nasser, en Khan Younis, al sur de Gaza — el punto que los equipos de televisión usaban desde hacía días por su vista de la ciudad —, emitía en directo, como cada mañana. El primer misil impactó exactamente allí. La señal se cortó en seco: Hussam al-Masri, el cámara de Reuters que filmaba, murió con su lente. Unos diez minutos después, cuando rescatadores y periodistas ya se habían subido escaleras arriba a buscar a los heridos, llegó el segundo impacto — la táctica conocida como «doble toque» [3]. El balance: al menos 22 muertos, entre ellos cinco periodistas — al-Masri (Reuters), Mariam Dagga (colaboradora de Associated Press), Mohammed Salama (Al Jazeera), Moaz Abu Taha (colaborador de Reuters) y Ahmed Abu Aziz (Middle East Eye y Quds News Network) [1][3]. Los análisis posteriores de los vídeos, por parte de NBC y de CNN, contaron hasta cuatro municiones [3]. La oficina del primer ministro Netanyahu lo llamó «un contratiempo trágico», y el ejército anunció una investigación [3].

Hay una ironía atroz en esta escena, y conviene mirarla de cara: la prueba del ataque quedó filmada por la misma cámara que el ataque destruía. El directo de Reuters es a la vez la última imagen de Hussam al-Masri y la evidencia de cómo murió. En esta guerra, la imagen ya no acompaña a los hechos: es el campo de batalla.

La escena ocurre, además, en una guerra que el mundo no ha podido ir a ver: desde octubre de 2023, la prensa internacional tiene vetada la entrada independiente a Gaza [6]. Y ocurre en el conflicto que el Committee to Protect Journalists (CPJ) describe como «el esfuerzo más letal y deliberado por matar y silenciar periodistas» que haya documentado nunca [1]. Cerrar la puerta a los de fuera, matar o señalar a los de dentro, y negar las imágenes que pese a todo salen — «montaje», «actores», «esto es IA» —: tres estrategias que convergen en un mismo objetivo, que ninguna prueba sobreviva. Este libro entero ha defendido que la confianza puede volverse verificable; este penúltimo capítulo la lleva donde todo es más difícil y más necesario a la vez: allí donde informar mata y donde negar es gratis. La tesis es la de siempre, llevada al límite: si cada foto y cada vídeo nacen con una prueba de existencia anclada en una cadena pública que ningún estado, ninguna plataforma y ningún consorcio controla, matar al testigo deja de matar la prueba — y negarla deja de salir gratis.

Este capítulo camina sobre piedras que el libro ya ha puesto: la imagen como testigo y las credenciales de contenido, en el capítulo 17; la evidencia de crímenes de guerra con huellas y blockchain — eyeWitness, el Starling Lab, el Protocolo de Berkeley —, en el capítulo 20; el testigo orbital, en el capítulo 104; el dividendo del mentiroso en las urnas, en el capítulo 106; la prueba simétrica en la calle, en el capítulo 109; y la cadena de custodia del socorro — incluido el terremoto de Venezuela —, en los capítulos 49 y 50. Aquí todas estas piezas se encuentran en su escenario extremo.

Un asedio también informativo

La primera capa del asedio es la puerta cerrada. Desde el inicio de la guerra, Israel no permite la entrada independiente de periodistas extranjeros a Gaza; solo visitas puntuales escoltadas por el ejército, caso por caso — un formato que la Foreign Press Association, que agrupa a los corresponsales extranjeros, denuncia como insuficiente para cualquier cobertura real [6]. La cronología judicial lo dice todo: en enero de 2024, el Tribunal Supremo israelí rechazó la primera petición de la FPA — no hay «ningún derecho adquirido» a entrar, dijo, y pesan las razones de seguridad —; la FPA volvió a recurrir en septiembre de 2024; siguieron prórrogas y más prórrogas; y en enero de 2026, ya con el alto el fuego en vigor, el gobierno volvió a decir al tribunal que el veto debía mantenerse «por razones de seguridad» — y el tribunal volvió a aplazar la decisión [6]. Más de dos docenas de organizaciones informativas de todo el mundo han reclamado conjuntamente poder entrar [6]. El resultado es una anomalía histórica: la primera gran guerra de este siglo que el mundo ha visto casi exclusivamente a través de los ojos de quien la sufre.

La segunda capa es lo que ha pasado a los que estaban dentro. El CPJ contabiliza 263 periodistas y trabajadores de medios muertos desde el 7 de octubre de 2023 — además de 108 encarcelados y 174

heridos — y sostiene que ningún otro actor había matado tantos periodistas desde que la organización recoge datos, en 1992 [1]. El informe «News Graveyards» del proyecto Costs of War de la Universidad de Brown (abril de 2025) puso una perspectiva difícil de olvidar: más periodistas muertos en Gaza que en la Guerra Civil americana, las dos guerras mundiales, Corea, Vietnam, Yugoslavia y Afganistán combinadas — una comparación que hay que tomar con el matiz de que la propia base de datos histórica en que se basa desaconseja comparar épocas con métodos de recuento diferentes [2]. Reporteros Sin Fronteras (RSF), que cuenta más de 210 muertos y tiene motivos razonables para creer que al menos 56 fueron atacados deliberadamente por su trabajo, ha presentado cinco denuncias ante la Fiscalía del Tribunal Penal Internacional — la última, el 30 de septiembre de 2025 —, y documenta también el patrón del doble bombardeo: un segundo misil que llega cuando los rescatadores y los reporteros ya están sobre el terreno del primero [7].

Dos nombres condensan el mecanismo. Anas al-Sharif, corresponsal de Al Jazeera, murió el 10 de agosto de 2025 en el ataque contra la tienda de prensa frente al hospital al-Shifa, con cuatro compañeros más; el ejército israelí lo declaró «operativo de Hamás», una acusación que Al Jazeera y el CPJ rechazan. El detalle que importa es anterior: ya en julio, el CPJ y la relatora especial de las Naciones Unidas Irene Khan habían alertado de la campaña de descrédito contra él y del riesgo que corría su vida [4]. Primero la duda, después el misil. Y Wael al-Dahdouh, jefe de la corresponsalía de Al Jazeera en Gaza, supo en directo, mientras informaba, que un ataque aéreo acababa de matar a su esposa, a su hijo Mahmoud, a su hija Sham y a su nieto Adam, el 25 de octubre de 2023. Continuó informando [5].

Y cuando la prensa de fuera está en la puerta y la de dentro está bajo las bombas, el vacío lo llena el testigo. La guerra la han contado al mundo figuras como Bisan Owda — reportera de veinticinco años, con cuatro millones de seguidores, que en septiembre de 2024 ganó un Emmy por «It's Bisan From Gaza — and I'm Still Alive», pese a una campaña para descalificarla — o el fotoperiodista Motaz Azaiza, cuyas imágenes dieron la vuelta al mundo [8]. En Gaza, la frontera entre el fotoperiodista profesional y el testigo ciudadano se ha borrado: a menudo son la misma persona, con el mismo móvil. Y esto hace inevitable la pregunta de este capítulo: ¿qué fuerza probatoria tiene lo que graban?

«Fake»: el dividendo del mentiroso en tiempos de guerra

El libro ha visto el dividendo del mentiroso en las urnas (capítulo 106) y sabe que detectar no basta (capítulo 15). La guerra enseña su forma más cruda: no hace falta falsificar nada — basta con decir «falso» a todo. «Pallywood», la acusación de que los palestinos escenifican el sufrimiento, vivió una explosión medible: BBC Verify contó un pico de 220.000 usos del término en X solo en noviembre de 2023 [9]. Las «pruebas» que lo acompañaban solían ser material reciclado — una protesta egipcia de 2013, un disfraz de Halloween tailandés, un rodaje publicitario en Argelia —, presentado como si fuera Gaza [9].

Dos casos enseñan las dos caras del mecanismo. El primero: el Jerusalem Post publicó — y después tuvo que retirar — que el cuerpo de un bebé palestino de cinco meses era una muñeca; la cuenta oficial de Israel en X amplificó la acusación; la BBC localizó a la familia y a los fotógrafos y confirmó que era el cuerpo real de un niño [9]. El segundo, inverso y aún más corrosivo: una foto difundida por Israel del cuerpo carbonizado de un bebé asesinado el 7 de octubre fue tildada masivamente de «generada por IA» porque un detector comercial, «AI or Not», dio positivo. La empresa acabó reconociendo el falso positivo — culpa de la compresión y de una etiqueta difuminada —, y varios expertos consideraron la foto genuina [9]. La lección corta en los dos sentidos: los detectores se equivocan con fotos falsas y con fotos reales, y un detector malo es el sueño del negacionista — cualquier imagen auténtica se puede «desmentir» con una herramienta gratuita y una captura de pantalla.

El sociólogo Ron Dudai lo ha descrito con precisión: las viejas teorías conspirativas, elaboradas y laboriosas, han dado paso a una forma más cruda de negacionismo — la documentación se descarta con una sola palabra, «Fake» [9]. Y el descrédito no se queda en la retórica: RSF documenta cómo las acusaciones de «montaje» contra los periodistas gazatíes — lo que llama «Gazawood» — los convierten en objetivos [7]. Es el camino que recorrió al-Sharif: la duda sembrada en julio precedió al misil de agosto [4].

El dividendo del mentiroso no tiene bandera: lo cobra cualquier poder interesado en que una imagen no exista — en Gaza, en Siria, donde sea —, y lo paga siempre el mismo: el testigo que dice la verdad y no lo puede demostrar. Contra un «¡falso!» que cuesta cero, la respuesta no puede ser un peritaje que cuesta meses. Debe ser una prueba que ya existía.

Cuando el asedio es en casa: Minneapolis, invierno de 2026

No hace falta una zona de guerra ni una dictadura para que el mecanismo se dispare. En diciembre de 2025, el Departamento de Seguridad Nacional de Estados Unidos lanzó sobre Minneapolis y Saint Paul la operación Metro Surge — «la mayor operación de control migratorio jamás llevada a cabo», en palabras del propio departamento —: miles de agentes del Servicio de Inmigración y Aduanas (ICE) y de la Patrulla Fronteriza, más de cuatro mil en el punto álgido según las cifras que un juez tuvo que obligar a revelar, y cerca de tres mil ochocientas detenciones en dos meses, menos de una cuarta parte con antecedentes penales [21]. La ciudad era, precisamente, aquella donde el vídeo de una adolescente con un móvil había cambiado la historia en 2020 (capítulo 109). Lo que allí pasó es el experimento más limpio que existe sobre la pregunta de este libro: qué vale el testigo cuando quien niega es el propio estado.

Renée Good: tres tiros y demasiadas cámaras

El 7 de enero de 2026 por la mañana, Renée Good — treinta y siete años, escritora, ciudadana estadounidense — estaba al volante de su coche en una calle del sur de Minneapolis, detenida perpendicularmente al paso de unos vehículos federales; iban también su pareja, una criatura de seis años y el perro [22]. El agente de ICE Jonathan Ross le disparó tres tiros. La versión oficial llegó en horas y desde lo más alto: la secretaria de Seguridad Nacional, Kristi Noem, afirmó que Good había intentado «atropellar y embestir» a los agentes y que llevaba todo el día «acosando y obstruyendo» el operativo — de esto último no se ha presentado nunca ninguna prueba —, y el presidente Trump escribió que había atropellado al agente «de manera violenta, deliberada y encarnizada» y que este «se recuperaba en el hospital» [22].

Los vídeos decían otra cosa, y había muchos: de testigos, de cámaras de vigilancia y del móvil del propio Ross. La reconstrucción del New York Times fijó la secuencia — un tiro al parabrisas y dos más, a corta distancia, por la ventanilla de la conductora, con el coche girando para alejarse y el agente de pie, a unos pasos, fuera de la trayectoria —, y otro ángulo mostraba a Good, pocos minutos antes, cediendo el paso a los vehículos federales y haciéndoles señal de que pasaran [22]. Y un detalle que vale un tratado entero: la grabación del propio Ross se sacude hacia arriba justo en el momento decisivo, y lo deja fuera de cuadro [22]. El registro del estado quedó ciego exactamente cuando más hacía falta; los de los ciudadanos, no.

Alex Pretti: el testigo tiroteado

Diecisiete días después — al día siguiente de una huelga general que había llenado el centro de la ciudad [21] —, el operativo mató a Alex Pretti: treinta y siete años, enfermero de cuidados intensivos en el hospital de veteranos, ciudadano estadounidense, sin antecedentes y con permiso de armas en regla, como confirmó el jefe de la policía de Minneapolis [23]. Pretti era aquella mañana una de las personas que documentaban con el móvil un operativo de ICE — la figura exacta del testigo del capítulo 109. La secretaria Noem declaró que se había acercado a los agentes «con una pistola»; el departamento añadió que quería «hacer el máximo daño y masacrar a las fuerzas del orden» y que llevaba «dos cargadores y ningún tipo de identificación»; el subjefe de gabinete de la Casa Blanca, Stephen Miller, lo llamó «terrorista doméstico» [23].

Los vídeos de los presentes — múltiples ángulos, revisados y verificados por Reuters, la BBC, el Wall Street Journal, AP, CNN, el New York Times y The Guardian — muestran una secuencia diferente: Pretti con el teléfono en la mano derecha; rociado con espray de pimienta cuando intentaba ayudar a una mujer que había caído; media docena de agentes inmovilizándolo en el suelo; un agente sacándole la pistola de la funda de la cadera — y, un segundo después, otro disparándole a bocajarro una decena de tiros en cinco segundos, los últimos cuando ya yacía inmóvil [23]. Ningún agente le practicó la reanimación, y una pediatra que se ofreció fue apartada [23]. La forense del condado dictaminó la muerte: homicidio [23]. Y los nombres de los dos agentes no los hizo públicos el gobierno: los publicó ProPublica [24].

El asedio a la evidencia

La densidad hizo su trabajo. Las versiones oficiales no aguantaron ni una semana: el alcalde y el gobernador, tras ver los vídeos, desmintieron públicamente el relato federal [23]; un juez federal contó al menos noventa y seis órdenes judiciales violadas por ICE en un mes, y otro constató que la «mayoría abrumadora» de los detenidos estaba en el país legalmente [21]; y el 12 de febrero, el «zar de la frontera» de la Casa Blanca anunciaba el fin del operativo en una rueda de prensa donde evitó pronunciar los dos nombres [21].

Pero la misma maquinaria cerró filas en torno a la prueba: al día siguiente del primer tiroteo, el FBI revocó a la agencia de investigación criminal del estado el acceso a las evidencias [22]; en abril, el móvil de Pretti seguía retenido, el coche de Good continuaba precintado en un almacén federal sin que ningún investigador estatal lo hubiera podido examinar, y los nombres y expedientes de los agentes se negaban sistemáticamente [24]. Minnesota y el condado de Hennepin tuvieron que presentar una demanda para obtener unas pruebas que — sostienen — se retienen «para escudar a los agentes implicados» [24]. Mientras escribimos esto, ningún agente ha sido acusado de nada: el hombre que disparó contra Renée Good estuvo tres días apartado del servicio y meses después operaba en otro estado [22], y la única medida disciplinaria conocida de todo el operativo son dos agentes en permiso administrativo por «declaraciones falsas» sobre el tercer tiroteado, un hombre herido de bala en la pierna [24]. La fiscal del condado mantiene abiertas diecisiete investigaciones penales contra un muro de inmunidades [24]. «Parece que estén impidiendo activamente que el estado investigue», lo resumía una profesora de derecho [24].

El patrón: Chicago, Houston

Minneapolis no es una anomalía: es el caso mejor documentado de un patrón. Tres meses antes, en Chicago, un agente había disparado cinco tiros a Marimar Martinez, una maestra que seguía los vehículos federales tocando el claxon para avisar a los vecinos — y la acusada de embestirlos fue ella; la cámara corporal acabó mostrando el vehículo de los agentes girando hacia el suyo justo después de que uno dijera «es hora de ponerse agresivos», y los mensajes del propio agente presumiendo de ello — «cinco tiros y siete agujeros» —; los cargos contra ella se archivaron con carácter definitivo [25].

Aquel mismo noviembre, la jueza federal Sara Ellis confrontó, en un dictamen de doscientas veintitrés páginas, los informes oficiales de uso de la fuerza con los vídeos de las cámaras corporales que ella misma había ordenado activar: el relato del gobierno era «sencillamente no creíble», el jefe del operativo había ido cambiando bajo juramento el orden de los hechos — el gas lanzado antes de la piedra que decía haber recibido —, y un agente había redactado el informe oficial de un incidente con ChatGPT a partir de «una frase breve sobre un encuentro y varias imágenes» [25]. Conviene detenerse en este último detalle: en la disputa por la realidad entre el ciudadano y el estado, el relato sintético era el oficial. El recuento acumulado desde enero de 2025 llega a los treinta y ocho tiroteos por agentes de inmigración, con nueve muertos [25]. Y no se detiene: el 7 de julio de 2026, mientras se acababa de escribir este capítulo, un hombre de cincuenta y dos años moría en Houston por un tiro de un agente de ICE que alega — una vez más — una embestida; los agentes no llevaban cámaras corporales, los relatos sobre los momentos previos se contradicen, y la forense del condado ha dictaminado el homicidio [26].

El contrafactual: un solo testigo, sin ancla

Ahora, el ejercicio que este libro no se puede ahorrar. Repetid el 7 de enero con una sola variación: no hay multitud. Ninguna cámara de vigilancia apuntando a la calle, ningún vecindario congregado; solo alguien que, asustado, lo graba a escondidas desde una ventana — y que tarda semanas en hacerlo público, porque tiene miedo. Para entonces, la versión oficial ya lleva un mes siendo «la verdad»: consta en declaraciones, en comparecencias, en boca del presidente. Cuando el vídeo salga, el manual que este capítulo ya ha descrito se disparará solo: «montaje», «actores», «es IA» — y bastará con un detector gratuito y un falso positivo como el que ya hemos visto [9] para fabricar el «desmentido».

Contra la palabra jurada de un estado, un archivo sin fecha cierta ni integridad demostrable es solo eso: un archivo. Porque lo que salvó la verdad en Minneapolis no fue ninguna institución: fue la densidad — demasiadas cámaras, demasiados testigos, demasiados ángulos para negarlos todos a la vez. Y la densidad es un accidente: estaba ahí porque el operativo era masivo y contestado, y la comunidad, avisada y mirando. La próxima Renée Good puede tener un solo testigo; el próximo Alex Pretti, ninguno. Y allí donde no quedan contrapesos — ningún juez que cuente órdenes violadas, ningún fiscal de condado que pueda demandar, ninguna huelga general — la versión oficial no es que gane: es la única que existe. En un estado así, abiertamente dictatorial, el testigo de la ventana no tiene un vídeo: tiene una acusación de falsificación esperándolo.

Con la prueba de existencia, el mismo escenario cambia de física. Si el vídeo clandestino se selló al nacer — la huella, y solo la huella, salió del móvil hacia el ancla pública, con la fecha del mismo 7 de enero [20] —, el testigo puede esperar semanas o años, o revelarlo desde el exilio: su ancla será siempre anterior al relato oficial, y el «esto se ha fabricado después» deja de ser una salida. Es exactamente lo que no puede ofrecer ningún registro que dependa del poder: la cámara del agente que se alza en el momento decisivo, el móvil retenido, el coche precintado — cada vacío conveniente del registro oficial se hace visible cuando el resto de pruebas llevan fecha cierta e integridad verificable. Y la simetría que este capítulo reivindica más

adelante vale aquí en las dos direcciones: el mismo sello habría amparado a un agente que dijera la verdad. No pide confiar en nadie; solo hace que mentir salga caro, en todas direcciones.

Cuando la multitud está, la verdad puede ganar por densidad; cuando solo hay un testigo, todo se juega en si su prueba nació sellada. Y cuando no hay ni multitud ni sello, queda el oficio lento de rehacer los hechos a posteriori — un oficio heroico cuyo precio, en tiempo y en duda, es el que viene ahora.

La forénsica de después: gana, pero tarde

La reconstrucción forense independiente es la heroína de esta guerra informativa. Y a la vez, la demostración de cuánto cuesta llegar tarde. Tres casos, en gradación.

Shireen Abu Akleh: cuatro meses para tumbar una versión

Shireen Abu Akleh, corresponsal de Al Jazeera, murió de un tiro en la cabeza el 11 de mayo de 2022 en Jenín, con casco y chaleco de PRENSA. La primera versión oficial apuntó a fuego palestino indiscriminado. Lo que vino después es la cadencia exacta del desmentido: la investigación de CNN (24 de mayo) no encontró ningún combate activo cerca y, con testigos y análisis de audio, apuntó a fuego israelí; AP, el New York Times y el Washington Post publicaron reconstrucciones coincidentes; la Oficina de Derechos Humanos de la ONU concluyó en junio que los tiros venían de las fuerzas israelíes — «varios tiros aislados y aparentemente bien apuntados» —; Estados Unidos evaluó en julio que lo más probable era fuego israelí, con una bala demasiado dañada para una balística concluyente; y el 5 de septiembre de 2022 el ejército israelí admitió que «probablemente» la había matado uno de sus soldados. Sin cargos [11]. Casi cuatro meses y media docena de investigaciones independientes para tumbar la primera versión — con acceso al terreno, en relativa calma y con una víctima famosa. En Gaza, sin acceso, este camino se multiplica — o se vuelve imposible.

Hind Rajab: 355 impactos y una llamada

Hind Rajab tenía seis años. El 29 de enero de 2024 quedó atrapada en un coche tiroteado en la ciudad de Gaza, rodeada de los cuerpos de su familia, y suplicó auxilio por teléfono a la Media Luna Roja Palestina; su cuerpo, el de seis familiares y el de los dos sanitarios de la ambulancia que había salido a buscarla aparecieron dos semanas después. La reconstrucción de Forensic Architecture con la ONG Earshot y Al Jazeera estableció que el coche había recibido 355 impactos de bala; y el análisis acústico de la llamada — el intervalo entre el sonido de cada impacto y el de la boca de cañón — situó al tirador a entre 13 y 23 metros [12]. Vale la pena detenerse en qué es, aquí, la prueba central: el audio de una llamada de móvil. El testigo digital espontáneo ya decide investigaciones internacionales; lo que aún no tiene es una manera de nacer indiscutible.

Las fotos Caesar: una década hasta Coblenza

Y el precedente que cierra el círculo viene de Siria, de una dictadura: un fotógrafo forense de la policía militar siria, nombre en clave «Caesar», huyó en 2013 con unas 53.000 fotografías de muertos bajo tortura en las prisiones del régimen. Autenticarlas costó años — peritajes de los metadatos del sistema del propio régimen, que numeraba dispositivos y registros, y un análisis médico forense de miles de imágenes a cargo de expertos de la Universidad de Colonia, que encontró tortura y muerte sistemáticas [13]. El 13 de enero de 2022, el tribunal de Coblenza, en Alemania, juzgando por jurisdicción universal, condenó a Anwar Raslan, exjefe de interrogatorios de la Rama 251, a cadena perpetua por crímenes contra la humanidad — con las fotos Caesar como pieza clave [13]. Entre el riesgo de muerte de un hombre sacando discos duros de un país en guerra y la sentencia: casi una década. El coraje salvó la prueba; el sistema tardó diez años en poder fiarse de ella.

Tribunales que esperan, pruebas que no llegan

Esta evidencia, cuando llega, ya tiene adónde ir. El Tribunal Penal Internacional emitió el 21 de noviembre de 2024 órdenes de detención contra Benjamin Netanyahu y Yoav Gallant — por el crimen de guerra del hambre como método de guerra y por crímenes contra la humanidad — y contra el comandante de Hamás Mohammed Deif [14]; el Tribunal Internacional de Justicia, en el caso presentado por Sudáfrica bajo la Convención del Genocidio, dictó medidas provisionales vinculantes en enero, marzo y mayo de 2024 [15]; y el marco para aceptar evidencia digital de fuentes abiertas — el Protocolo de Berkeley — ya existe (capítulo 20). No faltan tribunales. Falta que la prueba llegue entera, rápida e indiscutible.

Porque cuando no llega, pasa lo que pasó con el hospital al-Ahli. La explosión del 17 de octubre de 2023 — 471 muertos según el Ministerio de Salud de Gaza; entre 100 y 300 según la inteligencia estadounidense — puso a los mejores equipos forenses del mundo a trabajar sobre los mismos vídeos. Y divergieron: AP, CNN y otros medios concluyeron que lo más probable era un cohete fallido lanzado desde Gaza; el New York Times acabó diciendo que la causa era incierta; Human Rights Watch vio en ello el patrón de un cohete propulsado pero exigió una investigación independiente; Forensic Architecture concluyó que el proyectil venía de la dirección de Israel [10]. Sin acceso al cráter, con vídeos recomprimidos y recortados, sin hora cierta ni integridad verificable de los archivos clave, la misma evidencia sostuvo conclusiones opuestas — y cada bando se quedó con la suya. La forénsica no falló: le faltaron los fundamentos. Exactamente los que un sello en el origen le habría dado.

Sellar en el origen: la prensa acreditada bajo asedio

Que una redacción puede sellar lo que publica ya no es una hipótesis. Reuters y el Starling Lab lo ensayaron en 2020 y 2021 con «78 Days»: durante los setenta y ocho días de la transición presidencial estadounidense — asalto al Capitolio incluido —, más de doscientas fotografías se capturaron con metadatos criptográficos y se anclaron en cadenas públicas, con la procedencia de cada imagen verificable por cualquier lector [18]. Si se pudo hacer para una transición política en Washington, se puede hacer para una guerra. Es exactamente donde más hace falta.

El flujo de t2p para la prensa empieza en el dispositivo de quien dispara: la huella SHA-512 — calculada en el móvil, de los bytes exactos del archivo — recibe su sello de tiempo RFC 3161/eIDAS y queda anclada en la blockchain pública; la imagen no sale del dispositivo para generar la prueba [20]. La posición GPS se añade cuando es fiable. Y todo ello viaja en un paquete .asice verificable sin conexión, de la zona de conflicto a la redacción y, si hace falta, a la fiscalía — la misma cadena de custodia que el capítulo 50 aplica al socorro, aplicada al testigo [20]. Es, de hecho, lo que el Protocolo de Berkeley pedirá mañana a cualquier prueba (capítulo 20), generado por defecto hoy.

La credencial resuelve la otra mitad del problema: la agencia firma la vinculación — «este material es de un colaborador acreditado nuestro» — sin publicar quién es ni dónde está, la divulgación selectiva del capítulo 20 [20]. La redacción puede demostrar la procedencia ante el lector y ante el juez, y a la vez proteger a la persona. Y si la matan — en Gaza no es una cláusula de estilo [1] —, su archivo sellado sigue probando qué vio y cuándo. Matar al mensajero deja de matar el mensaje.

Y aquí es donde la doctrina de este libro se vuelve literal. Las credenciales de contenido firmadas en la cámara (capítulo 17) son el complemento perfecto — pero son metadatos que viajan con el archivo, y una recompresión las borra; y todo sistema de certificación tiene un propietario, y todo propietario tiene una ventanilla donde llamar. El ancla en una cadena pública no la tiene: ningún gobierno — tampoco el que niega las imágenes — puede despublicar una huella ni antedatarla. El capítulo 112 preguntaba quién controla la prueba; aquí la respuesta decide vidas: cuando el acusado es un estado, la prueba no puede depender de ninguna autoridad que ese estado pueda presionar. La neutralidad de la cadena no es una virtud abstracta — es el requisito técnico para que la prueba valga contra cualquier poder, el propio incluido.

El testigo con el móvil: la misma prueba para todos

La idea de que el testigo ciudadano merece herramientas de prueba no es nueva. WITNESS y el Guardian Project lanzaron ProofMode en 2017: una aplicación gratuita que firma y calcula la huella de cada foto y vídeo en el momento de la captura, con una instantánea de los sensores, y notariza su huella — con OpenTimestamps, el anclaje en Bitcoin que el libro ya conoce, entre sus sistemas de notaría [19]. Y eyeWitness to Atrocities hace algo parecido desde 2015 para documentadores entrenados, con más de 20.000 ítems ya usados como prueba judicial (capítulo 20). Lo que faltaba no es la idea: es que sea universal, por defecto, y pensada para quien no es activista ni periodista — para cualquier persona que una mañana se encuentra grabando el peor día de su vida.

Para este escenario — el peor — el sello debe tener cuatro propiedades, y ninguna es opcional.

Solo la huella sale del móvil. La foto no se sube a ningún lado para generar la prueba: el dispositivo calcula la huella SHA-512 y es esto — solo esto — lo que recibe el sello de tiempo y el ancla en la blockchain pública [20]. En un control militar, en un registro, no hay ninguna subida que delate al testigo; la imagen puede vivir cifrada o en una copia fuera del dispositivo, y la huella anclada espera su momento.

Sella ahora, publica cuando sea seguro. Es el compromiso y revelación de los capítulos 45 y 46, aplicado a la supervivencia: la víctima sella hoy la huella del vídeo y lo revela dentro de un mes, un año, o desde el exilio — y la fecha cierta que cuenta es la de hoy. El negacionista que diga «esto se ha fabricado después» choca contra un ancla anterior a su propia negación.

La prueba póstuma. Si el testigo muere — y 263 veces no es una hipótesis [1] —, el sello sobrevive: cualquiera que tenga la copia puede demostrar qué existía y cuándo. El archivo de cada Bisan y de cada Motaz [8] se vuelve indestructible por decapitación: se puede matar a quien graba; no se puede matar el hecho de que aquello ya estaba grabado.

La simetría. Esta prueba no distingue bandos: el vídeo de un civil israelí el 7 de octubre y el de una familia de Khan Younis bajo las bombas tienen exactamente la misma fuerza de anclaje. Es la prueba simétrica del capítulo 109: la cámara de Darnella Frazier valió porque era auténtica, no porque fuera de nadie. La tecnología que ampara al testigo palestino ampara igual al israelí, al ucraniano y al sudanés — y por eso, y solo por eso, puede aspirar a ser un estándar global.

Queda el límite ético, y es innegociable (capítulos 49 y 50): nunca biometría obligatoria para las víctimas. La prueba de vida y el vídeo-selfie son opciones para quien quiere reivindicar la autoría — no un peaje. Quien documenta un crimen no debe pagar con su identidad; y la geolocalización se revela cuando el testigo decide, no antes (capítulo 20).

La promesa y el peligro

La promesa es una guerra donde el veto de acceso ya no fabrica oscuridad, porque cada móvil de dentro es un notario [19][20]; donde el «¡fake!» reflejo se responde con una huella fechada y no con un peritaje de meses [9]; donde el próximo al-Ahli se dirime sobre vídeos con hora cierta e integridad verificable [10]; donde el archivo del periodista muerto sigue acusando [1]; y donde la fiscalía del TPI recibe paquetes de evidencia que cumplen el Protocolo de Berkeley por defecto [14] (capítulo 20). La verdad seguirá costando vidas; al menos, que no se pueda enterrar con ellas.

La posesión que mata — un móvil con un archivo sellado puede ser una sentencia en un registro. El diseño debe asumirlo: solo huellas fuera del dispositivo, contenido cifrado o fuera del móvil, revelación diferida [20]. Pero ninguna arquitectura elimina el riesgo físico del testigo — y prometer invulnerabilidad sería mentir. El sello protege la prueba; proteger a la persona sigue siendo trabajo del derecho, de los medios que publican — y responsabilidad de quien la quiere callar.

El apagón — sin red no hay ancla: Gaza acumula al menos veintitrés apagones de comunicaciones documentados desde octubre de 2023, por ataques a la fibra y por falta de combustible — la conectividad civil convertida en medio y método de guerra, en palabras de Access Now [16]. El sello local se genera igual y se ancla cuando vuelve la señal; pero entonces la cadena solo prueba el «no después». El remedio parcial es el sándwich temporal: incorporar a la captura un valor público reciente e impredecible — la huella del último bloque conocido antes del apagón — prueba el «no antes», y el ancla posterior, el «no después». La ventana queda cerrada por los dos lados; y más vale una horquilla honesta de días que una promesa falsa de instantaneidad.

El GPS que miente — en la región, la perturbación y la suplantación de la señal GPS son masivas y están documentadas: más de 50.000 vuelos afectados en 2024, aplicaciones civiles situando a usuarios en Beirut o El Cairo [17]. Un sistema honesto lo reconoce: cuando la señal no es fiable, la posición se degrada o se omite — y el valor central del sello, la hora cierta y la integridad, no depende de ella [20]. Una geolocalización suplantada presentada como cierta haría más daño que ninguna geolocalización.

El sello no santifica — la prueba de existencia acredita cuándo existía un archivo y que nadie lo ha tocado: no acredita qué pasaba fuera de encuadre, ni impide sellar una escenificación el mismo día. Quien quiera hacer teatro con fecha cierta, podrá. La respuesta es la de siempre en este libro: corroboración — más testigos, más ángulos, el satélite (capítulo 104), la forénsica (capítulo 15) — sobre una base que al menos ya no se discute: qué archivos, de cuándo, sin retoques. El sello no sustituye al periodismo ni al peritaje: les ahorra la mitad estéril del trabajo.

El registro que persigue — el mismo rastro que ampara al testigo puede desanonimizarlo si se diseña mal (capítulo 20): anclas enlazables entre sí, metadatos que dibujan patrones, geolocalización por defecto. Divulgación selectiva, identificadores no correlacionables y control del testigo sobre cada campo no son

extras de lujo: son la diferencia entre una herramienta de derechos humanos y una lista de detecciones a disposición del perseguidor.

Es hora de actuar

El asedio a la verdad se combate antes de que empiece — cuando la foto nace.

Para las agencias y los medios: el precedente de «78 Days» ya os ha enseñado el camino [18] — haced del sello en la captura el estándar de todo material de zona de conflicto, propio o de colaborador; publicad la procedencia verificable con cada pieza; y firmad la credencial de vuestros colaboradores locales sin exponerlos [20]. Su riesgo ya es el máximo: que al menos su palabra no se pueda borrar.

Para los fotoperiodistas y colaboradores dentro de la zona: sellad todo, aunque no lo publiquéis — el compromiso y revelación [20] permite documentar hoy y revelar cuando estéis fuera; y vuestra agencia o vuestra familia podrán probarlo aunque vosotros ya no estéis. El chaleco de PRENSA no detiene misiles; la huella anclada no detiene mentiras — pero las hace caducar.

Para las organizaciones de derechos humanos y las fiscalías internacionales: exigid y enseñad el sello en el origen — las investigaciones como las de Abu Akleh, Hind Rajab o los archivos Caesar [11][12][13] habrían ganado meses o años; el Protocolo de Berkeley (capítulo 20) ya os da el marco para aceptarlo; y cada taller de documentación segura en una zona de conflicto vale más que diez comunicados posteriores.

Para los ciudadanos y las víctimas: vuestro móvil es un notario que no pide permiso a nadie [19][20]. Sellad lo que veis — solo la huella sale del dispositivo; publicad cuando sea seguro; y si elegís el anonimato, la prueba valdrá igual. Nadie os puede exigir la identidad como precio del derecho a que os crean.

Para las plataformas: preservar las credenciales y las huellas del material de conflicto en lugar de borrarlas al recomprimir (capítulo 17) es la diferencia entre ser el canal del testigo o su trituradora; y etiquetar la procedencia verificada — sin censurar lo que no la tiene — da al lector el criterio que los detectores no le pueden dar [9].

Para los gobiernos democráticos y los organismos internacionales: si el compromiso con la prensa libre es de verdad, vale también cuando la guerra es vuestra o de un aliado — acceso para la prensa acreditada [6], conectividad civil protegida [16], y reconocimiento procesal de la prueba de existencia, para que el testigo de la próxima guerra no dependa del coraje de un funcionario huyendo con 53.000 fotos [13].

Al fin y al cabo, todo este libro — y este capítulo más que ningún otro — defiende algo antiguo: que el testimonio de una persona vale, y que su palabra merece poder ser creída. La tecnología solo añade lo que la fuerza siempre le ha querido quitar: la prueba. Por todos los que grabaron hasta el último segundo, time2act.

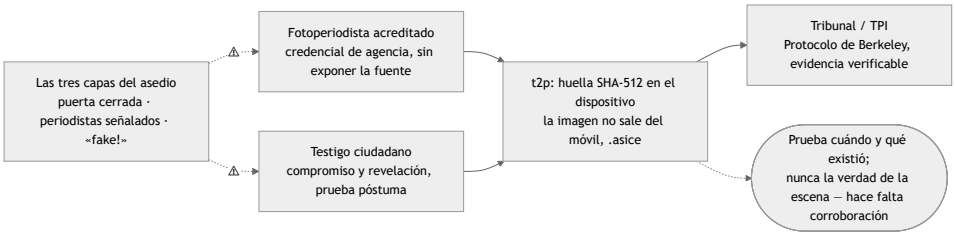


Figura 113.1 — La prueba bajo asedio, del objetivo al tribunal (t2p: huella SHA-512 en el dispositivo — la imagen no sale del móvil —, sello RFC 3161/eIDAS, ancla en la blockchain pública, paquete .asice): el fotoperiodista acreditado con credencial de agencia sin exponer la fuente; el testigo ciudadano con compromiso y revelación (sella ahora, publica cuando sea seguro) y prueba póstuma; las tres capas del asedio (puerta cerrada a la prensa internacional, periodistas locales muertos o señalados, «¡fake!» contra las imágenes reales) y dónde las rompe el sello. Límites: el apagón retrasa el ancla (sándwich temporal «no antes / no después»); el GPS suplantado degrada la posición, no la hora; el sello prueba cuándo y qué — nunca la verdad de la escena: la corroboración sigue siendo imprescindible. Fuentes: CPJ; RSF; Costs of War (Brown); OHCHR; Forensic Architecture; ECCHR/Coblenza; Access Now; Starling Lab/Reuters; WITNESS/Guardian Project.

[1] CPJ (Committee to Protect Journalists) — *Israel-Gaza War* (263 periodistas y trabajadores de medios muertos desde el 7-oct-2023; 108 encarcelados; 174 heridos; «el esfuerzo más letal y deliberado por matar y silenciar periodistas que el CPJ haya documentado nunca») y *At least 5 Gazan journalists killed in Israeli strike on Nasser Hospital* (25-ago-2025).

https://cpj.org/issue/israel-gaza-war/ · https://cpj.org/2025/08/at-least-5-gazan-journalists-killed-in-israeli-strike-on-nasser-hospital/ ↩

[2] Watson Institute (Brown University), proyecto Costs of War — *News Graveyards: How Dangers to War Reporters Endanger the World* (Nick Turse, 1-abr-2025: más periodistas muertos en Gaza que en las grandes guerras del siglo XX combinadas — comparativa que la propia base de datos usada matiza; ~13 periodistas palestinos muertos al mes); Foreign Policy — *War in Gaza the 'Worst Ever Conflict for Reporters'*. https://watson.brown.edu/costsofwar/papers/2025/Journalists · https://foreignpolicy.com/2025/04/01/gaza-war-worst-ever-for-reporters-costs-of-war-project/ ↩

[3] Wikipedia (EN) — *2025 Nasser Hospital strikes* (25-ago-2025; primer impacto ~10:00 contra la posición de la cámara de Reuters — que emitía en directo — y segundo impacto ~10 min después contra rescatadores y periodistas; ≥22 muertos, 5 periodistas: Hussam al-Masri/Reuters, Mariam Dagga/AP, Mohammed Salama/Al Jazeera, Moaz Abu Taha, Ahmed Abu Aziz; «tragic mishap»); CNN — *New video reveals third strike* (27-ago-2025). https://en.wikipedia.org/wiki/2025_Nasser_Hospital_strikes · https://www.cnn.com/2025/08/27/middleeast/gaza-nasser-hospital-israel-attack-three-strikes-intl ↩

[4] CPJ — *Israel kills Al Jazeera journalists in targeted Gaza City airstrike* (Anas al-Sharif y cuatro compañeros, 10-ago-2025; la alerta previa del CPJ y de la relatora de la ONU Irene Khan, jul-2025); NPR — *Israeli airstrike kills Al Jazeera's Anas al-Sharif in Gaza*. https://cpj.org/2025/08/israel-kills-al-jazeera-journalists-in-targeted-gaza-city-airstrike/ · https://www.npr.org/2025/08/12/g-s1-82143/gaza-anas-al-sharif-al-jazeera-israel ↩

[5] Al Jazeera — *Family of Al Jazeera Gaza bureau head killed in Israeli air raid* (25-oct-2023: la esposa, el hijo Mahmoud, la hija Sham y el nieto Adam de Wael al-Dahdouh) y *To kill a family: the loss of Wael Dahdouh's family*. https://www.aljazeera.com/news/2023/10/25/family-of-al-jazeera-gaza-bureau-head-killed-in-israeli-air-raid · https://www.aljazeera.com/news/2023/11/1/to-kill-a-family-the-loss-of-wael-dahdouhs-family-to-israeli-bombs ↩

[6] The Times of Israel / Al Jazeera / Courthouse News — el veto de acceso de la prensa internacional a Gaza: rechazo de la petición de la FPA (ene-2024, «no vested right»), nueva petición (sep-2024), el gobierno mantiene el veto «por razones de seguridad» pese al alto el fuego (ene-2026) y el Supremo aplaza de nuevo (28-ene-2026); más de dos docenas de organizaciones informativas reclaman acceso. https://www.timesofisrael.com/ban-on-media-access-to-gaza-should-stay-in-place-israel-tells-high-court/ · https://www.aljazeera.com/news/2026/1/7/media-body-condemns-israels-continued-ban-on-foreign-media-access-to-gaza · https://www.aljazeera.com/news/2026/1/28/israels-top-court-delays-gaza-press-access-ruling-amid-years-long-ban · https://www.courthousenews.com/over-two-dozen-global-news-organizations-call-on-israel-to-allow-gaza-access/ ↩

[7] RSF (Reporteros Sin Fronteras) — *RSF files fifth complaint with ICC about Israeli war crimes against journalists in Gaza* (30-sep-2025; cinco denuncias desde oct-2023; ≥210 periodistas muertos, 56 con motivos razonables para creerlos deliberadamente atacados; patrón de «doble bombardeo») y *«Gazawood»: the deadly accusations against Gaza's journalists*. https://rsf.org/en/rsf-files-fifth-complaint-icc-about-israeli-war-crimes-against-journalists-gaza · https://rsf.org/en/gazawood-deadly-accusations-against-gaza-s-journalists ↩

[8] Al Jazeera / The National — *Palestinian journalist Bisan Owda and AJ+ win Emmy for Gaza war documentary* (25-sep-2024, «It's Bisan From Gaza — and I'm Still Alive»; ~4 millones de seguidores; campaña de descalificación fallida) y el fotoperiodista Motaz Azaiza. https://www.aljazeera.com/news/2024/9/26/palestinian-journalist-bisan-owda-and-aj-win-emmy-for-gaza-war-documentary · https://www.thenationalnews.com/arts-culture/film-tv/2024/09/26/bisan-owda-emmy-award-palestine/ ↩

[9] Wikipedia (EN) / NPR — *Misinformation in the Gaza war* y *Pallywood* (pico de 220.000 usos en X en nov-2023 según BBC Verify; el caso de la «muñeca» publicado y retirado por el Jerusalem Post y amplificado por la cuenta oficial de Israel en X; el falso positivo del detector «AI or Not» sobre una foto real; Ron Dudai: la documentación descartada con una sola palabra, «Fake»); NPR — *False 'crisis actor' claims spread about Israel-Hamas war*. https://en.wikipedia.org/wiki/Misinformation_in_the_Gaza_war · https://en.wikipedia.org/wiki/Pallywood · https://www.npr.org/2023/11/27/1214451419/civilian-deaths-are-being-dismissed-as-crisis-actors-in-gaza-and-israel ↩

[10] Human Rights Watch / CNN / Forensic Architecture — la explosión en el hospital al-Ahli (17-oct-2023; 471 muertos según el Ministerio de Salud de Gaza, 100-300 según la inteligencia de EE. UU.) y la divergencia forense: HRW (patrón consistente con cohete propulsado; hace falta investigación independiente), CNN y AP (cohete fallido desde Gaza, lo más probable), NYT (causa incierta), Forensic Architecture (proyectil desde la dirección de Israel). https://www.hrw.org/news/2023/11/26/gaza-findings-october-17-al-ahli-hospital-explosion · https://www.cnn.com/2023/10/21/middleeast/cnn-investigates-forensic-analysis-gaza-hospital-blast · https://forensic-architecture.org/investigation/israeli-disinformation-al-ahli-hospital ↩

[11] OHCHR / CNN — el asesinato de Shireen Abu Akleh (11-may-2022): conclusión de la ONU (jun-2022: tiros de las fuerzas israelíes, «aparentemente bien apuntados»), investigación de CNN (24-may-2022) y admisión del ejército israelí (5-sep-2022: «probablemente» fuego propio; sin cargos). https://www.ohchr.org/en/press-briefing-notes/2022/06/killing-journalist-occupied-palestinian-territory · https://www.cnn.com/2022/05/24/middleeast/shireen-abu-akleh-jenin-killing-investigation-cmd-intl · https://www.cnn.com/2022/09/05/middleeast/idf-shireen-abu-akleh-investigation-intl/index.html ↩

[12] Forensic Architecture / Earshot — *The Killing of Hind Rajab* (29-ene-2024: 355 impactos en el coche; análisis acústico de la llamada: tiros desde 13-23 m). https://forensic-architecture.org/investigation/the-killing-of-hind-rajab · https://www.earshot.ngo/investigations/the-killing-of-layan-hamada-and-hind-rajab ↩

[13] ECCHR / Syria Justice & Accountability Centre / CBS — los archivos Caesar (~53.000 fotos sacadas de Siria en 2013; autenticación pericial de metadatos y forénsica médica) y la condena de Coblenza (13-ene-2022: cadena perpetua a Anwar Raslan por crímenes contra la humanidad). https://www.ecchr.eu/en/case/caesar-photos-document-systematic-torture/ · https://syriaaccountability.org/inside-the-raslan-trial-a-forensic-analysis-of-the-caesar-photos/ · https://www.cbsnews.com/news/syria-war-bashar-assad-police-officer-crimes-against-humanity-germany/ ↩

[14] Tribunal Penal Internacional — *ICC Pre-Trial Chamber I rejects the State of Israel's challenges to jurisdiction and issues warrants of arrest for Benjamin Netanyahu and Yoav Gallant* (21-nov-2024; crimen de guerra del hambre como método de

guerra; crímenes contra la humanidad; orden también contra Mohammed Deif). https://www.icc-cpi.int/news/situation-state-palestine-icc-pre-trial-chamber-i-rejects-state-israels-challenges ↩

[15] Tribunal Internacional de Justicia — *Application of the Genocide Convention (South Africa v. Israel)*, medidas provisionales de 26-ene-2024, 28-mar-2024 y 24-may-2024 (vinculantes). https://www.icj-cij.org/case/192 ↩

[16] Access Now (#KeepItOn) / EFF — *Israel must stop cutting Gaza off from the world* (19-jun-2025: ≥23 apagones de comunicaciones desde oct-2023, por ataques a la fibra y falta de combustible; «la conectividad civil convertida en medio y método de guerra») y *Connectivity is a Lifeline, Not a Luxury*. https://www.accessnow.org/press-release/keepiton-israel-must-stop-cutting-gaza-off/ · https://www.eff.org/deeplinks/2025/06/connectivity-lifeline-not-luxury-telecom-blackouts-gaza-threaten-lives-and-digital ↩

[17] NPR / GPS World / The Times of Israel — perturbación y suplantación de GPS en la región (2024: >50.000 vuelos afectados; incremento ×6; aplicaciones situando a usuarios en Beirut o El Cairo; una base aérea israelí señalada como origen). https://www.npr.org/2024/04/22/1245847903/israel-gps-spoofing · https://www.gpsworld.com/israeli-air-base-identified-as-alleged-source-of-gps-disruptions-in-mideast/ · https://www.timesofisrael.com/gps-jamming-amid-wars-playing-havoc-with-airline-navigation-report/ ↩

[18] Starling Lab / Content Authenticity Initiative — *78 Days* (Reuters + Starling, nov-2020→ene-2021: >200 fotos de la transición presidencial con metadatos criptográficos anclados en Filecoin y Hedera; procedencia verificable por cualquiera). https://www.starlinglab.org/78days/ · https://contentauthenticity.org/blog/cai-spotlight-78-days-from-stanford-starling-lab-and-reuters ↩

[19] Guardian Project / WITNESS — *ProofMode* (desde 2017: firma OpenPGP y huella en la captura, instantánea de sensores, notarización — con OpenTimestamps entre los sistemas soportados; pensada para la documentación ciudadana de derechos humanos). https://guardianproject.info/apps/org.witness.proofmode/ · https://blog.witness.org/2017/04/proofmode-helping-prove-human-rights-abuses-world/ ↩

[20] t2p — manual de producto (huella SHA-512 calculada en el dispositivo — solo la huella sale del móvil —; sello de tiempo RFC 3161/eIDAS; anclaje en la blockchain pública; GPS forense con degradación honesta; modo sin conexión con anclaje diferido; compromiso y revelación; paquete .asice verificable sin conexión; certificado con QR). Véanse los capítulos 13 y 15; el compromiso y revelación, en los capítulos 45 y 46; la cadena de custodia del socorro, en el capítulo 50; la divulgación selectiva y la evidencia de crímenes de guerra, en el capítulo 20; las credenciales de contenido, en el capítulo 17. ↩

[21] Wikipedia (EN) — *Operation Metro Surge* (4-dic-2025 → feb-2026: «the largest immigration enforcement operation ever carried out» según el DHS; miles de agentes de ICE y CBP en Minneapolis–Saint Paul; ≥3.789 detenciones, menos de un 25 % con antecedentes; la huelga general del 23-ene-2026; el juez Schiltz: ≥96 órdenes judiciales violadas por ICE desde el 1-ene; el juez Blackwell: la «mayoría abrumadora» de los detenidos, con presencia legal); NPR — *Minnesota ICE crackdown will end* (12-feb-2026: Tom Homan anuncia el final del operativo — que «ha costado la vida a dos ciudadanos estadounidenses» — sin mencionar sus nombres); Sahan Journal — las cifras del despliegue (más de 4.000 agentes en el punto álgido), reveladas por orden judicial. https://en.wikipedia.org/wiki/Operation_Metro_Surge · https://www.npr.org/2026/02/12/nx-s1-5712280/minnesota-ice-surge-ends · https://sahanjournal.com/immigration/hundreds-ice-agents-leaving-minnesota-operation-metro-surge/ ↩

[22] Wikipedia (EN) — *Killing of Renée Good* (7-ene-2026, Portland Avenue, Minneapolis: el agente de ICE Jonathan Ross dispara tres tiros — parabrisas y ventanilla de la conductora — con el vehículo girando para alejarse, según la reconstrucción del New York Times; en el coche, la pareja y una criatura de seis años; las alegaciones de Noem y de Trump; la grabación del propio Ross, sacudida hacia arriba en el momento crítico; el acceso de la agencia estatal de investigación a las pruebas, revocado al día siguiente; Ross, tres días apartado y reasignado fuera del estado); The Intercept — *Video Shows ICE Agent's Fatal Shooting of Civilian in Minneapolis* (el tiro a corta distancia contra el vehículo que se iba; un segundo ángulo muestra a Good cediendo el paso a los vehículos federales minutos antes). https://en.wikipedia.org/wiki/Killing_of_Ren%C3%A9e_Good · https://theintercept.com/2026/01/07/video-ice-shooting-civilian-minneapolis/ ↩

[23] Wikipedia (EN) — *Killing of Alex Pretti* (24-ene-2026, Minneapolis: enfermero de UCI del hospital de veteranos, 37 años, permiso de armas y ningún antecedente; los vídeos de los testigos, revisados y verificados por Reuters, BBC, Wall Street Journal, AP, CNN, New York Times y The Guardian: el teléfono en la mano, el espray de pimienta, los agentes inmovilizándolo, el arma sacada de la funda y los tiros un segundo después; las alegaciones del DHS — «máximo daño», «dos cargadores y ningún tipo de identificación» — y de Stephen Miller; la forense del condado de Hennepin: homicidio; los agentes, identificados por ProPublica); NPR — *Videos refute DHS account of fatal shooting* (25-ene-2026: Noem — «se había acercado con una pistola» — contra los vídeos: no sacó nunca ningún arma; filmaba con el móvil); The Marshall Project — *How Many People Have Been Killed by ICE and Border Patrol?* (26-ene-2026: ninguna reanimación de los agentes; una pediatra apartada; en el caso Good, tres minutos sin llamar a emergencias; el desmentido público del alcalde Frey y el gobernador Walz tras ver los vídeos). https://en.wikipedia.org/wiki/Killing_of_Alex_Pretti · https://www.npr.org/2026/01/25/nx-s1-5687384/minneapolis-minnesota-shooting-video-dhs · https://www.themarshallproject.org/2026/01/26/ice-minneapolis-shooting-alex-pretti ↩

[24] ProPublica — *Minnesota's Fight to Hold Agents Who Shot Alex Pretti, Renee Good Accountable* (la demanda de Minnesota, el condado de Hennepin y la agencia estatal de investigación contra los departamentos de Justicia y de Seguridad Nacional, 24-mar-2026: pruebas retenidas «para escudar a los agentes implicados» — nombres, armas, informes, datos GPS y declaraciones de testigos negados pese a los requerimientos formales; las diecisiete investigaciones penales de la fiscal Moriarty; el obstáculo de la cláusula de supremacía; los agentes del caso Pretti, identificados por ProPublica el 1-feb); NPR — *Months after the ICE shootings in Minnesota, a federal probe remains elusive* (10-abr-2026: el móvil de Pretti, retenido; el coche de Good, precintado en un almacén del FBI sin examinar; investigadores estatales apartados físicamente de la escena; única medida disciplinaria del operativo: dos agentes en permiso administrativo por «declaraciones falsas» en el caso del tercer tiroteado, Julio Sosa-Celis; «Parece que estén impidiendo activamente que el estado investigue» — Rachel Moran, profesora de derecho). https://www.propublica.org/article/minnesota-trump-ice-shooting-lawsuit-alex-pretti-renee-good · https://www.npr.org/2026/04/10/nx-s1-5775847/alex-pretti-renee-good-ice-shootings-federal-investigations ↩

[25] Wikipedia (EN) — *Shooting of Marimar Martinez* (Chicago, 4-oct-2025: cinco tiros del agente de la Patrulla Fronteriza Charles Exum; la cámara corporal muestra el vehículo de los agentes girando hacia el de ella tras el «it's time to get aggressive»; los mensajes del agente — «fired 5 shots and she had 7 holes» —; los cargos contra Martinez y su codemandado, archivados con carácter definitivo el 20-nov-2025) y *List of shootings by U.S. immigration agents in the second Trump administration* (el recuento acumulado: 38 tiroteos y 9 muertos entre el 20-ene-2025 y el 7-jul-2026; los casos con cargos contra civiles retirados cuando el vídeo contradijo la versión de los agentes); AP (vía KSAT) — *Judge's blistering opinion details use of force in Chicago-area immigration crackdown* (nov-2025: el dictamen de 223 páginas de la jueza Sara Ellis — el relato del gobierno, «simply not credible», desmentido por las cámaras corporales que ella misma había ordenado activar; las versiones cambiantes de Bovino sobre la piedra y el gas; el informe de uso de la fuerza redactado con ChatGPT). https://en.wikipedia.org/wiki/Shooting_of_Marimar_Martinez · https://en.wikipedia.org/wiki/List_of_shootings_by_U.S._immigration_agents_in_the_second_Trump_administration · https://www.ksat.com/news/politics/2025/11/21/judges-blistering-opinion-details-use-of-force-in-chicago-area-immigration-crackdown/ ↩

[26] KPRC 2 / Click2Houston — *ICE agent shoots, kills Lorenzo Salgado Araujo during attempted arrest in east Houston* (7-jul-2026, Magnolia Park: ICE alega que «embistió un vehículo oficial» y que el agente disparó «en defensa propia»; los agentes no llevaban cámaras corporales, según el DHS; relatos en conflicto sobre los momentos previos; la forense del condado de Harris, 9-jul: homicidio). https://www.click2houston.com/news/local/2026/07/07/heavy-law-enforcement-presence-reported-in-east-houston-neighborhood/ ↩

La dignidad de quien existe: la «Magnifica Humanitas» y la prueba de existencia

«La persona acaba reduciéndose a un medio para obtener resultados, a un recurso para ser usado y explotado.»

— León XIV, encíclica Magnifica Humanitas, §51 (2026)

El 25 de mayo de 2026, en el Vaticano, pasó algo que ningún protocolo había previsto: por primera vez en la historia, un papa presentó personalmente una encíclica al mundo. Y León XIV no compareció solo. A su lado se sentaba **Chris Olah**, cofundador de Anthropic —una de las empresas punteras en inteligencia artificial— y **ateo declarado**: criado en Toronto en una familia evangélica devota, había dejado de creer a los quince años [8]. El texto, firmado diez días antes y titulado «Magnifica Humanitas», se presentó al mundo con una imagen tan insólita como deliberada: un creyente y un no creyente, el uno al lado del otro, diciendo a la vez que cada persona es única e irreemplazable [4][6].

El papa lo resumió con una frase que vale para todo este libro: «qué gran signo de esperanza que, con nuestras diferencias, podamos escucharnos los unos a los otros» [6]. Empecemos, pues, por aquí, y no por un argumento de fe. La fuerza de la idea que vertebra la encíclica —«la dignidad que pertenece a todo ser humano por el simple hecho de existir» (§52) [1]— no radica en quién la pronuncia, sino en el hecho de que la pueda suscribir igual un pontífice que un ingeniero que no cree en Dios. La dignidad de quien existe no pide ningún credo: es anterior a cualquier creencia y, precisamente por eso, puede ser el fundamento de una tecnología pensada para todos.

La encíclica se publica exactamente 135 años después de la «Rerum Novarum» de León XIII, el texto fundacional de la doctrina social católica que puso las bases del respeto por la dignidad del trabajador [2]. Esta coincidencia cronológica subraya una continuidad histórica: tal como el antiguo documento denunciaba las condiciones de explotación industrial, la nueva encíclica se dirige hacia un mundo dominado por algoritmos y datos. Su tema central —«la custodia de la persona humana en el tiempo de la inteligencia artificial»— resuena con la llamada que la propia Iglesia hizo hace más de un siglo, ahora transpuesta al contexto digital [1].

