time2act



www.time2act.info
read2act@proton.me

© 2026 Kimèric · Creative Commons BY-NC-ND 4.0 (Reconeixement-NoComercial-SenseObraDerivada).

Qui és Kimèric?

En el silenci d'una pàgina que es regala a tot aquell qui tingui la inquietud de llegir-la, la veu de *time2act* és un intent de sacsejar la psique del món que ens ha tocat viure.

Puc ser present dins de cada línia i, alhora, absent de la portada. Aquesta reserva no és un joc de misteri, sinó la condició mateixa del projecte: en un llibre que tracta de creure les coses per com són i no per qui te les explica, l'autor tria no demostrar res de si mateix. L'argument s'ha de sostenir sol, com una estructura que ressona independentment de qui la sostingui.

La confiança que demana aquest llibre no recau en la signatura, sinó en allò que es pot verificar. Cada afirmació ve acompanyada de les seves fonts; cada capítol convida el lector a comprovar, no a creure. Qui llegeix és convidat a jutjar el text amb els seus propis criteris, com un científic que examina la mostra sense saber qui l'ha dipositada.

El silenci al voltant del nom és part del pacte: no s'hi busca notorietat, sinó una empenta col·lectiva cap a la veritat compartida. Si el que hi ha escrit és cert, ho és digui qui ho digui. I si no ho fos, cap signatura no ho salvaria.

I, per ser didàctic amb allò que us mostrarem en aquesta obra, l'autor es podrà demostrar quan ell ho decideixi: l'edició inicial, amb el seu nom real, ha estat certificada a perpetuïtat a la blockchain en aquesta transacció.

SHA-512: 7ba4e231b30c5d9c8ff1ca31e126b0fa8f41195b93dfca65192d2f82c3fa1855
2b0b3a930be24a74e1c4d09ec271ab47e5b77c4e5f4ad99e2e4c4156546ab508

Transacció (Polygon): 57b78bdddd4926ceeea22d0d81bbc48440c59715ffda85b62aa76880a17769b9

https://polygonscan.com/tx/0x57b78bdddd4926ceeea22d0d81bbc48440c59715ffda85b62aa76880a17769b9

17 de juliol de 2026

Si en algun moment l'autor volgués desvetllar la seva identitat, en tindria prou de mostrar el contingut de l'arxiu que dona exactament el mateix hash que s'ha certificat a la blockchain, perquè qualsevol persona del món —inclosos els perits informàtics— tingui la certesa de la integritat de la dada.

Tots els drets d'aquesta obra queden reservats en la mateixa certificació blockchain, que en fixa el contingut i la data de manera inalterable. Amb aquesta reserva feta, l'obra és lliure: qualsevol tercer pot utilitzar-la, citar-la o difondre-la sempre que en nomeni la font, time2act.info. I si algú no ho fa i pretén apropiar-se de l'obra, totalment o parcialment, tard o d'hora la blockchain demostrarà què es va escriure, i quan; i això n'hi haurà prou per desemmascarar-lo.

Aprendre i aplicar aquesta senzilla però poderosa combinació és el que ens permetrà combatre les mentides en l'entorn digital que condiciona els designis del món que ens ha tocat viure.

Índex

- Pròleg — De 2004 a 2026: el dia que vam tocar el límit

Part I — El llenguatge de la confiança

- 1. El protocol de la confiança: com es prova que una cosa és certa

Part II — La màquina energètica, revisitada

- 2. Encendre el foc, revisitat
- 3. L'últim petroli fàcil... i per què ja importa menys
- 4. El futur ja és aquí: renovables, bateries i vehicle elèctric
- 5. L'energia és poder
- 6. Massa calent: el clima el 2026

Part III — Les conseqüències, avui

- 7. Donar a la gent el que vol: consum, eficiència i «menys és més»
- 8. Les grans energètiques, ansioses
- 9. La nova tensió: la IA com a salvació i com a set d'energia
- 10. La crisi de la veritat: desinformació i deepfakes

Part IV — Les solucions: IA i la capa de confiança

- 11. Seguretat energètica reinventada: xarxes intel·ligents i IA
- 12. La mà (ja no tan) invisible: blockchain com a capa de confiança
- 13. t2p: la prova d'existència contra les deepfakes
- 14. Hidrogen, captura i les apostes que falten