En el corazón del texto, en el párrafo cincuenta y dos, aparece una frase que parece una clave de bóveda para todo el debate que hemos conducido desde el capítulo 10 hasta el capítulo del sello (cap. 112): «la dignidad que pertenece a todo ser humano por el simple hecho de existir» (§52) [1]. No se trata de una declaración meramente teológica; es una afirmación que pretende fundamentar moralmente cualquier tecnología que pretenda validar la presencia y la integridad de un individuo.

La pregunta que este capítulo plantea, como hilo conductor de las secciones anteriores sobre identidad digital (cap. 47) y la crisis de la verdad provocada por las deepfakes (cap. 10), es clara: si la dignidad nace simplemente de existir, ¿qué papel puede jugar una herramienta que prueba la existencia —t2p— en este escenario? ¿Puede esta tecnología servir como guardián de la dignidad, certificando que alguien o algo existe sin reducirlo a un simple conjunto de datos? O, por el contrario, ¿podría convertirse en el «poder tecnológico con rostro privado» que la encíclica denuncia (§5) [1], transformando a la persona en una mercancía utilizable por intereses económicos y políticos?

Esta intersección entre fe y ciencia, entre moralidad e innovación, establece el marco donde se habrá de valorar tanto la promesa como el peligro de cualquier mecanismo que pretenda probar la existencia. La respuesta determinará si la «Magnifica Humanitas» se convierte en una brújula ética capaz de impulsar un futuro donde la tecnología no solo reconoce, sino también protege, la dignidad intrínseca de todo ser humano.

Un creyente, un ateo y la misma dignidad

Que el Vaticano eligiera a Chris Olah para presentar el texto al lado del papa no fue un gesto decorativo. Olah no estaba allí como creyente discreto invitado por cortesía, sino como uno de los ingenieros que construyen, desde dentro, los modelos que el mundo apenas empieza a comprender. Y su mirada —justamente porque viene de fuera de la fe— da a este capítulo el tono que queremos que prevalezca en él: primero la humanidad, después la religión.

Sus palabras en el Vaticano podrían ser el lema de este libro. Elogió a la Iglesia como «crítico informado» y habló del inicio de «una larga colaboración entre quienes construimos esto y quienes pueden ver lo que nosotros, desde dentro, no vemos» [7]. En una sola frase cabía toda la tesis de *time2act*: quien hace la tecnología no se puede juzgar a sí mismo. Por eso Olah reclamaba el diálogo con gente «no movida por el beneficio» [7] y advertía, sin rodeos, que la industria «no se puede gobernar a sí misma» [8]. Es exactamente la razón de ser de una prueba externa y verificable: que la verdad no dependa de la buena fe de quien la produce.

Esta convergencia —un papa y un ateo que afirman lo mismo— es, ella misma, la demostración de que la dignidad de quien existe no es una doctrina de unos cuantos, sino un mínimo común humano. Cuando León XIV escribe que cada persona es «única e irreemplazable» [1], no pide que lo creamos por fe: nombra una evidencia que un ingeniero escéptico reconoce igual de bien. Y es sobre este mínimo universal —no sobre ninguna teología particular— que una herramienta como la prueba de existencia (t2p) puede aspirar a servir a todos. Porque a todos, creyentes y no creyentes, nos corresponde la misma dignidad por el solo hecho de existir; y una tecnología que se limite a dar testimonio de ella, sin pretender otorgarla ni medirla, puede ser de todos sin ser de nadie.

Ciento treinta y cinco años después de *Rerum Novarum*

Desde el momento en que el papa León XIII publicó *Rerum Novarum* (1891), la doctrina social católica ha marcado el ritmo de una conversación mundial sobre trabajo, dignidad y responsabilidad colectiva [2]. Aquel documento, nacido de las tensiones de la Revolución Industrial, ponía como piedra angular la dignidad del trabajador ante la explotación. Un siglo después, *Centesimus Annus* (1991) celebraba el centenario de esta misión, recordándonos que el progreso económico debe estar al servicio del bienestar humano y no al revés [5]. En 2015, con *Laudato Si'*, Francisco amplió este marco a la «Casa común», advirtiendo del peligro de un paradigma tecnocrático que reducía la naturaleza —y, por extensión, la persona— a simples recursos explotables [3].

En 2026, en mayo, el papa León XIV ha publicado su primera encíclica, *Magnifica Humanitas*, una obra que se posiciona como continuación directa de este legado. Firmada el 15 del mes y difundida al final del mismo, por coincidencia con el aniversario de *Rerum Novarum* [1], se abre con la declaración que resuena en el corazón de todo debate: «la dignidad que pertenece a todo ser humano por el simple hecho de existir» (según el párrafo correspondiente) [1]. Esta afirmación, sencilla pero profunda, establece la base moral del proyecto *time2act*: una tecnología —la prueba de existencia (t2p)— que puede validar la presencia y la integridad de una persona sin intentar asignarle dignidad, ya intrínseca.

El elemento clave de la encíclica se encuentra en el primer párrafo, donde el papa plantea una elección decisiva para la humanidad: «una elección decisiva: levantar una nueva torre de Babel o edificar la ciudad donde Dios y la humanidad habiten juntos» (§1) [1]. Esta metáfora no es solo retórica; representa el punto de inflexión en que las tecnologías emergentes, como la inteligencia artificial y la blockchain, pueden convertirse tanto en puentes hacia una convivencia más justa como en nuevas torres que separan y fragmentan. El riesgo, ya advertido en el párrafo §9 de la encíclica, es que «la tecnología puede curar, conectar, educar… pero también puede dividir, descartar» [1]; y aún más, que el poder tecnológico adopte un rostro privado y dominante (§5) [1].

Como hemos visto en los capítulos 10, 47 y 112, esta narrativa converge en una elección moral: si la prueba de existencia se desarrolla como una herramienta humilde, capaz solo de certificar que alguien existe y es íntegro, puede servir como bastión para la dignidad humana siempre que no se convierta en «el poder tecnológico de rostro privado» denunciado (§5) [1]. *Magnifica Humanitas* nos recuerda que el futuro depende de nuestro compromiso ético; nuestra tarea, como lectores y creadores de estas tecnologías, es elegir la «ciudad donde Dios y la humanidad habiten juntos», asegurándonos de que cada innovación sea un puente hacia la dignidad y no una nueva torre de Babel que nos separe.

Figura 114.1 — La doctrina social de la Iglesia ante la economía y la técnica: de la 'Rerum Novarum' (1891, el trabajo) a la 'Laudato Si'' (2015, la Casa común) y la 'Magnifica Humanitas' (2026, la persona en tiempos de IA).

La dignidad de quien existe

El 25 de mayo de 2026 el papa León XIV presentó personalmente su primera encíclica, *Magnifica Humanitas*, que se convierte en el faro moral de este libro. En el párrafo cincuenta y dos la encíclica afirma con claridad y contundencia: «la dignidad que pertenece a todo ser humano por el simple hecho de existir» (§52) [1]. Esta afirmación, arraigada en la tradición social de la Iglesia desde *Rerum Novarum* (1891) —mencionada por León XIII como fundamento de la dignidad obrera— [2], no es una mera declaración abstracta; es el punto de arranque para cualquier tecnología que pretenda ser responsable. La dignidad, según la encíclica, es previa e intrínseca: la persona ya la posee simplemente por estar viva, tal como se recuerda en el párrafo cincuenta: «el hombre y la mujer son creados a imagen y semejanza del Dios trinitario» (§50) [1].

Esta premisa moral resuena directamente con el problema expuesto en el capítulo 47 sobre identidad digital. Millones de individuos en todo el mundo aún no disponen de una identidad legal reconocida; su existencia queda reducida a un número de archivo o, peor aún, a la ausencia total de un registro oficial. En este contexto, *t2p* —la prueba de existencia que hemos desarrollado— no pretende conferir dignidad; su papel es certificar una realidad que ya existe pero que a menudo se ve negada por las estructuras legales y administrativas.

El riesgo de confundir certificación con conferencia de dignidad está advertido en la encíclica. En el párrafo cincuenta y uno, León XIV denuncia la reducción de la persona a un simple medio: «la persona acaba reduciéndose a un medio para obtener resultados, a un recurso para ser usado y explotado» (§51) [1]. Este es el peligro que recuerdan las deepfakes descritas en el capítulo 10; sin una prueba fiable, la identidad puede ser sustituida o borrada por algoritmos que priorizan el engaño sobre la transparencia.

t2p, en este marco, actúa como escudo contra esta erosión. Cuando un sistema niega la existencia jurídica de un individuo —por ejemplo, una persona sin registro civil— la prueba de existencia puede registrar de forma inmutable que aquella voz es suya y que aquel acontecimiento ha tenido lugar. Esto no solo ofrece una defensa legal; es una reivindicación moral que apoya la afirmación del papa: la dignidad ya está presente, solo hay que reconocerla.

Sin embargo, la encíclica también nos advierte sobre el poder tecnológico privado (párrafo cinco): «el poder tecnológico adquiere así un rostro inédito, predominantemente 'privado'» (§5) [1]. Si la prueba de existencia se convierte en una herramienta controlada por entidades con intereses exclusivos, su potencial emancipador se anula y se transforma en una nueva forma de dominación. Nuestra responsabilidad, como creadores y usuarios, es garantizar que *t2p* sea una infraestructura abierta, transparente y sometida a principios de subsidiariedad (párrafo sesenta y ocho): «lo que pueden hacer las personas... no debe ser absorbido por instancias superiores» (§68) [1].

En definitiva, la prueba de existencia es una herramienta humilde pero poderosa. No otorga dignidad —esta ya existe por el simple hecho de estar—, sino que la fortalece al proporcionar un testimonio inequívoco de nuestra presencia en el mundo digital. Si se utiliza con sabiduría y responsabilidad, puede ser el puente que la encíclica describe entre la tecnología y la custodia amorosa de la humanidad: una ciudad donde Dios y el hombre cohabitan, más que una torre de Babel que nos separa.

Que la persona no se reduzca a un dato

La encíclica recuerda con claridad el peligro que amenaza nuestra esencia: «la persona acaba reduciéndose a un medio para obtener resultados, a un recurso para ser usado y explotado» (como hemos visto en el párrafo 51)[1]. Esta advertencia resuena especialmente en la era de las identidades digitales, donde el valor de una vida a menudo se mide en bits, tokens o puntuaciones algorítmicas. Un sistema mal diseñado puede convertirnos en simples registros, huellas o perfiles que la tecnología trata como recursos negociables, y no como seres con una dignidad intrínseca.

El modelo de prueba de existencia (t2p) pretende ser la oposición directa a esta reducción. No se trata de una herramienta que asigne un valor o una puntuación moral; su objetivo es certificar, con mínima intervención, que alguien existe y lo hace sin crear un archivo centralizado que pueda ser explotado. La clave del diseño reside en tres principios: **minimización de la huella**, **localidad del procesamiento** y **propiedad personal del sello**.

1. **Minimización de la huella, no del contenido.** En lugar de almacenar toda la historia de interacción o los datos biométricos completamente, el protocolo genera un hash único que representa solo la presencia verificable. Esto se traduce en una pequeña cadena de caracteres que, sin la clave privada del titular, no puede ser reconocida como información personal. Esta reducción evita que las plataformas acumulen grandes volúmenes de información sensible e impide el uso posterior con fines comerciales o de vigilancia.
2. **Procesamiento en el dispositivo, no en bases centrales.** La verificación se realiza íntegramente en el terminal del usuario: su teléfono inteligente o un dispositivo IoT autorizado. El cálculo del hash y la firma digital se ejecutan localmente, sin que ningún servidor externo tenga acceso a los datos originales. Así, la información no sale nunca del entorno controlado por la persona, y el riesgo de una filtración masiva se reduce drásticamente.
3. **El sello pertenece al titular.** Una vez generada la prueba, esta se almacena en una cartera digital que solo el propietario puede administrar. La clave privada es única e intransferible; ninguna entidad externa puede revocarla ni modificarla sin el consentimiento explícito del sujeto. Esto garantiza que el sello no se convierta en un activo negociable, sino en una certificación humilde de la presencia.

Estos principios reflejan el principio de subsidiariedad señalado en la encíclica (§68)[1] —«lo que pueden hacer las personas... no debe ser absorbido por instancias superiores»— y, como hemos visto antes, garantizan a cada individuo el control total sobre su propia prueba, protegiéndola de la tentación del poder tecnológico privado descrita en el párrafo (§5)[1]. No se trata solo de una cuestión técnica, sino de un compromiso ético: la tecnología debe ser una herramienta que **custodie** y no una máquina que **explote**.

En resumen, el diseño de t2p responde al aviso del papa León XIV, convirtiéndose en un puente entre la innovación y la custodia amorosa de la humanidad. Si se aplica con rigor y responsabilidad, puede impedir que la persona se reduzca a un dato, manteniendo viva la dignidad que le pertenece por el simple hecho de existir.

El rostro privado del poder

En mayo de 2026 el papa León XIV presentó personalmente su primera encíclica, *Magnifica Humanitas*, con una misión moral clara: «la custodia de la persona humana en el tiempo de la inteligencia artificial» [4]. Este momento, como hemos visto, marcaba un aniversario simbólico y establecía el hilo conductor de nuestro libro: la dignidad intrínseca de todo ser humano por el simple hecho de existir, tal como afirma la encíclica (§52) «la dignidad que pertenece a todo ser humano por el simple hecho de existir» [1].

La «crítica al rostro privado del poder» se desarrolla en varios párrafos de *Magnifica Humanitas*. Primero, el documento advierte que «el poder tecnológico adquiere así un rostro inédito, predominantemente 'privado'» y que hay que preguntar «quién detenta hoy este poder y hacia qué fines lo orienta» (§5) [1]. Esta pregunta se convierte en la piedra angular de la gobernanza democrática: si las infraestructuras digitales —patentes, algoritmos, plataformas, datos— son controladas por unos pocos actores, el riesgo es que la tecnología deje de ser una herramienta de custodia y se transforme en una extensión del poder personalizado. El capítulo 112, dedicado a quién controla la infraestructura, ya había mostrado cómo las grandes plataformas definen condiciones de acceso, reglas de visibilidad, formas de

relación e incluso oportunidades económicas (§71) [1]; así, lo que parecía un análisis técnico se revela como una continuidad directa de la crítica papal.

Seguidamente, la encíclica subraya que «la técnica toma el rostro de quien la concibe, la financia, la regula, la utiliza» (§9) [1]. Cada modelo de aprendizaje profundo es una extensión de su creador; cuando esta responsabilidad recae en manos privadas, la persona se reduce a un simple recurso. El aviso de la encíclica —«la persona acaba reduciéndose a un medio para obtener resultados, a un recurso para ser usado y explotado» (§51) [1]— resuena con las conclusiones del capítulo 10 sobre la crisis de la verdad y las deepfakes; como hemos visto, la ausencia de una prueba fiable facilita la manipulación masiva de imágenes y voces.

En este contexto, *t2p* aparece como una respuesta técnica humilde pero potente: certifica que alguien o algo existe y es íntegro sin otorgarle dignidad. La dignidad ya está garantizada por el simple hecho de existir (§52); la prueba solo puede reforzar esta realidad contra el engaño. Si el mecanismo se pone al servicio de un grupo reducido para consolidar poder —como una «carta de crédito digital» que controla el acceso a servicios esenciales—, se convierte en el mismo rostro privado que la doctrina condena.

Así, la intersección entre la encíclica y el capítulo 112 demuestra que cualquier implementación de *t2p* debe estar subordinada a principios de subsidiariedad (§68) y a una gobernanza abierta que asegure que «lo que pueden hacer las personas... no debe ser absorbido por instancias superiores» [1]. Solo así la tecnología puede cumplir su misión de custodia, tal como el papa recuerda en §15: «se trata de custodiar con amor esta magnífica humanidad... que ninguna máquina podrá nunca sustituir». Nuestra tarea es traducir este amor en estructuras democráticas y transparentes, evitando que la innovación se convierta en un instrumento de dominación.

El destino universal de los bienes digitales

El papa León XIV recuerda con una claridad sorprendente que el «destino universal de los bienes incluye hoy «patentes, algoritmos, plataformas digitales, infraestructuras tecnológicas, datos»» (§67) [1]. Este aviso moral sobre la nueva geografía del poder se mantiene vigente: las redes de blockchain y los sistemas de inteligencia artificial configuran la arquitectura de la confianza, y lo que antes era propiedad intelectual pasa a ser una parte integral del tejido social. Cada token y cada modelo entrenado con datos masivos se convierten en bienes colectivos que afectan a la dignidad de quien existe.

Según la encíclica, la respuesta ética es el principio de subsidiariedad: «lo que pueden hacer las personas... no debe ser absorbido por instancias superiores» (§68) [1]. En términos técnicos, esto implica una infraestructura de prueba de existencia (t2p) totalmente abierta y común. No puede ser un servicio gestionado por una corporación que, como advierte el párrafo §5, ha adquirido «un rostro inédito, predominantemente 'privado'» del poder tecnológico (§5) [1]. La centralización nominal —donde la propiedad de un nodo o de una clave se concentra en manos de pocos— no garantiza la transparencia ni la rendición de cuentas que la dignidad humana pide.

En la práctica, esto implica una arquitectura descentralizada real. Las redes distribuidas deben permitir que cualquier usuario verifique su propia identidad y la de otros sin depender de una autoridad superior. Como hemos visto en las plataformas que definen condiciones de acceso (§71) [1], el sistema t2p debería establecer reglas abiertas, auditorías independientes y mecanismos de gobernanza participativa. Un modelo de «gobernanza por consorcio», en el que las decisiones sobre las actualizaciones del protocolo se toman mediante votación entre entidades públicas y organizaciones de la sociedad civil, es un marco posible para evitar la captura por parte de un solo actor.

Esta configuración tiene una doble promesa. Primero, sirve a la dignidad de los excluidos: personas que viven en contextos de vulnerabilidad —refugiados digitales, trabajadores del sector informal o víctimas de deepfakes— pueden demostrar su existencia y proteger sus derechos sin depender de una empresa que podría vender sus datos. Segundo, refuerza la verdad contra el engaño: una prueba de existencia verificable impide que alguien manipule imágenes o audios para desacreditar a un individuo, como hemos visto en el capítulo 10.

No obstante, el peligro persiste. Si la infraestructura queda bajo el control de un grupo privado, se convierte en «un recurso para ser usado y explotado» (§51) [1], revirtiendo el objetivo de custodiar con amor esta magnífica humanidad (§15) [1]. Por tanto, el reto no es solo tecnológico sino institucional: hay que establecer marcos legales que obliguen a la transparencia y a la rendición de cuentas, tal como la doctrina social de 'Rerum Novarum' (1891) exigió en su momento para el trabajador industrial [2].

En resumen, el destino universal de los bienes digitales debe alinearse con la subsidiariedad y la descentralización genuina. Solo así la herramienta t2p puede ser una «herramienta humilde» que certifica la existencia sin usurpar la dignidad intrínseca de quien existe, convirtiéndose en el verdadero puente entre la tecnología y la moralidad que la encíclica tanto insistía en defender.

El límite que ninguna máquina sustituye

Hay un último límite que este libro debe reconocer. La encíclica hace una llamada a la responsabilidad: «la dignidad que pertenece a todo ser humano por el simple hecho de existir» (§52) y, a la vez, nos recuerda que esta dignidad no se puede delegar a ningún algoritmo ni a ninguna cadena de bloques. Esta doble afirmación establece el marco moral donde se inserta nuestra propuesta tecnológica —t2p.

La humildad es el principio central que la encíclica pide a los creadores y usuarios de tecnología. Así, «aceptar los límites y la fragilidad de la humanidad sin considerarlos un error que haya que corregir» (§12) implica reconocer que ningún sistema puede capturar la totalidad del ser humano. La prueba de existencia, tal como se describe a lo largo del libro, es una herramienta que certifica que un archivo existía íntegro y que una persona es quien dice ser. No pretende medir el alma, el mérito o la virtud; no pretende sustituir la confianza humana ni el cuidado que solo puede ofrecer una relación directa. Esto coincide con el aviso de León XIV sobre el peligro de reducir la persona a un medio: «la persona acaba reduciéndose a un medio para obtener resultados, a un recurso para ser usado y explotado» (§51) [1].

t2p se presenta como una «herramienta humilde». Su función es estrictamente documental: registra la integridad de un archivo en el momento de su creación y verifica que el emisor sea quien declara ser. Esta certificación puede proteger los derechos de los más vulnerables —como las víctimas de deepfakes descritas en el capítulo 10— pero no tiene capacidad para asignar dignidad ni determinar el valor intrínseco de una vida, tal como afirma el papa: «custodiar con amor esta magnífica humanidad… que ninguna máquina podrá nunca sustituir» (§15) [1].

El límite de la herramienta queda claro en sus especificaciones técnicas. En el contexto de la identidad digital (capítulo 47), t2p puede garantizar que una credencial digitalizada sea auténtica, pero no sustituye el reconocimiento personal de un intercambio cara a cara. De manera similar, en el capítulo sobre quién controla la infraestructura (capítulo 112) se insinúa que la centralización del poder tecnológico —«el poder tecnológico adquiere así un rostro inédito, predominantemente «privado»» (§5)— puede convertir cualquier herramienta en instrumento de dominación. Nuestra propuesta mantiene la subsidiariedad proclamada por la encíclica: «lo que pueden hacer las personas… no debe ser absorbido por instancias superiores» (§68) [1].

Así, el mensaje final de esta sección es una llamada a la moderación. La tecnología puede y debe servir como soporte a la dignidad humana, pero nunca como sustituto del compromiso moral que el hombre debe tener consigo mismo y con los demás. En este equilibrio —entre el potencial transformador de la prueba de existencia y el respeto por las limitaciones intrínsecas de cualquier máquina— se encuentra el verdadero valor de *t2p*: una herramienta al servicio de la persona, no un oráculo de su valor.

La promesa y el peligro

En el párrafo noveno de *Magnifica Humanitas* el papa León XIV describe la tecnología como una doble cara: «la tecnología puede curar, conectar, educar, cuidar de la Casa común; pero también puede dividir, descartar» (§9) [1]. Esta paradoja es el hilo conductor de lo que llamamos *t2p*: una herramienta capaz de certificar la existencia de una persona o de un activo digital con un grado de integridad hasta ahora inalcanzable. Si la prueba de existencia se despliega como mecanismo de transparencia, puede aportar una respuesta concreta a las crisis documentadas anteriormente —la manipulación de la verdad y la erosión de la identidad digital— y, como hemos visto, convertir el testimonio de una existencia en un registro público que nadie puede negar ni falsificar. Esto es literalmente volver a hacer la verdad verificable y dar «existencia probada» a quien ha sido privadamente negada.

No obstante, el mismo poder tecnológico que da vida a *t2p* contiene un peligro intrínseco. La encíclica avisa de que «el poder tecnológico adquiere así un rostro inédito, predominantemente 'privado'» (§5) [1]; y de que la persona puede acabar reduciéndose a un medio para obtener resultados, a un recurso para ser usado y explotado. Si una entidad —pública o privada— controla la emisión y el reconocimiento de estos certificados, se crea una nueva forma de dominación: decidir quién es «existente» y quién no lo es. En este escenario, la prueba de existencia se convierte en un instrumento de vigilancia masiva, similar al que

observamos, y podría ser utilizada para establecer «censura de existencia», excluyendo a individuos o grupos de la vida económica y social simplemente porque no disponen del certificado adecuado.

La encíclica ofrece una metáfora poderosa: «una elección decisiva: levantar una nueva torre de Babel o edificar la ciudad donde Dios y la humanidad habiten juntos» (§1) [1]. Si la prueba de existencia es gobernada por intereses privados, se construye una Torre de Babel digital —un laberinto de protocolos incompatibles que fragmenta la cooperación humana. En cambio, si su desarrollo sigue los principios de subsidiariedad, como hemos visto, y de custodia amorosa (§15) [1], puede surgir una «ciudad santa» donde cada certificado es testimonio de una dignidad preexistente, no la fuente de esta. Así, el peligro no reside en la herramienta en sí, sino en la intención y las estructuras de gobierno que la rodean.

El lector debe asumir este discernimiento: reconocer que *t2p* puede ser una clave para restaurar la confianza en un mundo saturado de deepfakes e identidades falsas, pero también es susceptible de reforzar las jerarquías de poder si se deja sin supervisión. Nuestra tarea —y la del libro— es ofrecer no solo la tecnología, sino el marco ético que garantice que la prueba de existencia sirva para «custodiar con amor esta magnífica humanidad» (§15) [1], y no para convertirla en una nueva forma de dominación. En este equilibrio entre promesa y peligro se encuentra el verdadero valor de *t2p*: un instrumento humilde que certifica la existencia sin intentar otorgar dignidad, dejando esta última como prerrogativa intrínseca de todo ser humano.

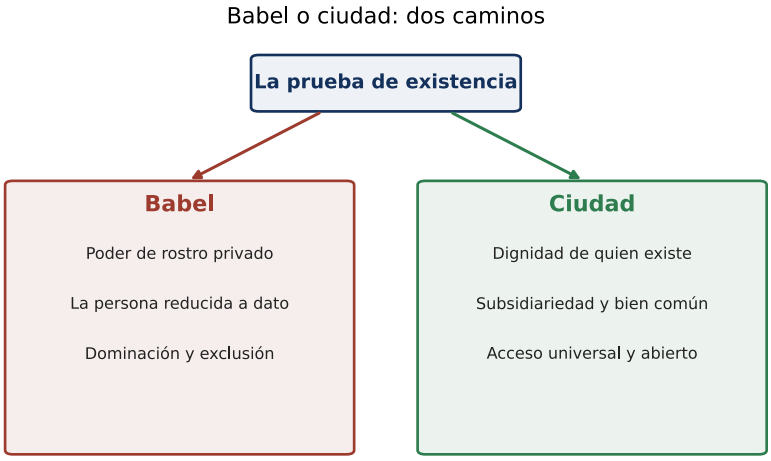


Figura 114.2 — La misma prueba de existencia, dos caminos (§1): hacia «Babel» (poder privado, reducción de la persona a dato, dominación) o hacia la «ciudad» (dignidad de quien existe, subsidiariedad, acceso universal). La diferencia no es técnica, sino de gobernanza y de fin.

Es hora de actuar

El almacén de las decisiones que la inteligencia artificial ya ha tomado sobre nuestra vida cotidiana se extiende como una alfombra infinita, y en su centro hay una llamada clara: «Elijamos... el camino de Nehemías... transformando la diversidad en un recurso» (§10) [1]. Estas palabras no son solo un ideal moral; son un plan de acción que, a través de los principios ya madurados a lo largo de *time2act*, puede guiarnos hacia una era donde la tecnología sirva realmente a la dignidad humana.

Primer principio — Prueba de existencia para los excluidos. Como hemos visto en el capítulo 47, la identidad digital se convierte en un refugio para quien no la tiene, ya sea un migrante sin documentos o una comunidad marginada que vive al margen de las redes tradicionales. La prueba de existencia (t2p) debe ser el puente que conecte a estas personas con su reconocimiento legal y social, sin que ninguna entidad pueda negarles el acceso a derechos fundamentales.

Segundo principio — Verdad como defensa contra las deepfakes. La crisis de la verdad descrita en el capítulo 10 muestra que los contenidos manipulados amenazan con anular cualquier base para un diálogo auténtico. En este contexto, la prueba de existencia actúa como una huella inmutable que certifica el origen y la integridad de las declaraciones, impidiendo que la información se convierta en una mera ilusión visual.

Tercer principio — La persona no debe reducirse a dato. La encíclica recuerda que «la persona acaba reduciéndose a un medio para obtener resultados, a un recurso para ser usado y explotado» (§51)

[1]; como hemos visto, la prueba de existencia debe quedar en manos de quien la posee, no en bases de datos centralizadas que podrían convertirla en un objeto negociable. Cada individuo debe poder validar su propio estado sin depender de un tercero que lo controla.

Cuarto principio — Gobernanza democrática y anti-rostro privado. El peligro del «poder tecnológico… con rostro inédito, predominantemente «privado»» (§5) [1] se ha expuesto en el capítulo 112, donde se detalla cómo la concentración de infraestructura puede erigir una nueva aristocracia digital. La respuesta debe ser un modelo de gobernanza abierta, con consejos representativos que reflejen la diversidad humana.

Quinto principio — Infraestructura común y subsidiariedad. La encíclica subraya que «el destino universal de los bienes incluye hoy patentes, algoritmos, plataformas digitales, infraestructuras tecnológicas, datos» (§67) [1] y que el principio de subsidiariedad pide que «lo que pueden hacer las personas… no debe ser absorbido por instancias superiores» (§68) [1]; así, la infraestructura que sostiene la prueba de existencia debe ser una red pública, cooperativa y descentralizada, accesible a todos sin barreras económicas ni políticas.

En resumen, el camino de Nehemías nos invita a transformar la diversidad en un recurso que garantice identidad para los invisibles, verdad para las sociedades fragmentadas y autonomía para cada persona. Es este el último paso del viaje iniciado con *Rerum Novarum* y continuado con *Laudato Si'*; ahora, en el corazón de la inteligencia artificial, nos encontramos ante la decisión más crucial: **custodiar la magnífica humanidad de quien existe —es, en la era de la IA, time2act**.

---

[1] León XIV — *Carta encíclica «Magnifica Humanitas»* (Vaticano, 15-25 de mayo de 2026; sobre la custodia de la persona humana en el tiempo de la inteligencia artificial). https://www.vatican.va/content/leo-xiv/es/encyclicals/documents/20260515-magnifica-humanitas.html ↩

[2] León XIII — *Rerum Novarum* (1891; origen de la doctrina social de la Iglesia). https://www.vatican.va/content/leo-xiii/es/encyclicals/documents/hf_l-xiii_enc_15051891_rerum-novarum.html ↩

[3] Francisco — *Laudato Si'* (2015; la Casa común y el paradigma tecnocrático). https://www.vatican.va/content/francesco/es/encyclicals/documents/papa-francesco_20150524_enciclica-laudato-si.html ↩

[4] Vatican News — *León XIV presenta su primera encíclica «Magnifica Humanitas»* (25 de mayo de 2026). https://www.vaticannews.va/es/papa/news/2026-05/papa-leon-xiv-primera-enciclica-magnifica-humanitas.html ↩

[5] Juan Pablo II — *Centesimus Annus* (1991; centenario de la 'Rerum Novarum'). https://www.vatican.va/content/john-paul-ii/es/encyclicals/documents/hf_jp-ii_enc_01051991_centesimus-annus.html ↩

[6] Vatican News / The Washington Post — *León XIV presenta «Magnifica Humanitas» en persona, con el cofundador de Anthropic Chris Olah; «con nuestras diferencias, podamos escucharnos los unos a los otros»* (25-05-2026). https://www.vaticannews.va/en/pope/news/2026-05/pope-leo-xiv-encyclical-magnifica-humanitas-ai.html ↩

[7] Anthropic — *Chris Olah's remarks on Pope Leo XIV's encyclical «Magnifica Humanitas»* (la Iglesia como «informed critics»; «a long collaboration between those of us who are building this and those who can see what we, from inside, cannot»; diálogo con gente «not motivated by profit») (2026). https://www.anthropic.com/news/chris-olah-pope-leo-encyclical ↩

[8] Fortune — *Who is Chris Olah? The atheist Anthropic cofounder the Pope chose to sit beside him at the Vatican* (criado evangélico en Toronto, ateo desde los 15; la industria «can't govern itself») (03-06-2026). https://fortune.com/2026/06/03/who-chris-olah-anthropic-cofounder-atheist-pope-leo-vatican-ai/ ↩

Bibliografía

1. AIE, *Oil 2025 — Executive summary*. https://www.iea.org/reports/oil-2025/executive-summary
2. IRENA (vía pv magazine), *Global average solar LCOE $0.043/kWh in 2024*. https://www.pv-magazine.com/2025/07/23/global-average-solar-lcoe-stood-at-0-043-kwh-in-2024-says-irena/
3. Copernicus C3S, *2024, first year above 1.5 °C*. https://climate.copernicus.eu/copernicus-2024-first-year-exceed-15degc-above-pre-industrial-level
4. AIE, *Energy and AI — Executive summary*. https://www.iea.org/reports/energy-and-ai/executive-summary
5. ethereum.org, *The Merge*. https://ethereum.org/roadmap/merge/
6. C2PA (2026), *funcionamiento y límites del estándar de procedencia*. https://truescreen.io/articles/c2pa-standard-history-limitations/
7. Tapscott, Don y Tapscott, Alex — *Blockchain Revolution* (Portfolio/Penguin, 2016). https://blockchain-revolution.com/
8. Mougayar, William — *Explaining the Blockchain via a Google Docs Analogy* (2016). https://medium.com/@wmougayar/explaining-the-blockchain-via-a-google-docs-analogy-56326b1bbe58
9. EU AI Act — *Article 50: Transparency Obligations* (Reglamento (UE) 2024/1689). https://artificialintelligenceact.eu/article/50/
10. Comisión Europea — *European Digital Identity Wallet (eIDAS 2.0)*. https://www.eudi-wallet.eu/
11. C2PA — *Content Credentials*. https://c2pa.org/
12. Deloitte — *Generative AI and the fraud risk for financial services* (proyección de fraude por IA). https://www2.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html
13. Europol — *Facing reality? Law enforcement and the challenge of deepfakes*. https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes
14. t2p — *Manual de usuario (Solución de Integridad de Datos)*, v1.0, 2026.
15. AIE, *Global Energy Review 2025 — Key findings*. https://www.iea.org/reports/global-energy-review-2025/key-findings
16. EIA/IEA, *precios del Brent y OPEP+ (2022-2025)*. https://www.eia.gov/todayinenergy/detail.php?id=55020
17. AIE, *Oil Market Report (sept. 2025) — esquisto EE. UU.*. https://www.iea.org/reports/oil-market-report-september-2025
18. BloombergNEF / AIE, *Global EV Outlook 2025 y precios de baterías*. https://www.iea.org/reports/global-ev-outlook-2025/electric-vehicle-batteries
19. AIE / CFR, *dominio chino en minerales y tecnologías limpias (2024-2025)*. https://www.iea.org/commentaries/with-new-export-controls-on-critical-minerals-supply-concentration-risks-become-reality
20. Sightline / análisis, *exportaciones limpias chinas al Sur Global (2024)*. https://www.sightlineclimate.com/research/a-tour-of-chinas-electrostate
21. IPCC AR6 (vía COP28 Global Stocktake), *recortes de emisiones 2030/2035*. https://www.iea.org/topics/cop28-tracking-the-energy-outcomes
22. UNFCCC / Comisión Europea, *resultados de COP28-COP30*. https://climate.ec.europa.eu/news-other-reads/news/what-did-cop30-achieve-2025-12-01_en
23. AIE, *Energy Efficiency 2024 — Executive summary*. https://www.iea.org/reports/energy-efficiency-2024/executive-summary
24. *Jevons paradox / rebound effect* (revisión). https://en.wikipedia.org/wiki/Jevons_paradox
25. Reclaim Finance, *Assessment of oil & gas companies' climate strategy (2024)*. https://reclaimfinance.org/site/en/assessment-of-oil-and-gas-companies-climate-strategy/
26. The Bureau of Investigative Journalism, *BP rowing back on renewables (2025)*. https://www.thebureauinvestigates.com/stories/2025-03-06/bp-renewables-net-zero-banks
27. IISD, *Public money: 5x more to fossil fuels than renewables*. https://www.iisd.org/articles/press-release/governments-five-times-more-public-money-fossil-fuels-than-renewables
28. Google DeepMind, *AI reduces data centre cooling energy by 40%*. https://deepmind.google/blog/deepmind-ai-reduces-google-data-centre-cooling-bill-by-40/
29. Union of Concerned Scientists, *Fossil fuel industry's decades of deceit*. https://www.ucs.org/about/news/new-ucs-report-details-fossil-fuel-industry-decades-deceit

30. Naciones Unidas, *Greenwashing*. https://www.un.org/en/climatechange/science/climate-issues/greenwashing
31. (deepfakes) Blockchain Council / Europol — véase research 00 §6. https://www.blockchain-council.org/blockchain/preventing-deepfake-fraud-with-blockchain-content-provenance-verification-workflows/
32. Beth Simone Noveck — *Reboot: AI and the Race to Save Democracy* (Yale UP, 2026), cap. 3.
33. FCC (2024). https://www.fcc.gov/document/fcc-makes-ai-generated-voice-robocalls-illegal
34. Google DeepMind / Data Center Frontier, *IA para la red*. https://www.datacenterfrontier.com/energy/article/55282719/googles-ai-powered-grid-revolution-how-data-centers-are-reshaping-the-us-power-landscape
35. IAEA / NucNet, *nuclear avanzado y SMR para la demanda de IA (2024-2025)*. https://www.iaea.org/bulletin/data-centres-artificial-intelligence-and-cryptocurrencies-eye-advanced-nuclear-to-meet-growing-power-needs
36. RWA.io / Powerledger, *RECs tokenizados y MRV en blockchain*. https://www.rwa.io/post/renewable-energy-credits-on-blockchain-a-tokenized-approach
37. Frontiers in Blockchain (2025), *estado de los mercados de carbono en blockchain*. https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2025.1603695/full
38. OpenTimestamps — *a timestamping proof standard*. https://opentimestamps.org/
39. London Blockchain — *Can blockchain save truth? (2025)*. https://londonblockchain.net/blog/blockchain-in-action/can-blockchain-save-truth-tackling-deepfakes-and-disinformation-in-2025/
40. C2PA — *Content Credentials Explainer (especificación oficial)*. https://spec.c2pa.org/specifications/specifications/2.4/explainer/Explainer.html
41. arXiv — *Provenance Verification via a Perceptual Hash Registry Anchored on Blockchain*. https://arxiv.org/html/2602.02412v1
42. Beth Simone Noveck — *Reboot* (Yale UP, 2026), cap. 3.
43. IEA, *Global Hydrogen Review 2025* / CleanTechnica. https://www.iea.org/reports/global-hydrogen-review-2025/executive-summary
44. IEA / The Extractor, *coste del H₂ verde 2022-2025*. https://cleantechnica.com/2025/07/07/hydrogens-brutal-month-billions-lost-as-mega-projects-collapse/
45. arXiv — *DeepFake-Eval-2024: A Multi-Modal In-the-Wild Benchmark of Deepfakes*. https://arxiv.org/html/2503.02857v4
46. ManageEngine Insights — *Content provenance is our best chance in the fight against deepfakes* (Hany Farid). https://insights.manageengine.com/artificial-intelligence/content-provenance-is-our-best-chance-in-the-fight-against-deepfakes/
47. WITNESS — *Prepare, Don't Panic: Synthetic Media and Deepfakes* (Sam Gregory). https://www.witness.org/portfolio_page/sam-gregory/
48. CISA / NSA / FBI — *Contextualizing Deepfake Threats to Organizations* (2023). https://www.cisa.gov/news-events/alerts/2023/09/12/nsa-fbi-and-cisa-release-cybersecurity-information-sheet-deepfake-threats
49. C2PA — *Content Credentials Explainer*. https://spec.c2pa.org/specifications/specifications/2.2/explainer/_attachments/Explainer.pdf
50. Peter Todd — *Carbon Dating the Internet Archive with OpenTimestamps*. https://petertodd.org/2017/carbon-dating-the-internet-archive-with-opentimestamps
51. ProofStamper — *File timestamp tools compared (RFC 3161 + blockchain anchoring)*. https://proofstamper.com/en/compare/file-timestamp-tools-2026/
52. Sumsub — *Global deepfake incidents surge tenfold*. https://sumsub.com/newsroom/sumsub-research-global-deepfake-incidents-surge-tenfold-from-2022-to-2023/
53. CNN Business — *Finance worker pays out $25 million after video call with deepfake 'CFO'* (caso Arup). https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk · World Economic Forum. https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/
54. Deloitte — *Generative AI is expected to magnify the risk of deepfakes and other fraud in banking* (≈40 mil M$ en 2027). https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html
55. FinCEN — *Alert on Fraud Schemes Involving Deepfake Media* (13-nov-2024). https://www.fincen.gov/system/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf

56. iProov / Biometric Update — *Biometric injection attack surge* (KYC, NIST SP 800-63-4). https://www.biometricupdate.com/202604/biometric-injection-attack-surge-spreads-to-ios-iproov-report
57. Signaturit — *eIDAS 2.0: Qualified Electronic Ledgers and Archiving*. https://www.signaturit.com/blog/eidas-2-regulation/
58. Thomson Reuters Institute — *Deepfakes on trial: evidence authentication (FRE 707, 901(c))*. https://www.thomsonreuters.com/en-us/posts/ai-in-courts/deepfakes-evidence-authentication/
59. Forbes (Thomas Brewster) — *Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find* (14-10-2021; documentos judiciales de los EAU: al menos 17 implicados, 400.000 $ rastreados hasta cuentas del Centennial Bank en EE. UU.). https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/
60. NPR — *Fake viral images of an explosion at the Pentagon were probably created by AI* (mayo 2023). https://www.npr.org/2023/05/22/1177590231/fake-viral-images-of-an-explosion-at-the-pentagon-were-probably-created-by-ai
61. NPR / Harvard Ash Center — *AI was everywhere in 2024's elections, but deepfakes were only part of the picture*. https://ash.harvard.edu/articles/the-apocalypse-that-wasnt-ai-was-everywhere-in-2024s-elections-but-deepfakes-and-misinformation-were-only-part-of-the-picture/
62. Content Authenticity Initiative — *5,000 members* (2025). https://contentauthenticity.org/blog/5000-members-building-momentum-for-a-more-trustworthy-digital-world
63. Nikon Rumors — *AFP validates a C2PA certification test using a prototype Nikon camera* (feb 2025). https://nikonrumors.com/2025/02/18/afp-validates-a-certification-test-of-its-photos-via-the-c2pa-standard-using-a-prototype-nikon-camera.aspx/
64. IPTC — *C2PA news: France Télévisions, IBC «Stamping Your Content»*. https://iptc.org/news/tag/c2pa/
65. Content Authenticity Initiative — *Leica launches world's first camera with Content Credentials*. https://contentauthenticity.org/blog/leica-launches-worlds-first-camera-with-content-credentials
66. arXiv — *Why the C2PA specifications fall short* (metadatos eliminables). https://arxiv.org/html/2604.24890v1
67. NSA/CISA — *Content Credentials: Strengthening Multimedia Integrity* (ene 2025); JPEG Trust ISO/IEC 21617-1. https://media.defense.gov/2025/Jan/29/2003634788/-1/-1/0/CSI-CONTENT-CREDENTIALS.PDF
68. Beth Simone Noveck — *Reboot* (Yale UP, 2026), cap. 3; Infobae (2025). https://www.infobae.com/peru/2025/06/06/blockchain-y-elecciones-2026-como-se-desarrollara-en-peru-el-voto-digital-obligatorio-para-militares-y-ciudadanos-en-el-extranjero/
69. Mirsky et al. — *CT-GAN: Malicious Tampering of 3D Medical Imagery* (USENIX Security 2019). https://www.usenix.org/conference/usenixsecurity19/presentation/mirsky · resumen con cifras: https://www.pindrop.com/article/threat-deepfakes-in-healthcare/
70. TruthScan / Pindrop — *AI-driven fraud in healthcare: deepfake doctors and synthetic patients* (2025). https://truthscan.com/blog/ai-driven-fraud-in-global-healthcare-2025-trends-and-countermeasures/
71. STAT News — *Cassava Sciences scientist indicted (fabricated Western Blots)* (28-jun-2024); Retraction Watch / Bik. https://www.statnews.com/2024/06/28/cassava-sciences-indictment-alzheimers-hoau-yan-wang/
72. FDA — *Cybersecurity in Medical Devices: final guidance* (Federal Register, 27-jun-2025). https://www.govinfo.gov/content/pkg/FR-2025-06-27/html/2025-11669.htm
73. HIPAA Vault — *Blockchain integration for healthcare records (audit trails)* (2025). https://www.hipaavault.com/resources/blockchain-integration-healthcare-records/
74. Bentham/RRCT (PubMed) — *Blockchain as a Prime Guardian of clinical-trial data* (2025); Triall. https://pubmed.ncbi.nlm.nih.gov/39851126/
75. HEPI — *Student Generative AI Survey 2025*. https://www.hepi.ac.uk/reports/student-generative-ai-survey-2025/
76. TEQSA — *The evolving risk to academic integrity posed by generative AI* (2024). https://www.teqsa.gov.au/sites/default/files/2024-08/evolving-risk-to-academic-integrity-posed-by-generative-artificial-intelligence.pdf
77. U.S. DOJ — *Operation Nightingale: fraudulent nursing diplomas* (2023; Fase II 2025). https://www.justice.gov/usao-sdfl/pr/fraudulent-nursing-diploma-scheme-leads-federal-convictions

78. Open edX — *Proctoring in the age of AI: deepfake impersonation* (2025). https://openedx.org/blog/proctoring-in-the-age-of-ai-tackling-modern-cheating-techniques/
79. MIT Technology Review — *Digital diplomas (Blockcerts)* (2018); MIT Registrar. https://www.technologyreview.com/2018/04/25/143311/digital-diplomas/
80. European Commission — *EBSI Verifiable Credentials*; Europass *European Digital Credentials for Learning*; W3C VC Data Model 2.0. https://europass.europa.eu/en/european-digital-credentials-learning
81. NPR — *Zelenskyy deepfake telling Ukrainians to surrender* (16-mar-2022). https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia
82. EU DisinfoLab — *Doppelganger* (campaña de desinformación rusa). https://www.disinfo.eu/doppelganger-hub/
83. FCC — *Proposed $6M fine for AI-deepfake Biden robocall* (2024); IPI (Eslovaquia). https://www.fcc.gov/document/fcc-proposes-6m-fine-nh-robocalls
84. University of Washington — *Deepfake geography: AI falsifies satellite images* (Bo Zhao, 2021). https://www.washington.edu/news/2021/04/21/a-growing-problem-of-deepfake-geography-how-ai-falsifies-satellite-images/
85. International Bar Association — *eyeWitness to Atrocities* (hash en la captura; casos en Ucrania). https://www.ibanet.org/IBA-founded-eyeWitness-to-Atrocities-marks-ten-years-of-capturing-evidence-of-human-rights-crimes
86. USC Shoah Foundation — *Starling Lab & Hala Systems file cryptographic war-crimes evidence to the ICC* (2022); Protocolo de Berkeley (OHCHR). https://sfi.usc.edu/news/2022/06/33571-starling-lab-and-hala-systems-file-cryptographic-submission-evidence-war-crimes
87. DARPA — *Semantic Forensics (SemaFor)* y *Deepfake Defense* (2024); NATO StratCom COE. https://www.darpa.mil/research/programs/semantic-forensics
88. Comisión Europea — *About the EU Emissions Trading System* (cobertura ~40 %, 175.000 M€ recaudados, −47 % vs 2005, −62 % en 2030). https://climate.ec.europa.eu/eu-action/carbon-markets/about-eu-ets_en
89. Trading Economics — *EU Carbon Permits* (EUA 80,58 €/t el 19-jun-2026; máximo histórico 105,73 € en feb-2023). https://tradingeconomics.com/commodity/carbon
90. Comisión Europea (Taxation and Customs Union) — *Carbon Border Adjustment Mechanism (CBAM)* (fase definitiva desde el 1-ene-2026). https://taxation-customs.ec.europa.eu/carbon-border-adjustment-mechanism_en
91. S&P Global — *Brussels confirms first CBAM certificate price for Q1 2026 at €75.36/tCO2e* (7-abr-2026). https://www.spglobal.com/energy/en/news-research/latest-news/energy-transition/040726-brussels-confirms-first-cbam-certificate-price-for-q1-2026-at-eur7536mtco2e
92. International Carbon Action Partnership (ICAP) — *EU Emissions Trading System (EU ETS)* (MSR, factor CBAM, asignación gratuita). https://icapcarbonaction.com/en/ets/eu-emissions-trading-system-eu-ets
93. Comisión Europea — *ETS2: buildings, road transport and additional sectors* (inicio aplazado a 2028; acuerdo nov-2025). https://climate.ec.europa.eu/eu-action/carbon-markets/ets2-buildings-road-transport-and-additional-sectors_en
94. EASA — *ICAO CORSIA* (emisiones internacionales 2024 ≈ 597 $MtCO_2$; ≈ 58 $MtCO_2$ a compensar). https://www.easa.europa.eu/en/domains/environment/icao-carbon-offsetting-and-reduction-scheme-international-aviation-corsia
95. Comisión Europea — *Monitoring, reporting and verification of EU ETS emissions* (MRR y AVR; informe verificado antes del 31 de marzo). https://climate.ec.europa.eu/eu-action/carbon-markets/eu-emissions-trading-system-eu-ets/monitoring-reporting-and-verification_en
96. Europol — *Carbon Credit fraud causes more than 5 billion euros damage for European Taxpayer* (hasta el 90 % del volumen fraudulento en algunos países). https://www.europol.europa.eu/media-press/newsroom/news/carbon-credit-fraud-causes-more-5-billion-euros-damage-for-european-taxpayer
97. Marius-Christian Frunza — *Fraud and Carbon Markets: The Carbon Connection* (Routledge, 2013) y *An Assessment of Carousel VAT Fraud in the European Carbon Market* (Review of Law & Economics, 2014). https://www.routledge.com/Fraud-and-Carbon-Markets-The-Carbon-Connection/Frunza/p/book/9781138928091
98. Comisión Europea — *Announcement: transitional measure for the EU ETS registry system* (19-ene-2011) y OCCRP — *Germany: Six Executives Stand Trial for Emissions Fraud* (~850 M€; seis condenados). https://climate.ec.europa.eu/news-your-voice/news/announcement-transitional-

measure-eu-ets-registry-system-2011-01-19_en · https://www.occrp.org/en/news/germany-six-executives-stand-trial-for-emissions-fraud
99. Banco Mundial — *Why data infrastructure is key for a transparent carbon market* y plataforma *Climate Action Data Trust*. https://blogs.worldbank.org/en/climatechange/why-data-infrastructure-key-transparent-carbon-market · https://climateactiondata.org/
100. The Guardian / Die Zeit / SourceMaterial — Patrick Greenfield, *Revealed: more than 90% of rainforest carbon offsets by biggest certifier are worthless* (18-ene-2023). https://www.theguardian.com/environment/2023/jan/18/revealed-forest-carbon-offsets-biggest-provider-worthless-verra-aoe
101. Verra — *Verra Response to Guardian Article on Rainforest Offset Credits* (réplica). https://verra.org/verra-response-guardian-rainforest-carbon-offsets/
102. Mongabay — *Head of Verra, top carbon credit certifier, to leave in June* (dimisión de David Antonioli, 22-mayo-2023). https://news.mongabay.com/2023/05/head-of-verra-top-carbon-credit-certifier-to-leave-in-june/
103. Verra — *Verra Acts on Kariba Project: Cancels Excess Credits and Advances Independent Review* (15.220.520 créditos en exceso de 26.822.953; ~57 %). https://verra.org/verra-acts-on-kariba-project-cancels-excess-credits-advances-independent-review/
104. South Pole — *Statement on the Kariba REDD+ project* (27-oct-2023). https://www.southpole.com/news/statement-27october
105. Alejandro Guizar-Coutiño et al. — *A global evaluation of the effectiveness of voluntary REDD+ projects* (Conservation Biology, 2022; deforestación −47 %). https://pmc.ncbi.nlm.nih.gov/articles/PMC10086997/
106. West et al. — *Action needed to make carbon offsets from forest conservation work for climate change mitigation* (Science, 2023; 26 emplazamientos en 6 países; resultado disputado, réplica arXiv 2312.06793). https://www.science.org/doi/10.1126/science.ade3535
107. Ecosystem Marketplace / Forest Trends — *State of the Voluntary Carbon Market 2024* (mercado ~2.000 M$ en 2021 → 723 M$ en 2023; volumen −56 %; precio medio 6,53 $/t). https://www.ecosystemmarketplace.com/articles/report-the-voluntary-carbon-market-contracted-in-2023-driven-by-drop-off-in-transactions-for-redd-and-renewable-energy/
108. ICVCM — *Core Carbon Principles* y *First high-integrity CCP-labelled carbon credits* (junio 2024; ~27 M de créditos). https://icvcm.org/core-carbon-principles/ · https://icvcm.org/integrity-council-announces-first-high-integrity-ccp-labelled-carbon-credits-as-assessments-continue/
109. VCMI — *Claims Code of Practice* (28-junio-2023). https://vcmintegrity.org/launch-claims-code/
110. CarbonPlan — Danny Cullenward y Grayson Badgley, *Zombies on the blockchain* (7-abr-2022; ~28 % de créditos zombi). https://carbonplan.org/research/toucan-crypto-offsets
111. Verra — *Verra Addresses Crypto Instruments and Tokens* (prohibición de tokenizar créditos retirados, 25-mayo-2022). https://verra.org/verra-addresses-crypto-instruments-and-tokens/
112. S&P Global Commodity Insights — *COP29: rules for UN-led carbon market under Article 6.4 approved in Baku* (11-nov-2024). https://www.spglobal.com/commodity-insights/en/news-research/latest-news/energy-transition/111124-cop29-rules-for-un-led-carbon-market-under-article-64-approved-in-baku
113. CIFOR-ICRAF / Open Forest Protocol — *Blockchain platform offers reforestation efforts access to carbon finance* (MRV digital abierto). https://forestsnews.cifor.org/76905/blockchain-platform-offers-reforestation-efforts-access-to-carbon-finance
114. Comisión Europea — *Energy Efficiency Directive* (Directiva 2023/1791, art. 8; nuevos ahorros hasta el 1,9 % anual en 2028-2030; «more than doubles» hacia 2028). https://energy.ec.europa.eu/topics/energy-efficiency/energy-efficiency-targets-directive-and-rules/energy-efficiency-directive_en
115. BOE — *Real Decreto 36/2023, de 24 de enero* (Sistema CAE; 1 CAE = 1 kWh de energía final acreditado; sujetos obligados/delegados, verificador, coordinador). https://www.boe.es/buscar/doc.php?id=BOE-A-2023-2027
116. BOE — *Orden TED/845/2023, de 18 de julio* (catálogo de medidas estandarizadas de eficiencia energética). https://www.boe.es/buscar/doc.php?id=BOE-A-2023-16940
117. Funcas — *Sistema de Certificados de Ahorro Energético (CAE): el motor que ya impulsa la transformación energética en España* (resultados 2024: ~1.200 actuaciones, ~2 TWh, ~500.000 t CO_2, ~230 M€; industria 68 %). https://www.funcas.es/articulos/sistema-de-certificados-de-ahorro-energetico-cae-el-motor-que-ya-impulsa-la-transformacion-energetica-en-espana/
118. MITECO — *Memoria de la Orden de Obligaciones del Sistema CAE 2025* (objetivo acumulado de ahorro 2021-2030: 53.593 ktep). https://www.miteco.gob.es/content/dam/miteco/es/energia/files-

1/es-ES/Participacion/Documents/aeip-fnee-2025/Memoria%20OM_Obligaciones%202025_TA.pdf
119. Légifrance — *Décret n° 2025-1048 du 30 octobre 2025* (CEE, 6.º periodo 2026-2030; 1.050 TWh cumac/año). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000052486193
120. Légifrance — *Loi n° 2025-594 du 30 juin 2025* (sanciones hasta el 10-12 %; fotografías *horodatées et géolocalisées* o vídeo a distancia, conservadas 6 años). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000051824277
121. DGCCRF (economie.gouv.fr) — *Rénovation énergétique : focus sur l'isolation à 1 euro* (469 establecimientos controlados; 56 % de incumplimiento). https://www.economie.gouv.fr/dgccrf/laction-de-la-dgccrf/les-enquetes/renovation-energetique-focus-sur-lisolation-1-euro
122. Hellio / Gobierno francés — *Fraude aux CEE* (480 M€ de fraude bloqueado en 2024, 236 M€ en CEE; tasa de control 10 %→15 %). https://www.hellio.com/actualites/reglementation/fraude-cee
123. ANSA / PordenoneToday — *Contributi per 10 milioni su certificati bianchi inesistenti* (292 proyectos ficticios; 50.322 TEE; daño ~10,4 M€). https://www.ansa.it/sito/notizie/cronaca/2025/06/23/contributi-per-10-milioni-su-certificati-bianchi-inesistenti_dd57abfb-77ba-483a-8f42-c240874fc308.html
124. EnergiaMercato / Consiglio di Stato — *GSE y la anulación de títulos de eficiencia energética* (doctrina de la «formación progresiva»; caso 4ESCO). https://www.energiamercato.it/notizie/project-finance/gse-conferma-la-legittimita-dellannullamento-di-titoli-di-efficienza-energetica-a-4esco
125. Louis-Gaëtan Giraudet, Matthieu Glachant y Jean-Philippe Nicolaï — *Selling and Saving Energy: Energy Efficiency Obligations in Liberalized Energy Markets* (The Energy Journal, 2020). https://ideas.repec.org/f/pgi337.html
126. UNEF — *El autoconsumo fotovoltaico en España alcanza los 9,3 GW instalados* (informe sobre 2025: +1.139 MW en el año, −3,7 % vs 2024; 36.330 hogares nuevos +229 MW; comercial +176 MW; industrial +679 MW; quinta fuente de generación por potencia instalada, por delante de la nuclear; objetivo PNIEC 19 GW); UNEF — *El autoconsumo sigue avanzando, superando ya el umbral de los 8 GW* (2024: +1.182 MW, acumulado 8.137 MW). https://www.unef.es/es/comunicacion/comunicacion-post/el-autoconsumo-fotovoltaico-en-espana-alcanza-los-9-3-gw-instalados · https://www.unef.es/es/comunicacion/comunicacion-post/el-autoconsumo-sigue-avanzando-superando-ya-el-umbral-de-los-8gw-instalados · https://www.eseficiencia.es/2026/02/02/autoconsumo-fotovoltaico-alcanza-9-3-gw-potencia-instalada-espana-segun-datos-unef
127. BOE — *Real Decreto 244/2019, de 5 de abril* (condiciones administrativas, técnicas y económicas del autoconsumo; compensación simplificada de excedentes ≤100 kW, voluntaria, en la factura mensual —facturación neta; autoconsumo individual y colectivo; registro administrativo); MITECO — *Preguntas frecuentes sobre autoconsumo*; UNEF — *Real Decreto 244/2019*; Puentes de Muras — *RD 244/2019: novedades* (ampliación del radio del autoconsumo colectivo hasta 5 km, plantas hasta 5 MW). https://www.boe.es/buscar/doc.php?id=BOE-A-2019-5089 · https://www.miteco.gob.es/en/energia/energia-electrica/electricidad/autoconsumo-electrico/preguntas-frecuentes-autoconsumo.html · https://autoconsumo.unef.es/real-decreto-244-2019/ · https://puentesdemuras.com/es/rd-244-2019-normativa-fotovoltaica-espana/
128. t2p — manual de producto (certificar cualquier archivo por lotes —solo la huella viaja; captura de pantalla y de página web con imagen completa + código fuente; escáner de documentos hasta 50 páginas; foto con GPS forense; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; los CAE, en el capítulo 23; el acta de la comunidad, en el capítulo 37; la factura, en el capítulo 34.
129. Parlamento Europeo (EPRS) — Enrico Pastori y Raffaele Vergnani, *Odometer manipulation in motor vehicles in the EU* (2018; daño de 5.600-9.600 M€/año; 30-50 % en ventas transfronterizas). https://www.europarl.europa.eu/RegData/etudes/STUD/2018/615637/EPRS_STU(2018615637_EN.pdf
130. ETSC (European Transport Safety Council) — *EU should act against mileage tampering on second-hand cars* (hasta el 50 % de los coches transfronterizos). https://etsc.eu/eu-should-act-against-mileage-tampering-on-second-hand-cars/
131. carVertical — *The cost of odometer fraud in Europe* (2024; ~5.300 M€/año; sobreprecio medio del 26,3 %). https://www.carvertical.com/en/blog/cost-of-odometer-fraud-in-europe
132. Car-Pass (Bélgica) — *Annual report 2022* (1.344 casos en 2022, <0,2 %; importaciones 2,4 %→0,87 %). https://www.car-pass.be/en/blog/car-pass-annual-report-2022

133. MITECO — *Catálogo de fichas CAE: sector transporte* (fichas TRA010 a TRA050). https://www.miteco.gob.es/en/energia/eficiencia/cae/catalogo-de-fichas/catalogo-vigente-de-fichas/transporte.html
134. ICCT — *Real-world use cases for zero-emission trucks: heavy tractor-trailers for goods transport in the EU* (agosto 2025; 65 % menos energía; autonomía real +11-19 %). https://theicct.org/publication/rw-use-cases-for-zet-heavy-tractor-trailers-for-goods-transport-in-the-eu-aug25/
135. Upstream Security — *2026 Global Automotive & Smart Mobility Cybersecurity Report* (494 ciberataques en 2025; 92 % remotos; 67 % a telemática/nube). https://upstream.auto/press-releases/upstream-security-research-ransomware-attacks-on-automotive-and-smart-mobility-more-than-doubled-in-2025/
136. Eurojust — *Suspects arrested in Romania, Belgium and Austria for defrauding EUR 420,000 using cloned fuel cards* (2022). https://www.eurojust.europa.eu/news/suspects-arrested-romania-belgium-and-austria-defrauding-eur-420000-using-cloned-fuel-cards
137. MOBI (Mobility Open Blockchain Initiative) — *Vehicle Identity (VID) standard* (2019) y *Global Battery Passport MVP* (2024). https://dlt.mobi/mobi-announces-the-first-vehicle-identity-vid-standard-on-blockchain-in-collaboration-with-groupe-renault-ford-and-bmw-among-others/
138. Reglamento (UE) 2023/1542 — *Pasaporte de Batería digital* (obligatorio desde el 18-feb-2027 para baterías de VE e industriales de más de 2 kWh; acceso por QR). https://www.circularise.com/blogs/eu-battery-passport-regulation-requirements
139. Smart Freight Centre — *GLEC Framework v3.0 / ISO 14083:2023* (contabilidad de emisiones del transporte de mercancías). https://www.smartfreightcentre.org/en/about-sfc/news/a-solid-foundation-to-further-accelerate-freight-decarbonization-smart-freight-centre-releases-updated-glec-framework-version-30/
140. Reglamento (UE) 910/2014 (eIDAS), artículos 41-42 — presunción legal de exactitud del sello de tiempo cualificado. https://eur-lex.europa.eu/eli/reg/2014/910/oj
141. Susan Shaheen y Elliot Martin (UC Berkeley, Transportation Sustainability Research Center) — *Impacts of car2go: One-Way Carsharing in North America* (2016; cada vehículo compartido retira 7-11 coches privados; VMT y GEI a la baja). https://phys.org/news/2016-07-car-mobility-decreases-greenhouse-gas.html
142. *Does free-floating carsharing reduce private vehicle ownership? The case of SHARE NOW in European cities* (Transportation Research Part A, 2020; media de 3,3 coches sustituidos; rango 2,1-5,3). https://pmc.ncbi.nlm.nih.gov/articles/PMC7544607/
143. BlaBlaCar — *Sustainability Report 2024* (2,5 Mt CO_2 evitadas en 2024; 92 millones de pasajeros). https://newsroom.blablacar.com/news/sustainability-report-2024
144. NACTO — *A micromobility record: 157 million trips on bike and scooter share in 2023*. https://nacto.org/latest/a-micromobility-record-157-million-trips-on-bike-and-scooter-share-in-2023/
145. Insurance Journal (fiscalía EDNY) — *Two charged in $40M ride-hail surge-pricing GPS spoofing scheme* (caso «Fake GPS», agosto 2024). https://www.insurancejournal.com/news/east/2024/08/30/790683.htm
146. Hai Yang y Xiaolei Wang — *Managing network mobility with tradable credits* (Transportation Research Part B, 45(3), 2011, pp. 580-594). https://ideas.repec.org/a/eee/transb/v45y2011i3p580-594.html
147. Oded Cats et al. — *Design and classification of tradable mobility credit schemes* (Transport Policy, 136, 2023) y *Tradable mobility credits for long-distance travel in Europe* (Transportation Research Part A, 186, 2024). https://ideas.repec.org/a/eee/trapol/v136y2023icp59-69.html
148. Aljamal et al. — *Tradable credit scheme for mobility management: state of the art* (Transportation Research Interdisciplinary Perspectives, 2025; ninguna implementación a escala real hasta ahora). https://www.sciencedirect.com/science/article/pii/S2590198225002908
149. Next Mobility / ONSS — *Mobility budget in Belgium: ONSS figures 2024* (18.386 trabajadores con presupuesto de movilidad; 17.030 sin coche de empresa). https://www.nextmobility.be/en/post/mobility-budget-belgium-onss-figures-2024/
150. Bruxelles Environnement — *Prime Bruxell'Air* (ayuda de 505-1.010 €/año por dar de baja la matrícula, vigente en 2024). https://environnement.brussels/citoyen/services-et-demandes/primes-et-aides-financieres/la-prime-mobilite-bruxellair-pour-se-deplacer-autrement-dans-la-capitale
151. SCS Global Services / Turo — *Turo becomes first global carbon-neutral certified car-sharing marketplace* (2023). https://www.prnewswire.com/news-releases/turo-becomes-first-global-

carbon-neutral-certified-car-sharing-marketplace-301799877.html
152. MOBI (Mobility Open Blockchain Initiative) — *Vehicle Identity (VID) standard on blockchain*. https://www.traffictechnologytoday.com/news/smart-cities/mobi-creates-the-first-vehicle-identity-standard-on-blockchain.html
153. Newtral — *Cómo cambió Renfe las indemnizaciones por retraso del AVE* (1-7-2024: eliminadas las indemnizaciones de 15 y 30 minutos para AVE, Avlo, Alvia, Euromed e Intercity; nuevo régimen 50 % a partir de 60 min y 100 % a partir de 90; devolución del 200 % en puntos o 150 % en vales; justificación: liberalización y ajuste a la legislación); Renfe — *Compromiso de puntualidad* y nota de prensa de la actualización; Xataka — *el debate sobre indemnizar desde los 15 minutos* (situación normativa abierta). https://www.newtral.es/renfe-indemnizacion-retraso-ave-gobiernos-pp-psoe/20250801/ · https://www.renfe.com/es/es/ayuda/compromiso-puntualidad · https://www.renfe.com/es/es/grupo-renfe/comunicacion/renfe-al-dia/sala-de-prensa/renfe-actualiza-compromiso-voluntario-puntualidad-ave-avlo-alvia-euromed-intercity · https://www.xataka.com/movilidad/renfe-esta-obligada-a-indemnizar-retrasos-15-minutos-a-partir-1-enero-gobierno-quiere-impedirlo
154. EUR-Lex — *Reglamento (CE) 261/2004* (compensaciones de 250/400/600 € por cancelación y, por la doctrina Sturgeon del TJUE, gran retraso ≥3 horas a la llegada; excepción de circunstancias extraordinarias; derecho de atención; jurisprudencia del TJUE: la «hora de llegada» es la apertura de puertas). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32004R0261
155. t2p — manual de producto (foto con GPS forense —fijado genuino ~50 m / ≤30 s, la ubicación simulada bloquea la certificación; certificación en segundo plano que se reanuda al recuperar cobertura —modo avión; captura de pantalla certificada; escáner de documentos; proyectos para agrupar el expediente de un viaje; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; la reclamación de servicios, en el capítulo 33; el reloj del proveedor, en el capítulo 59.
156. Coalition Against Insurance Fraud — *The Impact of Insurance Fraud on the U.S. Economy* (2022; 308.600 M$/año, ~933 $ por persona). https://insurancefraud.org/wp-content/uploads/The-Impact-of-Insurance-Fraud-on-the-U.S.-Economy-Report-2022-8.26.2022.pdf
157. Insurance Europe — *Annual Report 2023-2024* (capítulo Fraud) y *The impact of insurance fraud* (~10 % del gasto en siniestros; estimación de 2013, ~13.000 M€ referidos a 2017). https://www.insuranceeurope.eu/downloads/ar-2024-fraud/Fraud.pdf
158. Association of British Insurers (ABI) — *Fraudulent insurance claims continue to top £1 billion* (2024: 1.160 M£; 98.400 reclamaciones). https://www.abi.org.uk/news/news-articles/2025/11/fraudulent-insurance-claims-continue-to-top-1-billion/
159. ICEA — *El sector detectó 285.407 casos sospechosos de fraude, de los que evitó un 63,7 %* (España, 2024). https://segurosnews.com/news/el-sector-detecto-285-407-casos-sospechosos-de-fraude-de-los-que-evito-un-637
160. Verisk (con el National Insurance Crime Bureau) — *AI editing tools are fueling a new era of insurance fraud* (marzo 2026; 36 % de consumidores, Gen Z 55 %; 99 % de las aseguradoras). https://www.verisk.com/company/newsroom/ai-editing-tools-are-fueling-a-new-era-of-insurance-fraud-according-to-new-research-from-verisk/
161. The Guardian (vía PetaPixel) — *Fraudsters are editing photos of damaged vehicles to claim insurance* (caso LV=; +300 % de fotos manipuladas, Allianz/Zurich). https://petapixel.com/2024/05/07/fraudsters-are-editing-photos-of-damaged-vehicles-to-claim-insurance/
162. Allianz UK — *Allianz UK detects frauds totalling £93m in first half of 2025* (15.800 casos). https://www.allianz.co.uk/news-and-insight/news/allianz-uk-detects-frauds-totalling-93m-in-first-half-of-2025.html
163. Zurich Insurance — *AI poses challenges, offers tantalizing solutions to insurers fighting fraud* (metadatos + análisis de nivel de error). https://www.zurich.com/insights/business/ai-poses-challenges-offers-tantalizing-solutions-to-insurers-fighting-fraud
164. Swiss Re Institute — *SONAR 2025: How deepfakes, disinformation and AI amplify insurance fraud* (+700 %; recomienda prueba de vida y anclaje en blockchain). https://www.swissre.com/institute/research/sonar/sonar2025/how-deepfakes-disinformation-ai-amplify-insurance-fraud.html
165. Línea Directa — *VII Barómetro del Fraude al Seguro* (8,8 % de los partes de auto en España). https://www.lineadirectaaseguradora.com/-/vii-barometro-de-fraude-al-seguro

166. OCDE / EUIPO — *Mapping Global Trade in Fakes 2025* (falsificaciones: 467.000 M$ en 2021, 2,3 % de las importaciones mundiales; UE 4,7 %). https://www.oecd.org/en/publications/mapping-global-trade-in-fakes-2025_94d3b29f-en.html
167. Organización Mundial de la Salud — *Substandard and falsified medical products* (≥1 de cada 10 en los países de renta baja/media; ~30.500 M$/año). https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products
168. OMS — *Medical Product Alert N°6/2022* (Gambia; jarabes de Maiden Pharmaceuticals contaminados con dietilenglicol). https://www.who.int/news/item/05-10-2022-medical-product-alert-n-6-2022-substandard-(contaminated-paediatric-medicines
169. OMS — *Medical Product Alert N°5/2025* (India; jarabe «Coldrif» de Sresan Pharmaceuticals). https://www.who.int/news/item/13-10-2025-medical-product-alert-n-5-2025--substandard-(contaminated-oral-liquid-medicines
170. EUR-Lex — *Reglamento (UE) 2023/1115* (EUDR; coordenadas de geolocalización de parcelas; 7 materias primas; fecha de corte 31-dic-2020). https://eur-lex.europa.eu/eli/reg/2023/1115/oj/eng
171. Comisión Europea (Access2Markets) — *Delay until December 2026 — implementation of the EUDR* (segunda prórroga, Reg. UE 2025/2650; aplicación 30-dic-2026 / 30-jun-2027). https://trade.ec.europa.eu/access-to-markets/en/news/delay-until-december-2026-and-other-developments-implementation-eudr-regulation
172. EMA — *Falsified medicines: overview* (Directiva 2011/62/UE; identificador único 2D obligatorio desde el 9-feb-2019). https://www.ema.europa.eu/en/human-regulatory-overview/public-health-threats/falsified-medicines-overview
173. Aura Blockchain Consortium — *About* (fundado en 2021 por LVMH, Prada y Cartier; >50 M de productos registrados). https://auraconsortium.com/about
174. WWD — *Aura Blockchain crosses 50 million products* (LVMH, Prada, OTB; septiembre 2024). https://wwd.com/business-news/technology/aura-blockchain-crosses-50-million-products-lvmh-prada-otb-1236606994/
175. Federal Trade Commission — *FTC Announces Final Rule Banning Fake Reviews and Testimonials* (14 de agosto de 2024; en vigor el 21 de octubre de 2024; hasta 51.744 $ por infracción; prohíbe la compraventa de reseñas, las reseñas de insiders sin revelación, las webs de reseñas controladas, la supresión selectiva y los indicadores falsos de influencia social); Federal Register — *Trade Regulation Rule on the Use of Consumer Reviews and Testimonials*. https://www.ftc.gov/news-events/news/press-releases/2024/08/federal-trade-commission-announces-final-rule-banning-fake-reviews-testimonials · https://www.federalregister.gov/documents/2024/08/22/2024-18519/trade-regulation-rule-on-the-use-of-consumer-reviews-and-testimonials
176. Infobae — *Amazon demanda a miles de grupos de Facebook por publicar reseñas falsas* (19 de julio de 2022; más de 10.000 grupos; EE. UU., Reino Unido, Alemania, Francia, Italia, España y Japón); Marketing4eCommerce — *Amazon denuncia a los administradores de más de 10.000 grupos de Facebook* («Amazon Product Review», más de 43.000 miembros; 10 $ por reseña; más de 10.000 grupos reportados a Meta desde 2020, la mitad eliminados); La Nación — *Amazon demanda a los administradores de 10.000 grupos de Facebook*. https://www.infobae.com/america/agencias/2022/07/19/amazon-demanda-a-miles-de-grupos-de-facebook-por-publicar-resenas-falsas/ · https://marketing4ecommerce.net/amazon-reviews-falsas/ · https://www.lanacion.com.ar/tecnologia/amazon-demanda-a-los-administradores-de-10000-grupos-de-facebook-por-promover-resenas-falsas-nid19072022/
177. OCU — *Black Friday: descuentos que no son reales* (solo 1 de cada 3 productos se abarata; subidas medias del 13 % en las semanas previas en categorías como relojes inteligentes, cámaras y auriculares; el 43 % de los productos dispara el precio; ahorro anunciado del 23 % vs precios reales un 3 % más caros; en el 99 % de los casos el «precio anterior» no es el menor de los últimos 30 días; monitorización desde septiembre); Público — *La trampa del Black Friday: precios inflados, rebajas ficticias*. https://www.ocu.org/consumo-familia/compras-online/noticias/bf-precios-rebajados · https://www.publico.es/sociedad/trampa-black-friday-precios-inflados-rebajas-ficticias-fiebre-compras-detiene.html
178. Centro Europeo del Consumidor en España (Ministerio de Consumo) — *España amplía la garantía legal mínima de dos a tres años* (desde el 1 de enero de 2022; transposición de las Directivas (UE) 2019/770 y 2019/771; presunción de origen del defecto ampliada de 6 meses a 2 años —1 año para segunda mano—; recambios durante 10 años; prescripción de 3 a 5 años); OCU — *Garantía de los productos: se amplía el plazo*. https://portal-cec.consumo.gob.es/en/comunicacion/noticias/2022/espana-amplia-la-garantia-legal-minima-de-

dos-tres-anos · https://www.ocu.org/consumo-familia/derechos-consumidor/noticias/novedades-garantia

179. t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; acreditación sin identificación —la prueba de compra viaja, la identidad nunca; contenido en el dispositivo y revelación voluntaria). Véanse los capítulos 13 y 15; el origen del producto, en el capítulo 29.
180. Digital Perito — *Estafas en Wallapop y Vinted: cómo denunciar con pruebas* (>19 millones de usuarios activos en Wallapop en España; mercado de segunda mano >13.000 M€ anuales; las estafas de plataformas de segunda mano como grueso de los >412.000 fraudes informáticos de 2024; +60 % de denuncias en 2025); Público — *Así operan los estafadores en plataformas de segunda mano* (tipologías: pago fuera de plataforma, triangulación/«cambiazo» aprovechando la protección al comprador, phishing, etiquetas fraudulentas, suplantación); OKDiario / Genbeta — alertas de la Guardia Civil y trucos de detección. https://digitalperito.es/blog/estafas-wallapop-vinted-como-denunciar-pruebas-2026/ · https://www.publico.es/sociedad/asi-operan-estafadores-plataformas-segunda-mano-vinted-wallapop.html · https://okdiario.com/curiosidades/fraude-que-arrasa-plataformas-segunda-mano-guardia-civil-lanza-advertencia-sobre-vinted-wallapop-15912396 · https://www.genbeta.com/seguridad/estas-estafas-wallapop-comunes-varios-trucos-para-pillarlas-rapidamente
181. Marco civil de la compraventa entre particulares (vicio oculto; ausencia de garantía comercial de consumo). Véase el capítulo 30 para la garantía B2C y el capítulo 36 para la estafa del anuncio falso.
182. t2p — manual de producto (vídeo con fecha/hora sobreimpresa; foto con GPS forense —fijado genuino ~50 m / ≤30 s, la ubicación simulada bloquea la certificación; captura de pantalla certificada; certificar cualquier archivo; proyectos para agrupar el expediente de una venta; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; el pago engañado, en el capítulo 69.
183. Dirección General de Consumo (DSCA) — *Prácticas irregulares de compañías españolas de alquiler de coches* (indemnizaciones desproporcionadas de 300 a 1.000 € por rasguños o desperfectos pequeños, cargadas a la tarjeta del depósito con cuantía fijada unilateralmente); CEC-España (Centro Europeo del Consumidor) — *Alquiler de vehículos: derechos y recomendaciones* (cargos posteriores por limpieza o daños menores; revisiones sin la presencia del consumidor; recomendaciones: devolver con la oficina abierta, revisar con el personal, pedir justificante y «hacer fotografías del interior y el exterior como prueba»); AEA — *Líder europeo del rent-a-car condenado a devolver el importe de unos daños cobrados indebidamente*. https://www.dsca.gob.es/sites/default/files/consumo_masinfo/PRACTICAS_IRREGULARES_ALQUILER_COCHES · https://portal-cec.consumo.gob.es/sites/default/files/documentos/Folleto_Alquiler_Coches.pdf · https://portal-cec.consumo.gob.es/en/comunicacion/noticias/2021/cec-espana-recuerda-los-derechos-de-las-personas-consumidoras-cuando · https://aeaclub.org/rent-a-car-reclamacion-coche-alquiler-cobro-indebido/
184. t2p — manual de producto (vídeo con fecha/hora sobreimpresa; foto con GPS forense —fijado genuino ~50 m / ≤30 s, la ubicación simulada bloquea la certificación; escáner de documentos; proyectos para agrupar el expediente de un alquiler; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; el inventario del piso, en el capítulo 36; el estado de la cosa vendida, en el capítulo 31; el cargo a la tarjeta, en el capítulo 69.
185. BOE — *Ley 10/2025, de 26 de diciembre, por la que se regulan los servicios de atención a la clientela* (BOE 27-12-2025; 12 meses de adaptación; 95 % de llamadas en <3 minutos; código identificativo de seguimiento; respuesta en 15 días —5 para cargos no autorizados; aviso 15 días antes de renovaciones automáticas; baja sencilla con DNI y número de contrato; prohibición de atención exclusivamente automatizada); La Moncloa — *Ley de Servicios de Atención a la Clientela: objetivos y medidas*; Sepín — *Novedades de la Ley 10/2025*. https://www.boe.es/buscar/act.php?id=BOE-A-2025-26698 · https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/derechos-sociales-consumo-agenda-2030/paginas/2025/ley-servicios-atencion-al-cliente.aspx · https://blog.sepin.es/blog/2026/01/14/novedades-ley-10-2025-servicios-atencion-clientela/
186. FACUA — *Multa de 20.000 euros a Vodafone: cobró a una socia de FACUA servicios de terceros que había desconectado* (vulneración del derecho de desconexión hasta tres veces; obstrucción a la inspección; 20.100 € con reducción); FACUA — *Multa a Movistar por acosar a través de una gestora de cobros a una socia por una deuda falsa* (1.741 € por líneas nunca contratadas); FACUA

— *El Supremo confirma la multa de 765.000 € a Telefónica por limitar el derecho a recibir facturas en papel*; Xataka Móvil — *FACUA denuncia a Telefónica por la penalización por baja anticipada*. https://facua.org/noticias/multa-de-20-000-euros-a-vodafone-cobro-a-una-socia-de-facua-servicios-de-terceros-que-habia-desconectado/ · https://www.facua.org/es/noticia.php?Id=9279 · https://facua.org/noticias/el-supremo-confirma-la-multa-de-765000-de-la-junta-de-andalucia-a-telefonica-por-limitar-el-derecho-a-recibir-facturas-en-papel/ · https://www.xatakamovil.com/conectividad/facua-denuncia-a-telefonica-por-la-penalizacion-por-baja-anticipada-en-movistar-fusion

187. t2p — manual de producto (grabación de audio en segundo plano; captura y grabación de pantalla certificadas con verificación de la app en primer plano; captura de página web con imagen completa + código fuente; escáner de documentos hasta 50 páginas; proyectos para agrupar capturas por caso; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión; solo huellas en la cadena). Véanse los capítulos 13 y 15; la licitud de grabar conversaciones propias, en el capítulo 75; la voz clonada, en el capítulo 68.
188. AEAT — *Sistemas Informáticos de Facturación (SIF) y VERI*FACTU *(RD 1007/2023: registro de facturación normalizado con huella encadenada —cada registro contiene el hash del anterior—, firma electrónica y QR de verificación; modalidades «Verifactu» de envío inmediato voluntario y conservación inalterable; FAQ oficial); Guía Fiscal* — Verifactu 2026-2027 *y Davisa* — Guía Verifactu 2026* (calendario aplazado por el RD-ley 15/2025, de 2 de diciembre: 1-1-2027 sociedades, 1-7-2027 resto; sanciones de hasta 50.000 €/ejercicio para usuarios y 150.000 € para fabricantes). https://sede.agenciatributaria.gob.es/Sede/iva/sistemas-informaticos-facturacion-verifactu.html · https://sede.agenciatributaria.gob.es/Sede/iva/sistemas-informaticos-facturacion-verifactu/preguntas-frecuentes/sistemas-verifactu.html · https://guiafiscal.es/autonomos/verifactu-2026-guia/ · https://www.davisa.es/guia-verifactu-2026/
189. BOE — *Ley 3/2004, de 29 de diciembre, de medidas de lucha contra la morosidad en las operaciones comerciales* (60 días naturales de máximo pactado entre empresas, 30 por defecto desde la recepción; interés de demora automático; 40 € de costes de cobro por factura; AAPP 30 días —Ley 15/2010); Togas — *Los intereses de demora en el primer semestre de 2025: 11,15 %* (Resolución del Tesoro de 30-12-2024); PMcM / Revista Limpiezas — *Informe sobre morosidad 2025* (el 85 % de las grandes compañías incumple los plazos; AAPP a 70 días de media, +3 en 2025; sector privado a 67). https://www.boe.es/buscar/act.php?id=BOE-A-2004-21830 · https://togas.biz/articulos/articulo-profesionales--los-intereses-de-demora-en-las-operaciones-comerciales-en-el-primer-semestre-de-2025-quedan-fijados-en-un-11-15-por-resoluci-n-de-30-de-diciembre-de-2024-de-la-secretar-a-general-del-tesoro-y-financiacion-internacional/ · https://www.revistalimpiezas.es/actualidad/normativa-limpiezas/informe-morosidad-pmcm-el-85-de-las-grandes-companias-incumple-los-plazos-de-pago-y-se-financia-en-parte-a-costa-de-las-pymes-segun-la-pmcm_20260417.html · https://pmcm.es/informe-morosidad-estudio-plazos-pago-espana-2024/
190. t2p — manual de producto (foto con GPS forense —fijado genuino ~50 m / ≤30 s, la ubicación simulada bloquea la certificación; certificación en segundo plano que se reanuda al recuperar cobertura; escáner de documentos hasta 50 páginas en un PDF; captura de pantalla y de correo certificadas; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión; solo huellas en la cadena). Véanse los capítulos 13 y 15; el comercio internacional, en el capítulo 54; la auditoría, en el capítulo 55.
191. Banco Mundial — Laura Tuck y Wael Zakout, *7 reasons for land and property rights to be at the top of the global agenda* (~30 % de la población con título registrado). https://blogs.worldbank.org/en/voices/7-reasons-land-and-property-rights-be-top-global-agenda
192. Prindex — *Tenure insecurity on the rise* (2024; ~1.100 M de adultos, 23 %, inseguros sobre su tierra/vivienda). https://www.prindex.net/news-and-stories/tenure-insecurity-on-the-rise/
193. FAO (informe SOFA, vía UN News) — *Global report highlights slow progress in expanding secure land tenure* (~35 % de la tierra documentada; >1.100 M temen perderla). https://news.un.org/en/story/2026/02/1167037
194. FBI IC3 (vía National Association of Realtors) — *Online real estate fraud climbed to $275M in 2025* (12.368 víctimas). https://www.nar.realtor/magazine/real-estate-news/online-real-estate-fraud-climbed-to-275m-in-2025-fbi-says

195. American Land Title Association (ALTA) — *Seller Impersonation Fraud Attempts Increase, Study Shows* (julio 2024; 28 %; suelo sin edificar 85 %; credenciales de notario falsas 43 %). https://www.alta.org/news-and-publications/news/20240730-Seller-Impersonation-Fraud-Attempts-Increase-Study-Shows
196. FBI Boston (vía ALTA) — *FBI Boston Issues Quit Claim Deed Fraud Warning* (abril 2025; fraude inmobiliario 2019-2023: 58.141 víctimas / 1.300 M$). https://www.alta.org/news-and-publications/news/20250410-FBI-Boston-Issues-Quit-Claim-Deed-Fraud-Warning
197. Exonum / Bitfury — *The story of Georgia* (NAPR; ~1,5 M de títulos anclados a Bitcoin; «nadie puede alterar la marca de tiempo»). https://exonum.com/story-georgia
198. Eurasianet — *Georgia authorities use blockchain technology for developing land registry* (ampliación feb-2017; Hernando de Soto, asesor). https://eurasianet.org/georgia-authorities-use-blockchain-technology-for-developing-land-registry
199. Computer Weekly — *Sweden trials blockchain for land registry management* (Lantmäteriet + ChromaWay; >100 M€/año de ahorro). https://www.computerweekly.com/news/450421958/Sweden-trials-blockchain-for-land-registry-management
200. CoinDesk — *Blockchain land title project stalls in Honduras* (Factom; encallado por cuestiones políticas, 2015). https://www.coindesk.com/markets/2015/12/26/blockchain-land-title-project-stalls-in-honduras
201. Libertad Digital — *Cae en Cádiz una red criminal por una «estafa inmobiliaria a nivel nacional»* (6 de mayo de 2026; Operación ISLEDA; 3 detenidos de 19-34 años en San Fernando; destapada en Valladolid; cuentas abiertas con identidades robadas en falsas ofertas de trabajo; estafa, blanqueo y organización criminal); Cádiz Directo — *La Guardia Civil destapa en San Fernando una trama nacional de falsas viviendas de alquiler*. https://www.libertaddigital.com/andalucia/2026-05-06/san-fernando-cadiz-valladolid-guardia-civil-detiene-tres-hombres-acusados-de-estafa-inmobiliaria-conocido-portal-web-alquiler-y-venta-de-pisos-utilizaban-sus-datos-para-cuentas-falsas-victimas-por-todo-el-pais-destapado-en-valladolid-1b-7400307/ · https://www.cadizdirecto.com/cadiz/la-guardia-civil-destapa-en-san-fernando-una-trama-nacional-de-falsas-viviendas-de-alquiler
202. Idealista/News — *La última estafa en los anuncios de alquiler y los consejos para no caer en ella* (precios-gancho, propietarios «en el extranjero», pagos antes de la visita); Maldita.es — *Anuncios de alquiler falsos e inmobiliarias fantasma: cómo reconocer timos inmobiliarios*. https://www.idealista.com/news/inmobiliario/vivienda/2022/11/18/800160-la-ultima-estafa-en-los-anuncios-de-alquiler-y-los-consejos-para-no-caer-en-ella · https://maldita.es/malditobulo/20230830/inmobiliaria-fantasma-alquiler-piso-fraude-verano/
203. Idealista/News — *Todo lo que tienes que saber sobre la devolución de la fianza del alquiler* (plazo de un mes; intereses legales; acuerdo de liquidación con inventario); Ático Jurídico — *Devolución de la fianza del alquiler* (los tribunales exigen pruebas a quien retiene: facturas, informes); Fotocasa Life — *Cómo proceder si no nos devuelven la fianza del alquiler*. https://www.idealista.com/news/inmobiliario/vivienda/2022/07/03/797535-todo-lo-que-tienes-que-saber-sobre-la-devolucion-de-la-fianza-del-alquiler · https://aticojuridico.com/devolucion-fianza-alquiler/ · https://www.fotocasa.es/fotocasa-life/alquiler/como-proceder-si-no-nos-devuelven-la-fianza/
204. Housage — *Ley antiokupas 2025: desalojo en 15 días, cómo funciona y a quién no protege* (LO 1/2025 en vigor el 3 de abril de 2025; allanamiento art. 202 CP y usurpación art. 245 CP por juicio rápido; desalojo policial dentro de las primeras 48 horas; supresión del informe de vulnerabilidad en esta vía); Blegal — *La Ley 1/2025 agiliza el desalojo de okupas*; Vento Abogados — *Juicio rápido por okupación: la nueva regulación de la LO 1/2025*. https://housage.es/articulos/actualidad-inmobiliaria/ley-antiokupas-2025-desalojo-en-15-dias-como-funciona-y-a-quien-no-protege/ · https://www.blegal.eu/la-reforma-de-la-ley-organica-1-2025-agilizara-los-juicios-rapidos-para-facilitar-el-desalojo-de-okupas/ · https://vento.es/juicio-rapido-por-okupacion/
205. t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; el contenido no sale nunca del dispositivo; revelación voluntaria; los vacíos de la serie quedan fechados). Véanse los capítulos 13 y 15; para la titularidad y el registro, el capítulo 35.
206. Vecindia — *Condenado administrador de fincas por apropiación indebida* (Gijón: 1 año y medio de prisión confirmados; 2.984,04 € de la cuenta comunitaria; maniobras engañosas en el libro de actas haciendo firmar a expresidentes; recibos de obra y cerrajería falsos para encubrirse; descubierto al cambiar presidente y tesorero); ADADE — *El Tribunal Supremo ratifica la condena por*

apropiación indebida a un administrador de fincas; El Derecho — *Responsabilidad penal del administrador de fincas* (art. 253 CP). https://vecindia.es/comunidades-de-propietarios/condenado-administrador-fincas-apropiacion-indebida/ · https://www.adade.es/comunicacion/sala-de-prensa/el-tribunal-supremo-ratifica-la-condena-por-apropiacion-indebida-a-un-administrador-de-fincas · https://elderecho.com/cuando-puede-concurrir-responsabilidad-penal-en-el-administrador-de-fincas-por-su-actuacion-en-una-comunidad-de-propietarios/

207. Ley de Propiedad Horizontal (impugnación de acuerdos contrarios a la ley, lesivos o abusivos; convocatorias y actas; juntas telemáticas habilitadas por reforma reciente); Mundojurídico — *Responsabilidad del administrador de la Comunidad*; Oliva-Ayala — *Falsedad documental y certificaciones de juntas*. https://mundojuridico.info/responsabilidad-del-administrador-de-la-comunidad/ · https://www.oliva-ayala.es/wp-content/uploads/2024/03/Alcacer-2024-LLPenal-Falsedades.pdf
208. t2p — manual de producto (escáner de documentos hasta 50 páginas en un PDF certificado; grabación de audio; captura de pantalla y correo certificadas; foto con GPS forense; proyectos para agrupar el expediente de una obra; certificar cualquier archivo —solo la huella viaja; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; la propiedad y el registro, en el capítulo 35; el alquiler, en el capítulo 36.
209. Atlántico — *Investigan varias estafas en reformas de viviendas en Vigo y su comarca* (al menos seis víctimas; hasta 10.000 € cada una; constructor que inicia obras y desaparece); Liberal de Castilla — *Un vecino de Guadalajara pierde sus ahorros ante un falso albañil de internet* (Guardia Civil; estafador localizado en Madrid); Telemadrid — *Destapamos al presunto estafador de las reformas*; Allende Abogados — *Estafas en reformas* (patrón: oferta digital atractiva, presupuesto barato, anticipo «para materiales», desaparición; pérdidas que superan los 77.000 € en algunos casos). https://www.atlantico.net/articulo/vigo/investigan-estafa-reformas-menos-media-docena-victimas/20221017222637946245.html · https://www.liberaldecastilla.com/un-vecino-de-guadalajara-pierde-sus-ahorros-ante-un-falso-albanil-de-internet-la-guardia-civil-acorrala-al-estafador-en-madrid/ · https://www.telemadrid.es/programas/la-redaccion/Destapamos-presunto-estafador-reformas-2-2339786043--20210510052540.html · https://www.allendeabogados.com/estafas-reformas/
210. Marco del contrato de obra (Código Civil) y normativa de consumo aplicable a reformas con consumidores (presupuesto previo y factura). Véase el capítulo 34 para el cobro del profesional y el capítulo 37 para la obra común.
211. t2p — manual de producto (escáner de documentos hasta 50 páginas en un PDF certificado; foto con GPS forense —fijado genuino ~50 m / ≤30 s; vídeo con fecha/hora sobreimpresa; proyectos para ligar presupuesto, fases, evidencias y pagos; firma con vídeo-selfie, retos de vida y biometría; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; la derrama, en el capítulo 37; la factura, en el capítulo 34.
212. BCG y ADDX — *Relevance of On-chain Asset Tokenization in 'Crypto Winter'* (2022; ~16,1 billones $ en 2030, ~10 % del PIB mundial). https://www.bcg.com/publications/2022/relevance-of-on-chain-asset-tokenization
213. McKinsey — *From ripples to waves: the transformational power of tokenizing assets* (2024; caso base ~2 billones $, rango 1-4, excluye stablecoins). https://www.mckinsey.com/industries/financial-services/our-insights/from-ripples-to-waves-the-transformational-power-of-tokenizing-assets
214. CoinDesk (informe RedStone / Gauntlet / RWA.xyz) — *Real-world asset tokenization market has grown almost fivefold in 3 years* (~24.000 M$; crédito privado ~14.000 M$). https://www.coindesk.com/business/2025/06/26/real-world-asset-tokenization-market-has-grown-almost-fivefold-in-3-years
215. BlackRock / BusinessWire — *BlackRock Launches Its First Tokenized Fund, BUIDL, on the Ethereum Network* (20-mar-2024). https://www.businesswire.com/news/home/20240320771318/en/BlackRock-Launches-Its-First-Tokenized-Fund-BUIDL-on-the-Ethereum-Network
216. Securitize / PR Newswire — *BlackRock's BUIDL surpasses $1B in AUM* (marzo 2025). https://www.prnewswire.com/news-releases/blackrock-usd-institutional-digital-liquidity-fund-buidl-tokenized-by-securitize-surpasses-1b-in-aum-302401480.html

217. Paxos — *PAXG transparency* (barras serializadas en Brink's Londres; atestaciones mensuales de KPMG). https://www.paxos.com/paxg-transparency
218. Financial Stability Board — *The Financial Stability Implications of Tokenisation* (octubre 2024; custodios y oráculos como nuevos puntos de vulnerabilidad). https://www.fsb.org/2024/10/the-financial-stability-implications-of-tokenisation/
219. Moody's (vía CoinDesk) — *Tokenized fund adoption grows but brings technology risks* (2024; fallos de oráculo, historial limitado). https://www.coindesk.com/markets/2024/01/15/tokenized-fund-adoption-grows-but-brings-technology-risks-moodys
220. Standard Chartered y Synpulse — *Trade finance to play substantial role in $30.1 trillion tokenised real-world assets market by 2034*. https://www.sc.com/en/press-release/trade-finance-to-play-substantial-role-in-usd-30-1-trillion-tokenised-real-world-assets-market-by-2034/
221. InvestmentNews — *Larry Fink takes aim at investment inequality* (carta anual 2025 de BlackRock; la verificación de identidad como condición). https://www.investmentnews.com/alternatives/larry-fink-takes-aim-at-investment-inequality/259910
222. NPR — *The New York Times sues OpenAI and Microsoft for copyright infringement* (27-dic-2023; anexo de 127 páginas con salidas de GPT-4). https://www.npr.org/2023/12/27/1221821750/new-york-times-sues-chatgpt-openai-microsoft-for-copyright-infringement
223. Bloomberg Law — *OpenAI must turn over 20 million ChatGPT logs, judge affirms* (enero 2026). https://news.bloomberglaw.com/ip-law/openai-must-turn-over-20-million-chatgpt-logs-judge-affirms
224. Getty Images — *Getty Images statement* (acción contra Stability AI; consentimiento y licencia, enero 2023). https://newsroom.gettyimages.com/en/getty-images/getty-images-statement
225. Judiciary of England and Wales — *Getty Images v Stability AI [2025] EWHC 2863 (Ch)* (nov 2025; desestima la mayor parte de las reclamaciones de copyright). https://www.judiciary.uk/judgments/getty-images-v-stability-ai/
226. Copyright Alliance — *Andersen v. Stability AI* (Sarah Andersen, Kelly McKernan, Karla Ortiz; discovery desde agosto 2024). https://copyrightalliance.org/andersen-v-stability-ai-copyright-case/
227. Karla Ortiz — *Testimony before the U.S. Senate Judiciary Committee* (12-jul-2023; «nunca me han preguntado, acreditado ni compensado»). https://www.judiciary.senate.gov/imo/media/doc/2023-07-12_pm_-testimony-_ortiz.pdf
228. Variety — *AI-generated fake Drake/The Weeknd song 'Heart on My Sleeve'* (abril 2023; retirada por Universal Music Group). https://variety.com/2023/music/news/fake-ai-generated-drake-weeknd-collaboration-heart-on-my-sleeve-1235585451/
229. Wikipedia — *2023 SAG-AFTRA strike* (14-jul a 9-nov-2023; consentimiento para la «réplica digital»). https://en.wikipedia.org/wiki/2023_SAG-AFTRA_strike
230. U.S. Copyright Office — *Copyright and Artificial Intelligence, Part 2: Copyrightability* (29-ene-2025; la autoría humana como fundamento). https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf
231. USPTO — *America Invents Act (AIA): Frequently Asked Questions* (primero en presentar desde el 16-mar-2013; «la fecha de la invención es irrelevante»). https://www.uspto.gov/patents/laws/america-invents-act-aia/america-invents-act-aia-frequently-asked
232. WIPO (Organización Mundial de la Propiedad Intelectual) — *Patents: Frequently Asked Questions* (prior art; la divulgación previa destruye la novedad; el periodo de gracia no es universal). https://www.wipo.int/en/web/patents/faq_patents
233. BitLaw — *What does a patent application cost?* (redacción 9.000-17.000 $; presupuestar 15.000-25.000 $ antes de la concesión). https://www.bitlaw.com/guidance/patent/what-does-a-patent-application-cost.html
234. USPTO — *Fee Schedule* (solicitud provisional: fija fecha, 12 meses; tasas oficiales). https://www.uspto.gov/sites/default/files/documents/USPTO-fee-schedule_current.pdf
235. McLane Middleton — *Know the Law: Is the 'Poor Man's Patent' Real?* (sin valor legal; obsoleta desde el first-to-file de 2013). https://www.mclane.com/insights/know-the-law-is-the-poor-mans-patent-real/
236. Technical Disclosure Commons — *FAQ* (gratuito; fecha de publicación automática; indexado por Google Patents). https://www.tdcommons.org/faq.html
237. IP.com — *Publishing Disclosures to the Prior Art Database* (sello de tiempo mediante Surety AbsoluteProof). https://kb.ip.com/pad/knowledge-base/publishing-disclosures-to-the-prior-art-database-pad/

238. Richard Coller III y Alexander Covington (IPWatchdog) — *Defensive Publications: A Cost-Effective Tool to Supplement Your Patent Strategy* (2020). https://ipwatchdog.com/2020/05/25/defensive-publications-cost-effective-tool-supplement-patent-strategy/
239. Oficina Europea de Patentes (EPO) — *Espacenet reaches 160 million patent documents* (abril 2025). https://agip-news.com/news.aspx?id=76074&lang=en
240. WIPO — *PATENTSCOPE* (~128 millones de documentos de patente; 5,4 M de solicitudes PCT). https://patentscope2.wipo.int/
241. CNBC — *Trump pardons Anthony Levandowski, the engineer who stole self-driving car secrets from Google* (miles de archivos descargados antes de marcharse; Otto comprada por Uber; acuerdo Waymo-Uber de 2018 valorado por la prensa en ~245 M$ en acciones; culpabilidad en marzo de 2020; 18 meses de prisión —juez William Alsup: «the biggest trade secret crime I have ever seen»; indulto total el 20-1-2021, último día de mandato); TechCrunch — *Former Google engineer Anthony Levandowski among list of last-minute Trump pardons*; Wikipedia — *Anthony Levandowski* (acuerdo global de 2022: 25-30 M$). https://www.cnbc.com/2021/01/20/anthony-levandowski-pardoned-after-stealing-trade-secrets-from-google.html · https://techcrunch.com/2021/01/19/former-google-engineer-anthony-levandowski-among-list-of-last-minute-trump-pardons/ · https://en.wikipedia.org/wiki/Anthony_Levandowski
242. BOE — *Ley 1/2019, de 20 de febrero, de Secretos Empresariales* (transposición de la Directiva (UE) 2016/943; tres requisitos: secreto + valor empresarial + medidas razonables; alcance: fórmulas, procesos, bases de datos, listas de clientes, algoritmos, know-how; equilibrio: no cubre la experiencia y competencias adquiridas honestamente por el trabajador ni puede restringir su movilidad; medidas de confidencialidad procesales); Garrigues — *Aprobada la ley que protege los secretos empresariales*. https://www.boe.es/buscar/act.php?id=BOE-A-2019-2364 · https://www.garrigues.com/en_GB/new/law-will-protect-trade-secrets-has-been-approved
243. t2p — manual de producto (certificar cualquier archivo —solo la huella viaja, el contenido no sale nunca del dispositivo; escáner de documentos hasta 50 páginas; firma con vídeo-selfie, retos de vida y biometría; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice con revelación selectiva verificable sin conexión). Véanse los capítulos 13 y 15; el prior art y la patente, en el capítulo 41; los registros de un ataque, en el capítulo 57; los alertadores, en el capítulo 62.
244. Spend Network / Banco Mundial — *The $13 trillion global value of public procurement* (~13-15 % del PIB; menos del 3 % en datos abiertos). https://www.spendnetwork.com/13-trillion-the-global-value-of-public-procurement/
245. Banco Mundial — *The hidden $1 trillion: halting waste in public procurement* (~una cuarta parte malgastada; ~1 billón $/año). https://blogs.worldbank.org/en/voices/hidden-1-trillion-halting-waste-public-procurement
246. CoST – Infrastructure Transparency Initiative — *This is why construction is so corrupt* (10-30 % del valor de la obra pública; ~6 billones $/año hacia 2030). https://infrastructuretransparency.org/2016/02/05/this-is-why-construction-is-so-corrupt/
247. OCDE — *Guidelines for Fighting Bid Rigging in Public Procurement (2025 Update)* (la colusión puede encarecer los contratos un 20 % o más). https://www.oecd.org/en/publications/2025/09/oecd-guidelines-for-fighting-bid-rigging-in-public-procurement-2025-update_127880ea.html
248. Transparency International — *Corruption Perceptions Index 2025* (media mundial 42/100, mínimo histórico; Dinamarca 89, octavo año a la cabeza). https://www.transparency.org/en/news/cpi-2025-findings-insights-corruption
249. Open Contracting Partnership — *The impact of ProZorro in Ukraine* (~6.000 M$ ahorrados; Dozorro, 33.000+ licitaciones). https://www.open-contracting.org/impact-stories/impact-ukraine/
250. e-Estonia — *KSI Blockchain* (primer Estado con blockchain en producción, 2012; Guardtime; solo se ancla la huella). https://e-estonia.com/solutions/cyber-security/ksi-blockchain/
251. World Economic Forum — *Exploring Blockchain Technology for Government Transparency to Reduce Corruption* (Colombia, Programa de Alimentación Escolar, BID, 2020). https://www.weforum.org/publications/exploring-blockchain-technology-for-government-transparency-to-reduce-corruption/
252. EUR-Lex — *Reglamento eIDAS (UE 910/2014), artículo 41* (presunción legal de exactitud del sello de tiempo cualificado). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
253. Banco Mundial — *GovTech Maturity Index* (198 economías; cuatro áreas de madurez del gobierno digital). https://www.worldbank.org/en/programs/govtech/gtmi

254. BOE — *Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas* (art. 21: plazo general de tres meses para resolver y notificar; silencio administrativo con efectos desde el vencimiento; certificado acreditativo del silencio expedido de oficio en 15 días; notificaciones electrónicas: 10 días naturales desde la puesta a disposición, transcurridos los cuales se entiende rechazada); Administrativando — *Silencio administrativo: qué es y cuáles son sus efectos*; Conceptos Jurídicos — *Silencio administrativo en España*. https://www.boe.es/buscar/pdf/2015/BOE-A-2015-10565-consolidado.pdf · https://administrativando.es/silencio-administrativo/ · https://www.conceptosjuridicos.com/silencio-administrativo/
255. Noticias Jurídicas — *El mercado negro de citas para extranjería: venta de citas para asilo internacional* (bots que acaparan citas; reventa; sistema desbordado); OKDiario — *El caos en la web de Extranjería impulsa a las mafias que cobran hasta 350 € por cita* (reventa por WhatsApp de 50 a 350 €, hasta 600 €); Parainmigrantes — *El problema de la cita previa llega al Defensor del Pueblo* (quejas constantes, ≈3.000 en un año; >163.000 solicitudes de asilo en 2023; «demoras excesivas»); Iberoeconomía — *España perseguirá a las mafias que revenden citas para trámites públicos*. https://noticias.juridicas.com/contenido-patrocinado/articulo/19314-el-mercado-negro-de-citas-para-extranjeria:-venta-de-citas-para-asilo-internacional/ · https://okdiario.com/espana/caos-web-extranjeria-impulsa-mafias-que-cobran-300-cita-cada-inmigrante-13835137 · https://www.parainmigrantes.info/el-problema-de-la-gestion-de-la-cita-previa-para-tramites-de-extranjeria-llega-al-defensor-del-pueblo/ · https://iberoeconomia.es/inmigracion/espana-perseguira-a-las-mafias-que-revende-citas-para-tramites-publicos/
256. t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; contenido en los sistemas de cada parte, solo huellas en la cadena; rastro verificable por ambas partes). Véanse los capítulos 13 y 15; la contratación pública, en el capítulo 43.
257. AFAPNA — *Oposiciones 2026: sorteo de letras de tribunales y aspirantes*; OpositaTest — *Sorteo por letra del orden de actuación en oposiciones* (sorteo público de letras; procedimientos reglados posteriores; sistema «espejo» de inversión del orden del DNI); USTEA — *Resultado del sorteo para la designación de vocales de los tribunales*. https://afapna.es/educa/oposiciones-2026-sorteo-letras-de-tribunales-y-aspirantes/ · https://blog.opositatest.com/dudas-letra-del-orden-de-actuacion-de-los-opositores/ · https://educacion.ustea.org/oposiciones-2026-resultado-del-sorteo-para-la-designacion-de-vocales-de-los-tribunales/
258. esPúblico — *La notificación en el procedimiento de adjudicación de viviendas protegidas mediante sorteo* (sorteo ante notario según el procedimiento de cada administración; posibilidad de impugnación); elDiario.es (Canarias Ahora) — *Los Llanos espera que la impugnación del sorteo de las 40 viviendas se resuelva «con prontitud y máxima transparencia»*. https://www.administracionpublica.com/adjudicaciondeviviendasprotegidas/ · https://www.eldiario.es/canariasahora/lapalmaahora/municipios/los_llanos_de_aridane/los-llanos-espera-impugnacion-sorteo-viviendas-resuelva-prontitud-maxima-transparencia_1_4583333.html
259. t2p — manual de producto (huella SHA-512; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; compromiso previo por huella —los datos personales no se exponen—; actas ancladas y reverificables). Véanse los capítulos 13 y 15; la integridad electoral, en el capítulo 48.
260. Cloudflare / League of Entropy — *Distributed Randomness Beacon* (drand: baliza de aleatoriedad distribuida y públicamente verificable; miembros fundadores: Cloudflare, EPFL, Kudelski Security, Protocol Labs y Universidad de Chile; valores imparciales, impredecibles y verificables a intervalos fijos; criptografía de umbral; aplicaciones: loterías y elecciones); PR Newswire — *The League of Entropy launches production drand network* (primera baliza pública verificable en producción); GitHub — *drand/drand*. https://www.cloudflare.com/leagueofentropy/ · https://www.prnewswire.com/news-releases/the-league-of-entropy-launches-production-drand-network-providing-the-first-publicly-verifiable-distributed-randomness-beacon-301109096.html · https://github.com/drand/drand
261. Redacción Médica — *Un informe revela filtraciones de 19 exámenes en hasta 12 OPE de Osakidetza* (OPE 2016-2017 del servicio vasco de salud; denuncias sindicales en Anestesia y Angiología; indicios en 19 exámenes de 12 especialidades; dimisiones del consejero de Salud Jon Darpón, la directora general de Osakidetza y dos directivos de RRHH); Deia — *Archivan la causa por las presuntas filtraciones en la OPE de Osakidetza en 2018 por falta de pruebas* (diciembre de 2024: archivo «al

no existir indicios racionales de la comisión del ilícito», provisional para dos investigados de Cirugía Plástica); elDiario.es — *La Justicia cierra sin culpables la investigación* y *Ocho años del inicio de la investigación… sin fecha para el juicio*. https://www.redaccionmedica.com/autonomias/pais-vasco/un-informe-revela-filtraciones-de-19-examenes-en-hasta-12-ope-de-osakidetza-4796 · https://www.deia.eus/actualidad/sociedad/2024/12/12/archivan-causa-filtraciones-ope-osakidetza-9042604.html · https://www.eldiario.es/euskadi/justicia-cierra-responsabilidad-investigacion-filtraciones-oposiciones-medicas-vascas_1_11896007.html

262. t2p — manual de producto (certificar cualquier archivo —solo la huella viaja, el contenido no sale nunca de la custodia; foto con fecha cierta; escáner de documentos; captura de publicaciones oficiales con fecha; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; el sorteo de tribunales, en el capítulo 45; las credenciales, en el capítulo 19; los alertadores, en el capítulo 62.
263. Banco Mundial (ID4D) — *Global progress in identification: 3 findings from the latest data* (2025; ~800 M sin identidad oficial; >50 % son niños no registrados). https://blogs.worldbank.org/en/digital-development/global-progress-in-identification--3-findings-from-the-latest-da
264. UNHCR — *Global Trends Report 2024* (4,4 M de apátridas oficiales, hasta ~10 M reales; rohinyás ~1,8 M). https://www.unhcr.org/sites/default/files/2025-06/global-trends-report-2024.pdf
265. UNICEF — *Birth registration steadily increases worldwide, but 150 million children still invisible* (diciembre 2024). https://www.unicef.org/press-releases/birth-registration-steadily-increases-worldwide-150-million-children-still-invisible
266. Comisión Europea — *European Digital Identity (eIDAS 2.0)* (Reg. UE 2024/1183; EUDI Wallet obligatoria a finales de 2026; divulgación selectiva). https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation
267. W3C — *Verifiable Credentials Data Model v2.0 becomes a W3C Recommendation* (15-mayo-2025) y *Decentralized Identifiers (DID) v1.0* (2022). https://www.w3.org/press-releases/2025/verifiable-credentials-2-0/
268. Gobierno de la India (Press Information Bureau) — *Aadhaar* (~1.340 millones de titulares vivos; >99,9 % de los adultos; >170.000 millones de autenticaciones). https://www.pib.gov.in/PressReleasePage.aspx?PRID=2241778
269. Business Standard / Resecurity — *Aadhaar data of millions of Indians put on sale on the dark web* (~815 millones de registros, octubre 2023). https://www.business-standard.com/india-news/aadhaar-data-of-millions-of-indians-put-on-sale-on-the-dark-web-reports-123103000993_1.html
270. Scroll.in — *Denied food because she did not have an Aadhaar-linked ration card, Jharkhand girl dies of starvation* (Santoshi Kumari, 2017). https://scroll.in/article/854225/denied-food-because-she-did-not-have-aadhaar-linked-ration-card-jharkhand-girl-dies-of-starvation
271. Reetika Khera (IIT Delhi) — investigación sobre Aadhaar y la exclusión en programas de bienestar (*Economic & Political Weekly*). https://www.epw.in/engage/article/aadhaar-failures-food-services-welfare
272. MIT Technology Review — *Inside the Jordan refugee camp that runs on blockchain* (WFP Building Blocks; reconocimiento de iris EyePay). https://www.technologyreview.com/2018/04/12/143410/inside-the-jordan-refugee-camp-that-runs-on-blockchain/
273. Edward Snowden — *Vigilancia permanente* (Planeta, 2019).
274. Biometric Update / ICLG — *Worldcoin: prohibiciones y órdenes de supresión* (2024-2025). https://www.biometricupdate.com/202510/colombia-orders-world-shut-down-citing-biometrics-compliance-failures
275. Wikipedia (con BBC / Al Jazeera) — *2017 Kenyan presidential election petition* (anulación 4-2; CJ David Maraga; primera en África). https://en.wikipedia.org/wiki/2017_Kenyan_presidential_election_petition
276. The Standard (Kenia) — *Presidential petition: what scrutiny of key IEBC forms revealed* (291 formularios 34B; 56 sin rasgos de seguridad, 31 sin número de serie, 32 sin firma). https://www.standardmedia.co.ke/article/2001253102/presidential-petition-what-scrutiny-of-key-iebc-forms-revealed
277. NYU Center on International Cooperation / Congo Research Group — *Who really won the Congolese elections?* (Fayulu ~60 %; CENCO 39.824 observadores; correlación 0,976-0,991; ~3,6 M de votos). https://cic.nyu.edu/resources/who-really-won-the-congolese-elections/