Part V — Cinc fronts contra les deepfakes

- 15. Detectar no n'hi ha prou: la prova d'existència com a defensa duradora
- 16. Diners i confiança: frau, compliance i finances
- 17. La imatge com a testimoni: fotoperiodisme i mitjans
- 18. Vida o mort de les dades: salut i imatge mèdica
- 19. Credencials i autoria: educació i recerca
- 20. La veritat com a arma: defensa i drets humans

Part VI — La confiança al servei del clima: crèdits, certificats i mobilitat

- 21. Crèdits de carboni: el mercat del compliment
- 22. El mercat voluntari del carboni: promesa, frau i la cursa per la integritat
- 23. CAE: certificar l'estalvi sense fer trampa
- 24. Autoconsum i comunitats energètiques: la lectura verificable
- 25. Mobilitat I: flotes i empreses, evidència sòlida
- 26. Mobilitat II: cotxe compartit i particulars, repartir la confiança
- 27. Retards de transport: provar l'hora d'arribada

Part VII — La prova d'existència a l'economia real: actius, béns, idees i institucions

- 28. Assegurances: la prova del sinistre
- 29. Cadena de subministrament: l'origen verificable contra la falsificació
- 30. Consum: ressenyes falses, preus inflats i garanties amb rellotge
- 31. La segona mà entre particulars: l'estat de l'article, amb data certa
- 32. El lloguer de coses: l'estat en agafar i en tornar
- 33. El client contra la companyia: la baixa, la permanència i el call center
- 34. La factura i la morositat: el rellotge del cobrament
- 35. Immobiliari: l'estat de la propietat i el registre de la terra
- 36. Lloguer i habitatge: l'estat de les coses, amb data certa
- 37. La comunitat de propietaris: actes, derrames i acords amb data certa
- 38. Reformes a casa: la bestreta, l'obra i la prova
- 39. Actius del món real: tokenitzar amb proves, no a cegues

- 40. Autoria creativa: provar qui ho va fer primer en l'era de la IA
- 41. Patents i prior art: la publicació defensiva amb data certa
- 42. Secrets empresarials: provar sense revelar
- 43. Govtech: contractació pública i registres a prova de manipulació
- 44. El ciutadà davant l'Administració: el rellotge del silenci
- 45. L'atzar verificable: sortejos que ningú no pot carregar
- 46. Oposicions i exàmens: la prova segellada abans

Part VIII — Confiança per a la societat: persones, institucions, mercats i cultura

- 47. Identitat digital: la prova que existeixes
- 48. Integritat electoral: provar què va passar a les urnes
- 49. Ajuda humanitària: provar que l'ajuda arriba
- 50. L'ajuda en espècie: la cadena de custòdia del socors
- 51. Fronteres i asil: l'evidència de qui fuig
- 52. Testaments i herència: l'última voluntat, demostrable
- 53. Dret de família: la coparentalitat amb data certa
- 54. Trade finance: el mateix carregament finançat dues vegades
- 55. Auditoria: comptes i informes a prova de manipulació
- 56. Frau publicitari: l'anunci que ningú va veure
- 57. Ciberseguretat: registres que l'atacant no pot reescriure
- 58. Les teves dades filtrades: la reclamació del ciutadà
- 59. La caiguda documentada: SLA, núvol i continuïtat
- 60. Art i antiguitats: la procedència contra la falsificació i l'espoli
- 61. Memòria històrica: els arxius contra el negacionisme
- 62. Whistleblowing: provar sense delatar-se

Part IX — Confiança a les noves fronteres: ciència, cos, màquines i mercats

- 63. Integritat de la recerca: la dada que ningú pot repetir
- 64. Pensions: provar que encara hi ets, avui
- 65. Prova de vida: segrestos virtuals, desapareguts i la veu que no era
- 66. Integritat esportiva: la mostra que algú va canviar de nit
- 67. Música i espectacles: l'humà real darrere del play
- 68. Telecom i veu: autenticar qui truca de debò
- 69. El frau bancari del pagament «autoritzat»
- 70. Maquinari: el pedigrí d'un xip que no podia fallar
- 71. Programari: el pedigrí del codi que tot ho fa anar
- 72. Pesca i minerals: l'origen que es va enfonsar amb el vaixell
- 73. Filantropia: on va el meu euro
- 74. Caixes negres: la dada que el fabricant deia que no existia
- 75. La caixa negra personal: evidència preventiva per a víctimes i per a innocents
- 76. Dades genòmiques: el consentiment d'un exposa molts
- 77. Justícia penal: la prova que el tribunal ha de poder creure
- 78. Historials mèdics: qui va tocar el registre, i quan