278. Sunoo Park, Michael Specter, Neha Narula y Ronald L. Rivest — *Going from bad to worse: from Internet voting to blockchain voting* (Journal of Cybersecurity, 2021). https://academic.oup.com/cybersecurity/article/7/1/tyaa025/6137886
279. MIT News / USENIX Security — *Researchers find security flaws in Voatz; «The Ballot is Busted Before the Blockchain»* (2020). https://news.mit.edu/2020/voting-voatz-app-hack-issues-0213
280. Pierrick Gaudry (CNRS/INRIA) — *Breaking the encryption scheme of the Moscow Internet voting system* (2019; roto en ~20 minutos). https://arxiv.org/abs/1908.05127
281. Philip B. Stark (UC Berkeley) — *A Gentle Introduction to Risk-Limiting Audits* (2012). https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf
282. Election Academy (Universidad de Minnesota) — *Colorado successfully completes the nation's first risk-limiting audit* (2017; límite de riesgo del 9 %). https://electionacademy.lib.umn.edu/2017/11/27/colorado-successfully-completes-nations-first-risk-limiting-audit/
283. OSCE/ODIHR — *Election Observation Handbook* (6.ª edición; observadores de corto y largo plazo; distinguir lo aislado de lo sistemático). https://cdn.osce.org/sites/default/files/f/documents/5/e/68439.pdf
284. The Carter Center — *Election Standards y Declaration of Principles for International Election Observation* (2005). https://electionstandards.cartercenter.org/our-mission/
285. Shoshana Zuboff — *La era del capitalismo de la vigilancia* (Paidós, 2020).
286. L2BEAT; MEV Watch (2026). https://www.mevwatch.info/
287. WFP — *Building Blocks* (~555 M$ en transferencias; ~6 M de personas; Ucrania: 337 M$ coordinados, ~35 M$ de solapamiento evitado; 159 organizaciones en 2025). https://www.wfp.org/building-blocks
288. UN Innovation Network — *How the Building Blocks blockchain network is transforming humanitarian aid* (>1 M de refugiados cada mes). https://www.uninnovation.network/blog/how-the-building-blocks-blockchain-network-is-transforming-humanitarian-aid
289. UNHCR — *UNHCR's Biometric Tools in 2023* (base de 15,7 M de personas; PRIMES/BIMS). https://www.unhcr.org/blogs/unhcrs-biometric-tools-in-2023/
290. Development Initiatives — *Cash and Voucher Assistance* (~10,6 mil M$ en 2022 → 9,7 mil M$ en 2023; WFP, mayor proveedor). https://devinit.org/resources/falling-short-humanitarian-funding-reform/cash-voucher-assistance/
291. CALP Network — *The State of the World's Cash 2023*. https://www.calpnetwork.org/collection/the-state-of-the-worlds-cash-2023-report/
292. Human Rights Watch — *UN Shared Rohingya Data Without Informed Consent* (Lama Fakih; ~830.000 nombres compartidos con Myanmar). https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent
293. UN News — *Yemen: WFP pauses food distributions* (disputa biométrica con los hutíes, 2019-2023). https://news.un.org/en/story/2023/12/1144417
294. GiveDirectly / The New Humanitarian — *DRC mobile-cash fraud* (~1,2 M$ desviados; ~1.900 familias). https://www.givedirectly.org/drc-case-2023/
295. Carmela Troncoso et al. (EPFL SPRING Lab, con el CICR) — *Janus: Safe Biometric Deduplication for Humanitarian Aid Distribution* (IEEE S&P 2024; revela solo un bit, sin base biométrica). https://arxiv.org/abs/2308.02907
296. FTC (2024); Autoriteit Persoonsgegevens / EDPB (2024). https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en
297. Wikipedia (ES) — *Terremotos de Venezuela de 2026* (doblete M7,2 San Felipe + M7,5 Yumare, 24-6-2026, 39 s de diferencia; >3.342 muertos, >16.840 heridos, >68.000 desaparecidos; aeropuerto Simón Bolívar suspendido; conflictos de distribución: suministros retenidos en Altamira, centros de acopio civiles prohibidos en Charallave y Campo Elías, distribución impedida en El Limón, acceso restringido en La Guaira; respuesta: >30 países, >3.600 rescatistas, >1.000 toneladas); ReliefWeb — *Terremoto en Venezuela: panorama de la situación (25-6-2026)*; SkyAlert — *Actualización del terremoto en Venezuela*. https://es.wikipedia.org/wiki/Terremotos_de_Venezuela_de_2026 · https://reliefweb.int/report/venezuela-bolivarian-republic/terremoto-en-venezuela-panorama-de-la-situacion-25-de-junio-de-2026 · https://skyalert.mx/articulos/actualizacion-sismos-venezuela-2026
298. Ayuda en Acción — *Terremotos en Venezuela: qué ha pasado y situación actual* (contexto humanitario; donaciones: José Andrés/World Central Kitchen 1 M$, Rosalía 2 M$ a UNICEF, Metallica 100.000 $). https://ayudaenaccion.org/blog/ayuda-humanitaria/terremotos-venezuela/

299. Departamento del Tesoro de EE. UU. — *Treasury Disrupts Corruption Network Stealing From Venezuela's Food Distribution Program (CLAP)* (25-7-2019; red de Alex Saab; Group Grand Ltd; sobreprecios); Voz de América — *¿Qué son los CLAP y qué tienen que ver con Alex Saab?*; InsightCrime — *How Criminals Take Advantage of Venezuela's Food Aid System*; Excélsior — *Despensas CLAP, una red de corrupción* (~12 M cajas desde México, ~30 $/caja de sobreprecio, ~360 M$; leche por debajo de etiquetado — Armando.Info). https://home.treasury.gov/system/files/136/2019-07-25-Venezuela-Alex-Saab-Network-SPANISH-TRANSLATION.pdf · https://www.vozdeamerica.com/a/que-son-los-clap-y-que-tienen-que-ver-con-alex-saab-/6277181.html · https://insightcrime.org/news/criminals-take-advantage-venezuelas-food-aid-system/ · https://www.excelsior.com.mx/internacional/despensas-clap-red-corrupcion-maduro-larga-historia
300. Wikipedia (ES) — *Envío de ayuda humanitaria en Venezuela de 2019* (puente de Tienditas bloqueado con cisterna y contenedores; 23-2-2019: 14 camiones/280 toneladas, 2 camiones quemados; cierre de frontera); CNN en Español — *Venezuela bloquea puente en frontera con Colombia* (6-2-2019); Infobae — *Maduro ordenó retirar los contenedores del puente Tienditas* (dic. 2022). https://es.wikipedia.org/wiki/Env%C3%ADo_de_ayuda_humanitaria_en_Venezuela_de_2019 · https://cnnespanol.cnn.com/2019/02/06/venezuela-bloquea-puente-en-frontera-con-colombia · https://www.infobae.com/america/venezuela/2022/12/14/tras-impedir-el-paso-de-la-ayuda-humanitaria-en-2019-maduro-ordeno-retirar-los-contenedores-del-puente-tienditas/
301. NBC News — *Red Cross: $6 million for Ebola fight stolen through fraud* (nov. 2017; ≥6 M$ sobre >124 M$; Sierra Leona ~2,13 M colusión con banco sobre el tipo de cambio; Guinea ~1,17 M facturación fraudulenta de un proveedor de despacho aduanero; Liberia ~2,7 M precios inflados de artículos de socorro, nóminas e incentivos); IFRC/ReliefWeb — *IFRC statement on fraud in Ebola operations*; Newsweek — *Red Cross Loses $6 Million In Fraud During Ebola Crisis*. https://www.nbcnews.com/storyline/ebola-virus-outbreak/red-cross-6-million-ebola-fight-stolen-through-fraud-n817701 · https://reliefweb.int/report/sierra-leone/ifrc-statement-fraud-ebola-operations · https://www.newsweek.com/red-cross-outraged-6-million-fraud-loss-during-ebola-outbreak-702231
302. UN News — *UN food agency welcomes review of its food distribution programme in Somalia* (2010; Grupo de Monitoreo: «hasta la mitad» desviada; contratistas/milicias/personal local; familia Adaani); VOA — *WFP Report says No Evidence of Food Diversion in Somalia* (negación del WFP — Josette Sheeran; auditoría propia sin evidencia); ODI — *Somalia food aid diversion*. https://news.un.org/en/story/2010/03/332792-un-food-agency-welcomes-review-its-food-distribution-programme-somalia · https://www.voanews.com/a/un-official-slams-report-on-somalia-food-diversion-89115947/153849.html · https://odi.org/en/insights/somalia-food-aid-diversion/
303. IPS Noticias — *Corrupción-España: investigación de ONG refuerza transparencia* (2007; Intervida: >45 M€ desviados según la Fiscalía Anticorrupción, ~10.000 donantes de baja; Anesvad: presidente detenido el 5-4-2007 por apropiación indebida, denunciado por los trabajadores). https://ipsnoticias.net/2007/04/corrupcion-espana-investigacion-de-ong-refuerza-transparencia/
304. Natural Hazards Center (Univ. Colorado) — *Avoiding the "Second Disaster" of Unwanted Donations* (convergencia material; donaciones no solicitadas colapsan pistas y almacenes); TED Ideas — *After a disaster, don't send toys or clothing — send money* (José Holguín-Veras: 50-70 % de los bienes que llegan no son necesarios ni apropiados; el caso del avión de juguetes). https://hazards.colorado.edu/news/research-counts/avoiding-the-second-disaster-of-unwanted-donations · https://ideas.ted.com/after-a-disaster-dont-send-toys-or-clothing-send-money-heres-why/
305. WFP — *UN Humanitarian Response Depot (UNHRD)* (depósitos en Brindisi, Accra, Kuala Lumpur, Ciudad de Panamá y Dubái; despacho en 48 h; stocks para múltiples organizaciones); UNHRD — *Our Services*; World Economic Forum — *Logistics Emergency Team: 20 years* (Clúster Logístico liderado por el WFP). https://www.wfp.org/unhrd · https://unhrd.org/our-services · https://www.weforum.org/stories/global-cooperation/logistics-emergency-team-humanitarian-aid-20-years/
306. UNICEF Office of Innovation — *Why blockchain is the future of humanitarian response* (StaTwig: trazabilidad de viales de vacunas del depósito al centro de salud); WFP Innovation Accelerator — *3 ways blockchain innovation is enhancing humanitarian work* (trazabilidad de alimentos; Building Blocks); LSE — *How Blockchain is Contributing to the Humanitarian Sector as of 2025* (piloto IFRC/AID:Tech con la Cruz Roja irlandesa y libanesa).

https://www.unicef.org/innovation/stories/why-blockchain-future-humanitarian-response · https://wfpinnovation.medium.com/3-ways-that-blockchain-innovation-is-enhancing-humanitarian-work-e40dd3e85dee · https://blogs.lse.ac.uk/internationaldevelopment/2025/07/10/how-blockchain-is-contributing-to-the-humanitarian-sector-as-of-2025/

307. t2p — manual de producto (rueda de modos; escáner de documentos hasta 50 páginas en un PDF; huella SHA-512 calculada en el dispositivo; certificación en segundo plano que se reanuda al recuperar cobertura; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; GPS forense —fijado genuino ~50 m / ≤30 s, la ubicación simulada bloquea la certificación; comprobación de integridad del dispositivo y attestation de hardware; superposición de fecha/hora en el vídeo; firma con vídeo-selfie, retos de vida y biometría; paquete de evidencia .asice ETSI EN 319 162 verificable sin conexión; solo huellas en la cadena). Véanse los capítulos 13 y 15; la entrega de efectivo y la desduplicación, en el capítulo 49; el euro del donante, en el capítulo 73.
308. Wikipedia — *2023 Pylos migrant boat disaster* (el Adriana; salida de Libia; ≈750 personas a bordo; más de 600 muertos; 104 supervivientes; 82 cuerpos; versión de la guardia costera); Human Rights Watch — *Greece: Disparities in Accounts of Pylos Shipwreck Underscore the Need for Human Rights Compliant Inquiry* (errores de las autoridades; alegaciones sobre el remolque). https://en.wikipedia.org/wiki/2023_Pylos_migrant_boat_disaster · https://www.hrw.org/news/2023/08/03/greece-disparities-accounts-pylos-shipwreck-underscore-need-human-rights-compliant
309. Amnistía Internacional — *Greece: Trial of Pylos shipwreck survivors must not be a shield in the investigation of the alleged responsibilities of the Greek authorities* (mayo de 2024; nueve supervivientes procesados; crítica de las organizaciones de derechos humanos). https://www.amnesty.org/en/latest/news/2024/05/greece-trial-of-pylos-shipwreck-survivors-must-not-be-a-shield-in-the-investigation-of-the-alleged-responsibilities-of-the-greek-authorities/
310. Refugee Support Aegean — *Pylos Shipwreck: Criminal prosecution for felonies against 17 members of the Coast Guard* (26 de mayo de 2025; capitán de la ΠΠΛΣ-920 acusado de causar naufragio con resultado de muerte de al menos 82 personas; querella en nombre de 40 supervivientes). https://rsaegean.org/en/pylos-shipwreck-criminal-prosecution-for-felonies-to-17-members-of-the-coast-guard/
311. Global Investigative Journalism Network — *How They Did It: Investigating the Pylos Shipwreck* (reconstrucción periodística con datos de tráfico marítimo, testimonios de supervivientes y material de sus teléfonos). https://gijn.org/stories/investigating-pylos-shipwreck/
312. t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; solo huellas en la cadena; publicación opcional; recuperación de copias verificables contra la huella). Véanse los capítulos 13 y 15; la evidencia de derechos humanos, en el capítulo 20; la posición de los barcos, en el capítulo 103.
313. Wikipedia — *Border Violence Monitoring Network* (coalición de más de 12 organizaciones, fundada en 2017); Statewatch — *The 'Black Book of Pushbacks': testimonies of pushbacks affecting over 12,000 people* (diciembre de 2020; 12.654 personas); Balkan Insight — *Study Reports 25,000 Violent Pushbacks at EU Borders* (edición ampliada de 2022: más de 3.000 páginas, 4 volúmenes). https://en.wikipedia.org/wiki/Border_Violence_Monitoring_Network · https://statewatch.org/news/2021/january/eu-the-black-book-of-pushbacks-testimonies-of-pushbacks-affecting-over-12-000-people/ · https://balkaninsight.com/2022/12/08/study-reports-25000-violent-pushbacks-at-eu-borders/
314. Iberley — *El TJUE refuerza la tutela judicial efectiva en casos de devoluciones sumarias de migrantes* (asunto C-136/24 P, sentencia de 18 de diciembre de 2025; nacional sirio despojado del teléfono y devuelto a Turquía con Frontex presente; adaptación de la carga de la prueba; Frontex como poseedora de la documentación). https://www.iberley.es/noticias/el-tjue-refuerza-tutela-judicial-efectiva-casos-devoluciones-sumarias-migrantes-35841
315. Hertfordshire Constabulary — *Three jailed for £4m inheritance fraud* (caso Leigh Voysey y el testamento de Maureen Renny; ~4,2 M£). https://www.herts.police.uk/news/hertfordshire/news/2024/december-2024/three-jailed-for-4m-inheritance-fraud/
316. Cerulli Associates — *Cerulli anticipates $84 trillion in wealth transfers through 2045* (2022; «gran transferencia de riqueza»). https://www.cerulli.com/press-releases/cerulli-anticipates-84-trillion-in-wealth-transfers-through-2045

317. Caring.com / YouGov — *Wills and Estate Planning Study 2025* (solo el 24 % de los adultos tiene testamento). https://www.caring.com/resources/wills-survey
318. Dutton Gregory / Probate Registry — *Inheritance dispute statistics* (11.362 caveats en 2024, +56 % en cinco años). https://www.duttongregory.co.uk/site/blog/personalnews/inheritance-dispute-statistics
319. Justia — *Will contests: testamentary capacity, undue influence, forgery* (motivos de nulidad). https://www.justia.com/estate-planning/wills/will-contests/
320. CBS News — *QuadrigaCX CEO took password to his grave* (Gerald Cotten; ~137 M$ bloqueados). https://www.cbsnews.com/news/gerald-cotten-quadrigacx-ceo-took-password-to-his-grave-leaving-company-unable-to-access-137-million/
321. Chainalysis (vía Decrypt) — *~3,7 millones de bitcoins perdidos para siempre* (2020; ~20 % de la oferta). https://decrypt.co/37171/lost-bitcoin-3-7-million-bitcoin-are-probably-gone-forever
322. American Bar Association — *Digital property and estate planning* (RUFADAA; la criptomoneda se pierde sin las claves). https://www.americanbar.org/groups/real_property_trust_estate/resources/estate-planning/digital-property/
323. Comisión Europea (Interoperable Europe) / e-Estonia — *Estonia's KSI blockchain: the Succession Registry* (primer servicio estatal sobre blockchain, 2012). https://e-estonia.com/blockchain-security-control-for-government-registers/
324. eSignGlobal — *Electronic wills legislation and remote notarization* (eIDAS QES; los testamentos a menudo excluidos de la notarización electrónica). https://www.esignglobal.com/blog/electronic-wills-legislation-remote-notary
325. INE / Gracia Carrión (análisis) — *Custodia compartida supera a la materna en España (INE 2024)* (49,7 % de los divorcios con hijos, +1,3 puntos; primera vez por encima de la custodia materna; 12,6 % en 2010); APFS — *Separaciones y divorcios en España 2024* (82.991 divorcios, +8,2 %); INE — *Estadística de nulidades, separaciones y divorcios*. https://graciacarrion.com/es/custodia-compartida-supera-materna/ · https://apfs.es/separaciones-y-divorcios-en-espana-2024-tendencias-y-claves-segun-el-ine/ · https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=estadistica_C&cid=1254736176798&menu=ultiDatos&idp=1254735573206
326. OurFamilyWizard — *Herramientas para la custodia compartida* (aplicación de coparentalidad de referencia para tribunales y profesionales en los 50 estados de EE. UU., Canadá, Reino Unido, Australia y Nueva Zelanda; mensajes con marca de tiempo y sin borrado; confirmaciones de lectura; calendarios con historial; informes para juicios; ToneMeter); Crianza y Crecimiento — *Aplicaciones de coparentalidad aprobadas por tribunales*. https://es.ourfamilywizard.com/homepage · https://crianzaycrecimiento.com/aplicaciones-coparentalidad-aprobadas-tribunales/
327. El Español — *Una abogada, sobre solicitar la custodia compartida: «Después de 10 años, necesitas un plan de parentalidad»* (el plan de parentalidad como marco común de crianza más allá del convenio regulador). https://www.elespanol.com/mujer/relaciones/20251214/abogada-solicitar-custodia-compartida-despues-anos-necesitas-plan-parentalidad/1003744039064_0.html
328. t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; registro bilateral; contenido en los dispositivos, solo huellas en la cadena; revelación ante el juzgado). Véanse los capítulos 13 y 15; la grabación legal de conversaciones propias, en el capítulo 75.
329. Banco Asiático de Desarrollo (ADB) — *Global trade finance gap expands to $2.5 trillion in 2022* (Trade Finance Gaps, Growth and Jobs Survey). https://www.adb.org/news/global-trade-finance-gap-expands-25-trillion-2022
330. McKinsey — *The multi-billion-dollar paper jam: unlocking trade by digitalizing documentation* (2022; ahorro de 6.500 M$ + comercio nuevo). https://www.mckinsey.com/industries/logistics/our-insights/the-multi-billion-dollar-paper-jam-unlocking-trade-by-digitalizing-documentation
331. DCSA / FIT Alliance — *eBL adoption* (penetración real del conocimiento de embarque electrónico: 5,7 %, enero 2025). https://dcsa.org/standards/booking/adoption-guide-booking-and-bill-of-lading
332. Caixin Global — *Dezheng founder jailed over Qingdao port forgery scandal* (Chen Jihong, 23 años; ~12.300 M yuanes con recibos falsos). https://www.caixinglobal.com/2018-12-12/dezheng-founder-gets-32-years-in-prison-over-port-forgery-scandal-101358154.html
333. Singapore Police Force / SCMP — *Hin Leong founder OK Lim jailed* (17,5 años, reducidos a 13,5 en apelación en marzo de 2026; ~112 M$ a HSBC). https://www.police.gov.sg/media-hub/news/2024/20241118_founder_of_hin_leong_trading_sentenced_and_jailed_for_cheating_and_instigating_fc

334. FINMA — *Greensill / Credit Suisse* (insolvencia 2021; ~10.000 M$ en cuatro fondos; facturas ficticias). https://www.finma.ch/en/news/2023/02/20230228-mm-greensill/
335. Maersk — *Maersk and IBM to discontinue TradeLens* (cierre del consorcio, 2022-2023). https://www.maersk.com/news/articles/2022/11/29/maersk-and-ibm-to-discontinue-tradelens
336. UNCITRAL — *Model Law on Electronic Transferable Records (MLETR): status* (13 jurisdicciones; incluye el Reino Unido). https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records/status
337. Clifford Chance — *UK Electronic Trade Documents Act 2023* (equivalencia legal del conocimiento de embarque electrónico). https://www.cliffordchance.com/briefings/2023/08/uk-electronic-trade-documents-act-2023--a-further-step-towards-p.html
338. International Chamber of Commerce (ICC) — *Survey shows steady rise of global adoption of electronic bills of lading* (~4.000 M de documentos/día; reglas UCP 600). https://iccwbo.org/news-publications/news/survey-shows-steady-rise-of-global-adoption-of-electronic-bills-of-lading/
339. Financial Times (vía S&P Global) — *Wirecard auditor did not independently verify its bank balance* (EY; cuentas de garantía inexistentes; extractos fabricados). https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/wirecard-auditor-did-not-independently-verify-its-bank-balance-8211-financial-times-59219155
340. CNN Business — *Germany bans EY from taking on new audit clients over Wirecard* (APAS: «negligencia grave»; multa de 500.000 € y prohibición de 2 años). https://www.cnn.com/2023/04/03/business/wirecard-ey-ban-germany/index.html
341. Dan McCrum (Financial Times) — *Money Men: A Hot Startup, a Billion-Dollar Fraud, a Fight for the Truth* (2022). https://danmccrum.com/
342. Wikipedia — *Enron scandal* (>74.000 M$ perdidos; Arthur Andersen, ~85.000 empleados; origen de la Sarbanes-Oxley). https://en.wikipedia.org/wiki/Enron_scandal
343. U.S. Securities and Exchange Commission — *Luckin Coffee agrees to pay $180 million penalty to settle accounting fraud charges* (~311 M$ de ventas fabricadas). https://www.sec.gov/newsroom/press-releases/2020-319
344. PCAOB — *AS 2310, The Auditor's Use of Confirmation* (adoptada en septiembre de 2023; confirmación externa directa). https://pcaobus.org/oversight/standards/auditing-standards/details/AS2310
345. Association of Certified Fraud Examiners (ACFE) — *Report to the Nations 2024* (5 % de los ingresos; fraude de estados financieros, mediana de 766.000 $ por caso). https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf
346. Comisión Europea — *Corporate sustainability reporting (CSRD)* (aseguramiento limitado obligatorio; normas ESRS de EFRAG). https://finance.ec.europa.eu/financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en
347. Accountancy Europe — *Omnibus explained: key changes to the CSRD and CSDDD* (umbral de >1.000 empleados y >450 M€; el aseguramiento limitado se mantiene). https://accountancyeurope.eu/publications/omnibus-explained-key-changes-to-the-csrd-and-csddd/
348. IAASB — *ISSA 5000: General Requirements for Sustainability Assurance Engagements* (2024; primera norma global de aseguramiento de sostenibilidad). https://www.iaasb.org/publications/international-standard-sustainability-assurance-5000-general-requirements-sustainability-assurance
349. Juniper Research (vía PR Newswire) — *22% of online ad spend is wasted due to ad fraud in 2023* (84.000 M$ en 2023 → 172.000 M$ en 2028; móvil 30 %). https://www.prnewswire.com/news-releases/new-ad-fraud-study-22-of-online-ad-spend-is-wasted-due-to-ad-fraud-in-2023-according-to-juniper-research-301938050.html
350. Association of National Advertisers (ANA) — *Programmatic Media Supply Chain Transparency Study* (diciembre 2023; 36 céntimos por dólar; ~22.000 M$ recuperables; MFA 15 %). https://www.ana.net/miccontent/show/id/rr-2023-12-ana-programmatic-media-supply-chain-transparency-study
351. eMarketer — *5 key stats on ad waste, fraud, MFAs and brand risks* (MFA del 15 % al 4 %). https://www.emarketer.com/content/5-key-stats-ad-waste-fraud-mfas-brand-risks-beyond
352. Imperva — *2024 Bad Bot Report* (los bots, el 49,6 % del tráfico de internet en 2023; bots maliciosos, el 32 %). https://www.imperva.com/company/press_releases/bots-make-up-half-of-all-internet-traffic-globally/
353. Department of Justice (EDNY) — *Two international cybercriminal rings dismantled (Methbot y 3ve)* (noviembre 2018; 1,7 M de ordenadores; >29 M$). https://www.justice.gov/usao-

edny/pr/two-international-cybercriminal-rings-dismantled-and-eight-defendants-indicted-causing
354. Krebs on Security / White Ops — *Report: $3-5M in ad fraud daily from Methbot* (2016; 300 M de visionados/día). https://krebsonsecurity.com/2016/12/report-3-5m-in-ad-fraud-daily-from-methbot/
355. The Record (Recorded Future) — *«King of Fraud» sentenced to 10 years for Methbot/3ve* (Aleksandr Zhukov, 10-nov-2021). https://therecord.media/king-of-fraud-sentenced-to-10-years-in-prison-for-role-in-methbot-3ve-botnet
356. IAB Tech Lab — *ads.txt (Authorized Digital Sellers)* (2017; contra la suplantación de dominios). https://iabtechlab.com/ads-txt/
357. CBS News / Cheq (Roberto Cavazos, Univ. de Baltimore) — *Influencer marketing fraud costs companies $1.3 billion* (2019). https://www.cbsnews.com/news/influencer-marketing-fraud-costs-companies-1-3-billion/
358. Augustine Fou (FouAnalytics) — investigación independiente sobre el fraude publicitario digital. https://www.linkedin.com/pulse/how-do-we-un-fu-digital-advertising-dr-augustine-fou
359. Mandiant / Google Cloud — *M-Trends 2026* (dwell time medio de 14 días en 2025; traspaso de acceso en 22 segundos). https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026
360. MITRE ATT&CK — *T1070 Indicator Removal / T1070.001 Clear Windows Event Logs* (el borrado deja el Event ID 1102). https://attack.mitre.org/techniques/T1070/001/
361. NIST — *SP 800-86: Guide to Integrating Forensic Techniques into Incident Response* (2006; fases forenses y cadena de custodia). https://csrc.nist.gov/pubs/sp/800/86/final
362. IBM — *Cost of a Data Breach 2025* (coste medio global de 4,44 M$ / 10,22 M$ en EE. UU.; 241 días para identificar y contener). https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai
363. Comisión Europea — *NIS2 Directive (UE 2022/2555)* (notificación en 24 h / 72 h; 23 estados en procedimiento de infracción). https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
364. EUR-Lex — *DORA, Reglamento (UE) 2022/2554* (aplicable desde el 17-ene-2025; reporting de incidentes TIC graves). https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
365. U.S. Securities and Exchange Commission — *Cybersecurity disclosure rule* (26-jul-2023; Form 8-K, ítem 1.05, en 4 días hábiles). https://www.sec.gov/newsroom/press-releases/2023-139
366. GDPR-info — *Article 33 GDPR* (notificación de brecha de datos en 72 horas). https://gdpr-info.eu/art-33-gdpr/
367. Global News — *Hamilton cyberattack cost* (la aseguradora deniega la cobertura por MFA incompleto; 18,3 M CAD). https://globalnews.ca/news/11313018/hamilton-cyberattack-cost/
368. Richard Bejtlich (TaoSecurity) — *Mandiant global median dwell time* (dos años consecutivos de deterioro). https://taosecurity.blogspot.com/2026/03/mandiant-global-median-dwell-time.html
369. Carissa Véliz (ed.) — *The Oxford Handbook of Digital Ethics* (Oxford UP, 2022).
370. FedScoop (2024-2025). https://fedscoop.com/ice-wants-more-blockchain-analytics-tech/
371. TJUE — *Sentencia de 4 de mayo de 2023, asunto C-300/21 (UI c. Österreichische Post)* (artículo 82 RGPD: tres condiciones acumulativas —infracción, daño y relación de causalidad; la mera infracción no da derecho a indemnización; el daño inmaterial es indemnizable sin umbral mínimo de gravedad; cuantificación según el derecho nacional con equivalencia y efectividad); análisis de Cuatrecasas, finReg360 y Confilegal. https://www.cuatrecasas.com/es/spain/art/indemnizacion-de-danos-morales-por-infraccion-del-rgpd · https://finreg360.com/alerta/el-tjue-dicta-sentencia-sobre-el-derecho-de-indemnizacion-por-tratamiento-de-datos-personales/ · https://confilegal.com/20230913-el-tjue-admite-que-los-danos-no-materiales-por-el-uso-ilicito-de-datos-personales-merecen-una-compensacion-economica/ · https://www.iberley.es/noticias/tjue-mero-incumplimiento-normativa-proteccion-datos-da-lugar-responsabilidad-pero-solo-dano-probado-resulta-indemnizable-33163
372. RGPD (arts. 33-34: notificación de brechas a la autoridad en 72 h y a los afectados en caso de alto riesgo; art. 82: derecho a indemnización); Have I Been Pwned como herramienta pública de comprobación de filtraciones. Véase el capítulo 57 para el lado de la empresa.
373. t2p — manual de producto (captura de pantalla y de página web certificadas —imagen completa + código fuente; grabación de audio de conversaciones propias; certificar cualquier archivo; proyectos para el diario de un incidente; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión; solo huellas en la cadena). Véanse los capítulos 13 y 15; el SIM-swap, en el capítulo 68; la estafa con datos filtrados, en el capítulo 85.
374. Wikipedia — *2024 Delta Air Lines disruption* / TechTarget — *CrowdStrike outage explained* (19-7-2024: actualización defectuosa de Falcon Sensor; ~8,5 millones de Windows; la caída informática

más grande de la historia; impacto en aerolíneas, hospitales, bancos, emergencias); CNBC — *Delta, CrowdStrike sue each other over widespread IT outage* (Delta: >7.000 vuelos cancelados en cinco días, >1,3 M de pasajeros; demanda de octubre de 2024 por ~550 M$; demandas cruzadas). https://en.wikipedia.org/wiki/2024_Delta_Air_Lines_disruption · https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next · https://www.cnbc.com/2024/10/25/delta-suit-against-crowdstrike-after-it-outage-caused-cancellations.html

375. Reglamento (UE) 2022/2554 (DORA — resiliencia operativa digital del sector financiero: gestión del riesgo TIC de terceros, reporte de incidentes; aplicable desde el 11-1-2025) y Directiva NIS2 (obligaciones ampliadas de notificación de incidentes). Véase el capítulo 57 para el contexto de seguridad y plazos de notificación.
376. t2p — manual de producto (certificar cualquier archivo —solo la huella viaja; captura de página web con imagen completa + código fuente; captura y grabación de pantalla certificadas; proyectos para agrupar el expediente de un incidente; certificación en segundo plano; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; los registros de un ataque, en el capítulo 57; la reclamación de seguro, en el capítulo 28.
377. CNBC — *This $80 million art scam fooled experts* (galería Knoedler; Pei-Shen Qian; <9.000 $ por obra). https://www.cnbc.com/2018/08/16/think-you-can-spot-a-fraud-this-80-million-art-scam-fooled-experts.html
378. The Art Newspaper — *How the detection of titanium white gave away Beltracchi* (2012; el pigmento imposible). https://www.theartnewspaper.com/2012/12/01/how-the-detection-of-titanium-white-gave-away-beltracchi
379. OCCRP — *India sentences notorious antiquities trafficker from Manhattan* (Subhash Kapoor; >2.500 piezas, ~143 M$; Shiva Chola). https://www.occrp.org/en/news/india-sentences-notorious-antiquities-trafficker-from-manhattan
380. Manhattan District Attorney's Office — *Antiquities Trafficking Unit* (~6.000 antigüedades de 29 países, >460 M$ recuperados). https://manhattanda.org/d-a-bragg-announces-return-of-antiquities-to-spain-and-cyprus/
381. The Conversation — *The Gurlitt case: how a routine customs check uncovered a Nazi-era art hoard* (1.406 obras). https://theconversation.com/the-gurlitt-case-how-a-routine-customs-check-uncovered-a-sensational-nazi-era-art-hoard-105604
382. U.S. Department of State — *Washington Conference Principles on Nazi-Confiscated Art* (1998; 44 países). https://www.state.gov/washington-conference-principles-on-nazi-confiscated-art
383. UNESCO — *1970 Convention against the illicit trafficking of cultural property* (~149 estados). https://www.unesco.org/en/fight-illicit-trafficking/about
384. INTERPOL — *Cultural heritage crime: the issues* (comercio ilícito de 225 M$ a 6.000 M$/año). https://www.interpol.int/en/Crimes/Cultural-heritage-crime/The-issues-cultural-property
385. Art Loss Register — *~700.000 objetos registrados; fundado por Julian Radcliffe (1991); >100 M$ recuperados*. https://www.artloss.com/
386. CNN — *The forensic archaeologist hunting trafficked antiquities* (Christos Tsirogiannis; «los papeles mienten»). https://edition.cnn.com/2025/12/13/style/forensic-archaeologist-trafficked-antiquities-scli-intl
387. UNESCO — *New UNESCO report warns that Generative AI threatens Holocaust memory* (junio de 2024, con el Congreso Judío Mundial; ChatGPT y el falso «Holocausto por ahogamiento»; citas de testimonios fabricadas por Bard; simplificación excesiva; recomendaciones a tecnológicas y sistemas educativos); comunicado de prensa en castellano (PDF). https://www.unesco.org/en/articles/new-unesco-report-warns-generative-ai-threatens-holocaust-memory · https://articles.unesco.org/sites/default/files/medias/fichiers/2024/06/PR_New_UNESCO_report_warns_that_Ge
388. Maldita.es — *El papa, Margarita Salas y escenas de la Guerra Civil generadas con IA, en portada: cómo el uso de imágenes falsas en webs y revistas puede desinformar* (25 de febrero de 2025; imágenes sintéticas de hechos y personajes reales publicadas sin etiqueta; alteración de la percepción histórica y desconfianza en los medios). https://maldita.es/malditatecnologia/20250225/imagenes-IA-acontecimientos-reales-desinformar/
389. Forbes — *Internet History Hacked, Wayback Machine Down — 31 Million Passwords Stolen* (octubre de 2024; 7 TB filtrados; token de GitLab expuesto desde finales de 2022; DDoS simultáneo sobre la Wayback Machine); NPR — *Hackers steal information from 31 million Internet Archive*

users; Hispasec — *Internet Archive sufre su segunda brecha* (más de 800.000 tiques de soporte expuestos). https://www.forbes.com/sites/daveywinder/2024/10/10/internet-hacked-wayback-machine-down-31-million-passwords-stolen/ · https://www.npr.org/2024/10/20/nx-s1-5159000/internet-archive-hack-leak-wayback-machine · https://unaaldia.hispasec.com/2024/10/internet-archive-sufre-su-segunda-brecha-de-seguridad-en-octubre-de-2024.html

390. Infobae — *La Ley de Memoria Democrática impulsa la exhumación de fosas y la reparación de 9.000 víctimas: todavía quedan más de 10.000 cuerpos por recuperar* (18 de noviembre de 2025; 8.941 restos localizados y recuperados; solo 70 identificados y entregados; Mapa Integrado de Fosas: 5.848 fosas, ≈1.500 abiertas; Banco Estatal de ADN); El Español — *La nueva Ley de Memoria entra en vigor: el Gobierno quiere exhumar otros 25.000 cadáveres* (octubre de 2022). https://www.infobae.com/espana/2025/11/18/la-ley-de-memoria-democratica-impulsa-la-exhumacion-de-fosas-y-la-reparacion-de-9000-victimas-todavia-quedan-mas-de-10000-cuerpos-por-recuperar/ · https://www.elespanol.com/espana/20221020/nueva-ley-memoria-gobierno-quiere-exhumar-cadaveres/712178865_0.html
391. t2p — manual de producto (huella SHA-512 en el origen; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; manifiestos por lotes; contenido en los sistemas de cada archivo, solo huellas en la cadena). Véanse los capítulos 13 y 15; los comunicados oficiales, en el capítulo 86; la evidencia de crímenes de guerra, en el capítulo 20.
392. EUR-Lex — *Directiva (UE) 2019/1937 sobre la protección de los denunciantes* (confidencialidad de la identidad; canales seguros; plazos). https://eur-lex.europa.eu/eli/dir/2019/1937/oj/eng
393. eucrim — *ECJ orders several member states to financial penalties for failing to transpose the Whistleblowers Directive* (marzo de 2025; ~39 M€; Alemania 34 M€; Estonia 500.000 € + 1.500 €/día). https://eucrim.eu/news/ecj-ordered-several-member-states-to-financial-penalties-for-failing-to-transpose-whistleblowers-directive/
394. Freedom of the Press Foundation — *SecureDrop* (más de 60 redacciones; servicio oculto de Tor; protección arquitectónica de la fuente). https://securedrop.org/overview/
395. ICIJ — *Panama Papers* (11,5 millones de documentos; 2,6 TB; >350 periodistas; la fuente «John Doe»). https://www.icij.org/investigations/panama-papers/
396. OCCRP — *John Doe: «The Revolution Will Be Digitized»* (manifiesto de la fuente de los Panama Papers). https://www.occrp.org/en/investigation/panama-papers-source-john-doe-the-revolution-will-be-digitized
397. Errata Security (Robert Graham) — *How The Intercept outed Reality Winner* (puntos de rastreo de la impresora; serie 29535218; 9-mayo-2017, 6:20). https://blog.erratasec.com/2017/06/how-intercept-outed-reality-winner.html
398. Freedom of the Press Foundation — *Reality Winner sentenced to 63 months* (la pena más larga en EE. UU. para una fuente de prensa). https://freedom.press/issues/whistleblower-reality-winner-sentenced-longest-prison-sentence-history-federal-leak-cases/
399. Electronic Frontier Foundation (EFF) — *List of printers which do or do not display tracking dots* (código de identificación de la máquina). https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots
400. Wikipedia — *Stylometry / Adversarial stylometry* (atribución de autoría con un 80-95 % de precisión). https://en.wikipedia.org/wiki/Stylometry
401. Wikipedia — *Frances Haugen* (filtración de Facebook; decidió revelar su identidad). https://en.wikipedia.org/wiki/Frances_Haugen
402. Carissa Véliz — *The Ethics of Privacy and Surveillance* (Oxford UP, 2024).
403. Nature (Richard Van Noorden) — *More than 10,000 research papers were retracted in 2023 — a new record* (Hindawi/Wiley, >8.000). https://www.nature.com/articles/d41586-023-03974-8
404. Elisabeth Bik, Arturo Casadevall y Ferric Fang — *The Prevalence of Inappropriate Image Duplication in Biomedical Research Publications* (mBio, 2016; 20.621 artículos, 3,8 %). https://journals.asm.org/doi/10.1128/mbio.00809-16
405. American Society for Microbiology / mBio — *Piloto de ImageTwin* (2.627 manuscritos; 410 con problemas de imagen; 6 aceptaciones revocadas). https://journals.asm.org/doi/10.1128/mbio.01990-25
406. U.S. Department of Justice — *Dana-Farber Cancer Institute agrees to pay $15M to settle fraud allegations* (imágenes/datos tergiversados en subvenciones a los NIH). https://www.justice.gov/opa/pr/dana-farber-cancer-institute-agrees-pay-15m-settle-fraud-allegations-related-scientific

407. Stanford Board of Trustees — *Report on the scientific work of Marc Tessier-Lavigne* (2023; dimisión del presidente). https://boardoftrustees.stanford.edu/news/board-trustees-statement-release-report-and-announcements
408. American Physical Society — *The Schön scandal* (comité Beasley; mala conducta en 16 de 24 cargos). https://www.aps.org/apsnews/2022/08/september-2002-schon-scandal-report
409. Retraction Watch (Ivan Oransky y Adam Marcus) — *The new retraction record holder* (Joachim Boldt, 184 retractaciones, julio de 2023). https://retractionwatch.com/2023/07/12/the-new-retraction-record-holder-is-a-german-anesthesiologist-with-184/
410. Ben Goldacre et al. (COMPare, Universidad de Oxford) — *COMPare: outcome-switching en ensayos clínicos* (Trials, 2019; 76,3 % de desenlaces primarios bien reportados). https://pmc.ncbi.nlm.nih.gov/articles/PMC6375128/
411. Center for Open Science (Brian Nosek) — *Registered Reports* (de 91 a más de 300 revistas; el protocolo antes de los resultados). https://www.cos.io/initiatives/registered-reports
412. eLife — *Reproducibility Project: Cancer Biology* (Amgen, 11 % de 53 estudios; efectos replicados un 85 % más pequeños). https://elifesciences.org/articles/71601
413. Wikipedia (con BBC / AFP / Japan Times) — *Sogen Kato* (momificado 32 años; pensión de supervivencia cobrada; ~9,5 M de yenes). https://en.wikipedia.org/wiki/Sogen_Kato
414. France 24 — *Over 230,000 listed centenarians missing in Japan* (234.354 sin confirmar; 77.118 con 120+ años). https://www.france24.com/en/20100910-over-230000-listed-centenarians-missing-presumed-dead-government-report-japan
415. SSA Office of the Inspector General — *State death report discrepancies led to $327M in improper payments* (2025) y *6,5 M de titulares de ≥112 años sin fecha de defunción en el Numident* (2015). https://oig.ssa.gov/news-releases/2025-03-19-state-death-report-discrepancies-led-to-327m-in-improper-payments-and-cost-ssa-millions-of-dollars-in-unnecessary-workloads/
416. Reuters (vía HuffPost) — *Greece stops pensions and benefits for 200,000 people* (~9.000 «centenarios»; hasta 800 M€/año de ahorro). https://www.huffpost.com/entry/greece-stops-pensions-benefits-200000-people-fraudulently_n_1451423
417. Moneyweb — *SASSA explains why it paid R140m in grants to 75,000 dead people* (2025; el 75 % del fraude, de funcionarios, según el IEJ). https://www.moneyweb.co.za/news/south-africa/sassa-explains-why-it-paid-r140m-in-grants-to-75-000-dead-people/
418. Outlook Money — *Jeevan Pramaan: digital life certificate* (~19 M de certificados; ~11,5 M por autenticación facial). https://www.outlookmoney.com/retirement/digital-life-certificate-over-14-million-super-seniors-generated-online-jeevan-pramaan-patra-in-fy25-26
419. The Wire (India) — *Digital Exclusion: Poor, Elderly Face the Brunt of Aadhaar-Based Authentication Errors* (huellas desgastadas; pensiones denegadas; huella no obligatoria). https://m.thewire.in/article/rights/digital-exclusion-poor-elderly-face-the-brunt-of-aadhaar-based-authentication-errors
420. GOV.UK (DWP) — *State Pension underpayments (operación LEAP)* (119.050 pagos insuficientes, 736 M£; >15.000 ya muertos). https://www.gov.uk/government/publications/state-pension-underpayments-progress-on-cases-reviewed-to-30-september-2024/state-pension-underpayments-progress-on-cases-reviewed-to-30-september-2024
421. International Social Security Association (ISSA) — *Proof of life in international social security* y la buena práctica VIVESS (pensionistas españoles en el extranjero). https://www.issa.int/analysis/proof-life-international-social-security-progress-and-persistent-challenges
422. Consultor Jurídico (Conjur, Brasil) — *Deepfakes, provas digitais e fraudes no INSS: o colapso da confiança* (2025). https://www.conjur.com.br/2025-mai-28/deepfakes-provas-digitais-e-fraudes-no-inss-colapso-da-confianca/
423. CNN en Español — *Una mujer cree que estafadores clonaron la voz de su hija en un falso secuestro* (caso Jennifer DeStefano, Arizona; llamada del 20 de enero cerca de las 16:55; hija de 15 años en una competición; rescate de 1 millón rebajado a 50.000 dólares; «la voz era tan real»; testimonio posterior ante un subcomité del Senado de EE. UU.); La Opinión — *Utilizan voz recreada por inteligencia artificial para fingir el secuestro de una niña y pedir rescate*. https://cnnespanol.cnn.com/2023/04/29/una-mujer-cree-que-los-estafadores-clonaron-la-voz-de-su-hija-en-un-falso-secuestro-trax/ · https://laopinion.com/2023/04/29/utilizan-voz-recreada-por-inteligencia-artificial-para-fingir-el-secuestro-de-una-nina-y-pedir-rescate/
424. FBI — *'Virtual Kidnapping' Extortion Calls on the Rise* (mecánica de la estafa; números internacionales; impedimento de contacto; rescate por transferencia; recomendaciones: calma, contactar por otra vía, preguntas que solo la persona real sabe responder); FBI Albuquerque — *Be*

on the Lookout for Virtual Kidnapping Scams. https://www.fbi.gov/contact-us/field-offices/sanantonio/news/press-releases/virtual-kidnapping-extortion-calls-on-the-rise · https://www.fbi.gov/contact-us/field-offices/albuquerque/news/press-releases/fbi-media-alert-be-on-the-lookout-for-virtual-kidnapping-scams

425. FBI / IC3 — *Criminals Using Altered Proof-of-Life Media to Extort Victims in Virtual Kidnapping for Ransom Scams* (alerta de 2025: fotos y vídeos alterados o generados con IA como falsa «prueba de vida», a menudo a partir de imágenes públicas; incoherencias como tatuajes o cicatrices ausentes; denuncia en ic3.gov con el material recibido); Axios — *AI-generated videos, photos used in new virtual kidnapping scams, FBI warns* (5 de diciembre de 2025). https://www.fbi.gov/investigate/cyber/alerts/2025/criminals-using-altered-proof-of-life-media-to-extort-victims-in-virtual-kidnapping-for-ransom-scams · https://www.axios.com/2025/12/05/ai-videos-photos-scam-virtual-fbi-victim-ransom-kidnapping
426. t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; prueba de vida con reto y frescura —nonce imprevisible respondido y sellado al minuto; rastro voluntario con momentos elegidos; ningún registro central; revocabilidad). Véanse los capítulos 13, 15 y 64; la voz clonada, en el capítulo 68.
427. La Moncloa / Ministerio del Interior — *Las Fuerzas de Seguridad investigaron la desaparición de 16.147 personas en 2024* (+6 %; el 72 % de los casos esclarecidos en menos de una semana; CNDES pionero en Europa); Ministerio del Interior — *Las Fuerzas de Seguridad investigaron la desaparición de 16.024 personas en 2025 y esclarecieron el 91 por ciento de las denuncias* (25.086 denuncias; 928 alertas publicadas, 132 activas; 11.461 episodios únicos, media de 3 denuncias en reincidentes). https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/paginas/2025/170325-marlaska-plan-personas-desaparecidas.aspx · https://www.interior.gob.es/opencms/es/detalle/articulo/Las-Fuerzas-de-Seguridad-investigaron-la-desaparicion-de-16.024-personas-en-2025-y-esclarecieron-el-91-por-ciento-de-las-denuncias/
428. Wikipedia (síntesis del *Informe McLaren*) — *McLaren Report* (≥643 positivos «desaparecidos»; ADN masculino en muestras femeninas). https://en.wikipedia.org/wiki/McLaren_Report
429. World Anti-Doping Agency — *Independent investigation confirms Russian state manipulation of doping control* (McLaren, Persona Independiente; >1.000 atletas). https://www.wada-ama.org/en/news/wada-statement-independent-investigation-confirms-russian-state-manipulation-doping-control
430. CNN — *WADA McLaren report: tampered samples* (44 muestras con marcas en los tapones, 12 de medallistas; Parte 2, 2016). https://www.cnn.com/2016/12/09/sport/wada-russia-doping-mclaren-report
431. Chemistry World — *Anti-doping scientists expose cheating Russian athletes* (8 muestras con sal fisiológicamente imposible). https://www.chemistryworld.com/news/anti-doping-scientists-expose-cheating-russian-athletes/2500159.article
432. Republik — *Bad bottles* (las botellas «inviolables» Berlinger, vulneradas). https://www.republik.ch/2018/02/21/bad-bottles
433. World Anti-Doping Agency — *Athlete Biological Passport* (detección indirecta; módulo hematológico 2009, esteroideo 2014). https://www.wada-ama.org/en/athlete-biological-passport
434. ESPN — *Pellizotti banned in landmark biological-passport ruling* (2 años sin positivo; primer caso validado por el TAS). https://www.espn.com/olympics/cycling/news/story?id=6192949
435. Europol — *Results from the largest football match-fixing investigation in Europe (Operation VETO)* (>380 partidos; 425 personas; >15 países). https://www.europol.europa.eu/media-press/newsroom/news/update-results-largest-football-match-fixing-investigation-in-europe
436. Sportradar — *Betting Corruption and Match-Fixing 2024* (>850.000 partidos; 1.108 sospechosos; sistema UFDS). https://sportradar.com/content-hub/news/sportradar-reports-notable-decline-in-match-fixing-in-2024/
437. The Washington Post — *Grigor Sargsyan, «the Maestro», and tennis match-fixing* (5 años; ~180 tenistas de >35 países; ~7 M€). https://www.washingtonpost.com/world/interactive/2023/tennis-match-fixing-itf-grigor-sargsyan/
438. U.S. Department of Justice / SDNY (vía Music Business Worldwide) — *North Carolina man pleads guilty to AI-assisted music streaming fraud* (Michael Smith; decomiso de 8,09 M$). https://www.musicbusinessworldwide.com/streaming-fraud-man-who-pocketed-8m-using-hundreds-of-thousands-of-ai-songs-streamed-billions-of-times-by-bots-pleads-guilty/

439. Rolling Stone — *Inside the AI streaming-fraud case* (de 1.040 a 10.000 cuentas-bot; 661.440 reproducciones/día; los correos). https://www.rollingstone.com/music/music-features/streaming-fraud-fake-streams-mike-smith-1235500686/
440. Beatdapp / Music Business Worldwide — *Streaming fraud costs the global music industry ~$2bn a year* (≥10 % de la actividad; estimación de parte). https://www.musicbusinessworldwide.com/streaming-fraud-costs-the-global-music-industry-2bn-a-year-according-to-beatdapp-now-its-partnering-with-beatport-to-combat-the-trend/
441. Spotify / Music Business Worldwide — *The 1,000-stream royalty threshold* (anunciado nov-2023; vigente abr-2024). https://www.musicbusinessworldwide.com/heres-exactly-spotifys-new-1000-annual-streams-royalty-policy-works123/
442. The MLC / Billboard — *Mechanical Licensing Collective receives over $424 million in unmatched royalties* (la «caja negra»). https://www.billboard.com/pro/mechanical-licensing-collective-receives-over-424-million-unmatched-royalties-streaming-services/
443. IFPI — *Global Music Report 2026* (31.700 M$; streaming >22.000 M$, el 69,6 %; «theft, plain and simple»). https://www.ifpi.org/global-music-report-2026-global-recorded-music-revenues-grow-6-4-as-record-companies-drive-innovation/
444. IFPI (Victoria Oakley) — *Brazilian authorities disrupt JustAnotherPanel* («fake streams… erode trust in our system»). https://www.ifpi.org/brazilian-authorities-launch-largest-ever-disruption-operation-against-major-streaming-fraud-platform-justanotherpanel/
445. Federal Trade Commission — *FTC brings first-ever cases under the BOTS Act* (2021; >150.000 entradas; >31 M$ en sanciones). https://www.ftc.gov/news-events/news/press-releases/2021/01/ftc-brings-first-ever-cases-under-bots-act
446. Federal Trade Commission — *FTC sues Live Nation/Ticketmaster* (2025; 5 revendedores, 6.345 cuentas, 246.407 entradas; «turn a blind eye as a matter of policy»). https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-sues-live-nation-ticketmaster-engaging-illegal-ticket-resale-tactics-deceiving-artists-consumers
447. Wikipedia — *Taylor Swift–Ticketmaster controversy* (gira Eras; 3.500 M de peticiones; ~12 M de «entidades» con bots). https://en.wikipedia.org/wiki/Taylor_Swift%E2%80%93Ticketmaster_controversy
448. FBI Internet Crime Complaint Center (IC3) — *2023 Internet Crime Report* (SIM-swapping: 1.075 denuncias, 48,8 M$ de pérdidas). https://www.ic3.gov/AnnualReport/Reports
449. NPR — *The AI deepfake Biden robocall and the FCC* (Nuevo Hampshire; Steve Kramer; multa de 6 M$). https://www.npr.org/2024/05/23/nx-s1-4977582/fcc-ai-deepfake-robocall-biden-new-hampshire-political-operative
450. Federal Communications Commission — *FCC makes AI-generated voices in robocalls illegal* (Declaratory Ruling, febrero de 2024). https://www.fcc.gov/document/fcc-makes-ai-generated-voices-robocalls-illegal
451. Federal Communications Commission — *FCC settles Lingo Telecom robocall investigation* (1 M$; STIR/SHAKEN + conocer al cliente y al proveedor). https://www.fcc.gov/document/fcc-settles-lingo-telecom-robocall-investigation
452. TransNexus — *SHAKEN statistics, April 2025* (solo el 42,5 % de llamadas firmadas; la brecha no-IP). https://transnexus.com/blog/2025/shaken-statistics-april/
453. Cifas — *Fraudscape 2025* (+1.055 % de SIM-swaps no autorizados en el Reino Unido). https://www.cifas.org.uk/newsroom/huge-surge-see-sim-swaps-hit-telco-and-mobile
454. SecurityWeek — *T-Mobile coughed up $33 million in SIM-swap lawsuit* (Josh Jones; ~38 M$ en criptomonedas). https://www.securityweek.com/t-mobile-coughed-up-33-million-in-sim-swap-lawsuit/
455. Federal Trade Commission — *Winners of the Voice Cloning Challenge (OriginStory)* (autenticar el origen humano de la voz en el punto de creación). https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-announces-winners-voice-cloning-challenge
456. GSMA — *Open Gateway / Mobile Identity APIs (SIM Swap API)* (la defensa migra a la capa de red). https://www.gsma.com/solutions-and-impact/technologies/mobile-identity/mobile-identity-and-data-apis/
457. The Next Web / The Wall Street Journal — *Fraudsters deepfake a CEO's voice* (2019; ~243.000 $; primer fraude de voz sintética conocido). http://thenextweb.com/news/fraudsters-deepfake-ceos-voice-to-trick-manager-into-transferring-243000
458. Payment Systems Regulator (Reino Unido) — *APP fraud reimbursement protections* (régimen obligatorio desde el 7-10-2024, primero del mundo; particulares, microempresas y entidades benéficas; Faster Payments y CHAPS; límite 85.000 £ —rebajado de 415.000 para alinearlo con el

FSCS; coste compartido 50/50 entre proveedor emisor y receptor; reembolso en 5 días hábiles o hasta 35 con investigación; sustituye el código voluntario CRM); análisis de Freshfields, A&O Shearman y Thomson Reuters. https://www.psr.org.uk/information-for-consumers/app-fraud-reimbursement-protections/ · https://www.freshfields.com/en/our-thinking/briefings/2024/09/authorised-push-payment-fraud-a-new-mandatory-reimbursement-regime-for-uk-psps/ · https://www.aoshearman.com/en/insights/ao-shearman-on-fintech-and-digital-assets/the-uks-authorised-push-payment-app-fraud-reimbursement-scheme · https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/app-fraud-uk/

459. PSD2 (Directiva (UE) 2015/2366, transpuesta en España por el RDL 19/2018): en operaciones de pago no autorizadas, devolución por parte del proveedor salvo fraude o negligencia grave del cliente; carga de la prueba de la autenticación correcta sobre el proveedor; autenticación reforzada (SCA); reforma europea de los pagos (PSD3/PSR) en tramitación.
460. t2p — manual de producto (grabación de audio de conversaciones propias; captura de pantalla y de página web certificadas —imagen completa + código fuente; certificar cualquier fichero por lotes; proyectos para el expediente de un incidente; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión; solo huellas en la cadena). Véanse los capítulos 13 y 15; la voz clonada y la SIM, en el capítulo 68; el CFO suplantado, en el capítulo 87; la caja negra personal, en el capítulo 75.
461. U.S. Senate Committee on Armed Services — *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain* (2012; >1 M de piezas; >70 % rastreadas a China; THAAD; Hong Dark). https://www.armed-services.senate.gov/press-releases/senate-armed-services-committee-releases-report-on-counterfeit-electronic-parts
462. U.S. Government Accountability Office — *DOD Supply Chain: Suspect Counterfeit Electronic Parts on Internet Platforms* (GAO-12-375; 16 de 16 piezas falsas). https://www.gao.gov/products/gao-12-375
463. Center for Public Integrity — *Counterfeit chips plague Pentagon weapons systems* (VisionTech; el abrillantador en los chips; McCloskey, 38 meses). https://publicintegrity.org/national-security/counterfeit-chips-plague-pentagon-weapons-systems/
464. Air & Space Forces Magazine — *C-27J and C-130J parts linked to counterfeit mills* (L-3; pantalla en blanco; defectos del 27 %). https://www.airandspaceforces.com/c-27jandc-130jpartslinkedtocounterfeitmills/
465. Semiconductor Industry Association — *Winning the battle against counterfeit semiconductor products* (>7.500 M$/año; ~11.000 puestos de trabajo). https://www.semiconductors.org/resources/winning-the-battle-against-counterfeit-semiconductor-products/
466. ERAI — *2024 Annual Report* (1.055 piezas sospechosas; el máximo desde 2015). https://www.erai.com/erai_blog/3187/_2024_annual_report
467. U.S. Department of Justice (NDCA) — *Steve H.S. Kim sentenced for selling $3.5M in counterfeit and substandard parts* (42 meses; submarino nuclear, sistema de misiles). https://www.justice.gov/usao-ndca/pr/california-resident-steve-hs-kim-sentenced-selling-35m-counterfeit-and-substandard
468. SAE International — *AS6171: test methods for suspect/counterfeit EEE parts* (laboratorios acreditados ISO/IEC 17025). https://www.sae.org/standards/content/as6171/7/
469. CALCE (University of Maryland) — *Counterfeit electronics detection and avoidance* (un chip reciclado puede parecer idéntico al auténtico). https://calce.umd.edu/counterfeit-electronics-detection-and-avoidance
470. Defense Microelectronics Activity (DMEA) — *Trusted Foundry / Trusted IC* (proveedores de confianza con pedigrí controlado; 2003, con la NSA). https://www.dmea.osd.mil/TrustedIC.aspx
471. Wikipedia — *XZ Utils backdoor* (CVE-2024-3094; CVSS 10,0; Andres Freund, ingeniero de Microsoft y desarrollador de PostgreSQL, investigando ~500 ms de latencia extra en SSH; report a Openwall el 28-29 de marzo de 2024; campaña de ingeniería social de «Jia Tan» con cuentas falsas presionando al mantenedor; código oculto en build-to-host.m4 y ficheros de test binarios dentro de los tarballs —invisible a la revisión del repositorio; potencial superior a SolarWinds; cazado antes del despliegue masivo); Akamai — *XZ Utils Backdoor — Everything You Need to Know*; JFrog — *XZ Backdoor Attack CVE-2024-3094*; Datadog Security Labs — *The XZ Utils backdoor*. https://en.wikipedia.org/wiki/XZ_Utils_backdoor · https://www.akamai.com/blog/security-research/critical-linux-backdoor-xz-utils-discovered-what-to-know · https://jfrog.com/blog/xz-

backdoor-attack-cve-2024-3094-all-you-need-to-know/ · https://securitylabs.datadoghq.com/articles/xz-backdoor-cve-2024-3094/