Part X — Quan tot es pot falsificar: identitat, imatge, veu i diners

- 79. Models d'IA: amb què es van entrenar, i què executem de debò
- 80. Els agents d'IA: el mandat verificable
- 81. La teva cara, la teva veu: drets d'imatge i rèpliques digitals
- 82. Sharenting: la imatge de qui no pot consentir
- 83. Imatges íntimes no consentides: el dany, la prova i la retirada
- 84. L'odi a les xarxes: el dany, la prova i la dignitat
- 85. Gent gran: la veu clonada i l'abús invisible
- 86. Comunicacions oficials: qui certifica que el cap d'Estat ha dit això?
- 87. Suplantar el director financer: qui ha autoritzat de debò aquest pagament?
- 88. La identitat en directe: qui hi ha de debò a l'altra banda de la pantalla?
- 89. Informació que mou mercats: qui ho ha dit, i quan ho va dir
- 90. Titularitat real: qui és la persona de carn i ossos darrere de l'empresa
- 91. Identitat laboral: qui contractem de debò en remot
- 92. Treball de plataforma: quan el cap és un algorisme

- 93. La jornada i el conflicte laboral: hores que consten

Part XI — El món físic no menteix: infraestructura, producte, treball i planeta

- 94. Construcció i infraestructura: qui demostra com es va aixecar de debò
- 95. El pedigrí d'una peça: quan un certificat fals pot matar
- 96. Emissions: el sensor que mentia abans que el paper
- 97. Ciència ciutadana ambiental: els sensors de baix, amb data certa
- 98. El passaport del producte: qui jura el contingut reciclat, i quan
- 99. Residus: on va de debò el contenidor
- 100. El camp i la PAC: el quadern verificable
- 101. Frau alimentari: quan l'etiqueta menteix sobre el que t'has menjat
- 102. Qui ho va fer, i en quines condicions: la diligència deguda en la mà d'obra
- 103. Integritat marítima: on és de debò aquell vaixell, i és qui diu ser?
- 104. Observació de la Terra: el testimoni orbital que també es pot falsificar
- 105. Protecció civil i emergències: qui sabia què, i quan

Part XII — Confiança per a la democràcia: eleccions, institucions i participació

- 106. Eleccions verificables: del «dividend del mentider» a l'evidència ancorada
- 107. IA pública auditable: el registre que es pot comprovar
- 108. Participació autèntica: una persona, una veu, sense vigilància
- 109. Manifestacions: la prova simètrica al carrer

Part XIII — Actuar o no actuar

- 110. Clavar els talons: el cost de no fer res
- 111. Com hi arribem? Un full de ruta
- 112. El segell i la cadena: qui controla la prova, i qui hi queda atrapat
- 113. El setge a la veritat: el testimoni que no es pot silenciar
- 114. La dignitat de qui existeix: la «Magnifica Humanitas» i la prova d'existència

Pròleg — De 2004 a 2026: el dia que vam tocar el límit

«Però fins i tot una mirada superficial revela que, malgrat tots els seus grans èxits, la nostra economia de l'energia és fatalment defectuosa, en gairebé tots els aspectes.»

— Paul Roberts, The End of Oil (2004)

Era el gener de 2003 i el sol de l'Aràbia Saudita escaldava la sorra del «Quarter Buit» com una manta incandescent. Paul Roberts, periodista i analista d'energia, es trobava al capdamunt d'una duna immensa, observant un horitzó que només trencaven les torres de perforació, alçades com punxes d'acer enmig del desert. Allà sota hi havia Ghawar, el camp petrolier més gran que mai s'ha descobert, el cor que durant mig segle havia bombat l'energia del món. Va ser llavors que un enginyer, amb veu baixa i resignada, va deixar anar la frase que ho canviaria tot: «El *water cut* de Ghawar ja arriba al 30 %.»