472. Palo Alto Unit 42 — *«Shai-Hulud» Worm Compromises npm Ecosystem in Supply Chain Attack* (14 de septiembre de 2025; primer gusano autorreplicante en npm; >500 paquetes; @ctrl/tinycolor con >2,2 millones de descargas semanales; paquetes de CrowdStrike; cosecha de credenciales AWS/GCP/Azure con TruffleHog; persistencia vía GitHub Actions; propagación con los derechos de publicación de los mantenedores); CISA — *Widespread Supply Chain Compromise Impacting npm Ecosystem* (alerta del 23 de septiembre de 2025); StepSecurity — *Shai-Hulud: Self-Replicating Worm Compromises 500+ NPM Packages*; Datadog — *The Shai-Hulud 2.0 npm worm* (segunda oleada, noviembre). https://unit42.paloaltonetworks.com/npm-supply-chain-attack/ · https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem · https://www.stepsecurity.io/blog/ctrl-tinycolor-and-40-npm-packages-compromised · https://securitylabs.datadoghq.com/articles/shai-hulud-2.0-npm-worm/
473. Sigstore — *Rekor: Software Supply Chain Transparency Log* (registro público append-only; >101 millones de entradas de >33.000 proyectos: Kubernetes, CPython, Istio, urllib3; método de firma por defecto para Kubernetes, npm, Maven y PyPI; atestaciones de procedencia en npm y PyPI); OpenSSF / Trail of Bits — *Catching malicious package releases using a transparency log* (diciembre de 2025; monitorización de Rekor para detectar publicaciones fraudulentas con credenciales robadas). https://docs.sigstore.dev/logging/overview/ · https://www.sigstore.dev/ · https://openssf.org/blog/2025/12/19/catching-malicious-package-releases-using-a-transparency-log/ · https://blog.trailofbits.com/2025/12/12/catching-malicious-package-releases-using-a-transparency-log/
474. DOUE / BOE — *Reglamento (UE) 2024/2847, de 23 de octubre de 2024* (Cyber Resilience Act: requisitos horizontales de ciberseguridad para productos con elementos digitales; en vigor en diciembre de 2024; obligaciones de notificación desde el 11 de septiembre de 2026; aplicación plena el 11 de diciembre de 2027; seguridad durante todo el ciclo de vida); Atalaya GRC — *CRA: fechas y obligaciones*; Red Seguridad — *Cyber Resilience Act: una nueva era para los fabricantes*. https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81720 · https://atalayagrc.com/normativas/cra/ · https://www.redseguridad.com/especialidades-tic/normativa-y-certificacion/cyber-resilience-act-cra-una-nueva-era-para-los-fabricantes_20260204.html
475. t2p — manual de producto (huella SHA-512; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; huellas de versiones y manifiestos por lotes; anclaje neutral y transversal, complementario a los registros de transparencia sectoriales). Véanse los capítulos 13 y 15; el pedigrí del hardware, en el capítulo 70; los registros imborrables, en el capítulo 57.
476. Agnew et al. (PLOS ONE) — *Estimating the worldwide extent of illegal fishing* (11-26 millones de toneladas; 10.000-23.500 M$/año). https://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0004570
477. Oceana — *Oceana study reveals seafood fraud nationwide* (33 % mal etiquetado; «red snapper» 87 %). https://oceana.org/reports/oceana-study-reveals-seafood-fraud-nationwide/
478. Global Fishing Watch / Nature — *Satellite mapping reveals extensive industrial activity at sea* (~75 % de barcos sin rastreo público). https://globalfishingwatch.org/press-release/new-research-harnesses-ai-and-satellite-imagery-to-reveal-the-expanding-footprint-of-human-activity-at-sea/
479. Comisión Europea — *Illegal fishing (IUU): catch certificates y CATCH* (Reg. (CE) 1005/2008; CATCH obligatorio desde el 10-ene-2026). https://oceans-and-fisheries.ec.europa.eu/fisheries/rules/illegal-fishing_en
480. Global Witness — *The ITSCI Laundromat* (hasta el 80-90 % de mineral «limpio» procedente de fuentes ilícitas). https://www.globalwitness.org/en/campaigns/natural-resource-governance/itsci-laundromat/
481. Kimberley Process / World Diamond Council — *The Kimberley Process fact sheet* (de ~15 % en los años 90 a <1 %; ~99 % de la producción). https://www.worlddiamondcouncil.org/wp-content/uploads/2022/02/The-Kimberley-Process-Fact-Sheet.pdf
482. Environmental Justice Foundation — *Thailand's Seafood Slaves* (esclavitud a bordo; la isla de Benjina). https://ejfoundation.org/reports/thailands-seafood-slaves
483. Science Advances (Park et al.) — *Illuminating Dark Fishing Fleets in North Korea* (>900 barcos; >164.000 t; >440 M$). https://www.science.org/doi/10.1126/sciadv.abb1197
484. Ledger Insights — *Everledger bankruptcy* (el riesgo de centralizar la trazabilidad de diamantes en una sola empresa). https://www.ledgerinsights.com/everledger-bankruptcy-esg-blockchain-

traceability/
485. The Africa Report — *Rubaya coltan mine at the heart of M23 financing* (~800.000 $/mes para un grupo armado). https://www.theafricareport.com/375904/drc-rwanda-rubaya-coltan-mine-at-the-heart-of-m23-financing/
486. ProPublica / NPR (Justin Elliott y Laura Sullivan) — *How the Red Cross raised half a billion dollars for Haiti and built six homes* (2015). https://www.propublica.org/article/how-the-red-cross-raised-half-a-billion-dollars-for-haiti-and-built-6-homes
487. Federal Trade Commission — *FTC, all 50 states and D.C. charge four cancer charities with bilking over $187 million* (familia Reynolds; <3 % a los pacientes). https://www.ftc.gov/news-events/news/press-releases/2015/05/ftc-all-50-states-dc-charge-four-cancer-charities-bilking-over-187-million-consumers
488. FBI Internet Crime Complaint Center — *PSA: charity and disaster-relief fraud* (2024; ~96 M$; la IA aumenta la legitimidad aparente). https://www.ic3.gov/PSA/2025/PSA250116
489. New York Attorney General (Letitia James) — *Pennies for Charity 2025* (los captadores se quedan el 25 %; <50 % en la mitad de campañas). https://ag.ny.gov/press-release/2025/attorney-general-james-releases-annual-pennies-charity-report
490. CBS News — *CBS News investigates Wounded Warrior Project spending* (de 1,7 a 26 M$ en conferencias; directivos destituidos en marzo de 2016). https://www.cbsnews.com/news/cbs-news-investigates-wounded-warrior-project-spending/
491. GuideStar, Charity Navigator y BBB Wise Giving Alliance — *The Overhead Myth* (2013; el overhead, mal indicador). https://learn.guidestar.org/news/news-releases/2013/2013-06-17-overhead-myth
492. GiveWell — *How much does it cost to save a life?* (entre ~3.000 y 5.500 $ por vida). https://www.givewell.org/how-much-does-it-cost-to-save-a-life
493. CharityWatch (Daniel Borochoff) — *Our charity rating process* (≥75 % a programa; ≤25 $ por recaudar 100 $). https://www.charitywatch.org/our-charity-rating-process
494. CBS News / Patrick Radden Keefe (*Empire of Pain*) — *The Met removes the Sackler name* (la filantropía como «reputation laundering»). https://www.cbsnews.com/news/metropolitan-museum-of-art-sackler-family-name-removed-purdue-pharma/
495. Federal Trade Commission — *Reported fraud losses hit $12.5 billion in 2024* (contexto del fraude). https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024
496. NPR — *Tesla ordered to pay $243 million in fatal Autopilot crash* (Benavides contra Tesla; 200 M$ en daños punitivos; 33 % de responsabilidad). https://www.npr.org/2025/08/02/nx-s1-5490930/tesla-autopilot-crash-jury-240-million-florida
497. Electrek — *Tesla withheld data and misdirected police in Autopilot crash* (la instantánea de colisión a +3 min; la imagen NAND; el perito Alan Moore). https://electrek.co/2025/08/04/tesla-withheld-data-lied-misdirected-police-plaintiffs-avoid-blame-autopilot-crash/
498. National Transportation Safety Board — *Collision Between an Uber ATG Test Vehicle and a Pedestrian (HAR-19-03)* (5,6 s; frenado de emergencia desactivado). https://www.ntsb.gov/investigations/Pages/HWY18MH010.aspx
499. California DMV — *Statement on Cruise LLC suspension* (24-oct-2023; el metraje del arrastre, omitido). https://www.dmv.ca.gov/portal/news-and-media/dmv-statement-on-cruise-llc-suspension/
500. National Transportation Safety Board — *Cockpit Voice Recorders and Flight Data Recorders* (supervivencia; ≥88 parámetros). https://www.ntsb.gov/news/Pages/cvr_fdr.aspx
501. Federal Register / FAA — *25-hour Cockpit Voice Recorder requirement for new aircraft* (2026; de 2 a 25 horas). https://www.federalregister.gov/documents/2026/02/02/2026-02110/25-hour-cockpit-voice-recorder-cvr-requirement-new-aircraft-production
502. eCFR — *49 CFR Part 563: Event Data Recorders* (captura pre-choque de 5 s a 20 s a 10 Hz). https://www.ecfr.gov/current/title-49/subtitle-B/chapter-V/part-563
503. DroneXL — *Drone pilot sentenced over Cape Canaveral Space Force base flights* (los registros de geofencing contradicen al operador). https://dronexl.co/2025/08/28/drone-pilot-sentenced-cape-canaveral-space-force-base/
504. CNN — *Jeju Air black boxes stopped recording before the crash* (los 4 minutos decisivos, fuera de la caja). https://www.cnn.com/2025/01/11/asia/south-korean-airline-black-boxes-stopped-recording-intl-hnk/index.html
505. National Transportation Safety Board — *EgyptAir 990 Aircraft Accident Brief (AAB-02/01)* (los mismos datos, causas opuestas). https://www.ntsb.gov/investigations/AccidentReports/Reports/AAB0201.pdf

506. Euronews — *Un fallo informático en las pulseras antimaltrato en España absuelve a decenas de agresores* (18 de septiembre de 2025; migración Telefónica → UTE Vodafone+Securitas; datos anteriores al 20 de marzo de 2024 inaccesibles; memoria de la Fiscalía General del Estado; ≈4.500 pulseras activas). https://es.euronews.com/2025/09/18/un-fallo-informatico-en-las-pulseras-antimaltrato-en-espana-absuelve-a-decenas-de-agresore
507. Diario Socialista — *Fallo en pulseras «antimaltrato» provoca absoluciones y pérdida de pruebas en casos de violencia machista* (18 de septiembre de 2025; «numerosas absoluciones y sobreseimientos provisionales»). https://diariosocialista.net/2025/09/18/fallo-en-pulseras-antimaltrato-provoca-absoluciones-y-perdida-de-pruebas-en-casos-de-violencia-machista/
508. OKDiario — *El Gobierno reconoce ahora que conocía desde «enero de 2024» los fallos en las pulseras antimaltrato*. https://okdiario.com/espana/pulseras-gobierno-reconoce-ahora-que-sabia-desde-enero-2024-fallos-pulseras-antimaltrato-15967835
509. La Nación (agencias) — *Redondo aborda en el Senado la gestión de pulseras para maltratadores tras ser reprobada en el Congreso* (septiembre de 2025; disculpas a las víctimas; posibles penalizaciones al contratista). https://www.lanacion.com.ar/agencias/redondo-aborda-este-miercoles-en-el-senado-la-gestion-de-pulseras-para-maltratadores-tras-ser-nid28092025/
510. Hay Derecho — Nuria Barona Martínez, *Pulseras antimaltrato: análisis jurídico y político de un sistema en crisis* (8 de octubre de 2025). https://www.hayderecho.com/2025/10/08/pulseras-antimaltrato-analisis-juridico-politico/
511. Tribunal Constitucional — *STC 114/1984, de 29 de noviembre* (grabar una conversación propia no vulnera el art. 18.3 CE; admisible como prueba documental; límite de la esfera íntima; origen laboral del caso). https://hj.tribunalconstitucional.es/es/Resolucion/Show/367 · https://www.boe.es/buscar/doc.php?id=BOE-T-1984-27955
512. Legal Today — *La grabación de las conversaciones entre particulares y su manifestación jurisprudencial* (doctrina consolidada del TS sobre grabaciones de participantes); Iberley — *La validez de las grabaciones privadas aportadas como prueba en el proceso penal*. https://www.legaltoday.com/practica-juridica/derecho-penal/penal/la-grabacion-de-las-conversaciones-entre-particulares-y-su-manifestacion-jurisprudencial-2014-08-14/ · https://www.iberley.es/revista/la-validez-las-grabaciones-privadas-aportadas-como-prueba-proceso-penal-1221
513. Gerson Vidal (abogados) — *¿Es delito grabar una conversación sin consentimiento?* (art. 197.1 CP: prisión de 1 a 4 años y multa de 12 a 24 meses; difusión: 2 a 5 años); Noticias Jurídicas — *Voces ocultas: la delgada línea entre grabar legalmente y cometer un delito*. https://www.gersonvidal.com/blog/delito-grabar-conversacion/ · https://noticias.juridicas.com/conocimiento/tribunas/18542-voces-ocultas:-la-delgada-linea-entre-grabar-legalmente-y-cometer-un-delito-/
514. Digital Perito — *Clonación de voz: deepfakes de audio y detección forense* (clones convincentes con 3-5 minutos de audio; algunos sistemas con 30 segundos; análisis de espectrogramas y prosodia). https://digitalperito.es/glosario/clonacion-voz/
515. Economist & Jurist — *La prueba sintética en el proceso judicial: retos probatorios de los deepfakes* (impugnar desplaza la carga; el TS exige impugnación técnica, no genérica; criterios de admisión reforzados); Rubén Blázquez (Instituto Vasco de Derecho Procesal) — *Deepfakes en el procedimiento probatorio*. https://www.economistjurist.es/noticias-juridicas/la-prueba-sintetica-en-el-proceso-judicial-retos-probatorios-de-los-deepfakes/ · https://www.institutovascodederechoprocesal.com/sites/default/files/files/Ruben%20Blazquez2.pdf
516. ICPM — *La Fiscalía señala que sólo el 0,01 % de las denuncias por violencia machista son falsas* (79 condenas firmes, el 0,0075 %). https://www.icpm.es/actualidad_noticias.asp?id=2382
517. Efeminista — *Casi 3 millones de denuncias por violencia de género en España desde 2004 y solo un 0,0082 % son falsas* (serie 2009-2024); ANAVID — *¿De dónde sale la cifra del 0,01 %?* (matiz metodológico: solo falsedad acreditada con dolo). https://efeminista.com/denuncias-falsas-violencia-de-genero-espana/ · https://anavid.es/de-donde-sale-la-cifra-del-001-de-denuncias-falsas-de-violencia-de-genero-por-parte-de-la-fiscalia-del-estado-y-el-cgpj/
518. Motorpasión — *¿Puedes usar una dashcam en España?* (criterios AEPD: grabación limitada al incidente, ~20 segundos antes y después, preferible sin sonido; válida como prueba por interés legítimo y tutela judicial); Adasfera — *Legalidad dashcam España: guía DGT y AEPD (2026)*. https://www.motorpasion.com/seguridad/pregunta-puedes-usar-dashcam-espana-respuesta-puedes-meterte-buen-lio-no-sabes-como · https://adasfera.com/2026/01/legalidad-dashcam-espana-dgt-multasson-legales-las-dashcams-en-espana-en-2026-guia-definitiva-dgt-y-aepd/

519. TodoDashcam — *Legislación sobre dashcams en España y Europa* (Portugal: Ley 58/2019, prohibido incluso llevarla; Alemania: admisión limitada al incidente; Francia: CNIL, conductor responsable del tratamiento). https://www.tododashcam.es/pages/blog-legislacion-dashcams-espana
520. AlertCops (Secretaría de Estado de Seguridad, Ministerio del Interior) — *AlertCops incorpora un botón SOS* (5 pulsaciones en menos de 6 segundos; ubicación + 10 segundos de audio a las FCSE; código AVDG para víctimas de violencia de género). https://alertcops.ses.mir.es/publico/alertcops/actualidad/detalleActualidad.html?entrada=AlertCops-incorpora-un-bot-n-SOS
521. Rastreator — *Guardia Civil y UNESPA, contra el fraude* (≈400.000 intentos de fraude anuales; ≈2.000 M€; 6 de cada 100 lesiones; accidentes simulados: 3,2 % de los declarados, 18 % del coste investigado; Procedimiento Operativo GC-UNESPA). https://www.rastreator.com/seguros/noticias/guardia-civil-y-unespa-luchan-contra-el-fraude-en-el-seguro.aspx
522. Infobae — *Detenidas 32 personas que fingían accidentes de tráfico para estafar al seguro* (2 de julio de 2025; siete accidentes simulados en ocho meses). https://www.infobae.com/espana/2025/07/02/detenidas-32-personas-que-fingian-accidentes-de-trafico-para-estafar-al-seguro-una-agencia-de-detectives-presento-la-denuncia/
523. t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; el contenido no sale nunca del dispositivo; revelación voluntaria). Véanse los capítulos 13 y 15.
524. TechCrunch — *23andMe confirms hackers stole ancestry data on 6.9 million users* (2023; las listas segmentadas por origen étnico). https://techcrunch.com/2023/12/04/23andme-confirms-hackers-stole-ancestry-data-on-6-9-million-users/
525. Yaniv Erlich, Tal Shor, Itsik Pe'er y Shai Carmi (Science) — *Identity inference of genomic data using long-range familial searches* (2018; el 2 % de la población basta). https://www.science.org/doi/10.1126/science.aau4832
526. CNBC — *23andMe bankruptcy: selling and deleting DNA* (2025; +526 % de tráfico; ~1,9 M de solicitudes de borrado). https://www.cnbc.com/2025/03/30/23andme-bankruptcy-selling-deleting-dna-genetic-testing.html
527. New York Attorney General (Letitia James) — *AG James sues 23andMe to protect genetic data* (coalición de 28 fiscales generales). https://ag.ny.gov/press-release/2025/attorney-general-james-sues-23andme-protect-new-yorkers-genetic-data
528. Bio-IT World — *Anne Wojcicki buys back 23andMe for $305M* (Regeneron, 256 M$ → TTAM, 305 M$; cierre el 14-jul-2025). https://www.bio-itworld.com/news/2025/07/02/anne-wojcicki-buys-back-23andme-for-305m-promises-data-security
529. Information Commissioner's Office (Reino Unido) — *ICO fines 23andMe £2.31 million* (155.592 residentes británicos; la sanción castiga la custodia). https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/06/23andme-fined-for-failing-to-protect-uk-users-genetic-data/
530. NPR — *In hunt for the Golden State Killer, investigators uploaded his DNA to a genealogy site* (el ADN lo subió un familiar). https://www.npr.org/sections/thetwo-way/2018/04/27/606624218/in-hunt-for-golden-state-killer-investigators-uploaded-his-dna-to-genealogy-site
531. The Legal Genealogist — *GEDmatch reverses course* (opt-out por defecto; solo ~14 % optaron por participar). https://www.legalgenealogist.com/2019/05/19/gedmatch-reverses-course/
532. National Human Genome Research Institute — *GINA: Genetic Information Nondiscrimination Act (2008)* (no cubre vida, invalidez ni cuidados de larga duración). https://www.genome.gov/27026050/president-bush-signs-the-genetic-information-nondiscrimination-act-of-2008
533. Taner Kuru (Computer Law & Security Review) — *Investigative genetic genealogy in Europe* (2025; subir tu ADN no hace «público» el de tus parientes). https://www.sciencedirect.com/science/article/pii/S0267364925000019
534. Fortune — *Tesla lawyers argue recordings of Musk touting Autopilot could be deepfakes* (Huang contra Tesla; jueza Evette Pennypacker). https://fortune.com/2023/04/27/elon-musk-lawyers-argue-recordings-of-him-touting-tesla-autopilot-safety-could-be-deepfakes/
535. 9to5Mac — *Rittenhouse lawyer's pinch-to-zoom argument* (la carga trasladada a la fiscalía; 20 minutos para un perito de Apple). https://9to5mac.com/2021/11/11/rittenhouse-lawyer-pinch-to-zoom/
536. NBC News — *Washington state judge blocks use of AI-enhanced video evidence* (State contra Puloka; juez Leroy McCullough; 29-mar-2024). https://www.nbcnews.com/news/us-

news/washington-state-judge-blocks-use-ai-enhanced-video-evidence-rcna141932
537. NPR — *Baltimore police caught planting drugs in body-cam footage* (el agente Pinheiro; el búfer de 30 segundos sin sonido). https://www.npr.org/sections/thetwo-way/2017/07/20/538279258/baltimore-police-caught-planting-drugs-in-body-cam-footage-public-defender-says
538. ProPublica — *How police have undermined the promise of body cameras* (solo el 42 % de 79 homicidios; «no existe» falso en 1 de cada 5). https://www.propublica.org/article/how-police-undermined-promise-body-cameras
539. Robert Chesney y Danielle Keats Citron — *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* (107 California Law Review 1753, 2019; el «dividendo del mentiroso»). https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security
540. U.S. Courts — *Advisory Committee on Evidence Rules: propuesta de Regla 707 (prueba generada por máquina) y 901(c)* (comentario hasta el 16-feb-2026). https://www.uscourts.gov/sites/default/files/document/2025-11_evidence_rules_commitee_agenda_book_final.pdf
541. American Bar Association — *New rules for self-authenticating electronic evidence (FRE 902(13)/(14))* (el valor hash autoautentica copias digitales). https://www.americanbar.org/groups/litigation/resources/newsletters/trial-evidence/new-rules-self-authenticating-electronic-evidence/
542. CYFOR / Expatriate Law — *Deepfake audio evidence used in a UK court* (audio editado después de la llamada para insertar amenazas). https://cyfor.co.uk/deepfake-audio-evidence-used-in-uk-court-to-discredit-father/
543. BBC (via LBC) — *150 reports of police officers misusing body cameras* (Inglaterra y Gales; Jim Colwell, NPCC). https://www.lbc.co.uk/article/150-reports-police-officers-misusing-body-cameras-investigation-england-wales-DWzgZZ_2/
544. Enigma Forensics — *Judge sanctions hospital for not producing complete EMR audit trail* (Prieto contra Rush University Medical Center; juez James O'Hara; «information blocking»). https://enigmaforensics.com/blog/judges-order-sanctions-hospital-not-producing-complete-emr-audit-trail/
545. Cornell Law (Legal Information Institute) — *45 CFR §164.312: HIPAA technical safeguards* (controles de auditoría obligatorios; integridad de la ePHI). https://www.law.cornell.edu/cfr/text/45/164.312
546. Cornell Law (Legal Information Institute) — *21 CFR §11.10: FDA electronic records* (audit trails con sello de tiempo; un cambio no puede ocultar el registro anterior). https://www.law.cornell.edu/cfr/text/21/11.10
547. HHS Office of Inspector General — *Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology* (OEI-01-11-00570, 2013; solo ~25 % con políticas de copiar-pegar). https://oig.hhs.gov/oei/reports/oei-01-11-00570.asp
548. HHS Office of Inspector General — *Trend Toward More Expensive Inpatient Hospital Stays in Medicare* (OEI-02-18-00380, 2021; casi la mitad del gasto al nivel máximo de severidad). https://oig.hhs.gov/oei/reports/OEI-02-18-00380.pdf
549. ProPublica / HHS OCR — *UCLA Health System pays $865,500 to settle celebrity-privacy allegations* (2011; el snooping en los historiales). https://www.propublica.org/article/ucla-health-system-pays-865000-to-settle-celebrity-privacy-allegations
550. U.S. Department of Justice — *Former UCLA healthcare worker sentenced (Huping Zhou)* (323 accesos; la primera condena de prisión por una violación de HIPAA). https://www.justice.gov/archive/usao/cac/Pressroom/pr2010/004.html
551. Federal Register / ONC — *21st Century Cures Act: interoperability and information blocking* (2020; acceso del paciente a su información de salud). https://www.federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification
552. Kantara Initiative — *Consent Receipt Specification v1.1* (base de la norma ISO/IEC TS 27560:2023). https://kantara.atlassian.net/wiki/spaces/archive/pages/3508790/Consent+Receipt+Specification
553. Dean F. Sittig y Adam Wright (Applied Clinical Informatics) — *Identifying a Clinical Informatics or EHR Expert Witness* (2023; el log es prueba que hay que interpretar). https://pmc.ncbi.nlm.nih.gov/articles/PMC10033222/
554. Stanford Internet Observatory / 404 Media — *Largest Dataset Powering AI Images Removed After Discovery of Child Sexual Abuse Material* (diciembre de 2023; 3.226 casos sospechosos en LAION-

5B; recomendación de deprecar los modelos). https://www.404media.co/laion-datasets-removed-stanford-csam-child-abuse/
555. LAION — *Releasing Re-LAION-5B: transparent iteration on LAION-5B with additional safety fixes* (agosto de 2024; 2.236 enlaces eliminados). https://laion.ai/blog/relaion-5b/
556. JFrog Security Research — *Data Scientists Targeted by Malicious Hugging Face ML Models with Silent Backdoor* (2024; técnica *nullifAI*, abuso de *pickle*, puerta trasera). https://jfrog.com/blog/data-scientists-targeted-by-malicious-hugging-face-ml-models-with-silent-backdoor/
557. The Hacker News — *Over 100 Malicious AI/ML Models Found on Hugging Face Platform* (marzo de 2024). https://thehackernews.com/2024/03/over-100-malicious-aiml-models-found-on.html
558. EU Artificial Intelligence Act — *Article 53: Obligations for providers of general-purpose AI models* (documentación técnica Anexo XI; resumen del contenido de entrenamiento; sanciones de hasta 15 M€ o 3 %). https://artificialintelligenceact.eu/article/53/
559. Comisión Europea — *General-Purpose AI Models in the AI Act: Questions & Answers* (plantilla del resumen de entrenamiento; aplicación desde el 2 de agosto de 2025; marcado del art. 50 desde el 2 de agosto de 2026). https://digital-strategy.ec.europa.eu/en/faqs/general-purpose-ai-models-ai-act-questions-answers
560. CycloneDX (OWASP) — *Machine Learning Bill of Materials (AI/ML-BOM)* (datasets, modelos y configuraciones con procedencia; desde la v1.5, 2023). https://cyclonedx.org/capabilities/mlbom/
561. *Operationalising AI bills of materials for verifiable AI provenance and lifecycle assurance* (Frontiers in Computer Science, 2026). https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2026.1735919/full
562. Margaret Mitchell et al. — *Model Cards for Model Reporting* (2019). https://arxiv.org/abs/1810.03993
563. Google / C2PA — *How Google and the C2PA are increasing transparency for gen AI content* (SynthID: más de 100.000 millones de contenidos marcados según Google I/O 2026 (mayo de 2026); credenciales de contenido). https://blog.google/innovation-and-ai/products/google-gen-ai-content-transparency-c2pa/
564. Cathy O'Neil — *Armas de destrucción matemática* (Capitán Swing, 2018).
565. Consejo de la UE / Pinsent Masons (2026). https://www.pinsentmasons.com/out-law/news/rules-high-risk-ai-delayed-under-eu-omnibus-deal
566. Beth Simone Noveck — *Reboot* (Yale UP, 2026), cap. 6.
567. VentureBeat (2020). https://venturebeat.com/ai/amsterdam-and-helsinki-launch-algorithm-registries-to-bring-transparency-to-public-deployments-of-ai
568. CBC News — *Air Canada found liable for chatbot's bad advice on bereavement rates* (Moffatt v. Air Canada, B.C. Civil Resolution Tribunal, febrero de 2024: el chatbot inventó una política de tarifa de duelo; 812 $ canadienses de compensación sobre 1.630,36 pagados; «Air Canada no tuvo el cuidado razonable de garantizar que su chatbot fuera exacto»; «es responsable de toda la información de su web —da igual que venga de una página estática o de un chatbot»); Forbes — *What Air Canada Lost In 'Remarkable' Lying AI Chatbot Case* (la alegación de que el chatbot era «una entidad legal separada»); McCarthy Tétrault — *Moffatt v. Air Canada: A Misrepresentation by an AI Chatbot*. https://www.cbc.ca/news/canada/british-columbia/air-canada-chatbot-lawsuit-1.7116416 · https://www.forbes.com/sites/marisagarcia/2024/02/19/what-air-canada-lost-in-remarkable-lying-ai-chatbot-case/ · https://www.mccarthy.ca/en/insights/blogs/techlex/moffatt-v-air-canada-misrepresentation-ai-chatbot
569. Visa — *Intelligent Commerce* (credenciales tokenizadas de alcance limitado para agentes; servidor MCP; un token de 200 $ no puede autorizar 500 $); Mastercard — *Agent Pay* (anunciado el 29-4-2025: Agentic Tokens que ligan credencial, agente, ámbito de comercios y política de consentimiento; «Agent Pay for Machines», junio de 2026); Google AP2 (septiembre de 2025, 60+ socios: Intent Mandate + Cart Mandate firmados como credenciales verificables); Eco/Paz — guías del comercio agéntico 2026 (runtimes: OpenAI Operator, Google Project Mariner, Anthropic Computer Use, Microsoft Copilot). https://www.visa.com/en-us/solutions/intelligent-commerce · https://www.mastercard.com/us/en/news-and-trends/press/2026/june/mastercard-launches-agent-pay-for-machines.html · https://eco.com/support/en/articles/14839400-what-is-agentic-commerce-the-2026-guide · https://www.paz.ai/glossary/agentic-commerce-protocol-acp
570. t2p — manual de producto (certificar cualquier fichero —el mandato y los registros, solo la huella viaja; captura de página web con imagen completa + código fuente; firma con vídeo-selfie, dos retos de vida aleatorios y verificación biométrica del dispositivo; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado

PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; la procedencia de los modelos, en el capítulo 79; los agentes del sector público, en el capítulo 107.

571. Voicebot.ai — *Tom Hanks Warns of Deepfake Hanks Dental Ad* (octubre de 2023; «I have nothing to do with it»). https://voicebot.ai/2023/10/02/tom-hanks-warns-of-deepfake-hanks-dental-ad/
572. NPR — *OpenAI pulls AI voice that was compared to Scarlett Johansson in the movie 'Her'* (mayo de 2024; análisis forense de la Universidad Estatal de Arizona: más parecida que el 98 % de las actrices). https://www.npr.org/2024/05/20/1252495087/openai-pulls-ai-voice-that-was-compared-to-scarlett-johansson-in-the-movie-her
573. SAG-AFTRA / Perkins Coie — *How the 2023 SAG-AFTRA contract addresses generative AI and digital replicas* (consentimiento informado; descripción específica del uso; consentimiento nuevo para la reutilización). https://perkinscoie.com/insights/blog/generative-ai-movies-and-tv-how-2023-sag-aftra-and-wga-contracts-address-generative
574. Davis Wright Tremaine — *Tennessee Passes ELVIS Act (Ensuring Likeness, Voice and Image Security Act)* (en vigor el 1 de julio de 2024; la voz al derecho de publicidad; responsabilidad de las herramientas de IA). https://www.dwt.com/blogs/artificial-intelligence-law-advisor/2024/04/tennessee-elvis-act-ai-voice-replica
575. United States Senate Judiciary Committee — *NO FAKES Act (Nurture Originals, Foster Art, and Keep Entertainment Safe)* (derecho federal sobre la réplica digital; versión revisada de 2026, aprobada por la Comisión Judicial del Senado el 18 de junio de 2026). https://www.judiciary.senate.gov/no-fakes-act
576. World Economic Forum — *Deepfake legislation: Denmark takes action* (presentada en junio de 2025; derecho de tipo copyright sobre cara, cuerpo y voz; retirada y compensación; excepciones de parodia; en trámite parlamentario, entrada en vigor prevista a mediados de 2026). https://www.weforum.org/stories/2025/07/deepfake-legislation-denmark-digital-id/
577. Variety — *Scarlett Johansson Reacts to OpenAI Sky Voice: 'Shocked' and 'Angered'* (mayo de 2024). https://variety.com/2024/digital/news/scarlett-johansson-responds-shocked-angered-openai-chatgpt-her-1236011135/
578. SAG-AFTRA — *Digital Replicas 101* (tipología y derechos de consentimiento del intérprete). https://www.sagaftra.org/sites/default/files/sa_documents/DigitalReplicas.pdf
579. Wikipedia — *ELVIS Act* (Ensuring Likeness, Voice and Image Security Act of 2024; reforma de la Personal Rights Protection Act de 1984). https://en.wikipedia.org/wiki/ELVIS_Act
580. Marc Goodman — *Delitos del futuro* (Ariel, 2015).
581. Wikipedia, *Jason Palmer (politician)*; TIME, *Albania's AI minister Diella* (2025). https://time.com/7324934/albania-ai-minister-diella/
582. Légifrance — *Ley núm. 2024-120, de 19 de febrero de 2024, para garantizar el respeto del derecho a la imagen de los niños* (modificación del art. 371-1 del Código civil: la autoridad parental incluye la protección de la vida privada y del derecho a la imagen del menor; protección ejercida en común por los dos progenitores, asociando al niño según edad y madurez; delegación judicial del ejercicio del derecho de imagen en caso de atentado grave a la dignidad o la integridad moral); DAJ/economie.gouv.fr — *Respect du droit à l'image des enfants: les apports de la loi* (contexto: un niño aparece de media en 1.300 fotografías en línea antes de los 13 años; riesgos: usurpación, chantaje, ciberacoso); Actu-Juridique — *Les 5 apports de la loi*. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049163317 · https://www.economie.gouv.fr/daj/lettre-de-la-daj-respect-du-droit-limage-des-enfants-les-apports-de-la-loi-du-19-fevrier-2024 · https://www.actu-juridique.fr/civil/personnes-famille/le-respect-du-droit-a-limage-des-enfants-et-les-5-apports-de-la-loi-du-19-fevrier-2024/
583. Marco español (LO 1/1982 sobre el honor, la intimidad y la propia imagen; LO 1/1996 de protección jurídica del menor; intervención del Ministerio Fiscal; doctrina judicial que exige el acuerdo de ambos progenitores para publicar imágenes de los hijos). Véase el capítulo 81 para el derecho de imagen general y el capítulo 53 para los registros de coparentalidad.
584. t2p — manual de producto (escáner de documentos; captura de pantalla y correo certificados; certificar cualquier fichero —solo la huella viaja, el contenido no sale nunca del dispositivo; firma con vídeo-selfie; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; la coparentalidad, en el capítulo 53; la difusión íntima, en el capítulo 83.
585. Euronews — *The Almendralejo case: when AI deepfakes are used to undress teenagers* (septiembre de 2023; testimonio de una madre; víctimas de 12-14 años).

https://www.euronews.com/next/2023/11/15/the-case-of-almendralejo-when-deepfakes-are-used-to-undress-teenagers-euronews-tech-talks-

586. Scottish Legal News / Reuters — *Spain: court punishes schoolboys for spreading AI deepfakes of girls* (julio de 2024; 15 menores condenados; 20 delitos de material de abuso infantil y 20 contra la integridad moral). https://www.scottishlegal.com/articles/spain-court-punishes-schoolboys-for-spreading-ai-deepfakes-of-girls
587. Wikipedia — *Taylor Swift deepfake pornography controversy* (enero de 2024; una publicación vista más de 47 millones de veces; X bloquea las búsquedas de su nombre). https://en.wikipedia.org/wiki/Taylor_Swift_deepfake_pornography_controversy
588. Congress.gov / The White House — *TAKE IT DOWN Act* (S.146; firmada el 19 de mayo de 2025; retirada en 48 h; cumplimiento a plataformas aplicado por la FTC desde el 19 de mayo de 2026; primera condena penal en abril de 2026). https://www.congress.gov/bill/119th-congress/senate-bill/146
589. Council of Europe — *Directive (EU) 2024/1385 of 14 May 2024 on combating violence against women and domestic violence* (en vigor el 13 de junio de 2024; tipifica el material íntimo manipulado; órdenes de retirada y preservación de pruebas). https://www.coe.int/en/web/cyberviolence/-/european-parliament-and-council-directive-eu-2024-1385-of-14-may-2024-on-combating-violence-against-women-and-domestic-violence
590. Euronews — *Nude deepfakes: is the EU doing enough to tackle the issue?* (2024; más del 90 % del contenido deepfake es pornográfico, casi todo contra mujeres). https://www.euronews.com/next/2024/03/17/nude-deepfakes-is-the-eu-doing-enough-to-tackle-the-issue
591. StopNCII.org — *How StopNCII.org works* (huella generada en el dispositivo; la imagen no sale nunca; más de 500.000 imágenes protegidas; socios Meta, TikTok, Reddit, Google). https://stopncii.org/how-it-works/
592. Skadden — *'Take It Down Act' requires online platforms to remove unauthorized intimate images and deepfakes when notified* (análisis del mecanismo de aviso y retirada). https://www.skadden.com/insights/publications/2025/06/take-it-down-act
593. RAINN — *TAKE IT DOWN Act* (perspectiva de las víctimas de violencia sexual). https://rainn.org/federal-legislation/take-it-down-act/
594. The Markup (2024). https://themarkup.org/artificial-intelligence/2024/12/11/1-in-6-congresswomen-targeted-by-ai-generated-sexually-explicit-deepfakes
595. The Local (Italia) — *Italy unanimously passes anti-cyberbullying law* (mayo 2017; Ley 71/2017; Carolina Picchio, 14 años, 2013; senadora Elena Ferrara). https://www.thelocal.it/20170517/italy-unanimously-passes-anti-cyberbullying-law-online-abuse-trolling
596. Pew Research Center — *Teens and Cyberbullying 2022* (15 de diciembre de 2022; 46 %; insultos 32 %, rumores 22 %, amenazas 10 %). https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/
597. OMS-Europa y estudio HBSC — *One in six school-aged children experiences cyberbullying* (27 de marzo de 2024; 16 %; 44 países; ≈280.000 jóvenes). https://www.who.int/europe/news/item/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study
598. Fundación ANAR y Fundación Mutua Madrileña — *VIII Informe de Prevención del Acoso Escolar* (2025; 12,3 % vs 9,4 %; 14,2 % con IA; 91,7 % del mismo centro; 17.562 alumnos). https://www.anar.org/crece-el-acoso-escolar-impulsado-por-el-ciberbullying-y-el-uso-de-la-ia-para-cometerlo/
599. ADL — *Online Hate and Harassment: The American Experience 2024* (junio de 2024; adolescentes 50 %; 36 % salto al mundo físico). https://www.adl.org/resources/report/online-hate-and-harassment-american-experience-2024
600. CBS News / ITV News — *Molly Russell inquest* (30 de septiembre de 2022; forense Andrew Walker; 2.100 de 16.300 posts; primer dictamen mundial). https://www.cbsnews.com/news/molly-russell-suicide-death-coroner-social-media-instagram-pinterest/
601. Candice Odgers — *The great rewiring: is social media really behind an epidemic of teenage mental illness?* (Nature, marzo de 2024; réplica a Jonathan Haidt, *The Anxious Generation*, 2024). https://www.nature.com/articles/d41586-024-00902-2
602. CNN — *Pikesville principal's voice on racist recording was an AI-generated deepfake* (Dazhon Darien / Eric Eiswert; enero-abril de 2024). https://www.cnn.com/2024/04/26/us/pikesville-principal-maryland-deepfake-cec/index.html
603. PNAS — *X under Musk's leadership: substantial hate and no reduction in inauthentic activity* (2025; +≈50 % odio; +70 % «me gusta»; actividad coordinada sin reducir).

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11819532/
604. Comisión Europea — *Guidelines on the protection of minors under the Digital Services Act* (14 de julio de 2025; ciberacoso, verificación de edad; riesgos sistémicos = discurso de odio ilegal). https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors
605. La Moncloa — *Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales* (Consejo de Ministros, 4 de junio de 2024; «alejamiento en línea»; verificación de edad). https://www.lamoncloa.gob.es/consejodeministros/resumenes/Paginas/2024/040624-rueda-de-prensa-ministros.aspx
606. Código Penal (España) — arts. 510 (delito de odio; prisión 1-4 años) y 172 ter (acoso/stalking; agravado por la edad de la víctima). https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444
607. Ofcom / GOV.UK — *Online Safety Act 2023: protection of children codes* (deberes en vigor el 25 de julio de 2025; bullying y contenido de odio; multas hasta el 10 % de la facturación mundial). https://www.gov.uk/government/collections/online-safety-act
608. eSafety Commissioner (Australia) — *Social media age restrictions* (Act 2024; menores de 16 desde el 10 de diciembre de 2025; primer país). https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions
609. t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice). Véanse los capítulos 13 y 15.
610. INCIBE / Infobae — *El teléfono de tu hijo no se dañó: la estafa en WhatsApp que pide dinero para una emergencia* (8 de mayo de 2025; mecánica del «hola mamá», variantes, recomendaciones de verificación); Policía Nacional (alerta) — OKDiario; Valencia News — *Así funciona la estafa del «hijo en apuros» por SMS y WhatsApp*. https://www.infobae.com/tecno/2025/05/08/el-telefono-de-tu-hijo-no-se-dano-la-estafa-en-whatsapp-que-pide-dinero-para-solucionar-una-emergencia/ · https://okdiario.com/curiosidades/policia-nacional-alerta-sobre-esta-estafa-hola-mama-telefono-esta-roto-10582931 · https://valencianews.es/tendencias/mama-se-me-ha-roto-el-movil-asi-funciona-estafa-del-hijo-en-apuros-sms-y-whatsapp/
611. HousingWire — *FBI: Seniors lost $7.75B to cybercrime in 2025 — a 59% jump* (201.266 denuncias de mayores de 60; 4.900 M$ en 2024, +43 %; >3.100 denuncias sénior con IA y >352 M$; >5 M$ en estafas de angustia con voz clonada); PPC Land — *AI-linked fraud costs Americans $893 million* (22.364 denuncias de IA en 2025). https://www.housingwire.com/articles/fbi-seniors-cybercrime-2025/ · https://ppc.land/ai-linked-fraud-costs-americans-893-million-fbi-reports-for-2025/
612. FBI / IC3 — *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud* (PSA-241203, 3 de diciembre de 2024; clonación de voz en estafas de angustia y suplantación de familiares). https://www.ic3.gov/PSA/2024/PSA241203
613. Factchequeado — *Qué son las estafas de romance y cómo identificarlas* (FTC: ≈60.000 denuncias y 1.200 M$ en 2024; la franja 65-74 con las pérdidas más altas); AARP — *Los estafadores de romance engañan a sus víctimas con fraudes de criptomonedas*. https://factchequeado.com/teexplicamos/20240126/estafa-romance-scam/ · https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2023/enganos-de-romance-con-criptomoneda.html
614. Wikipedia — *Estafa romántica* (crimen de Morata de Tajuña, 2023: tres hermanos mayores asesinados; estafa de hasta 263.000 €). https://es.wikipedia.org/wiki/Estafa_rom%C3%A1ntica
615. Ministerio del Interior — *Detenidas dos personas por la estafa conocida como «Romance Scam», timo del amor*. https://www.interior.gob.es/opencms/es/detalle/articulo/Detenidas-dos-persona-por-la-estafa-conocida-como-Romance-Scam-timo-del-amor/
616. Infobae — *Francia anuncia control de residencias de ancianos tras escándalo* (1 de febrero de 2022; «Les Fossoyeurs» de Victor Castanet; Orpea ≈260.000 residentes; racionamiento; investigaciones penales por maltrato, malversación e infracciones laborales; denuncias por homicidio involuntario); infoLibre — *El último escándalo de Orpea* (inyección estatal de 605 M€ por una participación mayoritaria). https://www.infobae.com/america/agencias/2022/02/01/francia-anuncia-control-de-residencias-de-ancianos-tras-escandalo/ · https://www.infolibre.es/politica/ultimo-escandalo-orpea-negocios-trama-societaria-oculta-luxemburgo_1_1232899.html
617. elDiario.es — *Condenada la trabajadora de una residencia cazada con una cámara oculta mientras maltrataba a una interna* (El Escorial; multa de 480 € e indemnización de 3.000 € confirmadas por la Audiencia Provincial de Madrid; cámara de las hijas avalada como prueba).

https://www.eldiario.es/madrid/condenada-trabajadora-residencia-cazada-camara-oculta-maltrataba-interna_1_12498186.html

618. El Foro de Labos — *El Tribunal Supremo confirma la validez de una prueba obtenida con cámara oculta* (2022); Pardo Geijo Abogados — *¿Es legal poner cámaras ocultas en casa?* (sospecha fundada de delito grave; cámara temporal y enfocada; triple juicio de proporcionalidad). https://www.elforodelabos.es/2022/09/el-tribunal-supremo-confirma-la-validez-de-una-prueba-obtenida-con-camara-oculta/ · https://pardogeijo.com/es-legal-grabar-camaras-ocultas-casa/
619. BOE — *Ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica* (apoyo, no sustitución; medidas voluntarias ante notario; aptitud para testar; rendición de cuentas; curatela excepcional); El Notario — *Una visión práctica de la Ley 8/2021*. https://www.boe.es/buscar/act.php?id=BOE-A-2021-9233 · https://www.elnotario.es/practica-juridica/11767-una-vision-practica-de-la-ley-8-2021-de-2-de-junio-sobre-personas-con-discapacidad
620. t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; prueba de vida con reto; contenido nunca fuera del dispositivo; revelación voluntaria). Véanse los capítulos 13, 15 y 64.
621. Atlantic Council — *Russian War Report: Hacked news program and deepfake video spread false Zelenskyy claims* (16 de marzo de 2022; pirateo del teletipo y la web de Ukraine 24; deepfake de rendición; desmentido con selfie de «provocación infantil»). https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-hacked-news-program-and-deepfake-video-spread-false-zelenskyy-claims/
622. NPR — *Impostor uses AI to impersonate Rubio and contact foreign and U.S. officials* (julio de 2025; voz clonada del secretario de Estado en Signal; cable del Departamento de Estado del 3 de julio). https://www.npr.org/2025/07/09/nx-s1-5462195/impostor-ai-impersonate-rubio-foreign-officials
623. Clarity — *Iranian Deepfake of Israeli Defense Minister Airs Live* (abril de 2025; reemisión no verificada de Channel 14 de un deepfake de Yoav Gallant; corte en directo y disculpa). https://www.getclarity.ai/ai-deepfake-blog/iranian-deepfake-of-israeli-defense-minister-airs-live---and-how-clarity-caught-it-instantly
624. Romania Insider — *Romanian central bank governor Mugur Isarescu targeted by deepfake* (febrero de 2024; deepfake de inversiones fraudulentas; patrón en varios bancos centrales). https://www.romania-insider.com/bnr-mugur-isarescu-deepfake-february-2024
625. Wikipedia — *2018 Hawaii false missile alert* (13 de enero de 2018; falsa alerta WEA de misil balístico; corrección de 38 minutos; error genuino). https://en.wikipedia.org/wiki/2018_Hawaii_false_missile_alert
626. FEMA — *Integrated Public Alert & Warning System (IPAWS)* (alertas oficiales firmadas digitalmente por la autoridad emisora y autenticadas por IPAWS-OPEN; línea base de autenticación en la emisión). https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system
627. Singapore Police Force — *Footage from Zoom video conference involving impersonation of senior government officials* (16 de mayo de 2026; deepfake del PM Lawrence Wong, el presidente Tharman y representantes de la MAS; pérdida de 4,9 M$ SGD por una sola víctima). https://www.police.gov.sg/media-hub/news/2026/05/20260516_footage_from_zoom_video_conference_involving_impersonation_of_senior_govern
628. Bulletin of the Atomic Scientists — *AI misinformation is threatening emergency communications. Here's how to fix that* (septiembre de 2025; alertas oficiales falsas, el «dividendo del mentiroso» y la autenticación de las comunicaciones de emergencia). https://thebulletin.org/2025/09/ai-misinformation-is-threatening-emergency-communications-heres-how-to-fix-that/
629. Fortune — *A deepfake 'CFO' tricked British design firm Arup in $25 million fraud* (Arup confirmado como víctima; HK$200M/US$25,6M; 15 transferencias; declaración del CIO Rob Greig). https://fortune.com/europe/2024/05/17/arup-deepfake-fraud-scam-victim-hong-kong-25-million-cfo/
630. FinCEN — *FinCEN Issues Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions* (alerta FIN-2024-Alert004, 13 de noviembre de 2024; recomienda verificación en vivo y MFA resistente al phishing). https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial
631. FBI/IC3 — *Senior US Officials Impersonated in Malicious Messaging Campaign* (PSA250515, 15 de mayo de 2025; voz/texto generados por IA; verificación fuera de banda y frases pactadas). https://www.ic3.gov/PSA/2025/PSA250515

632. Fortune — *Ferrari exec foils deepfake attempt by asking the scammer a question only CEO Benedetto Vigna could answer* (julio de 2024; clonación de voz desbaratada con una pregunta de control). https://fortune.com/2024/07/27/ferrari-deepfake-attempt-scammer-security-question-ceo-benedetto-vigna-cybersecurity-ai/
633. Marketing-Interactive — *WPP CEO Mark Read targeted by deepfake AI scam* (mayo de 2024; WhatsApp falso, Teams, voz clonada e imágenes de YouTube; intento fracasado; advertencia de Read). https://www.marketing-interactive.com/wpp-ceo-mark-read-deepfake-ai-scam
634. Tookitaki — *The Deepfake Deception: How a CEO Video Call Cost $499K in Singapore* (marzo de 2025; un director financiero autoriza 499.000 $ en una llamada de Zoom con todos los participantes deepfake). https://www.tookitaki.com/blog/deepfake-ceo-scam-singapore-2025
635. Nacha — *FBI's IC3 Finds Almost $8.5 Billion Lost to Business Email Compromise in Last Three Years* (~3.000 M$/año; ~8.500 M$ en tres años; base del fraude de pago). https://www.nacha.org/news/fbis-ic3-finds-almost-85-billion-lost-business-email-compromise-last-three-years
636. Trend Micro — *Deepfake CFO Video Calls Result in $25MM in Damages* (análisis técnico del patrón de ataque con videollamada multiparticipante empleado contra Arup). https://www.trendmicro.com/en_us/research/24/b/deepfake-video-calls.html
637. World Economic Forum — *Cybercrime: Lessons learned from a $25m deepfake attack* (febrero de 2025; análisis del caso Arup y de los fallos de control; argumento de la verificación fuera de banda). https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/
638. 9to5Mac (sobre el reportaje de WIRED) — *Latest romance scam tactic uses two phones with face-swap app* (abr-2024: los «Yahoo Boys» y el face-swap en tiempo real dentro de videollamadas —dos móviles en soportes y aro de luz, o portátil con webcam; presumen de los montajes en Telegram y los venden; Rachel Tobac: las apps han mejorado dramáticamente en un año). https://9to5mac.com/2024/04/18/romance-scam-face-swap/
639. iProov — *Threat Intelligence Report 2025: Remote Identity Under Attack* (ataques de cámara virtual nativa +2.665 %; face swaps +300 % respecto de 2023, dirigidos contra sistemas con protocolos de detección de vida; ~24.000 usuarios vendiendo tecnologías de ataque como servicio; la conversión de imagen a vídeo como vector nuevo; 127 herramientas de face-swap, 91 cámaras virtuales y 10 emuladores catalogados). https://www.iproov.com/reports/threat-intelligence-report-2025-remote-identity-attack · https://www.iproov.com/press/annual-identity-verification-threat-intelligence-report
640. Gartner (vía FutureCIO) — *Deepfakes to render identity verification and authentication solutions inefficient* (predicción de feb-2024: en 2026, el 30 % de las empresas ya no considerarán fiables aisladamente las soluciones de verificación de identidad y autenticación, por los deepfakes contra la biometría facial; ataques de inyección +200 % en 2023; los estándares de detección de ataques de presentación no cubren la inyección digital; Akif Khan: combinar PAD, IAD e inspección de imagen). https://futurecio.tech/deepfakes-to-render-identity-verification-and-authentication-solutions-inefficient/
641. FBI / IC3 — *Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions* (PSA del 28-jun-2022: deepfakes y datos personales robados para optar a empleos remotos de TI, programación, bases de datos y software —algunas con acceso a datos de clientes y sistemas corporativos; señales: labios y sonido desincronizados, tos o estornudos que no cuadran con la imagen). https://www.ic3.gov/PSA/2022/psa220628
642. Decrypt — *People Are Using Basic AI to Bypass KYC — But Should You?* (feb-2024: OnlyFake, carnets y pasaportes falsos generados «con redes neuronales» por 15 $ —EE. UU., Italia, China, Rusia, Argentina, Chequia, Canadá—; 404 Media superó el KYC del exchange OKX, que usa el verificador externo Jumio; usuarios los usaban para abrir cuentas bancarias y desbloquear cuentas cripto). https://decrypt.co/216188/ai-generated-fake-id-bypass-kyc-aml-banks-crypto-onlyfakes
643. Adler, Hitzig, Jain et al. (arXiv) / MIT News — *Personhood credentials: Artificial intelligence and the value of privacy-preserving tools to distinguish who is real online* (ago-2024; 32 autores, con investigadores del MIT, de OpenAI y de Microsoft: credenciales digitales para demostrar que eres una persona real —no una IA— sin revelar ningún dato personal; emisión presencial o institucional; verificación criptográfica; «AI is moving very fast, certainly much faster than the speed at which governments adapt»). https://arxiv.org/abs/2408.07892 · https://news.mit.edu/2024/3-questions-proving-humanity-online-0816
644. Comisión Europea / Corbado — el Reglamento (UE) 2024/1183 de identidad digital europea: los estados miembros han de ofrecer una cartera EUDI a ciudadanos, residentes y empresas (plazo: diciembre de 2026); menos de un tercio de los estados cumplen hoy el listón de preparación

(observatorio del Politecnico di Milano). https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/915931811/The+European+Digital+Identity+Regulation · https://www.corbado.com/blog/eudi-wallet-2026-deadline-rollout-eic-2026

645. t2p — manual de producto (firma con vídeo-selfie: «la firma más fuerte de la app» —la cámara frontal graba mientras firmas, parpadeo y dos retos de vida aleatorios (girar la cabeza, sonreír, inclinarla) en menos de 60 segundos, verificación biométrica del dispositivo obligatoria con PIN como alternativa, firma manuscrita, 2 créditos y dos transacciones; certificado dedicado con el documento, la firma, la evidencia en vídeo y las dos transacciones; solo una persona en el encuadre; certificado con SHA-512, sello RFC 3161/eIDAS, ancla a la blockchain pública, QR y verificación forense con integridad del dispositivo y attestation de hardware; paquete .asice ETSI verificable fuera de línea sin confiar en el fabricante; los ficheros permanecen en el dispositivo —solo la huella viaja; la prueba de vida confirma «una persona real y presente» al firmar). Véanse los capítulos 13 y 15; la suplantación de directivos y la regla «sin sello, no hay pago», en el capítulo 87; quién contratas en remoto, en el capítulo 91; el compromiso y revelación, en los capítulos 45 y 46; la persona única de la participación, en el capítulo 108.
646. 340B Report — *Fake Lilly Twitter account tweets 'Insulin Is Free Now,' temporarily wiping billions from company's stock value* (10 nov. 2022, 1:36 p.m. ET; caída de ~368 a ~346 $; ~15.000 M$ borrados; disculpa de la empresa y cuenta @LillyPad). https://340breport.com/fake-lilly-twitter-account-tweets-insulin-is-free-now-temporarily-wiping-billions-from-companys-stock-value/
647. University at Buffalo — *With one false tweet, computer-based 'Hack Crash' led to real panic* (23 abril 2013; tuit pirateado de AP; Dow –143,5 puntos; >136.000 M$ borrados en segundos; reacción algorítmica y de alta frecuencia). https://www.buffalo.edu/news/releases/2015/05/037.html
648. InvestmentNews — *Shareholders accuse Ostin Technology of deepfake-driven $950M pump-and-dump scheme* (2025; *deepfakes* de Kostin/Musk/Zuckerberg; identidades robadas de asesores FINRA; inflación del 1.175 %; caída del 94 % en un día; acusación del DOJ el sept. 2025). https://www.investmentnews.com/regulation-legal-compliance/legal-shareholders-accuse-ostin-technology-of-deepfake-driven-950m-pump-and-dump-scheme/265308
649. The Hans India — *BSE warns investors about fake deepfake video misusing CEO's identity* (avisos de 2026 sobre vídeos *deepfake* del consejero delegado Sundararaman Ramamurthy; incidentes recurrentes enero-abril; promesa de acciones legales). https://www.thehansindia.com/business/bse-warns-investors-about-fake-deepfake-video-misusing-ceos-identity-1038779
650. SEC / FINRA / NASAA — *Investor Alert: Artificial Intelligence (AI) and Investment Fraud* (Investor.gov, 25 ene. 2024; aviso explícito sobre vídeos *deepfake* de consejeros delegados para «manipular el precio de una acción»). https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/artificial-intelligence-fraud
651. PRNEWS — *Hoax Releases Hit Newswire Services* (comunicado falso Walmart-Litecoin vía GlobeNewswire; Litecoin +30 %; ángulo de autenticación de los teletipos). https://www.prnewsonline.com/hoax-releases-hit-newswire-services/
652. Sidley Austin — *SEC Enforcement FY2025 Results Signal Shift in Priorities* (456 acciones; 17.900 M$ ordenados; ajustado 1.400 M$ + 1.300 M$; prioridad a la manipulación de mercado y el fraude de revelación). https://www.sidley.com/en/insights/newsupdates/2026/04/sec-enforcement-fy2025-results-signal-shift-in-priorities-in-direct-critique-of-prior-administration
653. EUR-Lex / Lexparency — *MAR Regulation (EU) No 596/2014, Article 12 — Market manipulation* (difusión de información falsa o engañosa y de rumores a través de los medios e internet como manipulación de mercado). https://lexparency.org/eu/32014R0596/ART_12/
654. FINRA — *Artificial Intelligence (AI) and Investment Fraud* (versión de la FINRA del aviso; lenguaje sobre vídeos *deepfake* de consejeros delegados y noticias falsas para mover el precio de una acción). https://www.finra.org/investors/insights/artificial-intelligence-and-investment-fraud
655. Carissa Véliz — *Prophecy: Prediction, Power, and the Fight for the Future* (2025).
656. ICIJ — *About the Pandora Papers investigation* (3 de octubre de 2021; 11,9 millones de documentos, 2,94 TB, 14 proveedores, 29.000+ titulares reales, 35 líderes y 330+ políticos). https://www.icij.org/investigations/pandora-papers/about-pandora-papers-investigation/
657. Wikipedia — *Panama Papers* (3 de abril de 2016; 11,5 millones de documentos de Mossack Fonseca, 214.488 entidades, 150 investigaciones en 79 países, cierre en 2018). https://en.wikipedia.org/wiki/Panama_Papers
658. Transparency International — *Panama Papers: 10 years on* (~1.360 M USD recuperados; reformas CTA, registros UE, ROE; «la arquitectura del secreto offshore permanece intacta»). https://www.transparency.org/en/news/panama-papers-10-years

659. FinCEN — *FinCEN Removes Beneficial Ownership Reporting Requirements for U.S. Companies* (norma provisional de marzo de 2025; exoneración de sociedades domésticas; población cubierta < 12.000). https://www.fincen.gov/news/news-releases/fincen-removes-beneficial-ownership-reporting-requirements-us-companies-and-us
660. Journal of Accountancy — *BOI update: 6.5 million of 32 million reports filed so far* (estimación original de 32 M de sociedades obligadas; 6,5 M presentadas en noviembre de 2024). https://www.journalofaccountancy.com/news/2024/nov/boi-update-6-5-million-of-32-million-reports-filed-so-far/
661. Transparency International — *EU court ruling on beneficial ownership registers: legitimate access* (sentencia del TJUE de 22 de noviembre de 2022; invalidación del acceso público; marco de interés legítimo). https://www.transparency.org/en/blog/eu-court-ruling-on-beneficial-ownership-registers-legitimate-access
662. PwC Ireland — *The EU's new Anti-Money Laundering Authority* (AMLA Fráncfort operativa desde el 1 de julio de 2025; AMLR (UE) 2024/1624 aplicable el 10 de julio de 2027; registros UBO interoperables). https://www.pwc.ie/services/audit-assurance/insights/eu-new-anti-money-laundering-authority.html
663. GOV.UK — *Companies House confirms identity verification rollout from 18 November 2025* (ECCTA; verificación de identidad de administradores y PSC; 100.400 sociedades afectadas, 10.200+ solicitudes rechazadas). https://www.gov.uk/government/news/companies-house-confirms-identity-verification-rollout-from-18-november-2025
664. Transparency International US — *Unanimous Eleventh Circuit decision upholds the Corporate Transparency Act* (16 de diciembre de 2025; tribunal de mayor rango en confirmar la constitucionalidad de la CTA). https://us.transparency.org/news/unanimous-eleventh-circuit-decision-upholds-the-corporate-transparency-act/
665. FATF — *Beneficial Ownership* (Recomendación 24 revisada en 2022 y guía de 2023; información adecuada, exacta y actualizada; enfoque multidimensional). https://www.fatf-gafi.org/en/topics/beneficial-ownership.html
666. Open Ownership — *Verification of beneficial ownership data: Overview* (los datos autodeclarados necesitan verificación: conformidad, contrastes cruzados, evidencia de apoyo). https://www.openownership.org/en/publications/verification-of-beneficial-ownership-data/overview/
667. KnowBe4 — *How a North Korean Fake IT Worker Tried to Infiltrate Us* (Stu Sjouwerman; relato en primera persona: foto de stock retocada con IA, cuatro entrevistas en vídeo, detección EDR del 15 de julio de 2024, granja de portátiles mula, FBI/Mandiant). https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us
668. FBI/IC3 — *Public Service Announcement I-012325-PSA: North Korean IT Workers Conducting Data Extortion* (23 de enero de 2025; cambio de cara con IA en las entrevistas, giro hacia la extorsión, recomendaciones de verificación de identidad). https://www.ic3.gov/PSA/2025/PSA250123
669. US DOJ (USAO-DC) — *Arizona Woman Sentenced in $17M IT Worker Fraud Scheme for North Korea* (24 de julio de 2025; Christina Chapman, 102 meses, 309 empresas, 68 identidades robadas, 17 M$, granja de portátiles, 49 portátiles enviados al extranjero). https://www.justice.gov/usao-dc/pr/arizona-woman-sentenced-17m-it-worker-fraud-scheme-illegally-generated-revenue-north
670. Crowell & Moring — *DOJ Announces Major Enforcement Actions Targeting North Korean Remote IT Worker Schemes* (14 de noviembre de 2025; más de 136 empresas víctimas, más de 18 identidades comprometidas, más de 2,2 M$ de beneficios). https://www.crowell.com/en/insights/client-alerts/doj-announces-major-enforcement-actions-targeting-north-korean-remote-it-worker-schemes
671. The Decoder — *Gartner predicts that by 2028, one in four job applicant profiles will be fake* (previsión del 25 % para 2028; admisión del 6 % de suplantación en la entrevista, encuesta a 3.000 candidatos). https://the-decoder.com/gartner-predicts-that-by-2028-one-in-four-job-applicant-profiles-will-be-fake/
672. People Management — *Deepfakes and AI-enabled impersonation rank among top recruitment threats* (19 de enero de 2026; First Advantage 69 % de los líderes del Reino Unido; Checkr 23 % de fraude de identidad; Greenhouse 91 %). https://www.peoplemanagement.co.uk/article/1945557/deepfakes-ai-enabled-impersonation-rank-among-top-recruitment-threats-research-reveals
673. Pindrop — *The Growing Trend of Deepfakes in Interviews* (audio IA en ~1 de cada 106 reuniones; ~1.300 % interanual; voces sintéticas en el 0,33 % de las llamadas en el Q4 de 2024).

https://www.pindrop.com/article/growing-trend-of-deepfakes-in-interviews/
674. NIST — *SP 800-63-4 Digital Identity Guidelines* (final, julio de 2025; niveles de garantía IAL1/2/3 y taxonomía de verificación Remoto/Presencial × Atendido/No Atendido). https://pages.nist.gov/800-63-4/sp800-63.html
675. FBI — *Fraudulent Remote IT Workers from DPRK* (búsqueda/recomendaciones; uso de identidades robadas, ordenadores intermediarios e IA, con mitigaciones para los empleadores). https://www.fbi.gov/wanted/cyber/fraudulent-remote-it-workers-from-dprk
676. Microsoft Security — *Fake Employees, Real Threat: Decentralized Identity to combat Deepfake Hiring* (credenciales verificables y verificación continua de la identidad de *onboarding*; contexto de solución adyacente). https://techcommunity.microsoft.com/blog/microsoft-security-blog/fake-employees-real-threat-decentralized-identity-to-combat-deepfake-hiring/4479864
677. Fiscalía General de Nueva York (2021). https://ag.ny.gov/press-release/2021/attorney-general-james-issues-report-detailing-millions-fake-comments-revealing
678. DOUE / BOE — *Directiva (UE) 2024/2831 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativa a la mejora de las condiciones laborales en el trabajo en plataformas* (en vigor el 2 de diciembre de 2024; transposición hasta el 2 de diciembre de 2026; presunción de laboralidad por hechos de dirección y control con carga de la prueba sobre la plataforma; prohibición de datos sensibles en decisiones automatizadas; transparencia, supervisión humana e intervención humana en decisiones importantes); Laboral Social — *Directiva sobre plataformas digitales de trabajo*. https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81667 · https://eur-lex.europa.eu/eli/dir/2024/2831/oj?eliuri=eli:dir:2024:2831:oj&locale=es · https://www.laboral-social.com/directiva-plataformas-digitales-trabajo-mejora-condiciones-laborales
679. BOE — *Ley 12/2021, de 28 de septiembre* («Ley Rider»: presunción de laboralidad en el reparto mediante gestión algorítmica; derecho del comité de empresa a ser informado de los parámetros, reglas e instrucciones de los algoritmos que afectan a las condiciones de trabajo; régimen en vigor desde agosto de 2021); PwC Periscopio — *¿Ha cumplido sus objetivos la Ley Rider?*. https://www.boe.es/buscar/act.php?id=BOE-A-2021-15767 · https://periscopiofiscalylegal.pwc.es/luces-y-sombras-de-la-ley-rider/
680. elDiario.es — *El jefe de Glovo admite a la jueza que la regularización de los 'riders' busca evitar «discusiones» con Inspección de Trabajo* (causa penal en Barcelona; ≈200 M€ en cuotas y multas; Just Eat reclama 295 M€); elDiario.es — *El jefe de Glovo dice que la presión penal y las multas forzaron cambiar su modelo laboral: «La caja no te da para operar»* (10.000-15.000 riders; provisiones de Delivery Hero de 440-770 M€; impacto ≈100 M€ en el EBITDA de 2025); Crónica Global — *Óscar Pierre justifica el cambio de modelo laboral por «presión económica y penal»*. https://www.eldiario.es/catalunya/jefe-glovo-admite-jueza-regularizacion-riders-busca-evitar-discusiones-inspeccion-trabajo_1_11870197.html · https://www.eldiario.es/economia/jefe-glovo-dice-presion-penal-multas-forzaron-cambiar-modelo-laboral-caja-no-da-operar_1_12062602.html · https://cronicaglobal.elespanol.com/business/20250218/oscar-pierre-de-glovo-justifica-laboral-economica/925157487_0.html
681. Fountain Court Chambers — *Amsterdam Court Upholds Appeal in Algorithmic Decision-Making Test Case: Drivers v Uber and Ola* (abril de 2023; tres sentencias; Ola ha de explicar la lógica de la decisión totalmente automatizada, art. 22 RGPD); Worker Info Exchange — *Uber ordered to pay €584,000 for failure to comply with court order in robo-firing case* (más 4.000 €/día); UK Human Rights Blog — *Amsterdam Court orders reinstatement of Uber drivers dismissed by algorithm*. https://fountaincourt.uk/2023/04/amsterdam-court-upholds-appeal-in-algorithmic-decision-making-test-case-drivers-v-uber-and-ola/ · https://www.workerinfoexchange.org/post/uber-ordered-to-pay-584-000-for-failure-to-comply-with-court-order-in-robo-firing-case/ · https://ukhumanrightsblog.com/2021/05/18/amsterdam-court-orders-reinstatement-of-uber-drivers-dismissed-by-algorithm/
682. t2p — manual de producto (huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; contenido en el dispositivo, revelación voluntaria; los vacíos de la serie quedan datados). Véanse los capítulos 13 y 15; la procedencia de los modelos de IA, en el capítulo 79.
683. Ministerio de Trabajo / prensa especializada — *Registro horario digital obligatorio: la reforma en trámite* (tramitación urgente aprobada por el Consejo de Ministros el 30-9-2025, desacoplada de la reducción de jornada; objetivo de aprobación durante 2026, sin fecha de entrada en vigor publicada; requisitos del proyecto: registros electrónicos trazables e inmutables, sellado de tiempo, registro de pausas, acceso remoto y en tiempo real para la Inspección de Trabajo, historial de modificaciones con autoría y fecha); EPA/INE — más del 40 % de las horas extra no se remuneran; RD-ley 8/2019

— registro diario de jornada obligatorio. https://www.protime.eu/es-es/noticias/registro-horario-digital-obligatorio-2026 · https://factorial.es/blog/nuevo-registro-horario-digital-espana/ · https://www.inwout.com/post/registro-horario-digital-obligatorio-2026 · https://kronjop.com/es/newsroom/control-horario/digital/obligatorio/

684. Marco laboral general (papeleta del juicio de lo social; actas de la Inspección de Trabajo; papel de los delegados). Véase el capítulo 92 para el trabajo de plataforma y el capítulo 102 para la cadena de suministro laboral.
685. t2p — manual de producto (foto con GPS forense —fijo genuino ~50 m / ≤30 s, la ubicación simulada bloquea la certificación; captura de pantalla y correo certificados; certificar cualquier fichero —solo la huella viaja; certificación en segundo plano; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; las conversaciones propias y el acoso, en el capítulo 75.
686. The Dial — *Faulty Construction* (juicios por el terremoto de Turquía; Isias Grand Hotel; condenas de 18 años en diciembre de 2024; 75.000 edificios amnistiados; unos 13 millones de edificios no conformes). https://www.thedial.world/articles/news/issue-25/turkey-earthquake-trials
687. PBS Peril & Promise — *How unenforced building codes worsened the Turkey-Syria earthquake* (julio de 2023; amnistías, no aplicación de los códigos y fallos de calidad del hormigón). https://www.pbs.org/wnet/peril-and-promise/2023/07/unenforced-building-codes-worsened-the-impacts-of-the-earthquake-that-hit-turkey-and-syria/
688. NIST — *Champlain Towers South Collapse* (investigación federal oficial; 98 muertos; inicio por fallo de punzonamiento de la losa de la piscina; hormigón más débil que el código). https://www.nist.gov/disaster-failure-studies/champlain-towers-south-collapse
689. ICAC Hong Kong — *Consultant director jailed over false HZMB concrete cube test records* (19 trabajadores imputados; 384 informes falsificados; manipulación de fechas y sustitución de probetas; Albert Leung 2,5 años en junio de 2024). https://www.icac.org.hk/en/p/press/index_id_1890.html
690. The Real Deal — *Concrete tester exec convicted of falsifying safety reports for Yankee Stadium, Freedom Tower* (febrero de 2010; Testwell/Kancharla; Freedom Tower certificada a 12.000 PSI pero de unos 9.000 PSI; 7 a 21 años). https://therealdeal.com/new-york/2010/02/17/concrete-tester-exec-convicted-of-falsifying-safety-reports-for-yankee-stadium-freedom-tower/
691. Wikipedia — *Ponte Morandi collapse* (Génova, 14 de agosto de 2018; 43 muertos; 59 acusados; documentos de inspección «claramente falsos»; autovigilancia vía Spea; acuerdo de 30 M€ en 2023). https://en.wikipedia.org/wiki/Ponte_Morandi_collapse
692. Seton UK — *Understanding the Golden Thread: Building Safety Act 2022* (registro digital trazable y con control de versiones para edificios de alto riesgo, posterior a Grenfell). https://www.seton.co.uk/legislationwatch/article/understanding-the-golden-thread-the-building-safety-act-2022/
693. EUR-Lex — *Regulation (EU) 2024/3110* (Reglamento de Productos de Construcción revisado; en vigor el 7 de enero de 2025; Pasaporte Digital de Producto obligatorio para el marcado CE desde el 8 de enero de 2026). https://eur-lex.europa.eu/eli/reg/2024/3110/oj/eng
694. NIST — *Report to Congress provides update on Champlain Towers South investigation* (febrero de 2025; trabajo experimental completo, modelización en curso, presentación técnica en junio de 2025). https://www.nist.gov/news-events/news/2025/02/nist-report-congress-provides-update-champlain-towers-south-investigation
695. BSI — *ISO 19650 Building Information Modelling standards* (gestión de la información con BIM y registro as-built / gemelo digital a lo largo del ciclo de vida). https://www.bsigroup.com/en-GB/products-and-services/standards/iso-19650-building-information-modelling-bim/
696. SFO (GOV.UK) — *SFO secures 4-year prison sentence for aircraft parts fraud* (Zamora Yrala; 60.000 piezas; fraude de 39,3 M£; ARC falsificados; condena de 4 años y 8 meses; descubrimiento por Safran). https://www.gov.uk/government/news/sfo-secures-4-year-prison-sentence-for-aircraft-parts-fraud
697. SFO (GOV.UK) — *SFO case page: AOG Technics Ltd* (página oficial de la causa de la Serious Fraud Office). https://www.gov.uk/sfo-cases/aog-technics-ltd
698. Fortune — *Fake components went into 68 jet engines on Boeing 737 and Airbus A320 planes, lawsuit says* (demanda de CFM International: 78 documentos falsificados, 52 referencias del CFM56, 68 motores, álabes de turbina). https://fortune.com/2023/09/08/fake-components-68-jet-engines-boeing-737-airbus-a320-planes-lawsuit/

699. FAA — *Suspected Unapproved Parts (SUP) Program* (trazabilidad según 14 CFR Part 21/43, Form 8130-3, report con Form 8120-11). https://www.faa.gov/aircraft/safety/programs/sups
700. EASA — *Suspected Unapproved Parts* (base de datos y definiciones de la UE; casos de EASA Form 1 falsificados; marco de los SIB). https://www.easa.europa.eu/en/domains/aircraft-products/suspected-unapproved-parts
701. EASA — *Safety Information Bulletin SIB 2023-05* (boletín sobre las piezas sospechosas de AOG Technics y acciones de cuarentena/reemplazo recomendadas). https://ad.easa.europa.eu/blob/EASA_SIB_2023_05.pdf/SIB_2023-05_1
702. GE Aerospace — *Coalition delivers report to help prevent future unapproved parts entering aviation* (Aviation Supply Chain Integrity Coalition: 13 recomendaciones, 9 de octubre de 2024; digitalizar 8130-3/Form 1; trazabilidad; acreditación de proveedores). https://www.geaerospace.com/news/press-releases/coalition-delivers-report-help-prevent-future-unapproved-parts-entering-aviation
703. Connector Supplier — *Counterfeit Components Ground Airlines* (~520.000 piezas falsificadas o no aprobadas llegan a los aviones cada año, ~2 % de 26 millones; mercado de más de 2.000 M$). https://connectorsupplier.com/counterfeit-components-ground-airlines/
704. PR Newswire / CARFAX — *Odometer rollbacks see dramatic jump of 14% to 2.45 million vehicles* (diciembre de 2025; 2,45 millones de vehículos sospechosos; +14 % interanual; ~3.300 $ de pérdida media). https://www.prnewswire.com/news-releases/carfax-odometer-rollbacks-see-dramatic-jump-of-14-to-2-45-million-vehicles-302643855.html
705. EPA — *Volkswagen Clean Air Act Civil Settlement* (acuerdos 2016-2017; sanción civil de 1.450 millones de dólares; fondo de mitigación; ~590.000 vehículos en EE. UU.; descripción del dispositivo de desactivación). https://www.epa.gov/enforcement/volkswagen-clean-air-act-civil-settlement
706. Wikipedia — *Volkswagen emissions scandal* (NOx hasta 40 veces el límite; ~11 millones de coches; ~33.000 millones de dólares de coste total; cronología global). https://en.wikipedia.org/wiki/Volkswagen_emissions_scandal
707. EPA — *United States and California Announce Diesel Engine Manufacturer Cummins Inc. Agrees to Pay Record $1.675 Billion Civil Penalty* (10 de enero de 2024; la sanción civil más alta bajo la Clean Air Act; 630.000+ camiones RAM; 325 M$ en remedios; condiciones de la revisión). https://www.epa.gov/newsreleases/united-states-and-california-announce-diesel-engine-manufacturer-cummins-inc-agrees
708. EPA — *Summary of Criminal Prosecutions: Berkshire Power* (sesgo intencionado del CEMS, 2009-2011; ajuste fraudulento retirado antes de las auditorías; multa penal de 2,75 M$ a BPC; ~7,25 M$ en total en marzo de 2017). https://cfpub.epa.gov/compliance/criminal_prosecution/index.cfm?action=3&prosecution_summary_id=2981
709. AIE — *Global Methane Tracker 2024, Key Findings* (cerca de 120 Mt de metano fósil en 2023; UNFCCC ~50 % más bajo; OGMP 2.0 ~95 % más bajo; eventos de fuga por satélite +50 % interanual). https://www.iea.org/reports/global-methane-tracker-2024/key-findings
710. MethaneSAT (EDF) — *New Data Show US Oil and Gas Methane Emissions Over Four Times Higher Than EPA Estimates* (emisiones medidas >4 veces las estimaciones de la EPA; tasa de pérdida del 1,6 %, ocho veces el objetivo del 0,2 %; 30+ vuelos cubriendo ~70 % de la producción terrestre de EE. UU.). https://www.methanesat.org/project-updates/new-data-show-us-oil-and-gas-methane-emissions-over-four-times-higher-epa-estimates
711. EPA — *EPA and Justice Department Announce $241.5M Settlement with Marathon Oil* (11 de julio de 2024; 64,5 M$ de sanción civil, la más alta a una fuente fija; ~90 instalaciones; ~110.000 toneladas de COV/metano recortadas). https://www.epa.gov/newsreleases/epa-and-justice-department-announce-2415m-settlement-marathon-oil-reduce-climate-and
712. CJEU — *Press release on the July 2022 judgment that thermal-window defeat devices are in principle illegal* (PDF; definición legal del dispositivo de desactivación; sentencia previa de diciembre de 2020 sobre el reconocimiento del ciclo de prueba). https://curia.europa.eu/site/upload/docs/application/pdf/2022-07/cp220124en.pdf
713. EPA — *Key Things to Know About EPA's Final Methane Rule* (hoja informativa PDF; 58 millones de toneladas de metano evitadas 2024-2038; reducción del ~80 %; Programa de superemisores). https://www.epa.gov/system/files/documents/2023-12/key-things-to-know-about-epas-final-rule-for-oil-and-natural-gas-operations.fact-sheet.pdf
714. Comisión Europea — *New EU Methane Regulation to reduce emissions from fossil fuels* (Reglamento (UE) 2024/1787; MRV a escala de fuente con verificación de terceros; alerta rápida de superemisores por satélite; equivalencia MRV para los importadores desde 2027).

https://energy.ec.europa.eu/news/new-eu-methane-regulation-reduce-harmful-emissions-fossil-fuels-europe-and-abroad-2024-05-27_en

715. El Ágora Diario — *Europa condena a España por no proteger el agua y hábitats de Doñana* (sentencia del TJUE de 24 de junio de 2021; extracciones ilegales no computadas en el Plan Hidrológico 2015-2021; quejas desde 2009); Greenpeace — *Doñana, agua sin ley* (pozos, balsas y tuberías; invernaderos de fresas; deforestaciones). https://www.elagoradiario.com/agua/tribunal-justicia-europa-condena-espana-agua-donana/ · https://es.greenpeace.org/es/en-profundidad/sos-acuiferos/donana-agua-sin-ley/
716. BOE — *Ley 19/2022, de 30 de septiembre, para el reconocimiento de personalidad jurídica a la laguna del Mar Menor y su cuenca* (primer ecosistema de Europa; derechos a existir, evolucionar, protección, conservación y restauración; ILP con 639.826 firmas); Araoz & Rueda — *El TC reconoce la personalidad jurídica del Mar Menor*; BOE — *Real Decreto 90/2025* (comité de representantes: 13 miembros, 7 de la sociedad civil); Newtral — *Qué significa que el Mar Menor haya adquirido personalidad jurídica*. https://www.boe.es/buscar/doc.php?id=BOE-A-2022-16019 · https://www.araozyrueda.com/el-tribunal-constitucional-reconoce-mar-menor-sujeto-de-derechos/ · https://www.boe.es/diario_boe/txt.php?id=BOE-A-2025-2577 · https://www.newtral.es/mar-menor-personalidad-juridica/20220923/
717. Sensor.Community / World Air Quality Index — *Red de sensores de calidad del aire en tiempo real (antes luftdaten.info)* (más de 100 países; sensores ciudadanos de bajo coste); AireCiudadano — red abierta de monitores de partículas con mapa y API; SciStarter/CanAirIO — sensores abiertos de PM2,5. https://aqicn.org/network/luftdaten/es/ · https://aireciudadano.com/ · https://scistarter.org/crea-tu-propio-sensor-de-calidad-del-aire-con-cana
718. Perito Judicial — *Ruidos molestos y su reclamación: la clave está en la medición* (inspección municipal con sonómetro homologado y calibrado; actas con presunción de veracidad y pleno valor probatorio; límites interiores orientativos 35-45 dB día / 25-30 dB noche); COITTA — *La importancia de la prueba pericial acústica*; Defensor del Pueblo — *Comprobaciones ante las denuncias de ruidos molestos* (habilitar medios para comprobar las denuncias). https://peritojudicial.com/ruidos-molestos/ · https://www.aagit.org/la-importancia-de-la-prueba-pericial-acustica-y-la-proteccion-juridica-frente-al-ruido-como-agente-contaminante/ · https://www.defensordelpueblo.es/resoluciones/habilitar-los-medios-para-poder-realizar-comprobaciones-necesarias-cuando-se-denuncien-ruidos-molestos/
719. t2p — manual de producto (huella SHA-512 en el origen —sensor o dispositivo—; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; contenedor .asice; series por lotes en tiempo real; vacíos datados; contenido en el dispositivo y revelación voluntaria). Véanse los capítulos 13 y 15; el sensor industrial, en el capítulo 96; el testigo orbital, en el capítulo 104.
720. EUR-Lex — *Sustainability rules for batteries and waste batteries (Regulation (EU) 2023/1542 summary)* (pasaporte desde 2027 vía QR e identificador único; objetivos de contenido reciclado desde el 18 de agosto de 2031: Co 16 %, Pb 85 %, Li 6 %, Ni 6 %; acceso aduanero al registro). https://eur-lex.europa.eu/EN/legal-content/summary/sustainability-rules-for-batteries-and-waste-batteries.html
721. DigiProdPass — *EU Battery Regulation: Recycled Content Targets (2031-2036)* (porcentajes de 2031 —Co 16/Pb 85/Li 6/Ni 6— y de 2036 —Co 26/Pb 85/Li 12/Ni 15—, las afirmaciones falsificables que el pasaporte transporta). https://digiprodpass.com/blogs/eu-battery-regulation-recycled-content-targets
722. Minespider — *EU Battery Due Diligence Obligations postponed* (diligencia debida aplazada del 18 ago 2025 al 18 ago 2027 vía Reglamento (UE) 2025/1561 «stop-the-clock»; guía ampliada hasta el 26 jul 2026). https://www.minespider.com/blog/eu-battery-due-diligence-postponed-what-it-means-for-companies
723. Electrek — *Volvo EX90 launches world's first EV battery passport* (4 jun 2024; cinco años de desarrollo con Circulor; ~10 $/vehículo por 15 años; QR en el montante de la puerta; traza materiales, contenido reciclado y huella de carbono). https://electrek.co/2024/06/04/volvo-ex90-launch-worlds-first-ev-battery-passport/
724. IEEE Spectrum — *Volvo's Battery Passport Traces the Supply Chain* (más de 20.000 millones de puntos de datos en 150 millones de celdas; ~52 % de los fabricantes mundiales de celdas; 15 años de monitorización de estado de salud). https://spectrum.ieee.org/volvo-ex90-battery-passport
725. Global Battery Alliance — *World's First Battery Passport Proof of Concept* (Davos, 18 ene 2023; Audi/BASF/CATL/Glencore/Tesla/VW; los datos «no han sido plenamente verificados y se han complementado parcialmente con estimaciones razonables»). https://www.globalbattery.org/press-

releases/global-battery-alliance-launches-world%E2%80%99s-first-battery-passport-proof-of-concept/

726. Comisión Europea (Green Forum) — *Implementing the Ecodesign for Sustainable Products Regulation (ESPR)* (ESPR en vigor el 18 jul 2024; el pasaporte digital de producto como herramienta horizontal; plan de trabajo 2025-2030 adoptado el 16 abr 2025). https://green-forum.ec.europa.eu/implementing-ecodesign-sustainable-products-regulation_en
727. Hogan Lovells — *Digital Product Passports in the EU: expansion under ESPR and lessons from the Battery Passport pilot* (análisis jurídico que distingue el piloto de baterías del despliegue horizontal del ESPR; calendario de actos delegados). https://www.hoganlovells.com/en/publications/digital-product-passports-in-the-eu-comprehensive-expansion
728. CIRPASS — *Standardisation gaps and roadmap (v1.2, July 2024)* (modelo de datos del DPP, identificadores únicos, portadores de datos y lagunas de estandarización del JTC 24 —la arquitectura donde se enchufa el sello). https://cirpassproject.eu/wp-content/uploads/2024/07/CIRPASS-standardisation-gaps-and-roadmap-V1.2.pdf
729. DOUE/BOE — *Reglamento (UE) 2024/1157, de 11 de abril de 2024, relativo a los traslados de residuos* (deroga el Reglamento 1013/2006; aplicable de manera general desde el 21 de mayo de 2026; exportaciones de todos los residuos plásticos a terceros países sujetas a notificación y autorización previas por escrito; prohibición de exportar residuos para valorización a países no OCDE; tramitación electrónica); RETEMA — *Nuevo Reglamento de traslados de residuos*; Residuos Profesional — *Análisis del Reglamento (UE) 2024/1157* (contexto: Turquía recibió el 39 % de las exportaciones europeas de residuos —12,4 millones de toneladas, datos 2022). https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-80606 · https://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:32024R1157 · https://www.retema.es/blog/nuevo-reglamento-de-traslados-de-residuos-la-normativa-que-pone-en-jaque-la-industria-europea · https://www.residuosprofesional.com/reglamento-relativo-traslados-de-residuos/
730. Marco general de residuos (documentos de identificación y seguimiento de los traslados; responsabilidad ampliada del productor; jerarquía de residuos). Véase el capítulo 98 para el pasaporte digital de producto y el capítulo 96 para las emisiones.
731. t2p — manual de producto (foto con GPS forense —fijo genuino ~50 m / ≤30 s, la ubicación simulada bloquea la certificación; vídeo con fecha/hora sobreimpresa; escáner de documentos hasta 50 páginas; certificar cualquier fichero por lotes —solo la huella viaja; captura de página web con imagen completa + código fuente; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; el pasaporte de producto, en el capítulo 98; la ciencia ciudadana, en el capítulo 97.
732. Agrodigital — *El cuaderno digital de explotación será obligatorio a partir del 1 de enero de 2028* (CUE voluntario desde el 1-1-2024; aplazamientos; obligatorio desde el 1-1-2028 para explotaciones >30 ha de cultivos, >5 ha de regadío o >0,1 ha de invernadero; registro electrónico de tratamientos fitosanitarios obligatorio desde el 1-1-2027 —papel hasta el 31-12-2026); FEGA/Agronews — aclaraciones de entrada en vigor; Gobierno de Aragón — *Cuaderno digital (CUE)* (contenido: actuaciones fitosanitarias, fertilización, riegos y otras prácticas). https://agrodigital.info/2025/01/23/el-cuaderno-digital-de-explotacion-sera-obligatorio-a-partir-del-1-de-enero-de-2028/ · https://www.agronewscastillayleon.com/el-fega-publica-aclara-la-entrada-en-vigor-del-cuaderno-de-explotacion-y-el-plan-de-abonado/ · https://www.aragon.es/pac-2026/cuaderno-digital-cue · https://www.fega.gob.es/sites/default/files/files/document/10.2023.03.15-12.45h_blq-04_inmaculada-bravo_cue.el-cue-y-el-riego.pdf
733. PAC 2023-2027 — sistema de seguimiento por monitorización (imágenes Sentinel/Copernicus sobre las parcelas declaradas en el SIGPAC; requerimientos de fotografías georreferenciadas al agricultor cuando el sistema no puede concluir). Marco general del FEGA y de la Comisión Europea. Véase el capítulo 104 para la integridad del testigo orbital.
734. t2p — manual de producto (foto con GPS forense —fijo genuino ~50 m / ≤30 s, la ubicación simulada bloquea la certificación; certificación en segundo plano —el campo sin cobertura; certificar cualquier fichero por lotes; escáner de documentos; proyectos para el expediente de una campaña; huella SHA-512 en el dispositivo; anclaje de la huella en la blockchain pública; sello de tiempo RFC 3161/eIDAS complementario; certificado PDF con QR; paquete .asice verificable sin conexión). Véanse los capítulos 13 y 15; el satélite, en el capítulo 104; los alimentos, en el capítulo 101; los residuos, en el capítulo 99.

735. Europol — *EUR 91 million worth of counterfeit and substandard food seized in Europe-wide operation* (Operación OPSON XIII; 22.000 t de alimentos, 91 M€, 11 redes; Italia: virgen extra y clorofila; España: aceite y atún). https://www.europol.europa.eu/media-press/newsroom/news/eur-91-million-worth-of-counterfeit-and-substandard-food-seized-in-europe-wide-operation
736. Europol — *Counterfeit and substandard food worth EUR 95 million seized in global operation* (Operación OPSON XIV; 95 M€, 11.566 t, 631 denunciados, 13 grupos de crimen organizado, 31 países). https://www.europol.europa.eu/media-press/newsroom/news/counterfeit-and-substandard-food-worth-eur-95-million-seized-in-global-operation
737. CNN — *Italian authorities confiscate almost $1 million in fake olive oil* (11 de julio de 2024; registro de los Carabinieri en la Apulia, 42 t de falso virgen extra, 623 L de clorofila, 7 acusados, etiquetas y sellos falsos). https://www.cnn.com/2024/07/11/europe/italy-olive-oil-seizure-scli-intl/
738. Food Safety News — *Spanish and Italian investigators uncover olive oil fraud* (diciembre de 2023; Operación Omegabad: 260.000 L requisados, 11 detenciones, lampante vendido como virgen extra, Ciudad Real/Sicilia/Toscana, 91.000 € en efectivo). https://www.foodsafetynews.com/2023/12/spanish-and-italian-investigators-uncover-olive-oil-fraud/
739. Comisión Europea (DG SANTE) — *EU coordinated action on honey ('From the Hives')* (muestras 2021-2022; 46 % de 320 partidas sospechosas de adulteración con jarabe de azúcar; metodología y países participantes). https://food.ec.europa.eu/food-safety/eu-agri-food-fraud-network/eu-coordinated-actions/honey-2021-2022_en
740. FoodNavigator — *Geographical Indications worth a mouth-watering €75 billion, study finds* (valor de las IG de la UE: 74.800 M€ en 2017; prima de precio de unas 2 veces para los productos protegidos). https://www.foodnavigator.com/Article/2020/04/22/Geographical-Indications-worth-a-mouth-watering-75-billion-study/
741. Comisión Europea — *EU Agri-Food Fraud Network: reports and publications* (el fraude afecta a ~1 % de la industria y cuesta 10.000-40.000 M$/año; 758 sospechas en 2023, +26 %; carne, miel y aceite a la cabeza). https://food.ec.europa.eu/food-safety/eu-agri-food-fraud-network/reports-and-publications_en
742. EUR-Lex — *Regulation (EU) 2024/1143 on geographical indications* (en vigor el 13 de mayo de 2024; marco único de DOP/IGP/IG y ETG; protección como ingrediente y en línea). https://eur-lex.europa.eu/eli/reg/2024/1143/oj/eng
743. Food Safety News — *Four sentenced in France for roles in horse meat scandal* (juicio de 2019; Poujol (Spanghero) 2 años + 100.000 € de multa, Fasen 2 años + prohibición permanente; Comigel, 500+ t hacia 13 países). https://www.foodsafetynews.com/2019/04/four-sentenced-in-france-for-roles-in-horse-meat-scandal/
744. FDA — *Economically Motivated Adulteration (Food Fraud)* (definición de EMA, p. ej. aceite barato vendido como 100 % aceite de oliva; deber de controles preventivos de la FSMA). https://www.fda.gov/food/compliance-enforcement-food/economically-motivated-adulteration-food-fraud
745. Sensors (MDPI) — *Blockchain and IoT for food traceability in olive oil supply chains* (2024; estado del arte en sellado/anclaje de la procedencia del aceite y en autenticación analítica NMR/IRMS). https://www.mdpi.com/1424-8220/24/24/8189
746. OIT — *Data and research on forced labour (Global Estimates 2022)* (27,6 millones de personas en trabajo forzoso en 2021; 17,3 millones en la economía privada; los migrantes triplican el riesgo). https://www.ilo.org/topics/forced-labour-modern-slavery-and-trafficking-persons/data-and-research-forced-labour
747. OIT — *Annual profits from forced labour amount to US$236 billion* (marzo de 2024; +37 % desde 2014; 84.000 millones en Europa y Asia Central). https://www.ilo.org/resource/news/annual-profits-forced-labour-amount-us-236-billion-ilo-report-finds
748. Miller & Chevalier — *UFLPA Enforcement 2024 Year in Review* (16.755 envíos y 3.690 M$ retenidos; 1.340 M$ en 2024; 48 % de entradas denegadas; +1.600 % en el automóvil; *Entity List* a 144). https://www.millerchevalier.com/publication/trade-compliance-flash-uflpa-enforcement-2024-year-review
749. Business & Human Rights Resource Centre — *Volkswagen cars held up at US ports over part linked to allegations of forced labour in Xinjiang* (marcas, subcomponente, cronología diciembre 2023 – mediados de enero 2024). https://www.business-humanrights.org/en/latest-news/volkswagen-cars-held-up-at-us-ports-over-part-linked-to-allegations-of-forced-labour-in-xinjiang/

750. Human Rights Watch — *Asleep at the Wheel: Car Companies' Complicity in Forced Labor in China* (febrero de 2024; VW, BMW, Mercedes, GM y la cadena del aluminio). https://www.hrw.org/report/2024/02/01/asleep-wheel/car-companies-complicity-forced-labor-china
751. Comisión Europea — *Corporate Sustainability Due Diligence (CSDDD)* (Directiva 2024/1760, en vigor el 25 de julio de 2024; transposición hasta el 26 de julio de 2028, aplicación desde el 26 de julio de 2029 tras el Ómnibus). https://commission.europa.eu/business-economy-euro/doing-business-eu/sustainability-due-diligence-responsible-business/corporate-sustainability-due-diligence_en
752. Covington — *EU Forced Labour Regulation Enters Into Force* (diciembre de 2024; en vigor el 13 de diciembre de 2024, aplicación el 14 de diciembre de 2027; modelo de investigación sin presunción geográfica). https://www.cov.com/en/news-and-insights/insights/2024/12/eu-forced-labour-regulation-enters-into-force
753. BAFA — *Supply Chain Act (LkSG): Overview* (aplicación a empresas de 1.000 empleados desde el 1 de enero de 2024; multas hasta el 2 % de la facturación mundial; 486 auditorías en 2023). https://www.bafa.de/EN/Supply_Chain_Act/Overview/overview_node.html
754. ECCHR — *More for show than safety: Certificates in the textile industry* (Rana Plaza, 1.131 muertos, BSCI; Ali Enterprises, más de 250 muertos, SA8000; ambas habían pasado la inspección). https://www.ecchr.eu/en/case/more-for-show-than-safety-certificates-in-the-textile-industry/
755. Human Rights Watch — *Obsessed with Audit Tools, Missing the Goal: Why Social Audits Can't Fix Labor Rights Abuses* (noviembre de 2022; trabajadores aleccionados, dobles libros, nóminas falsas, niños escondidos). https://www.hrw.org/report/2022/11/15/obsessed-audit-tools-missing-goal/why-social-audits-cant-fix-labor-rights-abuses
756. COSH — *Living wages for EU garment workers* (el salario mínimo legal es el 31 % de un salario digno en la India, el 37 % en China y Bangladés, el 33 % en Camboya, el 13 % en Sri Lanka). https://cosh.eco/en/articles/living-wages-eu-garment-workers
757. GPS spoofing is scrambling ships in the Strait of Hormuz — *Scientific American* (spoofing en Ormuz durante la guerra Israel-Irán de 2025; buques sobre tierra y centrales nucleares; atribución de Humphreys a Irán; ~20 % del petróleo mundial por el estrecho). https://www.scientificamerican.com/article/gps-spoofing-is-scrambling-ships-in-the-strait-of-hormuz/
758. Iran's $800M oil-smuggling scheme uses tankers posing as Iraqi ships — *Fox News* (revelación de Windward, 29 de abril de 2026; VLCC con números IMO; escalas falsas en Khor al Zubair). https://www.foxnews.com/world/irans-800m-oil-smuggling-scheme-uses-tankers-posing-iraqi-ships-dodge-blockade-.amp
759. AIS spoofing: the fast track to sanctions — *Kpler* (261 buques falsearon el AIS antes de ser sancionados, enero 2024-julio 2025; escalas falsas en Khor al Zubair). https://www.kpler.com/blog/ais-spoofing-fast-track-to-sanctions
760. Maritime GNSS Interference Worldwide: A Cumulative Analysis 2025 — *GPSPATRON* (10.000+ buques afectados en el 2T 2025, ocho veces más que el 1T; puntos calientes regionales). https://gpspatron.com/maritime-gnss-interference-worldwide-a-cumulative-analysis-2025/
761. Widespread GPS jamming hits 1,000-plus ships in the Middle East Gulf — *Windward* (1 de marzo de 2026: 1.100+ buques en 24 h, 21+ núcleos; fijaciones falsas en Barakah y Al Hamra; Ormuz un tercio a la baja). https://windward.ai/blog/gps-jamming-disrupts-1100-ships-in-the-middle-east-gulf/
762. Russian Shadow Fleet Tracker — *Kyiv School of Economics (KSE) Institute* (tamaño de la flota; ~17 % de la flota petrolera mundial; 9.400 M$ de ingresos extra en 2024; peso creciente de la bandera rusa). https://kse.ua/about-the-school/news/russian-shadow-fleet-tracker-march-2026-share-of-russian-flagged-shadow-tankers-jumps-from-3-to-21-in-nine-months/
763. Council sanctions 41 vessels of the Russian shadow fleet — *Consejo de la UE (Consilium)* (18 de diciembre de 2025: el total de la UE llega a 444+ buques; prohibiciones de acceso a puerto y de servicios). https://www.consilium.europa.eu/en/press/press-releases/2025/12/18/russia-s-war-of-aggression-against-ukraine-council-sanctions-41-vessels-of-the-russian-shadow-fleet/
764. EU adopts 18th package of economic and individual measures — *Consejo de la UE (Consilium)* (18 de julio de 2025: techo del crudo rebajado de 60 a 47,60 $ con mecanismo dinámico 15 % por debajo del mercado). https://www.consilium.europa.eu/en/press/press-releases/2025/07/18/russia-s-war-of-aggression-against-ukraine-eu-adopts-18th-package-of-economic-and-individual-measures/
765. Treasury Maintains Pressure on Iranian Shadow Fleet (MS ENOLA) — *U.S. Department of the Treasury / Iran Primer* (diciembre de 2024; acción de la OFAC bajo la E.O. 13902 citando el MS

ENOLA «apagando el AIS»). https://iranprimer.usip.org/blog/2024/dec/19/us-sanctions-more-irans-dark-fleet
766. Estlink 2 incident / Eagle S shadow-fleet tanker — *NPR* (petrolero Eagle S de bandera de las Islas Cook, 25 de diciembre de 2024, daño al cable submarino del Báltico; dimensión de amenaza híbrida). https://www.npr.org/2024/12/31/nx-s1-5243302/finland-russia-severed-undersea-cable-shadow-fleet
767. AIS spoofing: vessel-identity manipulation typologies — *Lloyd's List Intelligence* (blanqueo de identidad, fraude del número IMO, apretón de manos AIS y mecánica del spoofing de posición). https://www.lloydslistintelligence.com/resources/blog/the-secret-lives-of-the-shadow-fleet-ais-spoofing-vessel-identity-manipulation
768. The Moscow Times — *Satellite Images Show Bodies in Bucha for Weeks, Rebutting Moscow Claim* (5 de abril de 2022; nueve imágenes de Maxar del 18/19/31 de marzo; cuerpos en la calle Yablónska; fosa común de 14 metros). https://www.themoscowtimes.com/2022/04/05/satellite-images-show-bodies-in-bucha-for-weeks-rebutting-moscow-claim-a77211
769. Aerospace America / AIAA — *Maxar describes its role in Bucha revelations* (captura del WorldView-3; Daniel Jablonsky sobre la recogida intensiva de Maxar; uso del New York Times el 4 de abril de 2022). https://aerospaceamerica.aiaa.org/maxar-bucha-insights/
770. BuzzFeed News — *Blanked-Out Spots On China's Maps Helped Us Uncover Xinjiang's Camps* (método ganador de un Pulitzer; imagen de Planet y teselas censuradas; 268 campos nuevos y 428 emplazamientos sospechosos). https://www.buzzfeednews.com/article/alison_killing/satellite-images-investigation-xinjiang-detention-camps
771. *Deepfake Geography: Detecting AI-Generated Satellite Images* (arXiv 2511.17766, noviembre de 2025; ViT 95,11 % frente a CNN 87,02 % sobre más de 130.000 imágenes; artefactos GAN frente a difusión). https://arxiv.org/abs/2511.17766
772. *Generating Synthetic Satellite Imagery With Deep-Learning Text-to-Image Models* (arXiv 2404.07754, abril de 2024; Nguyen, Glaser y Biessmann; imagen sintética fotorrealista de instalaciones incluidas centrales nucleares; control de armamento). https://arxiv.org/abs/2404.07754
773. Comisión Europea — *Observer: How Galileo OSNMA helps counter GNSS spoofing* (OSNMA operativo el 24 de julio de 2025; primera autenticación mundial de la señal del Servicio Abierto de un GNSS vía firmas criptográficas TESLA). https://defence-industry-space.ec.europa.eu/observer-how-galileo-osnma-helps-counter-gnss-spoofing-2025-09-08_en
774. SpaceNews — *NGA to launch $700 million program to help AI make sense of satellite images* (contrato de etiquetado Sequoia de hasta 708 M$ en 7 años, 2024; alimenta la visión por computador Maven; el contrato de datos mayor de la agencia). https://spacenews.com/nga-to-launch-700-million-program-to-help-ai-make-sense-of-satellite-images/
775. Open Geospatial Consortium — *Navigating Synthetic Imagery Trust in Geospatial Data* (iniciativa Integridad, Procedencia y Confianza, abril de 2025; define integridad/procedencia/confianza, pero sin firma criptográfica ni cadena de bloques). https://www.ogc.org/blog-article/navigating-synthetic-imagery-trust-geospatial-data/
776. Maldita.es — *Quién envió la alerta de las 20:11 horas en Valencia, qué dice el protocolo* (31 de octubre de 2024; ES-Alert a las 20:11 y 21:03; en nivel 2 la petición corresponde a la comunidad autónoma). https://maldita.es/malditateexplica/20241031/generalitat-valenciana-responsable-alerta-movil/
777. elDiario.es — *El envío de la alerta masiva a móviles se planteó en la reunión clave de la DANA pasadas las 18.00, dos horas antes* (CECOPI convocado a las 15:00, reunido a las 17:00; propuesta de alerta masiva pasadas las 18:00). https://www.eldiario.es/comunitat-valenciana/reunion-clave-dana-debatio-enviar-alerta-masiva-moviles-pasadas-18-00-horas_1_11802363.html
778. France 24 — *En cifras: 229 muertos y 17.800 millones de euros en pérdidas, a un año de la DANA* (28 de octubre de 2025). https://www.france24.com/es/europa/20251028-en-cifras-229-muertos-y-17-800-millones-de-euros-en-p%C3%A9rdidas-a-un-a%C3%B1o-de-la-dana
779. Wikipedia — *Inundaciones de la DANA de 2024 en España* (237 muertos en total: 229 en la provincia de Valencia, 7 en Castilla-La Mancha, 1 en Málaga; más de 2.600 heridos; 11.242 viviendas; ≈141.000 vehículos; 800 km de carreteras). https://es.wikipedia.org/wiki/Inundaciones_de_la_DANA_de_2024_en_Espa%C3%B1a
780. Maldita.es — *Qué sabemos de los datos de la riada en la Rambla del Poyo durante la DANA* (7 de noviembre de 2024; correos de la CHJ de las 13:42, 15:04, 16:13 y 18:43; caudales de las 17:00 y las 18:00; 2.282 m³/s a las 18:55; la estación de aforo, destruida por el agua hacia las 19:00, según el

comunicado de la CHJ del 4 de noviembre). https://maldita.es/clima/20241107/datos-rambla-poyo-dana-valencia/

781. El Debate — *«A las 17.40 del día de la dana la CHJ registró que el caudal del barranco del Poyo era cinco veces superior al del Ebro»* (24 de febrero de 2026). https://www.eldebate.com/espana/comunidad-valenciana/20260224/1740-dia-dana-chj-registro-caudal-barranco-poyo-cinco-veces-superior-ebro_388667.html
782. El Debate — *La Confederación del Júcar borra datos críticos del caudal del Poyo en plena crisis de la DANA* (5 de noviembre de 2024); esDiario — *Desaparecen y reaparecen los datos del barranco del Poyo de la web de la CHJ*. https://www.eldebate.com/espana/comunidad-valenciana/20241105/confederacion-jucar-borra-datos-criticos-caudal-poyo-plena-crisis-dana-valencia_242165.html · https://www.esdiario.com/comunidad-valenciana/241105/146265/desparecen-aparecen-datos-barranco-poyo-web-chj.html
783. Actualidad Valencia — *La CHJ omitió barrancos clave en su red de control y ocultó un medidor en Massanassa, según revela el SAIH*. https://actualidadvalencia.com/control-caudal-chj-barrancos-horteta-gallego-massanassa/
784. ORM — *La jueza de Catarroja llama a declarar como investigados en la causa por la DANA a Salomé Pradas y Emilio Argüeso* (instrucción abierta el 10 de marzo de 2025; Juzgado de Instrucción n.º 3 de Catarroja, jueza Nuria Ruiz Tobarra). https://www.orm.es/informativos/la-jueza-de-catarroja-llama-a-declarar-como-investigados-en-la-causa-por-la-dana-a-salome-pradas-y-emilio-arg-eso/
785. El Independiente — *La causa de la DANA afronta su recta final tras el varapalo del TSJ a la jueza de Catarroja* (17 de marzo de 2026; el TSJ rechaza investigar a Mazón). https://www.elindependiente.com/espana/2026/03/17/causa-dana-afronta-recta-final-varapalo-tsj-jueza-catarroja/
786. The Objective — *La jueza de la dana une a la causa los vídeos del Cecopi y pide a À Punt la hora de cada uno* (2 de octubre de 2025); El Español — *La jueza requiere a À Punt «todas las grabaciones de imagen y sonido» de la reunión del Cecopi* (los vídeos, de una productora contratada por la secretaría de Emergencias; se piden los originales para fijar la hora exacta de cada uno). https://theobjective.com/espana/tribunales/2025-10-02/jueza-dana-videos-cecopi-punt-hora/ · https://www.elespanol.com/valencia/20250919/jueza-dana-requiere-punt-todas-grabaciones-imagen-sonido-reunion-cecopi-octubre/1003743931870_0.amp.html
787. Maldita.es — *«Nos están ocultando los muertos» del parking de Bonaire (Aldaia): un año después, cómo funcionó la maquinaria de la desinformación* (29 de octubre de 2025; falsa acta municipal de «más de 220 cadáveres»; documentos falsos con más de 800 víctimas; ninguna víctima mortal en el aparcamiento). https://maldita.es/malditobulo/20251029/teoria-conspiracion-muertos-bonaire/
788. Newtral — *Un mes y más de 60 bulos desmentidos: la desinformación surgida a raíz de la dana* (29 de noviembre de 2024). https://www.newtral.es/desinformacion-dana/20241129/
789. COPE — *Quién está detrás de la creación de bulos de la DANA y qué herramientas digitales han usado* (la IA generativa como principal facilitador); elDiario.es — *Los bulos y falsedades sobre la DANA de València* (interferencia en las tareas de emergencia). https://www.cope.es/programas/la-linterna/audios/detras-creacion-bulos-dana-valencia-herramientas-digitales-han-usado-20241117_3046424.html · https://www.eldiario.es/comunitat-valenciana/bulos-falsedades-dana-valencia-cientos-cadaveres-bonaire-demolicion-pantanos_1_11791455.html
790. La Moncloa — *El Consorcio de Compensación de Seguros supera los 4.000 millones en pagos por indemnizaciones a afectados por la DANA* (26 de noviembre de 2025; 210.106 indemnizaciones). https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/economia-comercio-empresa/paginas/2025/261125-indemnizacion-dana.aspx
791. SegurosNews — *El Consorcio ya ha pagado 4.378 millones por la DANA de Valencia* (27 de marzo de 2026; 212.237 siniestros pagados; 251.249 expedientes; el 99,3 % tramitados; coste total estimado ≈4.800 M€). https://segurosnews.com/news/el-consorcio-ya-ha-pagado-4-378-millones-por-la-dana-de-valencia
792. Wikipedia — *Incendios forestales de España de 2025* (≈400.000 ha hasta el 19 de agosto; Ourense ≈150.000 ha; Uña de Quintana ≈40.000 ha; A Rúa >38.000 ha; Molezuelas de la Carballeda, más de 700 evacuados; 500 militares adicionales de la UME sobre más de 1.400). https://es.wikipedia.org/wiki/Incendios_forestales_de_Espa%C3%B1a_de_2025
793. Vallfirest — *La oleada de incendios forestales de agosto de 2025* (una veintena de grandes incendios en dos semanas, más de 300.000 ha; la peor temporada en más de 30 años). https://www.vallfirest.com/noticias/oleada-incendios-forestales-2025

794. Centro de Lauegi de Arán (Conselh Generau d'Aran) — *Butlletí de perill d'allaus i cartografia ATES* (boletín diario; «la información no sustituye la formación, la experiencia y el buen juicio»). https://lauegi.conselharan.org/ates/?lang=en
795. ICGC — *Butlletí de Perill d'Allaus (BPA)* (Pirineo catalán); AEMET — *Boletín de peligro de aludes* (resto de macizos). https://www.icgc.cat/en/Thematic-areas/Risks-and-emergencies/Avalanches/Avalanche-Danger-Bulletin-BPA · https://www.aemet.es/en/eltiempo/prediccion/montana/boletin_peligro_aludes
796. Protección Civil (España) — *Public Warning System / ES-Alert* (art. 110 de la Directiva (UE) 2018/1972, transpuesto por la Ley 11/2022 General de Telecomunicaciones; sistema operativo desde junio de 2022 y a disposición de los 112 autonómicos desde 2023; tecnología cell broadcast). https://www.proteccioncivil.es/coordinacion/redes/ran/public-warning-system · https://www.vademecumlegal.es/legislacion/articulo-110-codigo-europeo-comunicaciones-electronicas
797. esPúblico — *Responsabilidad patrimonial por daños por el estado de la calzada* (art. 106.2 CE; Ley 40/2015; nexo causal; el atestado de la Guardia Civil como prueba central; silencio administrativo de 6 meses). https://www.administracionpublica.com/responsabilidad-patrimonial-por-danos-por-el-estado-de-la-calzada/
798. t2p — manual de producto (huella SHA-512 en el dispositivo o en el origen del dato; sello de tiempo RFC 3161/eIDAS; anclaje en la blockchain pública; contenedor .asice). Véanse los capítulos 13 y 15.
799. Beth Simone Noveck — *Reboot: AI and the Race to Save Democracy* (Yale University Press, 2026), cap. 3 («Ballots and Bots»).
800. Munich Security Conference — *AI Elections Accord* (2024). https://securityconference.org/en/aielectionsaccord/
801. Utah State Legislature — *SB 131, Synthetic Media / disclosure of synthetic media* (2024). https://le.utah.gov/~2024/bills/sbillenr/SB0131.pdf
802. Microsoft / MSC — *Tech Accord to Combat Deceptive Use of AI in 2024 Elections* (16-02-2024). https://blogs.microsoft.com/on-the-issues/2024/02/16/ai-deepfakes-elections-munich-tech-accord/
803. Beth Simone Noveck — *Reboot* (2026), cap. 3 (Taiwán, Audrey Tang, Cofact).
804. The Washington Post — *AI mayoral candidate VIC, Cheyenne* (2024) https://www.washingtonpost.com/technology/2024/08/19/artificial-intelligence-mayor-cheyenne-vic/ ; Wikipedia — *Jason Palmer (politician)* https://en.wikipedia.org/wiki/Jason_Palmer_(politician ; TIME — *Albania's AI minister Diella* (2025) https://time.com/7324934/albania-ai-minister-diella/
805. Beth Simone Noveck — *Reboot* (2026), introducción y cap. 3 («possibilist, not Pollyanna»; la procedencia «alone will not solve the problem»).
806. Beth Simone Noveck — *Reboot* (2026), cap. 3 (ensayo coreano sobre alfabetización mediática y deepfakes).
807. IPI / VSquare / HKS Misinformation Review — *el deepfake de audio Šimečka–Tódová en Eslovaquia* (28-09-2023; moratoria de 48 horas; agujero de la política de audio de Meta; el debate sobre la influencia real en el resultado). https://ipi.media/slovakia-deepfake-audio-of-dennik-n-journalist-offers-worrying-example-of-ai-abuse/ · https://vsquare.org/slovak-election-targeted-by-pro-kremlin-deepfake-hoax/ · https://misinforeview.hks.harvard.edu/article/beyond-the-deepfake-hype-ai-democracy-and-the-slovak-case/
808. Beth Simone Noveck — *Reboot: AI and the Race to Save Democracy* (Yale University Press, 2026), cap. 8 ; y *Post Office Horizon Inquiry* (Sir Wyn Williams, 2024). https://en.wikipedia.org/wiki/British_Post_Office_scandal
809. Beth Simone Noveck — *Reboot* (2026), cap. 8 («Using procurement power»).
810. Beth Simone Noveck — *Reboot* (2026), cap. 6 (Policy Synth, runtime guardrails) ; The GovLab. https://thegovlab.org/
811. Beth Simone Noveck — *Reboot* (2026), cap. 8 («double opacity»; auditorías externas).
812. Gobierno de California — *Transparency in Frontier Artificial Intelligence Act (SB 53)* (29-09-2025). https://www.gov.ca.gov/2025/09/29/governor-newsom-signs-sb-53-advancing-californias-world-leading-artificial-intelligence-industry/
813. DeepSeek — *DeepSeek-R1 release* (20-01-2025). https://api-docs.deepseek.com/news/news250120
814. Beth Simone Noveck — *Reboot* (2026), cap. 8 (código abierto: los cinco elementos; registro de consultas y entrenamientos).
815. Beth Simone Noveck — *Reboot* (2026), introducción y cap. 6 («accountability in name only»; la IA como objeto).

816. Senado Federal de Brasil — *Portal e-Cidadania / Ley Joca* (2024-2025) https://www12.senado.leg.br/ecidadania/ ; y *Reboot* (Noveck, 2026), cap. 7.
817. Audrey Tang y E. Glen Weyl — *Plurality: The Future of Collaborative Technology and Democracy* (2024) ; y *Reboot* (2026), cap. 7.
818. Beth Simone Noveck — *Reboot* (2026), cap. 3 (APIs personales).
819. Beth Simone Noveck — *Reboot* (2026), cap. 7 (escala, acción, institucionalización; «participation without integration»).
820. time2act — capítulo 13 (t2p: firma con vídeo-selfie y prueba de vida en el dispositivo) ; T2P-Manual (v1.0, 2026).
821. Beth Simone Noveck — *Reboot* (2026), cap. 3 (encuesta Univ. de Madrid: 51% sustituirían políticos por IA).
822. NPR — *Pulitzer Board Recognizes Darnella Frazier For Recording George Floyd's Murder* (11 de junio de 2021; mención especial; cita literal del jurado). https://www.npr.org/2021/06/11/1005601724/darnella-frazier-teen-who-filmed-george-floyds-murder-wins-pulitzer-prize-citati
823. Wikipedia — *Darnella Frazier* (17 años al grabar; el vídeo como prueba en el juicio de Derek Chauvin). https://en.wikipedia.org/wiki/Darnella_Frazier
824. elDiario.es — *Juicio a tres policías por acusar en falso a una manifestante de agresión: «Ella no está condenada porque había un vídeo»* (caso «Rodea el Congreso»; el atestado inicial solo recogía insultos). https://www.eldiario.es/politica/juicio-tres-policias-acusar-falso-manifestante-si-no-llegamos-encontrar-video-hubieran-condenado_1_10922988.html
825. elDiario.es — *Absueltos los antidisturbios acusados de mentir en un juicio contra una manifestante del 'Rodea el Congreso'* (absolución; el tribunal no ve delito pese a la ausencia de pruebas de la agresión). https://www.eldiario.es/politica/absueltos-antidisturbios-acusados-mentir-juicio-manifestante-rodea-congreso_1_10979336.html
826. Togas.biz — *Si el atestado policial no ha sido ratificado en el plenario… las manifestaciones en él contenidas no tienen eficacia probatoria* (doctrina sobre la eficacia probatoria del atestado). https://togas.biz/articulos/articulo-profesionales--si-el-atestado-policial-no-ha-sido-ratificado-en-el-acto-del-plenario-por-los-agentes-de-la-autoridad-que-lo-confeccionaron-someti-ndose-al-principio-de-publicidad-y-contradicci-n-las-manifestaciones-en-l-contenidas-no-tiene-la-eficacia-probatoria/
827. Infobae — *El artículo de la 'ley mordaza' que derogarán PSOE y Sumar fue declarado inconstitucional y los policías ya no lo aplican* (17 de julio de 2024; art. 36.23; el TC anula el término «no autorizado»; reforma pactada: riesgo «constatable» y motivado). https://www.infobae.com/espana/2024/07/17/el-articulo-de-la-ley-mordaza-que-derogaran-psoe-y-sumar-fue-declarado-inconstitucional-y-los-policias-ya-no-lo-aplican/
828. Infobae — *Más de 400.000 multas y un tercer intento de reforma: la ley mordaza cumple 10 años* (31 de marzo de 2025; multas del conjunto de la ley). https://www.infobae.com/espana/2025/03/31/mas-de-400000-multas-y-un-tercer-intento-de-reforma-la-ley-mordaza-cumple-10-anos-en-medio-de-las-criticas-sobre-su-impacto-en-derechos-y-libertades/
829. Amnistía Internacional España — *Ley Mordaza: diez años de vulneraciones de derechos humanos y promesas incumplidas* (2025). https://www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/ley-mordaza-diez-anos-de-vulneraciones-de-derechos-humanos-y-promesas-incumplidas/
830. SME — Sindicat de Mossos d'Esquadra — *Consell de la Policia de 6 de febrer del 2025* (Axon Body 3 al 98 % del territorio con 800 cámaras; 5.000 agentes formados; autorización para 7.000 y 1.500 más; reglamento en actualización). https://sme-mossos.cat/consell-de-la-policia-de-6-de-febrer-del-2025/
831. USPAC — *Resum reunió subcomissió de materials, 27 de novembre de 2024* (300 cámaras más previstas; peticiones de generalización). https://uspac.cat/resums-reunions/resum-reunio-subcomissio-de-materials-27-novembre-2024/
832. Cámaras de Vigilancia IP — *Cámaras unipersonales de la Policía: funcionamiento y normativa* (DGU modelo AB3; extensión gradual; previsto para la Guardia Civil; objetivo: proteger ciudadanía y agentes). https://camarasdevigilanciaip.es/camaras-unipersonales-policia/
833. Telemundo — *Trump afirma falsamente que una foto de la multitud en un mitin de Harris en Detroit fue creada con inteligencia artificial* (agosto de 2024; foto de un miembro del equipo, sin manipular; periodistas de AP en la pista; 15.000 asistentes).

https://www.telemundo.com/noticias/noticias-telemundo/elecciones-estados-unidos-2024/trump-afirma-falsamente-que-una-foto-de-la-multitud-en-un-mitin-de-har-rcna166423
834. Univision — *Esas fotografías de eventos de campaña de Kamala Harris no fueron creadas con IA, como afirman Trump y en redes* (verificación). https://www.univision.com/noticias/fotografias-eventos-campana-kamala-harris-no-ia-como-afirman-trump-y-redes
835. t2p — manual de producto (huella SHA-512 en el dispositivo, por segmentos durante la grabación; sello de tiempo RFC 3161/eIDAS; anclaje en la blockchain pública; contenedor .asice; cadena de huellas continua para cámaras corporales; publicación opcional). Véanse los capítulos 13 y 15.
836. Oxford Economics, *The global economic costs of climate inaction*. https://www.oxfordeconomics.com/resource/the-global-economic-costs-of-climate-inaction/
837. Climate Policy Initiative, *The Cost of Inaction*. https://www.climatepolicyinitiative.org/the-cost-of-inaction/
838. (síntesis de modelización climática-económica) Earth.org. https://earth.org/have-economists-been-underestimating-the-cost-of-climate-change/
839. Orrick — *TAKE IT DOWN Act becomes law*; DEFIANCE Act (Senado, ene-2026). https://www.orrick.com/en/Insights/2025/05/TAKE-IT-DOWN-Act-Becomes-Law
840. Beth Simone Noveck — *Reboot* (Yale UP, 2026), cap. 8; Post Office Horizon Inquiry (Sir Wyn Williams, 2024).
841. L2BEAT — *Estado de descentralización de los L2 de Ethereum (secuenciadores)* (2026). https://l2beat.com/scaling/summary — y MEV Watch, *bloques con censura OFAC* (2026). https://www.mevwatch.info/
842. Jack Watling — *Statecraft: The New Rules of Power in a Divided World* (2023).
843. Dominic Frisby — *The Secret History of Gold* (2024).
844. Carissa Véliz — *Privacidad es poder* (Debate, 2021).
845. EDPB — *Opinion 08/2024 on «consent or pay»* (17-04-2024). https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en
846. FTC — *Acciones contra data brokers (X-Mode/Outlogic) y Avast* (2024). https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data — y Autoriteit Persoonsgegevens (NL), *multa de 30,5 M€ a Clearview AI* (2024). https://www.edpb.europa.eu/news/national-news/2024/dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en
847. Carissa Véliz — *The Ethics of Privacy and Surveillance* (Oxford University Press, 2024).
848. European Policy Centre — *Expansión de Eurodac (edad 12→6; acceso policial), Pacto de Migración 2024*. https://www.epc.eu/publication/managing-migration-through-data-the-expansion-and-integration-of-eurodac/
849. Carissa Véliz (ed.) — *The Oxford Handbook of Digital Ethics* (Oxford University Press, 2022).
850. time2act — *Guía de estilo (STYLE.md): «la promesa y el peligro»; «nada de tecno-utopía sin evidencia»*.
851. CPJ (Committee to Protect Journalists) — *Israel-Gaza War* (263 periodistas y trabajadores de medios muertos desde el 7-oct-2023; 108 encarcelados; 174 heridos; «el esfuerzo más letal y deliberado por matar y silenciar periodistas que el CPJ haya documentado nunca») y *At least 5 Gazan journalists killed in Israeli strike on Nasser Hospital* (25-ago-2025). https://cpj.org/issue/israel-gaza-war/ · https://cpj.org/2025/08/at-least-5-gazan-journalists-killed-in-israeli-strike-on-nasser-hospital/
852. Watson Institute (Brown University), proyecto Costs of War — *News Graveyards: How Dangers to War Reporters Endanger the World* (Nick Turse, 1-abr-2025: más periodistas muertos en Gaza que en las grandes guerras del siglo XX combinadas — comparativa que la propia base de datos usada matiza; ~13 periodistas palestinos muertos al mes); Foreign Policy — *War in Gaza the 'Worst Ever Conflict for Reporters'*. https://watson.brown.edu/costsofwar/papers/2025/Journalists · https://foreignpolicy.com/2025/04/01/gaza-war-worst-ever-for-reporters-costs-of-war-project/
853. Wikipedia (EN) — *2025 Nasser Hospital strikes* (25-ago-2025; primer impacto ~10:00 contra la posición de la cámara de Reuters — que emitía en directo — y segundo impacto ~10 min después contra rescatadores y periodistas; ≥22 muertos, 5 periodistas: Hussam al-Masri/Reuters, Mariam Dagga/AP, Mohammed Salama/Al Jazeera, Moaz Abu Taha, Ahmed Abu Aziz; «tragic mishap»); CNN — *New video reveals third strike* (27-ago-2025). https://en.wikipedia.org/wiki/2025_Nasser_Hospital_strikes · https://www.cnn.com/2025/08/27/middleeast/gaza-nasser-hospital-israel-attack-three-strikes-intl

854. CPJ — *Israel kills Al Jazeera journalists in targeted Gaza City airstrike* (Anas al-Sharif y cuatro compañeros, 10-ago-2025; la alerta previa del CPJ y de la relatora de la ONU Irene Khan, jul-2025); NPR — *Israeli airstrike kills Al Jazeera's Anas al-Sharif in Gaza*. https://cpj.org/2025/08/israel-kills-al-jazeera-journalists-in-targeted-gaza-city-airstrike/ · https://www.npr.org/2025/08/12/g-s1-82143/gaza-anas-al-sharif-al-jazeera-israel
855. Al Jazeera — *Family of Al Jazeera Gaza bureau head killed in Israeli air raid* (25-oct-2023: la esposa, el hijo Mahmoud, la hija Sham y el nieto Adam de Wael al-Dahdouh) y *To kill a family: the loss of Wael Dahdouh's family*. https://www.aljazeera.com/news/2023/10/25/family-of-al-jazeera-gaza-bureau-head-killed-in-israeli-air-raid · https://www.aljazeera.com/news/2023/11/1/to-kill-a-family-the-loss-of-wael-dahdouhs-family-to-israeli-bombs
856. The Times of Israel / Al Jazeera / Courthouse News — el veto de acceso de la prensa internacional a Gaza: rechazo de la petición de la FPA (ene-2024, «no vested right»), nueva petición (sep-2024), el gobierno mantiene el veto «por razones de seguridad» pese al alto el fuego (ene-2026) y el Supremo aplaza de nuevo (28-ene-2026); más de dos docenas de organizaciones informativas reclaman acceso. https://www.timesofisrael.com/ban-on-media-access-to-gaza-should-stay-in-place-israel-tells-high-court/ · https://www.aljazeera.com/news/2026/1/7/media-body-condemns-israels-continued-ban-on-foreign-media-access-to-gaza · https://www.aljazeera.com/news/2026/1/28/israels-top-court-delays-gaza-press-access-ruling-amid-years-long-ban · https://www.courthousenews.com/over-two-dozen-global-news-organizations-call-on-israel-to-allow-gaza-access/
857. RSF (Reporteros Sin Fronteras) — *RSF files fifth complaint with ICC about Israeli war crimes against journalists in Gaza* (30-sep-2025; cinco denuncias desde oct-2023; ≥210 periodistas muertos, 56 con motivos razonables para creerlos deliberadamente atacados; patrón de «doble bombardeo») y *«Gazawood»: the deadly accusations against Gaza's journalists*. https://rsf.org/en/rsf-files-fifth-complaint-icc-about-israeli-war-crimes-against-journalists-gaza · https://rsf.org/en/gazawood-deadly-accusations-against-gaza-s-journalists
858. Al Jazeera / The National — *Palestinian journalist Bisan Owda and AJ+ win Emmy for Gaza war documentary* (25-sep-2024, «It's Bisan From Gaza — and I'm Still Alive»; ~4 millones de seguidores; campaña de descalificación fallida) y el fotoperiodista Motaz Azaiza. https://www.aljazeera.com/news/2024/9/26/palestinian-journalist-bisan-owda-and-aj-win-emmy-for-gaza-war-documentary · https://www.thenationalnews.com/arts-culture/film-tv/2024/09/26/bisan-owda-emmy-award-palestine/
859. Wikipedia (EN) / NPR — *Misinformation in the Gaza war* y *Pallywood* (pico de 220.000 usos en X en nov-2023 según BBC Verify; el caso de la «muñeca» publicado y retirado por el Jerusalem Post y amplificado por la cuenta oficial de Israel en X; el falso positivo del detector «AI or Not» sobre una foto real; Ron Dudai: la documentación descartada con una sola palabra, «Fake»); NPR — *False 'crisis actor' claims spread about Israel-Hamas war*. https://en.wikipedia.org/wiki/Misinformation_in_the_Gaza_war · https://en.wikipedia.org/wiki/Pallywood · https://www.npr.org/2023/11/27/1214451419/civilian-deaths-are-being-dismissed-as-crisis-actors-in-gaza-and-israel
860. Human Rights Watch / CNN / Forensic Architecture — la explosión en el hospital al-Ahli (17-oct-2023; 471 muertos según el Ministerio de Salud de Gaza, 100-300 según la inteligencia de EE. UU.) y la divergencia forense: HRW (patrón consistente con cohete propulsado; hace falta investigación independiente), CNN y AP (cohete fallido desde Gaza, lo más probable), NYT (causa incierta), Forensic Architecture (proyectil desde la dirección de Israel). https://www.hrw.org/news/2023/11/26/gaza-findings-october-17-al-ahli-hospital-explosion · https://www.cnn.com/2023/10/21/middleeast/cnn-investigates-forensic-analysis-gaza-hospital-blast · https://forensic-architecture.org/investigation/israeli-disinformation-al-ahli-hospital
861. OHCHR / CNN — el asesinato de Shireen Abu Akleh (11-may-2022): conclusión de la ONU (jun-2022: tiros de las fuerzas israelíes, «aparentemente bien apuntados»), investigación de CNN (24-may-2022) y admisión del ejército israelí (5-sep-2022: «probablemente» fuego propio; sin cargos). https://www.ohchr.org/en/press-briefing-notes/2022/06/killing-journalist-occupied-palestinian-territory · https://www.cnn.com/2022/05/24/middleeast/shireen-abu-akleh-jenin-killing-investigation-cmd-intl · https://www.cnn.com/2022/09/05/middleeast/idf-shireen-abu-akleh-investigation-intl/index.html
862. Forensic Architecture / Earshot — *The Killing of Hind Rajab* (29-ene-2024: 355 impactos en el coche; análisis acústico de la llamada: tiros desde 13-23 m). https://forensic-architecture.org/investigation/the-killing-of-hind-rajab · https://www.earshot.ngo/investigations/the-killing-of-layan-hamada-and-hind-rajab

863. ECCHR / Syria Justice & Accountability Centre / CBS — los archivos Caesar (~53.000 fotos sacadas de Siria en 2013; autenticación pericial de metadatos y forénsica médica) y la condena de Coblenza (13-ene-2022: cadena perpetua a Anwar Raslan por crímenes contra la humanidad). https://www.ecchr.eu/en/case/caesar-photos-document-systematic-torture/ · https://syriaaccountability.org/inside-the-raslan-trial-a-forensic-analysis-of-the-caesar-photos/ · https://www.cbsnews.com/news/syria-war-bashar-assad-police-officer-crimes-against-humanity-germany/
864. Tribunal Penal Internacional — *ICC Pre-Trial Chamber I rejects the State of Israel's challenges to jurisdiction and issues warrants of arrest for Benjamin Netanyahu and Yoav Gallant* (21-nov-2024; crimen de guerra del hambre como método de guerra; crímenes contra la humanidad; orden también contra Mohammed Deif). https://www.icc-cpi.int/news/situation-state-palestine-icc-pre-trial-chamber-i-rejects-state-israels-challenges
865. Tribunal Internacional de Justicia — *Application of the Genocide Convention (South Africa v. Israel)*, medidas provisionales de 26-ene-2024, 28-mar-2024 y 24-may-2024 (vinculantes). https://www.icj-cij.org/case/192
866. Access Now (#KeepItOn) / EFF — *Israel must stop cutting Gaza off from the world* (19-jun-2025: ≥23 apagones de comunicaciones desde oct-2023, por ataques a la fibra y falta de combustible; «la conectividad civil convertida en medio y método de guerra») y *Connectivity is a Lifeline, Not a Luxury*. https://www.accessnow.org/press-release/keepiton-israel-must-stop-cutting-gaza-off/ · https://www.eff.org/deeplinks/2025/06/connectivity-lifeline-not-luxury-telecom-blackouts-gaza-threaten-lives-and-digital
867. NPR / GPS World / The Times of Israel — perturbación y suplantación de GPS en la región (2024: >50.000 vuelos afectados; incremento ×6; aplicaciones situando a usuarios en Beirut o El Cairo; una base aérea israelí señalada como origen). https://www.npr.org/2024/04/22/1245847903/israel-gps-spoofing · https://www.gpsworld.com/israeli-air-base-identified-as-alleged-source-of-gps-disruptions-in-mideast/ · https://www.timesofisrael.com/gps-jamming-amid-wars-playing-havoc-with-airline-navigation-report/
868. Starling Lab / Content Authenticity Initiative — *78 Days* (Reuters + Starling, nov-2020→ene-2021: >200 fotos de la transición presidencial con metadatos criptográficos anclados en Filecoin y Hedera; procedencia verificable por cualquiera). https://www.starlinglab.org/78days/ · https://contentauthenticity.org/blog/cai-spotlight-78-days-from-stanford-starling-lab-and-reuters
869. Guardian Project / WITNESS — *ProofMode* (desde 2017: firma OpenPGP y huella en la captura, instantánea de sensores, notarización — con OpenTimestamps entre los sistemas soportados; pensada para la documentación ciudadana de derechos humanos). https://guardianproject.info/apps/org.witness.proofmode/ · https://blog.witness.org/2017/04/proofmode-helping-prove-human-rights-abuses-world/
870. t2p — manual de producto (huella SHA-512 calculada en el dispositivo — solo la huella sale del móvil —; sello de tiempo RFC 3161/eIDAS; anclaje en la blockchain pública; GPS forense con degradación honesta; modo sin conexión con anclaje diferido; compromiso y revelación; paquete .asice verificable sin conexión; certificado con QR). Véanse los capítulos 13 y 15; el compromiso y revelación, en los capítulos 45 y 46; la cadena de custodia del socorro, en el capítulo 50; la divulgación selectiva y la evidencia de crímenes de guerra, en el capítulo 20; las credenciales de contenido, en el capítulo 17.
871. Wikipedia (EN) — *Operation Metro Surge* (4-dic-2025 → feb-2026: «the largest immigration enforcement operation ever carried out» según el DHS; miles de agentes de ICE y CBP en Minneapolis–Saint Paul; ≥3.789 detenciones, menos de un 25 % con antecedentes; la huelga general del 23-ene-2026; el juez Schiltz: ≥96 órdenes judiciales violadas por ICE desde el 1-ene; el juez Blackwell: la «mayoría abrumadora» de los detenidos, con presencia legal); NPR — *Minnesota ICE crackdown will end* (12-feb-2026: Tom Homan anuncia el final del operativo — que «ha costado la vida a dos ciudadanos estadounidenses» — sin mencionar sus nombres); Sahan Journal — las cifras del despliegue (más de 4.000 agentes en el punto álgido), reveladas por orden judicial. https://en.wikipedia.org/wiki/Operation_Metro_Surge · https://www.npr.org/2026/02/12/nx-s1-5712280/minnesota-ice-surge-ends · https://sahanjournal.com/immigration/hundreds-ice-agents-leaving-minnesota-operation-metro-surge/
872. Wikipedia (EN) — *Killing of Renée Good* (7-ene-2026, Portland Avenue, Minneapolis: el agente de ICE Jonathan Ross dispara tres tiros — parabrisas y ventanilla de la conductora — con el vehículo girando para alejarse, según la reconstrucción del New York Times; en el coche, la pareja y una criatura de seis años; las alegaciones de Noem y de Trump; la grabación del propio Ross, sacudida hacia arriba en el momento crítico; el acceso de la agencia estatal de investigación a las pruebas,

revocado al día siguiente; Ross, tres días apartado y reasignado fuera del estado); The Intercept — *Video Shows ICE Agent's Fatal Shooting of Civilian in Minneapolis* (el tiro a corta distancia contra el vehículo que se iba; un segundo ángulo muestra a Good cediendo el paso a los vehículos federales minutos antes). https://en.wikipedia.org/wiki/Killing_of_Ren%C3%A9e_Good · https://theintercept.com/2026/01/07/video-ice-shooting-civilian-minneapolis/

873. Wikipedia (EN) — *Killing of Alex Pretti* (24-ene-2026, Minneapolis: enfermero de UCI del hospital de veteranos, 37 años, permiso de armas y ningún antecedente; los vídeos de los testigos, revisados y verificados por Reuters, BBC, Wall Street Journal, AP, CNN, New York Times y The Guardian: el teléfono en la mano, el espray de pimienta, los agentes inmovilizándolo, el arma sacada de la funda y los tiros un segundo después; las alegaciones del DHS — «máximo daño», «dos cargadores y ningún tipo de identificación» — y de Stephen Miller; la forense del condado de Hennepin: homicidio; los agentes, identificados por ProPublica); NPR — *Videos refute DHS account of fatal shooting* (25-ene-2026: Noem — «se había acercado con una pistola» — contra los vídeos: no sacó nunca ningún arma; filmaba con el móvil); The Marshall Project — *How Many People Have Been Killed by ICE and Border Patrol?* (26-ene-2026: ninguna reanimación de los agentes; una pediatra apartada; en el caso Good, tres minutos sin llamar a emergencias; el desmentido público del alcalde Frey y el gobernador Walz tras ver los vídeos). https://en.wikipedia.org/wiki/Killing_of_Alex_Pretti · https://www.npr.org/2026/01/25/nx-s1-5687384/minneapolis-minnesota-shooting-video-dhs · https://www.themarshallproject.org/2026/01/26/ice-minneapolis-shooting-alex-pretti
874. ProPublica — *Minnesota's Fight to Hold Agents Who Shot Alex Pretti, Renee Good Accountable* (la demanda de Minnesota, el condado de Hennepin y la agencia estatal de investigación contra los departamentos de Justicia y de Seguridad Nacional, 24-mar-2026: pruebas retenidas «para escudar a los agentes implicados» — nombres, armas, informes, datos GPS y declaraciones de testigos negados pese a los requerimientos formales; las diecisiete investigaciones penales de la fiscal Moriarty; el obstáculo de la cláusula de supremacía; los agentes del caso Pretti, identificados por ProPublica el 1-feb); NPR — *Months after the ICE shootings in Minnesota, a federal probe remains elusive* (10-abr-2026: el móvil de Pretti, retenido; el coche de Good, precintado en un almacén del FBI sin examinar; investigadores estatales apartados físicamente de la escena; única medida disciplinaria del operativo: dos agentes en permiso administrativo por «declaraciones falsas» en el caso del tercer tiroteado, Julio Sosa-Celis; «Parece que estén impidiendo activamente que el estado investigue» — Rachel Moran, profesora de derecho). https://www.propublica.org/article/minnesota-trump-ice-shooting-lawsuit-alex-pretti-renee-good · https://www.npr.org/2026/04/10/nx-s1-5775847/alex-pretti-renee-good-ice-shootings-federal-investigations
875. Wikipedia (EN) — *Shooting of Marimar Martinez* (Chicago, 4-oct-2025: cinco tiros del agente de la Patrulla Fronteriza Charles Exum; la cámara corporal muestra el vehículo de los agentes girando hacia el de ella tras el «it's time to get aggressive»; los mensajes del agente — «fired 5 shots and she had 7 holes» —; los cargos contra Martinez y su codemandado, archivados con carácter definitivo el 20-nov-2025) y *List of shootings by U.S. immigration agents in the second Trump administration* (el recuento acumulado: 38 tiroteos y 9 muertos entre el 20-ene-2025 y el 7-jul-2026; los casos con cargos contra civiles retirados cuando el vídeo contradijo la versión de los agentes); AP (vía KSAT) — *Judge's blistering opinion details use of force in Chicago-area immigration crackdown* (nov-2025: el dictamen de 223 páginas de la jueza Sara Ellis — el relato del gobierno, «simply not credible», desmentido por las cámaras corporales que ella misma había ordenado activar; las versiones cambiantes de Bovino sobre la piedra y el gas; el informe de uso de la fuerza redactado con ChatGPT). https://en.wikipedia.org/wiki/Shooting_of_Marimar_Martinez · https://en.wikipedia.org/wiki/List_of_shootings_by_U.S._immigration_agents_in_the_second_Trump_administrat · https://www.ksat.com/news/politics/2025/11/21/judges-blistering-opinion-details-use-of-force-in-chicago-area-immigration-crackdown/
876. KPRC 2 / Click2Houston — *ICE agent shoots, kills Lorenzo Salgado Araujo during attempted arrest in east Houston* (7-jul-2026, Magnolia Park: ICE alega que «embistió un vehículo oficial» y que el agente disparó «en defensa propia»; los agentes no llevaban cámaras corporales, según el DHS; relatos en conflicto sobre los momentos previos; la forense del condado de Harris, 9-jul: homicidio). https://www.click2houston.com/news/local/2026/07/07/heavy-law-enforcement-presence-reported-in-east-houston-neighborhood/
877. León XIV — *Carta encíclica «Magnifica Humanitas»* (Vaticano, 15-25 de mayo de 2026; sobre la custodia de la persona humana en el tiempo de la inteligencia artificial). https://www.vatican.va/content/leo-xiv/es/encyclicals/documents/20260515-magnifica-humanitas.html

878. León XIII — *Rerum Novarum* (1891; origen de la doctrina social de la Iglesia). https://www.vatican.va/content/leo-xiii/es/encyclicals/documents/hf_l-xiii_enc_15051891_rerum-novarum.html
879. Francisco — *Laudato Si'* (2015; la Casa común y el paradigma tecnocrático). https://www.vatican.va/content/francesco/es/encyclicals/documents/papa-francesco_20150524_enciclica-laudato-si.html
880. Vatican News — *León XIV presenta su primera encíclica «Magnifica Humanitas»* (25 de mayo de 2026). https://www.vaticannews.va/es/papa/news/2026-05/papa-leon-xiv-primera-enciclica-magnifica-humanitas.html
881. Juan Pablo II — *Centesimus Annus* (1991; centenario de la 'Rerum Novarum'). https://www.vatican.va/content/john-paul-ii/es/encyclicals/documents/hf_jp-ii_enc_01051991_centesimus-annus.html
882. Vatican News / The Washington Post — *León XIV presenta «Magnifica Humanitas» en persona, con el cofundador de Anthropic Chris Olah; «con nuestras diferencias, podamos escucharnos los unos a los otros»* (25-05-2026). https://www.vaticannews.va/en/pope/news/2026-05/pope-leo-xiv-encyclical-magnifica-humanitas-ai.html
883. Anthropic — *Chris Olah's remarks on Pope Leo XIV's encyclical «Magnifica Humanitas»* (la Iglesia como «informed critics»; «a long collaboration between those of us who are building this and those who can see what we, from inside, cannot»; diálogo con gente «not motivated by profit») (2026). https://www.anthropic.com/news/chris-olah-pope-leo-encyclical
884. Fortune — *Who is Chris Olah? The atheist Anthropic cofounder the Pope chose to sit beside him at the Vatican* (criado evangélico en Toronto, ateo desde los 15; la industria «can't govern itself») (03-06-2026). https://fortune.com/2026/06/03/who-chris-olah-anthropic-cofounder-atheist-pope-leo-vatican-ai/

Índice de figuras

- Figura 0.1 — Línea de tiempo 2004 → 2026: los hitos de energía, clima, IA y blockchain que enmarcan este libro.
- Figura 0.2 — Del «pico de oferta» al «pico de demanda»: la proyección de Roberts (2004) frente a la trayectoria observada.
- Figura 1.1 — De la confianza centralizada a la distribuida: el viaje de un hecho, de la captura a la verificación que cualquiera puede rehacer.
- Figura 2.1 — El mundo todavía funciona con combustibles fósiles (~86,7 % del suministro primario en 2024), pero las renovables ya lideran el crecimiento.
- Figura 3.1 — El precio del Brent: del choque de 2022 (~130 $) a la estabilización hacia los ~67 $ en 2025.
- Figura 4.1 — El coste de la electricidad solar cayó cerca de un 90 % entre 2010 y 2024: la transformación de precio más rápida de la historia de la energía.
- Figura 4.2 — Las ventas de vehículos eléctricos superan los 17 millones en 2024 y ya son más de uno de cada cinco coches nuevos.
- Figura 5.1 — China domina la fabricación de la transición: del 60 % de los aerogeneradores al ~91 % del refinado de tierras raras.
- Figura 6.1 — El calentamiento global ha superado por primera vez los +1,5 °C en un año natural (2024).
- Figura 7.1 — La mejora de la eficiencia (~1 % en 2024) va muy por debajo del ritmo necesario para duplicarla hacia 2030.
- Figura 8.1 — Pese a la retórica verde, el 81 % de la inversión de las energéticas estatales del G20 todavía va a combustibles fósiles (2024).
- Figura 9.1 — El consumo eléctrico de los centros de datos se duplica hacia 2030 (~950 TWh), impulsado por la IA.
- Figura 10.1 — Las deepfakes se multiplican: de ~500.000 (2023) a 8 millones (2025), camino del 90 % del contenido en línea en 2026.
- Figura 11.1 — La IA orquesta renovables, almacenamiento, respuesta de la demanda y nuevo nuclear en una red resiliente.
- Figura 12.1 — Productor y consumidor intercambian energía y certificados directamente; la blockchain aporta confianza sin intermediario.
- Figura 13.1 — Del hash a la verificación descentralizada: nadie tiene que confiar en nadie; solo en las matemáticas.
- Figura 13.2 — C2PA demuestra «quién y cuándo» en origen; el anclaje en blockchain demuestra «esto existía y no se ha alterado».
- Figura 13.3 — El flujo de t2p: capturar, sellar la huella en la blockchain pública y poder verificarlo incluso sin conexión ni intermediarios.
- Figura 14.1 — El hidrógeno verde (4-7 €/kg) todavía es mucho más caro que el gris o el azul: el reto no es técnico, sino de coste y demanda.
- Figura 15.1 — La precisión de los detectores cae en el mundo real a medida que mejoran los generadores; un ancla de procedencia no se degrada con el tiempo.
- Figura 16.1 — En el fraude por deepfake, la confianza se rompe en la identidad y la instrucción; una prueba de existencia anclada al origen pone un punto de verificación independiente.
- Figura 17.1 — Cuando una imagen se resube, los metadatos C2PA pueden desaparecer; el hash anclado a la cadena pública sigue demostrando que el original existía, inalterado.
- Figura 18.1 — Si se calcula el hash de la imagen en el momento de la adquisición y se ancla con sello de tiempo, cualquier manipulación posterior (un tumor inyectado o borrado) se detecta al instante.
- Figura 19.1 — El emisor firma y ancla el hash de la credencial; el titular la presenta; cualquier verificador comprueba su autenticidad e integridad sin intermediarios.
- Figura 20.1 — Captura con hash en el origen → metadatos y geolocalización → anclaje inmutable → prueba admisible: la cadena que convierte un testimonio digital en evidencia.
- Figura 21.1 — El precio del derecho de emisión europeo (EUA) escaló hasta un máximo de 105,73 € en febrero de 2023 y se movía alrededor de los 80 € a mediados de 2026; en paralelo, el CBAM entró en fase definitiva el 1 de enero de 2026, con un primer certificado fijado en 75,36 €/t. Fuentes: Trading Economics; Comisión Europea; S&P Global.
- Figura 22.1 — A lo largo de la vida de un crédito —diseño y línea de base, implementación en el campo, MRV, emisión, venta y tokenización opcional— el fraude se infiltra sobre todo en la línea de

base inflada y en la evidencia de campo manipulable. La prueba de existencia ancla los eslabones de evidencia (foto, medición, informe) pero no corrige una metodología defectuosa. Fuentes: The Guardian; Verra; CarbonPlan; ICVCM.

- Figura 23.1 — Del catálogo de medidas a la emisión del certificado: la actuación se captura como evidencia (foto antes/después, contador, factura), se verifica y se convierte en CAE (1 CAE = 1 kWh). La prueba de existencia se inserta en el momento de capturar la evidencia —SHA-512, GPS forense, sello RFC 3161, prueba de vida y contenedor .asice—, justo donde la ley francesa ya exige fotografías fechadas y geolocalizadas. Fuentes: BOE (RD 36/2023); Légifrance (Ley 2025-594); Funcas.
- Figura 24.1 — El autoconsumo con prueba de existencia (t2p: huella SHA-512 en el dispositivo, RFC 3161/eIDAS, blockchain pública, .asice): la lectura propia del inversor y el contador sellada por lotes encadenados, la factura con compensación contrastada, el acta de la comunidad energética (coeficientes, altas y bajas con fecha cierta) y el contrato/PPA congelado el día de firmar. Contexto: 9,3 GW de autoconsumo en España (UNEF) —quinta fuente por potencia; RD 244/2019 (compensación simplificada mensual ≤100 kW; colectivo hasta 5 km). Límites: la lectura propia contrasta el contador fiscal, no lo sustituye; calibración primero; solo huellas en la cadena (la curva de consumo es intimidad). Fuentes: UNEF; BOE (RD 244/2019).
- Figura 25.1 — La lectura de un sensor (odómetro, bus CAN, GPS, sesión de carga OCPP) se resume en una huella SHA-512 en el dispositivo, se le ligan el GPS forense y un sello de tiempo RFC 3161/eIDAS con presunción legal, se ancla a la blockchain pública y se empaqueta en un contenedor .asice verificable sin conexión, listo para emitir un CAE (fichas TRA010-TRA050), un crédito de carbono o un informe CSRD. Caja comparativa: sin sello, hasta el 30-50 % de los odómetros transfronterizos están manipulados; con un registro sellado (modelo Car-Pass), menos del 0,2 %. Fuentes: Parlamento Europeo (EPRS); Car-Pass; MITECO.
- Figura 26.1 — El número de coches privados que retira de la calle un solo vehículo compartido varía enormemente según la ciudad y la metodología: de 3,3 de media en el estudio europeo de SHARE NOW hasta los 7-11 del estudio de car2go en Norteamérica, con escenarios aún más altos en algunas ciudades. La cifra de divulgación «uno por diez» es comercial, no consensuada. La lección: ningún número único; siempre un rango con su fuente. Fuentes: UC Berkeley TSRC (Shaheen y Martin, 2016); Transportation Research Part A (2020).
- Figura 27.1 — El retraso con prueba de existencia (sellado con t2p — capítulo 13): la llegada con GPS forense al abrirse las puertas (la definición del TJUE), el panel y el estado del vuelo congelados, el expediente del viaje (billete, embarque, gastos de atención) y la simetría del transportista (registros de operación anclados; la circunstancia extraordinaria sellada cuando ocurre). Contexto: Reglamento (CE) 261/2004 (250/400/600 €; Sturgeon ≥3 h); Renfe 1-7-2024: de los 15/30 min a los 60/90 (50 %/100 %). Límites: el juez decide lo extraordinario; documentar el viaje propio, nunca terceros. Fuentes: EUR-Lex; Renfe/Newtral.
- Figura 28.1 — Porcentaje de consumidores dispuestos a alterar digitalmente la imagen o el documento de un siniestro, aunque infrinja las normas de la aseguradora: un 36 % de media, pero hasta el 55 % entre la generación Z. La predisposición cae con la edad. Es el rostro del fraude de imagen por IA que el 99 % de las aseguradoras ya ha visto. Fuente: Verisk con el National Insurance Crime Bureau (2026).
- Figura 29.1 — En el punto de origen (parcela, cosecha, fábrica) se captura una foto georreferenciada que se sella con GPS forense, sello de tiempo eIDAS y huella SHA-512, y se empaqueta en un contenedor .asice verificable sin conexión. Esta capa de prueba del acto de origen se combina con la serialización (código 2D del FMD), la declaración de diligencia debida del EUDR o el pasaporte digital de Aura, hasta la verificación final en la aduana o en el estante. Fuentes: EUDR (UE 2023/1115); EMA; Aura Blockchain Consortium.
- Figura 30.1 — La capa de información del consumidor con prueba de existencia: la reseña con compra acreditada y anónima (el justificante sellado en el dispositivo; el mercado negro de reseñas se queda sin materia prima), la serie de precios con fecha cierta (la regla del menor precio de los 30 días se vuelve verificable) y el reloj de la garantía (compra, unboxing y avisos sellados activan y acreditan los 3 años legales). Límites: el sello no juzga la sinceridad ni la calidad; la acreditación de compra nunca puede identificar al comprador. Fuentes: FTC (norma 2024); Amazon vs. grupos de Facebook; OCU (Black Friday); CEC/Consumo (garantía de 3 años).
- Figura 31.1 — La segunda mano entre particulares con prueba de existencia (sellado con t2p — capítulo 13): el artículo filmado antes de enviar (fecha/hora sobreimpresa + GPS forense), el precintado en plano secuencia, la apertura simétrica del comprador y el expediente de la disputa (anuncio capturado, chat, pago, seguimiento). Simetría total: desarma el paquete falso Y el «cambiazo». Contexto: >19 M de usuarios en Wallapop; >13.000 M€/año; las estafas de segunda

mano, grueso de los >412.000 fraudes informáticos de 2024 (+60 % de denuncias en 2025). Límites: proporcionalidad según valor; el vicio oculto lo valora el perito; nunca grabar a terceros. Fuentes: Guardia Civil/prensa especializada.

- Figura 32.1 — El alquiler de cosas con prueba de existencia (sellado con t2p — capítulo 13): la vuelta de recogida filmada (fecha/hora sobreimpresa + GPS forense del aparcamiento), la vuelta de devolución —decisiva en devoluciones fuera de horas—, el contrato y la franquicia sellados, y el expediente contra el cargo tardío. Simetría: la inspección bilateral protege a la empresa honesta del cliente que niega el golpe; extensible al alquiler de maquinaria B2B. Contexto: prácticas irregulares documentadas (cargos de 300-1.000 € fijados unilateralmente; revisiones sin el cliente); el CEC ya recomienda fotos —faltaba la fecha cierta. Límites: uso normal vs daño y precios, cosa del contrato y el juez. Fuentes: Consumo/DSCA; CEC-España.
- Figura 33.1 — El cliente ante la compañía con prueba de existencia (sellado con t2p — capítulo 13): la baja sellada (grabación de la llamada propia, captura certificada del formulario), el contrato y sus versiones (captura web con código fuente), la promesa verbal grabada y el expediente .asice exportable a consumo. La Ley 10/2025 da los derechos (3 minutos, código de seguimiento, 15/5 días, baja simple); la fecha cierta los hace exigibles —y acredita a la compañía diligente. Límites: conversaciones propias, proporcionalidad con el teleoperador, la reclamación formal sigue siendo imprescindible. Fuentes: BOE (Ley 10/2025); FACUA (multas Vodafone/Movistar/Telefónica).
- Figura 34.1 — El reloj del cobro con prueba de existencia (sellado con t2p — capítulo 13): el albarán fotografiado con GPS forense en la entrega, la factura con doble fecha cierta (emisión y envío), el cómputo automático de la Ley 3/2004 (30/60 días; interés de demora 11,15 % + 40 €) y el expediente .asice para el monitorio. Contexto: VeriFactu (RD 1007/2023, aplazado a 2027 por el RD-ley 15/2025) ya impone registros de facturación con hash encadenado y QR —el Estado construye media prueba de existencia; t2p añade la capa oponible entre privados. Límites: el sello no cobra facturas ni valora el trabajo; VeriFactu protege a Hacienda, no al acreedor. Fuentes: AEAT; BOE; PMcM 2025 (85 % de grandes incumplidoras; AAPP a 70 días).
- Figura 35.1 — El estado de la vivienda (alquiler) o un documento (escritura, contrato) se captura y se sella en el dispositivo con SHA-512, GPS forense, sello de tiempo eIDAS y prueba de vida, se ancla a la blockchain pública y se empaqueta en un contenedor .asice verificable sin conexión, listo para el registro, el notario, el tribunal o la otra parte. La prueba de existencia aporta evidencia con fecha cierta, no el título legal (que crea el registro). Barra de contexto: ~70 % de la población mundial sin título registrado; ~1.100 M de personas inseguras sobre su propiedad; Georgia, ~1,5 M de títulos anclados. Fuentes: Banco Mundial; Prindex; Exonum/Bitfury.
- Figura 36.1 — El ciclo del alquiler con prueba de existencia: el anuncio acreditado (titularidad + sello, contra la estafa del piso inexistente), el inventario de entrada sellado bilateralmente, los avisos y reparaciones con fecha cierta durante el contrato, la cronología de posesión (contrato y recibos del inquilino; pruebas de estado periódicas del propietario; vía rápida LO 1/2025) y el inventario de salida que liquida la fianza sin guerra. Solo las huellas SHA-512 se anclan a la blockchain pública (RFC 3161/eIDAS, .asice); las imágenes del hogar no salen nunca de los dispositivos. Fuentes: Guardia Civil (Op. ISLEDA); Idealista/Maldita; LO 1/2025.
- Figura 37.1 — La comunidad de propietarios con prueba de existencia (sellado con t2p — capítulo 13): la convocatoria con fecha cierta de envío, el acta sellada el mismo día (libro de actas como cadena de versiones ancladas), la derrama trazable (presupuestos, acuerdo, facturas, certificaciones en un proyecto) y la comunicación fehaciente entre vecinos y administrador. Simetría: protege al vecino que impugna y al administrador honesto. Límites: acuerdos de junta para grabar, publicación solo por huella (datos personales), y ningún sello resuelve el fondo de las disputas (LPH). Fuentes: condena de Gijón (art. 253 CP); Ley de Propiedad Horizontal.
- Figura 38.1 — La reforma con prueba de existencia (sellado con t2p — capítulo 13): el presupuesto y sus versiones sellados el día de pactarse, el estado inicial fotografiado con GPS forense (la prueba que la obra borra), las fases con hitos —pagar contra hechos documentados— y la recepción firmada con vídeo-selfie de las dos partes. Simetría: protege a la familia de la estafa del anticipo y al profesional honesto del cliente que no quiere pagar. Contexto: investigaciones de la Guardia Civil (Vigo: ≥6 víctimas de hasta 10.000 €; pérdidas >77.000 € en algún caso). Límites: la calidad la valoran los peritos; proporcionalidad; no pagar por delante de los hechos. Fuentes: prensa/Guardia Civil; normativa de consumo.
- Figura 39.1 — Las dos proyecciones de referencia para el mercado de RWA tokenizados en 2030 difieren unas ocho veces: el escenario prudente de McKinsey (~2 billones de dólares, rango 1-4) y el optimista de BCG/ADDX (~16,1 billones); el punto de partida real era de unos 24.000 millones a mediados de 2025. La distancia depende, en el fondo, de cuánta «basura» se admita: del vacío entre

el token y la prueba de su respaldo —el problema del oráculo— que la prueba de existencia ayuda a cerrar. Fuentes: McKinsey (2024); BCG/ADDX (2022); CoinDesk/RWA.xyz (2025).

- Figura 40.1 — En el momento de crear (t0), la obra se sella con huella SHA-512 en el dispositivo, ancla a la blockchain pública, sello de tiempo eIDAS, GPS y prueba de vida: fecha cierta de qué, cuándo, dónde y quién. Al publicarla (t1), las credenciales C2PA pueden borrarse al subirla a las redes; cuando un modelo la ingiere o alguien la copia (t2), el contenedor .asice todavía demuestra que el archivo existía intacto en t0, antes de t2. La prueba de existencia demuestra precedencia, no originalidad. Fuentes: C2PA; U.S. Copyright Office; casos NYT, Getty, Andersen.
- Figura 41.1 — El inventor sella el documento de divulgación con huella SHA-512, ancla a la blockchain pública y sello de tiempo eIDAS (fecha cierta, integridad y autoría), por un coste marginal ante los 15.000-25.000 dólares de una patente. Si además lo publica (Technical Disclosure Commons, IP.com, web), se convierte en prior art indexado por Espacenet o Google Patents; cuando llega la solicitud de un rival, el examinador encuentra la divulgación fechada y la rechaza por falta de novedad. El sello prueba fecha y contenido, no la patentabilidad —que decide el examinador. Fuentes: USPTO; WIPO; Technical Disclosure Commons.
- Figura 42.1 — El secreto empresarial con prueba de existencia (t2p: huella SHA-512 en el dispositivo —el contenido no sale nunca—, RFC 3161/eIDAS, blockchain pública, .asice): el depósito sellado (posesión + perímetro + medida razonable del tercer requisito de la Ley 1/2019), la cronología del know-how versión a versión, el acta de salida del empleado y el NDA con perímetro por huella y firma con vídeo-selfie. Simetría: la cadena de fechas del acusado inocente prueba el desarrollo independiente. Espejo del capítulo 41: la patente protege publicando; el secreto, ocultando —y por eso solo la prueba que no revela lo puede defender. Fuentes: caso Waymo/Uber/Levandowski; Ley 1/2019.
- Figura 43.1 — Cada paso del dinero público —la oferta o el pliego, la adjudicación registrada y la obra entregada (foto con GPS y fecha)— se resume en una huella SHA-512, se ancla a la blockchain pública y recibe un sello de tiempo RFC 3161/eIDAS, con prueba de vida en la obra; todo se empaqueta en un contenedor .asice que un ciudadano o un auditor puede verificar de manera independiente y sin conexión. Contexto: contratación pública mundial ≈13 billones de dólares al año; entre el 10 % y el 30 % de la obra pública se pierde por corrupción y mala gestión. La prueba de existencia demuestra integridad, momento, lugar y persona —no la honestidad de la decisión ni la calidad de la obra. Fuentes: Banco Mundial; CoST; OCDE; eIDAS art. 41.
- Figura 44.1 — La relación ciudadano-Administración con prueba de existencia (huella SHA-512 en el dispositivo, sello de tiempo RFC 3161/eIDAS, blockchain pública, .asice): la presentación con contenido sellado (qué y cuándo), el reloj del silencio administrativo con vencimientos fechados (Ley 39/2015: 3 meses; certificado en 15 días), la notificación con rastro neutral (los 10 días auditables por ambas partes) y la disponibilidad de citas auditable (contra el mercado negro de la cita previa). Simetría: el mismo rastro acredita la diligencia de la Administración. Límites: no crea citas ni resuelve expedientes; ningún perfil ciudadano central. Fuentes: Ley 39/2015; Defensor del Pueblo (citas de extranjería).
- Figura 45.1 — El sorteo que nadie puede cargar, en dos mitades: el compromiso previo (lista de participantes y regla de adjudicación selladas con t2p —huella SHA-512, RFC 3161/eIDAS, blockchain pública— y publicadas por huella ANTES del sorteo) y el azar público verificable (baliza drand de la League of Entropy: valores imparciales, impredecibles y verificables, generados por criptografía de umbral entre operadores independientes). Resultado: adjudicación recomputable por cualquiera —resultado = regla(lista, azar). Límites: el sorteo limpio no cura la escasez; el ritual público y el notario se refuerzan, no se sustituyen. Fuentes: sorteos de oposiciones y de vivienda protegida; drand/League of Entropy.
- Figura 46.1 — La prueba sellada antes (t2p: huella SHA-512 —solo la huella se ancla, el contenido no sale de la custodia—, RFC 3161/eIDAS, blockchain pública, .asice): el examen certificado antes de la convocatoria con accesos registrados, la plantilla de corrección comprometida antes del examen (las anulaciones, transparentes y fechadas), la hoja de respuestas del opositor fechada al salir, y el expediente de impugnación verificable. Simetría: el tribunal limpio puede probar que no tocó nada —el caso Osakidetza (19 exámenes con indicios de filtración, dimisiones, ocho años y archivo por falta de pruebas) resuelto en días, en cualquier dirección. Patrón: el compromiso previo del capítulo 45, aplicado al contenido. Fuentes: Redacción Médica; Deia; elDiario.es.
- Figura 47.1 — Una persona sin papeles genera un gesto de prueba de vida («soy yo, estoy vivo»); en el dispositivo se calcula su huella SHA-512 con GPS forense y sello de tiempo eIDAS («aquí, ahora»), se ancla a la blockchain pública y puede acompañar una credencial verificable W3C; el titular guarda la prueba en su dispositivo y la comparte con divulgación selectiva, en un contenedor .asice

verificable sin conexión. Escala del reto: ~800 M sin identidad, ~4,4 M (hasta 10 M) apátridas, 150 M de niños no registrados. Fuentes: Banco Mundial ID4D; UNHCR; UNICEF; W3C.

- Figura 48.1 — En la mesa, el acta se fotografía y se sella con huella SHA-512, sello de tiempo eIDAS, GPS forense y prueba de vida del funcionario, en un contenedor .asice anclado a la blockchain pública; si la cifra se altera en tránsito hacia el centro de escrutinio, la huella no coincide y lo delata. Lo que la prueba de existencia NO hace: no es voto por internet, no es voto en blockchain, y no demuestra que el recuento sea verdadero —eso se audita sobre el papel (RLA). Fuentes: Tribunal Supremo de Kenia (2017); Rivest et al. (2021); Philip Stark.
- Figura 49.1 — En el punto de entrega, un recibo de entrega (beneficiario anónimo, importe, lugar, hora) se sella con huella SHA-512, sello de tiempo eIDAS y GPS forense, en un contenedor .asice verificable sin conexión; la prueba de vida en el dispositivo confirma una persona viva sin escáner central; y la desduplicación al estilo Janus revela solo un bit («ya registrado» o «nuevo»), sin crear ninguna base biométrica. Impacto real: en Ucrania se evitaron ~35 M$ de ayuda duplicada. Límite: no prueba qué pasa con el efectivo una vez cobrado (Yemen, Congo). Fuentes: WFP; EPFL/CICR (Janus); Human Rights Watch.
- Figura 50.1 — La cadena de custodia del socorro con prueba de existencia (t2p: huella SHA-512 en el dispositivo, sello RFC 3161/eIDAS, blockchain pública, .asice): el manifiesto sellado en el origen (escáner de hasta 50 páginas), las actas de aduana y almacén con GPS forense (fijado genuino ~50 m / ≤30 s; la ubicación simulada bloquea la certificación), el convoy con capturas reanudadas al recuperar cobertura, y la recepción firmada con vídeo-selfie y retos de vida —exportable como paquete .asice verificable sin conexión por el auditor del donante. Límites: el sello no acredita la calidad del contenido, no levanta bloqueos y nunca ficha a las víctimas. Fuentes: IFRC (fraude Ébola autodivulgado); ONU/WFP (Somalia 2010); OFAC (red CLAP); terremoto de Venezuela 2026.
- Figura 51.1 — Tres cronologías ancladas que se contrastan (huella SHA-512 en el dispositivo, sello de tiempo RFC 3161/eIDAS, blockchain pública, .asice): el rastro sellado de quien huye (sobrevive a la confiscación del teléfono; TJUE C-136/24 P), la documentación de los observadores (testimonios con fecha cierta; Black Book of Pushbacks) y los registros anclados de las autoridades (bitácoras y posiciones; el caso Pylos). La regla de oro: la evidencia anclada suma credibilidad; su ausencia nunca resta. Límites: ningún registro de personas, seguridad física primero, y el sello no decide el asilo ni la política migratoria. Fuentes: HRW/Amnistía (Pylos); RSA (imputación de 17 guardacostas); BVMN; TJUE C-136/24 P.
- Figura 52.1 — Tres entradas convergen en un testamento incontestable: el documento, cuya huella SHA-512 se ancla a la blockchain pública (integridad); la prueba de vida en vídeo, que liga identidad, presencia y voluntad (contra la influencia indebida y la falsificación); y el sello de tiempo eIDAS con GPS, que fija cuál es la versión definitiva (contra «existe un testamento posterior»). El resultado es un .asice verificable sin conexión. Límite: no sustituye testigos, notario ni homologación, y la capacidad la decide el juez o el médico. Fuentes: Cerulli Associates; e-Estonia/Guardtime; caso Voysey.
- Figura 53.1 — La logística coparental con prueba de existencia (huella SHA-512 en el dispositivo, sello de tiempo RFC 3161/eIDAS, blockchain pública, .asice), siempre bilateral y acordada: la comunicación con fecha cierta, la entrega acreditada desde los dos dispositivos (nunca cámaras ni menores fotografiados), los gastos con justificantes anclados y el plan de parentalidad versionado. El norte: el interés superior del menor; el registro es escudo, no arma. Límites: no decide custodias, no mide la crianza, y en situaciones de violencia la prioridad son los canales especializados. Fuentes: INE (custodia compartida 49,7 %, 2024); OurFamilyWizard (tribunales de 50 estados); plan de parentalidad.
- Figura 54.1 — El exportador emite un conocimiento de embarque que se sella con huella SHA-512, sello de tiempo RFC 3161/eIDAS y GPS, anclado a la blockchain pública (.asice). El banco A lo financia y lo marca como pignorado. Cuando un defraudador presenta el «mismo» documento al banco B, la huella coincide y consta como ya pignorado: la segunda financiación se bloquea. Límite: el sello no prueba que la mercancía exista físicamente en el almacén (el «metal fantasma» de Qingdao). Contexto: brecha de financiación del comercio de 2,5 billones de dólares; conocimiento de embarque electrónico real, solo el 5,7 %. Fuentes: Banco Asiático de Desarrollo; ICC; caso Qingdao.
- Figura 55.1 — En el modelo tradicional vulnerable, el extracto bancario pasa por el cliente (Wirecard) antes de llegar al auditor: es el punto donde se cuela la falsificación. Con t2p, la confirmación bancaria, el libro mayor o la factura se sellan en origen —huella SHA-512, sello de tiempo eIDAS, GPS, anclaje a la blockchain pública— y el auditor verifica una cadena de custodia inalterable (.asice). Límite: el sello no hace verdadero un dato fabricado desde la fuente (Wirecard,

Luckin, Enron). Contexto: Wirecard, 1.900 M€ inexistentes; fraude de estados financieros, mediana de 766.000 $ por caso. Fuentes: Financial Times; PCAOB; ACFE.

- Figura 56.1 — De cada dólar que un anunciante pone en la compra programática, solo 36 céntimos llegan al consumidor: 29 se pierden en costes de transacción y 35 en «pérdida de productividad mediática» (webs basura e inventario de baja calidad). El fraude publicitario digital costó 84.000 millones de dólares en 2023 —un 22 % de la inversión en línea— y los bots ya son la mitad del tráfico de internet. Fuentes: ANA (2023); Juniper Research; Imperva.
- Figura 57.1 — Los eventos del sistema (incluido el Event ID 1102, «se ha borrado el registro») se reenvían en tiempo real fuera del sistema atacado; los lotes de registros se resumen en una raíz de Merkle que se sella con huella SHA-512 y sello de tiempo RFC 3161/eIDAS y se ancla a la blockchain pública, encadenando cada raíz con la anterior (solo se puede añadir). Cualquier alteración posterior rompe la huella y delata al atacante. Límite: el anclaje no impide la brecha; solo protege lo que se ha registrado y reenviado a tiempo. Contexto: dwell time medio de 14 días en 2025; coste medio de una brecha, 4,44 M$. Fuentes: MITRE ATT&CK; Mandiant M-Trends; NIST SP 800-86.
- Figura 58.1 — La brecha vista desde el ciudadano, con prueba de existencia (sellado con t2p — capítulo 13): la notificación capturada (o su ausencia, fechada), el certificado de presencia en la filtración (captura web con código fuente), el diario del daño (phishing, llamadas, intentos —cada pieza sellada en el momento) y la reclamación .asice. Fundamento: TJUE C-300/21 —daño moral indemnizable sin umbral, pero con infracción + daño + causalidad PROBADOS. Simetría: la empresa diligente acredita su notificación. Límites: la valoración es del juez; correlación ≠ causalidad; el diario queda en el dispositivo. Fuentes: TJUE; RGPD art. 82.
- Figura 59.1 — La caída documentada con prueba de existencia (sellado con t2p — capítulo 13): la sonda independiente con cadena de registros sellados (el reloj del cliente), la página de estado del proveedor congelada con código fuente, el impacto de negocio documentado (grabación de pantalla, métricas por huella) y la reclamación .asice —para los créditos del SLA, la aseguradora y los reportes DORA/NIS2. Simetría: el proveedor que ancla su disponibilidad hace de ello su argumento comercial. Límites: la sonda acredita cuándo no respondía, no la causa; metodología primero; ningún sello sustituye la redundancia. Fuentes: CrowdStrike 19-7-2024 (8,5 M de Windows; Delta ~550 M$).
- Figura 60.1 — En una excavación legal (izquierda), la pieza se fotografía in situ con coordenadas GPS y sello de tiempo eIDAS antes de moverla: la procedencia queda documentada desde el segundo cero y se ancla a la blockchain pública (.asice). En el expolio (derecha), la «procedencia» en papel empieza años después del hallazgo y es fácil de fabricar —como el Shiva Chola vendido a Australia por 5,6 M$ con papeles falsos. Límite: el sello prueba integridad, fecha, lugar y persona, pero NO autentica el objeto (una foto sellada de una falsificación sigue siendo una falsificación). Contexto: comercio ilícito de antigüedades de 225 M$ a 6.000 M$/año. Fuentes: INTERPOL; fiscalía de Manhattan; Art Loss Register.
- Figura 61.1 — Cuatro frentes de una misma defensa (huella SHA-512, sello de tiempo RFC 3161/eIDAS, anclaje a la blockchain pública, .asice): los manifiestos anclados de los archivos y hemerotecas (ediciones silenciosas detectables), los testimonios de supervivientes sellados en vida (prioridad temporal contra la fabricación), los expedientes de exhumación con cadena de custodia anclada (Ley 14/2022, Banco Estatal de ADN) y el horizonte pre-IA de las colecciones fotográficas (el canon verificable contra la historia sintética). Límites: el sello no hace crítica de fuentes ni congela la interpretación; pluralidad de archivos, nunca un «archivo único de la verdad». Fuentes: UNESCO/CJM; Maldita.es; Internet Archive (brecha 2024); Ley 14/2022.
- Figura 62.1 — El denunciante calcula la huella SHA-512 del documento en su dispositivo y la ancla a la blockchain pública con sello de tiempo eIDAS: se prueba QUÉ y CUÁNDO, no QUIÉN. La capa que delataría —identidad, GPS, prueba de vida, metadatos, IP— se omite deliberadamente: lo que protege es lo que no se sella. Con una prueba de conocimiento cero, el periodista o el tribunal verifican que el documento es auténtico y anterior a una fecha, sin conocer la fuente. Límite: la cadena no bloquea los puntos de rastreo de la impresora (caso Winner), la estilometría ni los metadatos de red. Fuentes: ICIJ (Panama Papers); EFF; Freedom of the Press Foundation.
- Figura 63.1 — A lo largo de la vida de un experimento, el fraude puede entrar en el diseño (cambio de variables: COMPare encontró que solo el 76,3 % de los desenlaces primarios se reportaban bien), en la muestra (fabricación en origen, como Stapel), en la captura del fichero crudo o en la edición de la figura (duplicación de bandas: Bik las encontró en el 3,8 % de 20.621 artículos). El sello en la adquisición —huella SHA-512 + sello eIDAS— cubre el preregistro del protocolo y la captura del dato crudo, y hace detectable cualquier edición posterior; pero no demuestra que el dato fabricado en origen sea verdad. Fuentes: COMPare (Oxford); Bik et al. (mBio 2016); ASM/ImageTwin.

- Figura 64.1 — Cada ciclo de atestación parte de un reto fresco del día (nonce); el pensionista hace el gesto de vivacidad en el dispositivo; se calcula localmente la huella SHA-512 de {vivacidad + reto + GPS + hora}, se ancla a la blockchain pública con sello eIDAS y se cierra en un .asice verificable fuera de línea. El reto irrepetible impide reutilizar grabaciones antiguas: el muerto no puede responder al reto de hoy. La cara no sale nunca del dispositivo; en la cadena solo viaja una huella. Coste de no saber quién sigue vivo: Japón, 234.354 centenarios sin confirmar; EE. UU., 327 M$ a difuntos; Sudáfrica, 140 M de rands a 75.000 muertos. Fuentes: France 24; SSA OIG; SASSA/Moneyweb.
- Figura 65.1 — La prueba de vida en la era del deepfake: contra el secuestro virtual con voz clonada y la «prueba de vida» fabricada con IA (alerta FBI/IC3 2025), el protocolo de tres piezas —reto imprevisible, frescura del momento y sello t2p (huella SHA-512 en el dispositivo, RFC 3161/eIDAS, blockchain pública, .asice). Aplicaciones: el protocolo familiar, la negociación con datación, el último punto del mapa voluntario y el regreso verificable (CNDES: 132 alertas activas en 2025). Límites: el sello acredita frescura, no libertad; voluntario o nada; nunca un sustituto de la policía y los negociadores. Fuentes: CNN (caso DeStefano); FBI/IC3; Ministerio del Interior/CNDES.
- Figura 66.1 — La vida de una muestra antidopaje pasa por cinco nodos: obtención y firma del atleta, precinto de las botellas A y B, transporte, recepción en el laboratorio y análisis. En Sochi, el fraude entró en el nodo del laboratorio (el «agujero de ratón» por donde el servicio secreto intercambiaba la orina de noche). El sello de t2p —GPS forense, sello eIDAS y huella del número de kit anclados a la blockchain pública— hace que aquel intercambio deje una discontinuidad temporal y geográfica detectable. La evidencia forense que delató el fraude pese a las botellas «inviolables»: 44 tapones con marcas de manipulación (12 de medallistas), 8 muestras con sal imposible, 2 con ADN masculino, ≥643 positivos «desaparecidos». Límite: el sello no demuestra qué había en la botella antes de precintarla. Fuentes: Informe McLaren; CNN; Chemistry World.
- Figura 67.1 — La música en streaming reparte un fondo de suma fija: en 2025, más de 22.000 millones de dólares (IFPI). Cada escucha falsa no inventa dinero nuevo; roba su parte a los artistas con público real. La estimación de la industria cifra la fuga por fraude en unos 2.000 millones de dólares al año —al menos un 10 % de la actividad (Beatdapp). El caso Smith: 661.440 escuchas-bot al día, a medio céntimo, durante siete años. Con prueba de vida, las escuchas sin humano no entran en el reparto y el fondo vuelve a los artistas reales. Fuentes: IFPI Global Music Report 2026; Beatdapp; acusación de la fiscalía de Nueva York.
- Figura 68.1 — La capa de red (STIR/SHAKEN) autentica el número de origen —«¿desde qué número llama?»—, pero solo el 42,5 % de las llamadas llegan firmadas (abril de 2025), porque cualquier tramo no-IP rompe la firma. La capa de extremo (t2p: prueba de vida + SHA-512 + sello eIDAS + GPS) autentica el origen humano y el momento del acto —«¿quién, qué y cuándo, de verdad?». Son complementarias. Contexto: 52.800 millones de robocalls en EE. UU. en 2024; 48,8 M$ robados por SIM-swap (FBI, 2023). Fuentes: TransNexus; FCC; FBI IC3.
- Figura 69.1 — El fraude del pago «autorizado» con prueba de existencia (sellado con t2p — capítulo 13): el engaño documentado (llamada propia grabada, SMS y chats capturados), la sesión capturada (la pantalla con el aviso —o sin él), la reclamación datada (plazos) y la simetría del banco diligente (avisos y fricciones anclados por lotes; el alta de la cuenta receptora verificada). Contexto: Reino Unido, primer reembolso obligatorio del mundo (7-10-2024; £85.000; 50/50 emisor-receptor; 5/35 días); PSD2: en operaciones no autorizadas, la carga de la prueba es del banco. Límites: la negligencia grave la valora el juez; la prevención primero. Fuentes: PSR; PSD2/RDL 19/2018.
- Figura 70.1 — Cada evento de custodia de un componente de grado defensa —marcado por el fabricante original, recepción en el distribuidor, «origen» declarado por el broker, informe de ensayo AS6171, aceptación del contratista, instalación— se puede sellar con huella SHA-512, sello eIDAS, GPS forense y prueba de vida, anclados a la blockchain pública. El punto ciego (en rojo): la sustitución física de la pieza *después* del ensayo, que el sello no detecta sin un anclaje al silicio (ADN, huella física no clonable). Contexto: ~80 % de los chips falsos son reciclados o remarcados; la GAO compró 16 piezas militares en línea y las 16 eran falsas; un solo broker introdujo 84.000. Fuentes: Senado de EE. UU. (2012); GAO; IHS/ERAI.
- Figura 71.1 — La cadena de suministro del software con prueba de existencia: cada versión publicada se ancla (huella SHA-512 del tarball, sello de tiempo RFC 3161/eIDAS, blockchain pública, .asice) y se contrasta con el código fuente (la discrepancia de xz-utils, detectable); la cadena de publicación vigilada en los registros de transparencia (Sigstore/Rekor: >101 millones de entradas —prueba de existencia en producción) dispara la alarma ante publicaciones con claves robadas (el gusano Shai-Hulud); el inventario (SBOM) sellado por versión hace la respuesta a incidentes una consulta (Reglamento (UE) 2024/2847). Límites: el sello acredita origen e integridad, no bondad del código;

los mantenedores necesitan herramientas gratuitas y financiación. Fuentes: CVE-2024-3094; CISA (Shai-Hulud); Sigstore/Rekor; CRA.

- Figura 72.1 — El fraude y la opacidad por vertical: tres de cada cuatro barcos pesqueros industriales no emiten señal pública de posición (75 %, Global Fishing Watch); un tercio del marisco de EE. UU. está mal etiquetado —hasta el 87 % del «pargo rojo» (Oceana); una revisión global de más de treinta países encuentra un 36 % de mal etiquetado; y hasta el 90 % del mineral «etiquetado limpio» en dos zonas del Kivu del Sur procedía de fuentes ilícitas (Global Witness). t2p sella el origen en el punto de extracción, antes de la mezcla o el cambio de etiqueta; lo que el sello NO valida es la especie ni la legalidad de la zona. Fuentes: Global Fishing Watch; Oceana; Global Witness.
- Figura 73.1 — El recorrido de un dólar donado, con sus fugas reales: el captador profesional se queda 25 céntimos de media (fiscalía de Nueva York, 2024), y en la mitad de las campañas la entidad recibe menos de la mitad; en el fraude Reynolds, menos de 3 céntimos llegaban al paciente; en el proyecto de Haití, un 40 % se perdía en overhead. Como contrapunto, una ONG eficaz evita una muerte por unos 3.000-5.500 dólares (GiveWell). t2p sella tres nodos —la promesa restringida, cada desembolso y la evidencia de impacto (GPS + hora + prueba de vida)—, convirtiendo el «confía en el informe» en evidencia auditable. Límite: no juzga si la métrica declarada es honesta ni la eficacia del programa. Fuentes: fiscalía de Nueva York; FTC; ProPublica; GiveWell.
- Figura 74.1 — Los registradores (la caja negra de avión con más de 88 parámetros y ahora hasta 25 h de voz; el registrador del coche con los 20 s previos al choque; el registro de vuelo de un dron) capturan el dato. t2p no mejora la captura: en el instante en que el registrador cierra un evento, calcula su huella SHA-512 en el dispositivo y la ancla a la blockchain pública con sello eIDAS, de manera que negar el dato (Tesla), recortarlo (Cruise) o alterarlo deja una huella que no cuadra. Límite: el sello no corrige un dato erróneo, no resuelve la disputa pericial sobre la causa (EgyptAir 990), y no rellena lo que el sensor no grabó (Jeju Air, donde la grabación se cortó 4 minutos antes). Fuentes: NTSB; California DMV; caso Benavides contra Tesla.
- Figura 75.1 — La caja negra personal: el audio de una conversación propia (STC 114/1984), el clip de la dashcam (límites AEPD) o la foto datada se cifran y NO salen nunca del dispositivo; solo la huella SHA-512 con sello de tiempo RFC 3161/eIDAS se ancla a la blockchain pública (.asice). La revelación es decisión del titular, ante el juez. Dos salidas simétricas: la víctima que prueba el daño y el inocente que prueba la coartada. Límites: no acredita la verdad del contenido, no legaliza la grabación de un tercero (art. 197 CP), exige revocabilidad y ningún registro central. Fuentes: STC 114/1984; Fiscalía General del Estado (Cometa; denuncias falsas 0,0082 %); AEPD; UNESPA.
- Figura 76.1 — Dos verdades del dato genético. A la izquierda, el efecto familiar: basta con que el 2 % de una población esté en una base de datos para reidentificar a casi cualquier persona a través de un pariente lejano, y cerca del 60 % de los de ascendencia europea ya son identificables aunque nunca se hayan hecho un test (Erlich et al., 2018). A la derecha, el efecto multiplicador de la brecha: el ataque a 14.000 cuentas (el 0,1 %) expuso a 6,9 millones de usuarios a través de la función que conecta parientes. t2p puede sellar el acto de consentimiento —qué, cuándo y dónde—, pero no puede devolver la privacidad a un dato irrevocable que también es de tu familia. Fuentes: Science (Erlich et al.); TechCrunch; fiscalía de Nueva York.
- Figura 77.1 — La prueba digital sufre dos ataques opuestos. A la izquierda, el falso que engaña: un audio o vídeo fabricado con IA presentado como auténtico (como el audio editado de un caso de familia británico). A la derecha, el dividendo del mentiroso: una grabación auténtica negada como «deepfake» para eludir la responsabilidad (como en el litigio Huang contra Tesla, donde se alegó que los vídeos de Musk «podrían ser deepfakes»). La misma defensa vale para ambos: sellar el fichero en el segundo de la grabación con huella SHA-512, sello eIDAS y GPS (compatible con la regla 902(14): el hash autoautentica copias). Límite: el sello prueba integridad y momento, no la verdad de la escena —una cámara sellada que graba un montaje certifica el montaje. Fuentes: Chesney y Citron (2019); ProPublica; casos Tesla y Baltimore.
- Figura 78.1 — Una nota clínica vista en dos carriles. Arriba, la versión impresa: un solo punto, «02:03 — nota de medicación, Dr. X». Abajo, el rastro de auditoría real con sello de t2p: el evento de creación declarado a las 02:03 pero con la huella anclada a la blockchain pública a las 08:11 —un desfase de seis horas—, hecho desde una estación no clínica (GPS forense fuera del área de cuidados), con una modificación posterior retrodatada que no puede ocultar la información anterior (21 CFR 11.10(e)). El papel muestra un punto; el sello muestra la historia. Límite: el sello prueba quién y cuándo, no la verdad clínica de lo que se escribió. Fuentes: HIPAA y FDA (controles de auditoría); caso Prieto contra Rush; análisis forense de historiales.
- Figura 79.1 — El ciclo de vida de un modelo en cuatro eslabones: datos de entrenamiento → entrenamiento → pesos + AI-BOM (tarjeta de modelo, informe de evaluación) → despliegue. t2p

ancla la huella SHA-512 de los pesos y del manifiesto en la blockchain pública, con sello RFC 3161/eIDAS complementario (.asice). Dos puntos de riesgo: datos ilegales u opacos en el origen (LAION-5B) y pesos manipulados entre el laboratorio y el usuario (puerta trasera *nullifAI* vía *pickle*), que la comprobación de huella detecta. Límite: el sello prueba qué se declaró y cuándo, y que los pesos son los evaluados; no prueba que la declaración sea cierta ni que el modelo sea seguro. Fuentes: Stanford Internet Observatory (LAION-5B); JFrog (modelos maliciosos); Reglamento europeo de IA, art. 53 y 50; CycloneDX ML-BOM.

- Figura 80.1 — El mandato verificable para agentes de IA con prueba de existencia (sellado con t2p — capítulo 13): el mandato sellado antes de activar (presupuesto, ámbitos, vetos), el registro de acciones anclado por lotes encadenados, la captura certificada de la oferta que el agente vio (imagen + código fuente) y la autorización fuerte con vídeo-selfie por encima del umbral. Contexto: la industria ya construye mandatos firmados (Visa Intelligent Commerce, Mastercard Agent Pay, Google AP2 —Intent/Cart Mandate como credenciales verificables); la capa que falta es la neutral entre usuario, plataforma y comercio. Precedente: Moffatt v. Air Canada (2024) —quien despliega el agente responde. Fuentes: tribunal de la Columbia Británica; Visa/Mastercard/Google AP2.
- Figura 81.1 — Dos vías. Arriba: la persona crea, con prueba de vida, una concesión de consentimiento acotada (qué usos, para quién, hasta cuándo) ligada a una referencia biométrica (huella SHA-512; la cara no sale del dispositivo), anclada a la blockchain pública, con sello eIDAS complementario (.asice); una réplica legítima lleva un puntero verificable, y la revocación queda datada. Abajo: un anuncio deepfake sin ninguna concesión sellada —la ausencia misma demuestra la falta de consentimiento. Límite: el sello prueba si se consintió, de quién y cuándo; no detecta el deepfake ni impide su creación, y no juzga si el consentimiento fue libre. Fuentes: caso Tom Hanks; caso Johansson–OpenAI; acuerdo SAG-AFTRA; ELVIS Act; reforma danesa.
- Figura 82.1 — La imagen del menor con prueba de existencia (sellado con t2p — capítulo 13) —se documentan las decisiones de los ADULTOS, nunca el menor: la autorización escolar precisa y sellada (usos, canales, duración), el desacuerdo entre progenitores datado, la petición de retirada con respuesta o silencio datados, y la huella de la publicación para el futuro (el hijo mayor podrá acreditar qué se publicó de él, sin que ningún contenido viaje). Contexto: un niño aparece en ~1.300 fotos en línea antes de los 13 años; Ley francesa 2024-120 (derecho a la imagen dentro de la autoridad parental, ejercido en común; delegación judicial en casos graves). Límites: el interés superior del menor lo fija el juez; proporcionalidad; la prudencia primero. Fuentes: Légifrance; DAJ.
- Figura 83.1 — La víctima o la entidad de apoyo calcula en el dispositivo la huella SHA-512 del contenido (la imagen no sale del teléfono) y le añade dónde y cuándo se ha encontrado; la huella del conjunto se ancla en la blockchain pública, con sello eIDAS complementario (.asice). Dos resultados: a la izquierda, la retirada demostrable en todas las plataformas (modelo StopNCII, con recibo sellado de las 48 horas); a la derecha, evidencia datada y admisible para el tribunal (como en Almendralejo). Límite: el sello no retira la imagen, no impide crearla ni detecta el deepfake; nunca un registro de imágenes, solo huellas. Fuentes: caso Almendralejo; caso Taylor Swift; TAKE IT DOWN Act; Directiva (UE) 2024/1385; StopNCII.org.
- Figura 84.1 — La víctima, la familia o el centro educativo calcula en el dispositivo la huella SHA-512 del contenido de odio (el contenido no sale del teléfono) y le añade dónde y cuándo se ha encontrado y la solicitud de retirada; la huella del conjunto se ancla en la blockchain pública, con sello eIDAS complementario (.asice). Tres salidas: el expediente escolar, la denuncia penal (arts. 510 y 172 ter) y el notice-and-action de la plataforma (DSA/UK OSA), con recibo sellado. Límite: el sello no retira el post, no impide crear odio ni lo detecta; nunca un registro del contenido ni una herramienta de desanonimización, solo huellas en el dispositivo. Fuentes: caso Picchio; Molly Russell; ANAR; StopNCII.
- Figura 85.1 — Tres escudos para las personas mayores con una sola lógica (huella SHA-512 en el dispositivo, sello de tiempo RFC 3161/eIDAS, anclaje a la blockchain pública, .asice): la verificación familiar contra la voz clonada (reto + prueba de vida sellada), el cuidado acreditado (registros de residencia anclados; cámara solo dentro de la doctrina de proporcionalidad del TS) y la voluntad con fecha cierta (Ley 8/2021: apoyo, no sustitución). Límites: ningún registro central de voces, revocabilidad, y el control siempre en manos de la persona mayor. Fuentes: INCIBE; FBI/IC3; elDiario.es (El Escorial); Ley 8/2021.
- Figura 86.1 — El órgano emisor (oficina de prensa, centro de operaciones, banco central) calcula en el dispositivo la huella SHA-512 de la declaración oficial —vídeo, comunicado, decisión o alerta— sin que el fichero salga; para declaraciones en directo del principal le añade prueba de vida y GPS forense. La huella del conjunto se ancla en la blockchain pública, con sello RFC 3161/eIDAS complementario (.asice), y se publica su handle de verificación (QR/URL) en el canal oficial. Dos

resultados: a la izquierda, verificación pública en segundos por parte de periodistas y ciudadanos; a la derecha, el desmentido de una falsificación (teletipo pirateado, reemisión no verificada) contra el original sellado. Límite: el sello prueba origen, hora, autor e integridad, no que el contenido sea cierto, legal ni sensato; no detiene un deepfake nunca comparado ni protege al emisor de ser pirateado. Fuentes: caso Ukraine 24/Zelenski; imagen falsa del Pentágono; caso Rubio; caso Channel 14/Gallant; alerta de Hawái de 2018; artículo 50 del Reglamento de IA; IPAWS; CSI Content Credentials NSA/CISA.

- Figura 87.1 — El directivo genuino captura la instrucción de pago en el dispositivo (texto firmado, factura en PDF o vídeo con prueba de vida y GPS forense), calcula su huella SHA-512 sin que salga del dispositivo, y la ancla en la blockchain pública, con un sello de tiempo RFC 3161/eIDAS complementario (.asice). La tesorería verifica el sello contra el ancla pública: si cuadra, paga; si falta, detiene —la instrucción «urgente» sin sello es, por diseño, una bandera roja (modo de fallo de Arup). Límite: el sello prueba el acto de autorizar, no que la instrucción sea legítima; no detiene a un directivo coaccionado ni una clave robada, ni recupera fondos ya transferidos. Fuentes: caso Arup; alerta FinCEN FIN-2024-Alert004; FBI/IC3 PSA250515; eIDAS art. 41-42.
- Figura 88.1 — La identidad en directo con prueba de existencia (t2p: vídeo-selfie con retos de vida aleatorios —parpadear, girar, sonreír, inclinar— en <60 s, biometría o PIN del dispositivo, huella SHA-512, sello RFC 3161/eIDAS, ancla a la blockchain pública, certificado con la evidencia en vídeo y attestation de hardware, paquete .asice verificable fuera de línea): a la izquierda, el handshake de la reunión (hoja de la reunión como documento-reto firmado por cada participante antes de abrir micrófonos; comparación de la cara sellada con la de pantalla; la pregunta a contracorriente como capa extra); a la derecha, el alta como humano (el formulario de alta firmado con vídeo-selfie: seudónimo-pero-humano, la plataforma verifica sin custodiar biometría; identidad civil vía cartera EUDI cuando hace falta). Contexto: face-swap en tiempo real comercializado (Yahoo Boys), +2.665 % de ataques de cámara virtual nativa y +300 % de face swaps contra sistemas con liveness (iProov 2025), 30 % de desconfianza empresarial prevista (Gartner). Límites: los retos gestuales son un listón, no una muralla —capas y coste asimétrico (el fraude que firma queda notariado); la comparación de caras es del receptor, nunca de la app. Fuentes: WIRED/9to5Mac; iProov; Gartner; FBI IC3; Decrypt; arXiv/MIT; CE (EUDI).
- Figura 89.1 — El emisor (o su agente o teletipo) sella la revelación sensible al precio en el momento de emitirla: huella SHA-512 en el dispositivo → blockchain pública, con sello de tiempo RFC 3161/eIDAS complementario (.asice), con GPS forense y prueba de vida si hay un directivo filmando. La huella se publica junto a la cuenta oficial; cualquier periodista, bolsa, regulador o canal algorítmico confirma en milisegundos si un tuit o comunicado «de última hora» coincide con el genuino (Lilly, Pentágono-Bloomberg, BSE, Ostin) o es el impostor. Límite: el sello prueba quién lo emitió y cuándo, no que la revelación sea verdad; un comunicado de pump-and-dump sellado sigue siendo falso, y la manipulación sigue siendo tarea de la SEC/ESMA/FINRA y las bolsas. Fuentes: caso Eli Lilly; imagen falsa del Pentágono; Hack Crash de 2013; caso Ostin Technology; aviso SEC/FINRA/NASAA; MAR art. 12.
- Figura 90.1 — El titular real, el administrador o el proveedor de servicios societarios presenta la declaración y su evidencia (registro de accionistas, escritura de fideicomiso, identidad, prueba de vida con GPS forense sobre el terreno); se calcula la huella SHA-512 en el dispositivo —los documentos no salen— y se ancla la huella en la blockchain pública, con sello RFC 3161/eIDAS complementario (.asice). El recibo complementa los registros (FinCEN BOI · AMLR/AMLA · Companies House · GAFI R.24): prueba quién declaró qué y cuándo, y hace detectable la retrodatación. Límite: el sello no prueba que la persona declarada sea el titular real último; no atraviesa cadenas de sociedades pantalla ni detecta un testaferro. Fuentes: Papeles de Pandora (ICIJ); Papeles de Panamá; Transparency International; FinCEN; CJUE C-37/20 y C-601/20; GAFI R.24; Open Ownership.
- Figura 91.1 — La contratación remota sellada en tres eslabones: entrevista en vídeo con prueba de vida → verificación de identidad (documento + selfie) → atestación de *onboarding* ligada a quien recibe el portátil. En cada momento se calcula la huella SHA-512 en el dispositivo (la biometría no sale), con sello RFC 3161/eIDAS, GPS forense y anclaje a la blockchain pública (.asice). Resultado: una cadena de no repudio que demuestra que el mismo humano verificado estuvo en los tres puntos. Límite: el sello no prueba que la persona sea honesta, que la identidad no sea robada ni que no sea un nacional sancionado; complementa, no sustituye, el cribado de antecedentes, de sanciones y la detección de deepfakes. Fuentes: caso KnowBe4; caso Chapman (DOJ); FBI/IC3 I-012325-PSA; NIST SP 800-63-4; Pindrop.

- Figura 92.1 — La relación laboral de plataforma con prueba de existencia: el trabajador sella su diario laboral (horas, encargos, instrucciones, capturas de condiciones) en su dispositivo; la plataforma ancla el registro de decisiones algorítmicas y la revisión humana (art. 22 RGPD; Directiva (UE) 2024/2831); el comité recibe los parámetros del algoritmo con versionado sellado (Ley Rider). Tres salidas: la presunción de laboralidad probada con hechos datados, la desactivación auditable y la inspección que no empieza de cero. Límites: el sello no decide la laboralidad ni sustituye la negociación colectiva; el diario es del trabajador, nunca un filtro reputacional. Fuentes: DOUE (Dir. 2024/2831); BOE (Ley 12/2021); elDiario.es (caso Glovo); Worker Info Exchange (Drivers v. Uber/Ola).
- Figura 93.1 — La jornada con prueba de existencia (sellado con t2p — capítulo 13): el diario laboral del trabajador (fichaje, horas, turnos —en su dispositivo, solo huellas en la cadena), el fichaje con GPS forense (el momento, nunca el seguimiento), el cuadrante y la orden capturados con fecha cierta, y el registro oficial de la empresa certificado por lotes encadenados —demostrablemente íntegro ante Inspección y juzgado. Contexto: la reforma del registro horario digital (tramitación urgente desde el 30-9-2025) exigirá inmutabilidad, traza y acceso remoto de la Inspección; >40 % de las horas extra no se pagan (EPA). Límites: el convenio y el juez deciden el fondo; proporcionalidad siempre. Fuentes: EPA/INE; proyecto de registro horario digital.
- Figura 94.1 — Tres hitos irreversibles de una obra: inspección previa al hormigonado (armadura, encofrado, recubrimiento), ensayo de probeta a los 28 días, y planos as-built + informe geotécnico a la firma. En cada hito, t2p calcula la huella SHA-512, le añade GPS forense y prueba de vida si hay captura de campo, sella con RFC 3161/eIDAS y ancla a la blockchain pública (.asice); el contenedor fluye hacia el hilo dorado (BSA 2022) y el modelo BIM (ISO 19650) y se empareja con el Pasaporte Digital de Producto (Reglamento UE 2024/3110). Puntos de riesgo que la datación independiente hace demostrables: cambiar la fecha del ordenador (Hong Kong–Zhuhai–Macao) y escribir el valor de la especificación (Testwell). Límite: el sello prueba que un registro existía, quién lo hizo y cuándo, no que el edificio sea seguro ni que el material cumpla. Fuentes: terremotos de Turquía 2023 (Isias Grand Hotel); NIST (Champlain Towers South); ICAC (puente HZMB); Testwell; puente Morandi; Building Safety Act 2022; Reglamento (UE) 2024/3110.
- Figura 95.1 — Un evento de mantenimiento crea un registro (EASA Form 1 / FAA 8130-3, entrada de cuaderno, lectura de cuentakilómetros). El técnico calcula su huella SHA-512 en el dispositivo (el fichero no sale), le añade GPS forense y prueba de vida si hay captura de campo, y la huella del conjunto se ancla en la blockchain pública, con sello RFC 3161/eIDAS complementario (.asice). Cualquier parte posterior —recepción de mercancías, CAMO, regulador, comprador— verifica de manera independiente quién lo declaró y cuándo. Límite: el sello prueba el origen, el tiempo, el autor y la integridad del documento; no prueba que la pieza sea genuina, nueva o aeronavegable, ni que el kilometraje sea cierto —basura a la entrada, basura en la cadena. Fuentes: caso AOG Technics (SFO); demanda de CFM International; estimaciones FAA de piezas no aprobadas; CARFAX y Parlamento Europeo sobre cuentakilómetros; Aviation Supply Chain Integrity Coalition.
- Figura 96.1 — La cadena de un dato de emisiones en cuatro eslabones: captura en el sensor (CEMS, analizador de metano, banco de pruebas, vuelo de dron/satélite) → adquisición → informe regulador → auditoría. t2p calcula en el dispositivo la huella SHA-512 de la lectura cruda, le añade sello de tiempo RFC 3161/eIDAS y, en campo, GPS forense, y la ancla a la blockchain pública (.asice); el auditor confronta la cifra presentada con la captura sellada. Dos puntos de riesgo: el banco de pruebas trucado (dispositivo de desactivación VW/Cummins) y el sensor sesgado alrededor de las auditorías (CEMS de Berkshire), que el sello NO detecta. Límite: el sello prueba origen, tiempo, autor e integridad de la medición; no prueba que la medición sea cierta en el punto de captura, ni cuantifica emisiones ni juzga el cumplimiento. Fuentes: EPA (VW, Cummins, Berkshire, Marathon, norma de metano); AIE; MethaneSAT; TJUE (ventana térmica).
- Figura 97.1 — La ciencia ciudadana con prueba de existencia: el sensor del balcón, la foto del vertido y el diario del ruido se anclan en origen (huella SHA-512, sello de tiempo RFC 3161/eIDAS, blockchain pública, .asice) y se convierten en cronologías con integridad acreditada que activan la inspección oficial (acta con sonómetro homologado, con presunción de veracidad), orientan al perito y dan memoria a la voz legal de los ecosistemas (Mar Menor, Ley 19/2022). Límites: el sello no acredita la calibración ni sustituye el acta oficial; se documentan hechos, no personas. Fuentes: TJUE (Doñana, 2021); BOE (Ley 19/2022); Sensor.Community; Defensor del Pueblo.
- Figura 98.1 — El ciclo de vida de una batería en cuatro eslabones: materiales y mina → fabricación → uso y estado de salud → segunda vida / reciclaje. Cada eslabón genera un artefacto probatorio (certificado de reciclado, informe de huella de carbono del organismo notificado, exportación del BMS, acta de desmontaje); t2p calcula su huella SHA-512 en el dispositivo y la ancla en la blockchain

pública, con sello RFC 3161/eIDAS complementario (.asice), con GPS forense y prueba de vida en captura de campo. El QR del pasaporte enlaza la afirmación con el artefacto sellado, verificable fuera de línea por aduanas, auditores y compradores de segunda mano. Límite: el sello prueba origen, fecha, autor e integridad del artefacto; no prueba que el contenido reciclado sea real, que el estado de salud no se haya maquillado ni que la batería sea segura. Fuentes: Volvo EX90 / Circulor; Global Battery Alliance; Reglamento (UE) 2023/1542; ESPR (UE) 2024/1781.

- Figura 99.1 — La cadena del residuo con prueba de existencia (sellado con t2p — capítulo 13): el contenedor con lugar y hora en cada cambio de manos (GPS forense; precintado filmado con fecha sobreimpresa), el balance de masa sellado por lotes encadenados (entradas vs salidas datadas), el certificado de tratamiento final anclado y la afirmación verde congelada (captura web con código fuente). Contexto: Reglamento (UE) 2024/1157, aplicable desde el 21-5-2026 —notificación previa para todo residuo plástico exportado, prohibición hacia países no OCDE; Turquía recibía el 39 % de las exportaciones europeas (12,4 Mt). Límites: la traza acredita custodia, no calidad de tratamiento; primero reducir y reutilizar. Fuentes: DOUE/BOE; RETEMA.
- Figura 100.1 — El campo con prueba de existencia (sellado con t2p — capítulo 13): la entrada del cuaderno sellada al momento y en el campo (GPS forense), la foto georreferenciada que la monitorización pide —con fecha cierta neutral—, la serie de campaña como defensa contra el satélite que se equivoca (la simetría del capítulo 104, mirada desde abajo) y el expediente de la ayuda en .asice. Contexto: PAC vigilada por Sentinel/Copernicus; cuaderno digital (CUE) voluntario desde 2024, fitosanitarios electrónicos desde el 1-1-2027, CUE obligatorio el 1-1-2028 (>30 ha). Límites: complementa el cuaderno oficial, no lo sustituye; la brecha digital del campo exige cooperativas y técnicos como aliados. Fuentes: FEGA/normativa CUE; PAC 2023-2027.
- Figura 101.1 — El productor captura la prueba de campo geoetiquetada con prueba de vida y GPS forense (olivar, colmena, línea de envasado) y calcula su huella SHA-512 en el dispositivo; en paralelo, el organismo de control y el laboratorio sellan el certificado, el informe analítico, el número de lote y la etiqueta DOP/IGP. La huella del conjunto se ancla en la blockchain pública, con sello RFC 3161/eIDAS complementario (.asice), ligado a un identificador de lote. Cualquier inspector, aduana o tribunal lo verifica sin conexión: existencia, autor, fecha e integridad. Límite: el sello prueba el papel y el acto de campo, no que el aceite sea virgen extra ni que la miel no esté cortada —eso lo dice el laboratorio (NMR/IRMS/ADN/polen). Fuentes: OPSON XIII y XIV (Europol); caso Apulia; Operación Omegabad; «From the Hives»; Reg. (UE) 2024/1143.
- Figura 102.1 — Dos fuentes de prueba: el trabajador, el sindicato o el auditor de campo capturan en el dispositivo una imagen o un testimonio del taller (huella SHA-512 que no sale del teléfono, GPS forense, prueba de vida); la marca sella la declaración del proveedor y el registro de diligencia debida. La huella del conjunto se ancla en la blockchain pública, con sello de tiempo RFC 3161/eIDAS complementario (.asice). Resultados: testimonio del trabajador más difícil de desestimar como deepfake, y expediente fechado para la CBP, la BAFA o la autoridad de la UE. Límite: el sello prueba el acto, el lugar y la fecha; no prueba que las condiciones sean buenas, que la declaración sea veraz ni que el testimonio fuera libre. Fuentes: caso Volkswagen/CBP; OIT; Miller & Chevalier (UFLPA); HRW (auditorías y automóvil); ECCHR (certificados).
- Figura 103.1 — Al tomar una fijación, una unidad de a bordo o un inspector del estado del puerto captura el registro de navegación (GNSS + hora, IMO/MMSI, calado, trama AIS) y calcula su huella SHA-512 en el dispositivo; la huella del conjunto se ancla en la blockchain pública, con sello RFC 3161/eIDAS complementario (.asice), con GPS forense y prueba de vida cuando hay inspección física. Dos resultados: a la izquierda, un libro mayor de posición e identidad no repudiable; a la derecha, la ausencia de sello se convierte en una bandera roja para el cribado de la OFAC/UE. Límite: el sello certifica que el dispositivo registró esta fijación en este instante, no que la señal GNSS fuera genuina; una señal falseada ancla una posición falsa. Fuentes: caso Windward (esquema de 800 M$); Kpler (261 buques); GPSPATRON (10.000+ buques); Scientific American (Ormuz); OFAC (MS ENOLA).
- Figura 104.1 — La cadena de la observación de la Tierra en dos eslabones de sellado. En el origen, el operador (Maxar, Planet, Copernicus) calcula la huella SHA-512 de la escena cruda/L1 más los metadatos en el ingest de la estación de tierra, con sello RFC 3161/eIDAS anclado en la blockchain pública (.asice). En el otro extremo, el analista o periodista OSINT vuelve a sellar el recorte, la anotación y las coordenadas, con GPS forense y prueba de vida. Puntos de riesgo: imagen forjada con GAN/difusión (Stable Diffusion, StyleGAN2) e interferencia del GNSS, que la firma de Galileo OSNMA y los detectores de Vision Transformer mitigan pero no eliminan. Límite: el sello prueba origen, hora, autor e integridad bit a bit; no prueba que la escena sea observación auténtica ni que la

interpretación sea correcta. Fuentes: caso Bucha (Maxar); Bo Zhao (geografía deepfake); Xinjiang (BuzzFeed); arXiv 2511.17766; Galileo OSNMA; OGC IPT.

- Figura 105.1 — El dato de emergencia se sella en origen: la lectura del sensor (SAIH/Poyo), el acta y el vídeo del órgano de coordinación (CECOPI), la alerta (ES-Alert), la orden de evacuación y la foto de daños del ciudadano reciben la huella SHA-512 en el dispositivo o en la fuente, el sello de tiempo RFC 3161/eIDAS y el anclaje en la blockchain pública (.asice). Tres salidas: la instrucción judicial (cronología no repudiable), la reclamación a la aseguradora y al Consorcio, y la auditoría pública y periodística. Límite: el sello no predice, no avisa y no salva; solo hace la verdad indestructible. Fuentes: Maldita.es; CHJ/SAIH; Consorcio de Compensación de Seguros; Lauegi.
- Figura 106.1 — Ante la carrera a menudo perdida de la detección, el anclaje neutral demuestra que algo auténtico existió y no se ha alterado.
- Figura 107.1 — La decisión de IA pública deja un registro citado que, anclado con prueba de existencia, se convierte en una auditoría independiente y no repudiable.
- Figura 108.1 — La prueba de personalidad se puede hacer en el dispositivo, sin bases biométricas centralizadas: una persona, una voz, sin vigilancia.
- Figura 109.1 — La prueba simétrica en la calle: el vídeo del manifestante y la cámara corporal del agente se sellan en captura, por segmentos (huella SHA-512 en el dispositivo, sello de tiempo RFC 3161/eIDAS, anclaje en la blockchain pública, .asice), sin publicar nada ni identificar a nadie. En el juzgado, las dos cadenas se fusionan en una línea de tiempo verificable; cualquier corte o supresión se detecta. Límites: el sello no acredita el contexto fuera de plano, no valora la proporcionalidad y exige revocabilidad, publicación voluntaria y cero reconocimiento facial. Fuentes: Pulitzer/Frazier; elDiario.es («Rodea el Congreso»); SME/USPAC (Axon Body 3); Telemundo/Univision (Detroit).
- Figura 110.1 — Cuanto más sube la temperatura, más cae la economía: el coste de no actuar se dispara con cada décima de grado.
- Figura 111.1 — Cada actor —gobierno, empresa y ciudadanía— tiene acciones concretas a corto, medio y largo plazo.
- Figura 112.1 — El sello y la cadena: quién controla la prueba, y quién queda atrapado. Los riesgos que el capítulo desgrana —la neutralidad que no existe, el consentimiento cristalizado, la plusvalía de la prueba, el derecho al olvido eliminado, los algoritmos inapelables y la autocensura del registro permanente— y los contrapesos que reclama: solo-huella por defecto, revelación selectiva, gobernanza democrática de la infraestructura y el derecho a no sellar.
- Figura 113.1 — La prueba bajo asedio, del objetivo al tribunal (t2p: huella SHA-512 en el dispositivo — la imagen no sale del móvil —, sello RFC 3161/eIDAS, ancla en la blockchain pública, paquete .asice): el fotoperiodista acreditado con credencial de agencia sin exponer la fuente; el testigo ciudadano con compromiso y revelación (sella ahora, publica cuando sea seguro) y prueba póstuma; las tres capas del asedio (puerta cerrada a la prensa internacional, periodistas locales muertos o señalados, «¡fake!» contra las imágenes reales) y dónde las rompe el sello. Límites: el apagón retrasa el ancla (sándwich temporal «no antes / no después»); el GPS suplantado degrada la posición, no la hora; el sello prueba cuándo y qué — nunca la verdad de la escena: la corroboración sigue siendo imprescindible. Fuentes: CPJ; RSF; Costs of War (Brown); OHCHR; Forensic Architecture; ECCHR/Coblenza; Access Now; Starling Lab/Reuters; WITNESS/Guardian Project.
- Figura 114.1 — La doctrina social de la Iglesia ante la economía y la técnica: de la 'Rerum Novarum' (1891, el trabajo) a la 'Laudato Si'' (2015, la Casa común) y la 'Magnifica Humanitas' (2026, la persona en tiempos de IA).
- Figura 114.2 — La misma prueba de existencia, dos caminos (§1): hacia «Babel» (poder privado, reducción de la persona a dato, dominación) o hacia la «ciudad» (dignidad de quien existe, subsidiariedad, acceso universal). La diferencia no es técnica, sino de gobernanza y de fin.

Glosario

Uso obligatorio en las tres versiones para garantizar coherencia. Las marcas **time2act** y **t2p no se traducen nunca**. Anglicismos asentados (blockchain, deepfake, smart contract, token) se mantienen.

Concepto	Català (maestro)	Español	English	Nota
Pico de demanda	pic de demanda	pico de demanda	peak demand	Sustituye al viejo "peak oil" (pico de oferta)
Pico de oferta	pic d'oferta (peak oil)	pico de oferta (peak oil)	peak oil	Tesis clásica de Roberts
Transición energética	transició energètica	transición energética	energy transition	
Prueba de existencia	prova d'existència	prueba de existencia	proof of existence	Núcleo de t2p
Sellado de tiempo	segellat de temps	sellado de tiempo	timestamping	
Resumen criptográfico	resum criptogràfic (hash)	hash criptográfico	cryptographic hash	"hash" admitido
Cadena de bloques	cadena de blocs / blockchain	blockchain	blockchain	"blockchain" de uso común
Libro mayor distribuido	llibre major distribuït	libro mayor distribuido	distributed ledger	
Contrato inteligente	contracte intel·ligent	contrato inteligente	smart contract	
Prueba de participación	prova de participació (PoS)	prueba de participación (PoS)	proof of stake (PoS)	Ethereum desde 2022
Prueba de trabajo	prova de treball (PoW)	prueba de trabajo (PoW)	proof of work (PoW)	Minería intensiva en energía
Procedencia del contenido	procedència del contingut	procedencia del contenido	content provenance	Estándar C2PA
Protocolo de confianza	protocol de confiança	protocolo de confianza	trust protocol	Marco de Tapscott
Coste normalizado de electricidad	cost normalitzat de l'electricitat	coste normalizado de la electricidad	LCOE	Siglas LCOE en las 3 lenguas
Red eléctrica	xarxa elèctrica	red eléctrica	(power) grid	
Red inteligente	xarxa intel·ligent	red inteligente	smart grid	
MRV de carbono	MRV de carboni	MRV de carbono	carbon MRV	Medición, reporte y verificación
Garantía de origen	garantia d'origen	garantía de origen	guarantee of origin	Certificados de energía renovable
Tokenización	tokenització	tokenización	tokenization	
Crédito de carbono	crèdit de carboni	crédito de carbono	carbon credit	1 crédito = 1 tCO_2e evitada o eliminada
Mercado de cumplimiento	mercat de compliment (EU ETS)	mercado de cumplimiento (EU ETS)	compliance market (EU ETS)	Cap-and-trade regulado; el derecho es la EUA
CBAM	mecanisme d'ajust de carboni a la frontera (CBAM)	mecanismo de ajuste de carbono en frontera (CBAM)	Carbon Border Adjustment Mechanism (CBAM)	Fase definitiva desde el 1-ene-2026
CORSIA	CORSIA	CORSIA	CORSIA	Compensación de emisiones de la aviación (OACI)

Concepto	Català (maestro)	Español	English	Nota
Mercado voluntario	mercat voluntari del carboni (VCM)	mercado voluntario de carbono (VCM)	voluntary carbon market (VCM)	Verra, Gold Standard; sin obligación legal
Doble cómputo	doble còmput	doble cómputo	double counting	Contar el mismo ahorro o crédito dos veces
Crédito fantasma	crèdit fantasma	crédito fantasma	phantom credit	Crédito sin una reducción real detrás
Adicionalidad	addicionalitat	adicionalidad	additionality	¿Habría ocurrido igualmente sin el incentivo?
Línea de base	línia de base	línea de base	baseline	Escenario de referencia para medir el ahorro
Principios de Carbono de Base	ICVCM / Core Carbon Principles	ICVCM / Core Carbon Principles	ICVCM / Core Carbon Principles	Sello de integridad del mercado voluntario (2023)
Certificado de Ahorro Energético	CAE (Certificat d'Estalvi Energètic)	CAE (Certificado de Ahorro Energético)	Energy Saving Certificate (white certificate)	1 CAE ≈ 1 kWh acreditado; Sistema CAE (RD 36/2023)
Sujeto obligado	subjecte obligat / delegat	sujeto obligado / delegado	obligated / delegated party	Comercializadoras energéticas y sus delegados
Telemática	telemàtica	telemática	telematics	Datos GPS/CAN-bus del vehículo
Coche compartido	cotxe compartit	coche compartido	car-sharing	Un vehículo compartido sustituye a varios privados
tCO_2e	tCO_2e	tCO_2e	tCO_2e	Tonelada de CO_2 equivalente
Activos varados	actius varats	activos varados	stranded assets	Reservas fósiles no quemables
Hidrógeno verde	hidrogen verd	hidrógeno verde	green hydrogen	
Captura de carbono	captura de carboni (CCS)	captura de carbono (CCS)	carbon capture (CCS)	
Cero neto	zero net	cero neto	net zero	
Gases de efecto invernadero	gasos d'efecte hivernacle (GEH)	gases de efecto invernadero (GEI)	greenhouse gases (GHG)	
Vehículo eléctrico	vehicle elèctric (VE)	vehículo eléctrico (VE)	electric vehicle (EV)	
Ultrafalsificación	deepfake	deepfake	deepfake	Anglicismo; glosar 1ª vez
Desinformación	desinformació	desinformación	disinformation	
Credenciales de contenido	credencials de contingut (C2PA)	credenciales de contenido (C2PA)	Content Credentials (C2PA)	Estándar de procedencia firmada
Sello de tiempo RFC 3161	segell de temps RFC 3161	sello de tiempo RFC 3161	RFC 3161 timestamp	Sellado de tiempo de confianza
OpenTimestamps	OpenTimestamps	OpenTimestamps	OpenTimestamps	Sellado en Bitcoin vía árbol de Merkle
Identidad digital europea	eIDAS 2.0	eIDAS 2.0	eIDAS 2.0	Reglamento UE de identidad y confianza
Cartera de identidad digital europea	cartera EUDI	cartera EUDI	EUDI Wallet	Monedero europeo de identidad (eIDAS 2.0); cada estado debe

Concepto	Català (maestro)	Español	English	Nota
				ofrecerla desde dic-2026
Conozca a su cliente	KYC	KYC	KYC (know your customer)	Verificación de identidad en finanzas
Credencial verificable	credencial verificable	credencial verificable	verifiable credential	Modelo W3C; diplomas y títulos
Cadena de custodia	cadena de custòdia	cadena de custodia	chain of custody	Integridad probatoria
Protocolo de Berkeley	Protocol de Berkeley	Protocolo de Berkeley	Berkeley Protocol	Estándar OHCHR/Berkeley para evidencia digital de fuentes abiertas
Compromiso y revelación	compromís i revelació (commit-reveal)	compromiso y revelación (commit-reveal)	commit-reveal	Sellar hoy la huella, revelar el contenido cuando convenga
Investigación de fuentes abiertas	recerca en fonts obertes (OSINT)	investigación de fuentes abiertas (OSINT)	open-source intelligence (OSINT)	Verificación con material público: geolocalización, cronolocalización
Ataque de inyección	atac d'injecció	ataque de inyección	injection attack	Cámara virtual que burla el KYC
Dividendo del mentiroso	dividend del mentider	dividendo del mentiroso	liar's dividend	Eludir la responsabilidad negando como deepfake una grabación auténtica
Árbol de Merkle	arbre de Merkle	árbol de Merkle	Merkle tree	Raíz que resume miles de hashes en uno
Función SHA-512	SHA-512	SHA-512	SHA-512	Huella de 512 bits que usa t2p
Polygon	Polygon	Polygon	Polygon	Cadena pública (compatible con Ethereum) donde t2p ancla hoy; la implementación admite cualquier otra L2
Contenedor ASiC-E	contenidor ASiC-E (.asice)	contenedor ASiC-E (.asice)	ASiC-E container (.asice)	Paquete de evidencia verificable offline (ETSI EN 319 162)
Prueba de vida	prova de vida	prueba de vida	liveness / proof of life	Biometría anti-suplantación (vídeo-selfie)
Hash perceptual	hash perceptual	hash perceptual	perceptual hash	Huella robusta a recompresión o reescalado
Fraude de siniestros	frau de sinistres	fraude de siniestros	claims fraud	Reclamaciones de seguro infladas o inventadas
Falsificación	falsificació	falsificación	counterfeiting	Bienes o documentos imitados ilegalmente
Trazabilidad de origen	traçabilitat d'origen	trazabilidad de origen	provenance / traceability	Prueba verificable de dónde viene un bien
EUDR	EUDR (reglament antidesforestació)	EUDR (reglamento antideforestación)	EU Deforestation Regulation	Exige geolocalización de las parcelas de origen

Concepto	Català (maestro)	Español	English	Nota
Registro de la propiedad	registre de la propietat	registro de la propiedad	land registry	Padrón oficial de títulos de tierra
Activo del mundo real	actiu del món real (RWA)	activo del mundo real (RWA)	real-world asset (RWA)	Activo físico/financiero representado on-chain
Problema del oráculo	problema de l'oracle	problema del oráculo	oracle problem	Cómo probar que el dato off-chain es cierto
Publicación defensiva	publicació defensiva	publicación defensiva	defensive publication	Difundir una invención para crear prior art
Prior art / estado de la técnica	estat de la tècnica	estado de la técnica	prior art	Conocimiento previo que impide patentar
Contratación pública	contractació pública	contratación pública	public procurement	Compra de bienes y obras por el Estado
Manipulación de licitaciones	manipulació de licitacions	manipulación de licitaciones	bid-rigging	Acuerdo fraudulento para amañar un concurso
Identidad autosoberana	identitat autosobirana (SSI)	identidad autosoberana (SSI)	self-sovereign identity (SSI)	El usuario custodia sus propias credenciales
Identificador descentralizado	identificador descentralitzat (DID)	identificador descentralizado (DID)	decentralized identifier (DID)	Estándar W3C de identidad sin autoridad central
Apátrida	apàtrida	apátrida	stateless person	Persona sin nacionalidad reconocida por ningún Estado
Auditoría de riesgo limitado	auditoria de risc limitat (RLA)	auditoría de riesgo limitado (RLA)	risk-limiting audit (RLA)	Recuento estadístico que confirma el resultado electoral
Asistencia en efectivo y vales	assistència en efectiu i vals (CVA)	asistencia en efectivo y vales (CVA)	cash & voucher assistance (CVA)	Ayuda humanitaria entregada como dinero o vales
Deduplicación de beneficiarios	deduplicació de beneficiaris	deduplicación de beneficiarios	beneficiary deduplication	Evitar el doble registro de un mismo beneficiario
Testamento ológrafo	testament hològraf	testamento ológrafo	holographic will	Testamento escrito a mano por el testador
Conocimiento de embarque	coneixement d'embarcament	conocimiento de embarque	bill of lading (B/L)	Título de la mercancía transportada
Carta de crédito	carta de crèdit	carta de crédito	letter of credit (L/C)	Garantía bancaria de pago en el comercio internacional
Documento electrónico transferible	document electrònic transferible (MLETR)	documento electrónico transferible (MLETR)	electronic transferable record (MLETR)	Ley modelo UNCITRAL que da validez legal a los documentos electrónicos
Aseguramiento	assegurament	aseguramiento	assurance	Verificación independiente de un informe (financiero o de sostenibilidad)
CSRD	CSRD	CSRD	CSRD	Directiva UE de informes de sostenibilidad con aseguramiento obligatorio

Concepto	Català (maestro)	Español	English	Nota
Sitio hecho para anunciar	lloc fet per anunciar (MFA)	sitio hecho para anunciar (MFA)	made-for-advertising (MFA)	Web basura creada solo para captar gasto publicitario
Tiempo de permanencia	temps de permanència	tiempo de permanencia	dwell time	Días que un atacante pasa dentro de una red sin ser detectado
Registro a prueba de manipulación	registre inalterable	registro inalterable	tamper-evident log	Log cuyo hash anclado delata cualquier alteración
Procedencia de la obra	procedència de l'obra	procedencia de la obra	art provenance	Cadena verificable de propiedad y origen de una obra
Divulgación selectiva	divulgació selectiva	divulgación selectiva	selective disclosure	Probar un dato sin revelar el resto (zero-knowledge)
Integridad de la investigación	integritat de la recerca	integridad de la investigación	research integrity	Integridad del dato y la imagen científicos, no de la autoría
Pre-registro de ensayos	preregistre d'assaigs	preregistro de ensayos	trial pre-registration	Depósito con fecha cierta del protocolo antes de recoger datos
Fábrica de papers	fàbrica de papers	fábrica de papers	paper mill	Empresa que produce y vende artículos científicos falsos
Prueba de vida recurrente	prova de vida recurrent	prueba de vida recurrente	recurring proof of life	Atestación periódica de que el beneficiario sigue vivo
Pasaporte biológico	passaport biològic	pasaporte biológico	biological passport	Serie longitudinal de biomarcadores del atleta (detección indirecta de dopaje)
Amaño de partidos	amanyament de partits	amaño de partidos	match-fixing	Manipulación del resultado deportivo, detectada por patrones de apuestas
Fraude de streaming	frau de reproduccions	fraude de streaming	streaming fraud	Bots que inflan reproducciones para drenar el fondo de royalties
Intercambio de SIM	intercanvi de SIM	intercambio de SIM	SIM swapping	Robo del número de móvil para interceptar códigos de un solo uso
Autenticación del identificador	autenticació de l'identificador	autenticación del identificador	STIR/SHAKEN	Firma del número de origen de una llamada en la red
Componente reciclado/remarcado	component reciclat/remarcat	componente reciclado/remarcado	recycled/remarked component	Chip usado, lijado y revendido como nuevo
Pedigrí del componente	pedigrí del component	pedigrí del componente	component pedigree	Cadena de custodia documentada hasta el fabricante original
Pesca INDNR	pesca INDNR	pesca INDNR	IUU fishing	Ilegal, no declarada y no reglamentada
Minerales de conflicto (3TG)	minerals de conflicte (3TG)	minerales de conflicto (3TG)	3TG conflict minerals	Estaño, tántalo, wolframio y oro

Concepto	Català (maestro)	Español	English	Nota
Proceso de Kimberley	Procés de Kimberley	Proceso de Kimberley	Kimberley Process	Certificación contra los diamantes de sangre
Transparencia de donaciones	transparència de donacions	transparencia de donaciones	donation transparency	Rastreo del dinero del donante hasta el impacto demostrable
Registrador de datos (caja negra)	registrador de dades (caixa negra)	registrador de datos (caja negra)	data recorder (black box)	FDR/CVR/EDR/log de vuelo a prueba de manipulación
Dato genómico	dada genòmica	dato genómico	genomic data	Categoría especial; irrevocable y compartido con la familia
Recibo de consentimiento	rebut de consentiment	recibo de consentimiento	consent receipt	Constancia legible y procesable de un acto de consentimiento (Kantara/ISO 27560)
Registro de auditoría	registre d'auditoria	registro de auditoría	audit trail	Rastro de quién accedió o alteró un registro electrónico y cuándo
Lista de materiales del modelo	llista de materials del model (AI-BOM)	lista de materiales del modelo (AI-BOM)	AI/ML bill of materials (AI-BOM)	Inventario de datos, pesos y evaluaciones de un modelo (CycloneDX ML-BOM)
Tarjeta de modelo	targeta de model	tarjeta de modelo	model card	Documento de uso, rendimiento y límites de un modelo (Mitchell 2019)
Réplica digital	rèplica digital	réplica digital	digital replica	Recreación por IA de la voz o la imagen de una persona
Derecho a la propia imagen	dret a la pròpia imatge	derecho a la propia imagen	right of publicity / likeness rights	Control del uso de cara y voz (ELVIS Act, NO FAKES, ley danesa)
Imágenes íntimas no consentidas	imatges íntimes no consentides (NCII)	imágenes íntimas no consentidas (NCII)	non-consensual intimate imagery (NCII)	Difusión de imágenes sexuales sin consentimiento, reales o deepfake (TAKE IT DOWN Act)
Huella en el dispositivo	empremta al dispositiu	huella en el dispositivo	on-device hashing	El archivo no sale del dispositivo; solo viaja la huella (modelo StopNCII)
Fraude del directivo	frau del directiu (BEC)	fraude del directivo (BEC)	business email compromise (BEC)	Suplantación de un alto cargo para autorizar un pago (caso Arup)
Verificación fuera de banda	verificació fora de banda	verificación fuera de banda	out-of-band verification	Confirmar una orden por un canal independiente y pactado
Titular real último	titular real últim (UBO)	titular real último (UBO)	ultimate beneficial owner (UBO)	Persona física que controla de verdad una sociedad (GAFI R.24)
Sociedad pantalla	societat pantalla	sociedad pantalla	shell company	Empresa sin actividad real usada para ocultar al titular

Concepto	Català (maestro)	Español	English	Nota
Hilo dorado	fil daurat	hilo dorado	golden thread	Registro digital trazable del edificio (Building Safety Act 2022)
Planos as-built	plànols as-built	planos as-built	as-built drawings	Registro de cómo se construyó realmente, no de cómo se diseñó
Dispositivo de desactivación	dispositiu de desactivació	dispositivo de desactivación	defeat device	Trampa que falsea las emisiones durante la prueba (Dieselgate)
Monitorización continua de emisiones	monitoratge continu d'emissions (CEMS)	monitorización continua de emisiones (CEMS)	continuous emissions monitoring (CEMS)	Sensores que reportan emisiones en tiempo real
Pasaporte Digital de Producto	Passaport Digital de Producte (DPP)	Pasaporte Digital de Producto (DPP)	Digital Product Passport (DPP)	Registro de ciclo de vida (ESPR UE; batería obligatoria desde 2027)
Pieza sospechosa no aprobada	peça sospitosa no aprovada (SUP)	pieza sospechosa no aprobada (SUP)	suspected unapproved part (SUP)	Componente con certificado de aeronavegabilidad falsificado (AOG Technics)
Fraude alimentario	frau alimentari	fraude alimentario	food fraud	Adulteración o falsa indicación de origen (Operación OPSON)
Indicación geográfica	denominació d'origen (DOP/IGP)	denominación de origen (DOP/IGP)	geographical indication (PDO/PGI)	Sello de origen y método protegidos en la UE
Diligencia debida en la cadena	diligència deguda (CSDDD)	diligencia debida (CSDDD)	supply-chain due diligence (CSDDD)	Deber de vigilar el trabajo forzoso y los derechos humanos (UFLPA, CSDDD)
Falseamiento del AIS	falsejament de l'AIS	falseamiento del AIS	AIS spoofing	Falsear la posición o la identidad de un buque
Flota fantasma	flota fantasma	flota fantasma	shadow / dark fleet	Buques que evaden sanciones ocultando posición e identidad
Geografía deepfake	geografia deepfake	geografía deepfake	deepfake geography	Imagen de satélite sintética o manipulada; la imagen orbital como testigo y como blanco
Handshake de vida	handshake de vida	handshake de vida	liveness handshake	Intercambio de vídeo-selfies sellados sobre un documento-reto antes de una reunión o alta (cap. 88)
Credencial de personalidad	credencial de personalitat	credencial de personalidad	personhood credential	Probar que eres humano real sin revelar identidad (propuesta MIT/OpenAI/Microsoft 2024)