Aquell número —la proporció d'aigua que puja barrejada amb el cru— era, per a Roberts, l'esquerda en un sistema que semblava etern. Per mantenir el petroli fluint, els enginyers havien d'injectar quantitats creixents d'aigua als pous; com més aigua sortia, més a prop era el final. En aquell instant, amb el sol cremant-li l'esquena, Roberts va perdre la fe en l'economia energètica moderna. Ho explicaria després al seu llibre *The End of Oil* (2004): Ghawar era la metàfora perfecta del límit que la civilització estava a punt de tocar.

Han passat més de dues dècades. Som el 2026, i el paisatge ha canviat de maneres que Roberts no podia imaginar. Però la pregunta que va formular en aquella duna —fins quan pot durar un món construït sobre un recurs finit?— continua sent el nucli de la nostra incertesa. La diferència és que avui, al límit físic dels recursos, s'hi ha sumat un altre límit, més insidiós: el de la **veritat**.

Les apostes: per què aquella duna encara importa

El que Roberts va intuir com un senyal d'esgotament és avui una cruïlla de múltiples dimensions. No hem arribat només al límit d'un jaciment; hem arribat al límit d'una manera d'entendre el progrés. I per primera vegada en la història, la urgència energètica i climàtica conflueix amb una crisi de confiança que amenaça la nostra capacitat mateixa de posar-nos d'acord sobre els fets. Aquest llibre tracta d'aquesta convergència, i de les dues eines —la intel·ligència artificial i la blockchain— que poden ajudar-nos a resoldre-la abans no sigui massa tard.

De la predicció a la realitat (2004 → 2026)

Roberts temia, sobretot, l'esgotament de l'**oferta**. Basant-se en les tendències de consum de l'època, projectava una demanda mundial de **140 milions de barrils per dia (Mb/d) cap al 2035**, una set insaciable que xocaria contra uns jaciments cada cop més buits. El malson era el «pic d'oferta»: el dia que el món voldria més petroli del que la Terra podria donar.

La realitat de 2026 ha invertit el guió. La demanda no s'ha disparat fins als 140 Mb/d, sinó que tendeix a un **altiplà d'uns 105 Mb/d cap al 2030** [1]. El temor ja no és que se'ns acabi el petroli, sinó que deixem de necessitar-lo: és el «**pic de demanda**», empès per l'adopció massiva del vehicle elèctric i per una eficiència que supera totes les expectatives del passat. El recurs finit no s'ha esgotat; ha començat a quedar obsolet.

Hi ha una segona sorpresa, encara més esperançadora. Les energies renovables, que el 2004 es consideraven marginals i cares, són ara l'opció més barata del mercat. El cost nivellat de l'electricitat solar (LCOE) ha caigut **al voltant d'un 90 % entre 2010 i 2024**, fins a uns **0,043 $/kWh**, i el **91 % de la nova capacitat renovable instal·lada el 2024 va resultar més barata que qualsevol planta fòssil nova** [2]. La «promesa» que Roberts mirava amb escepticisme s'ha complert amb escreix.

I tanmateix, el seu avís més greu també s'ha materialitzat. El **2024 va ser el primer any natural que va superar els +1,5 °C** respecte al nivell preindustrial, segons Copernicus, amb unes emissions globals de gasos d'efecte hivernacle en màxims històrics [3]. Un sol any per sobre del llindar no equival a incomplir l'Acord de París —que es mesura com una mitjana de dècades—, però és un avís inequívoc: hem tocat el sostre simbòlic.

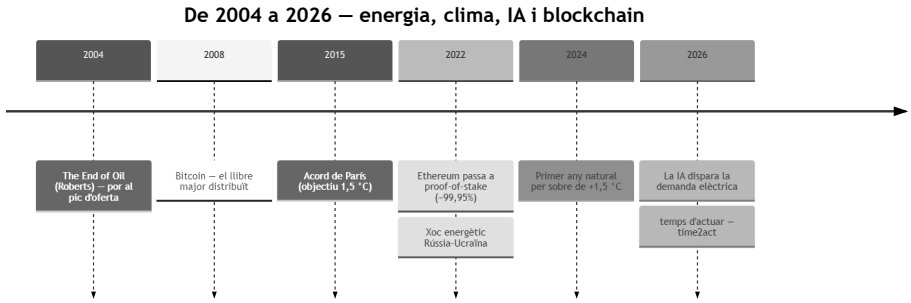


Figura 0.1 — Línia de temps 2004 → 2026: les fites d'energia, clima, IA i blockchain que emmarquen aquest llibre.

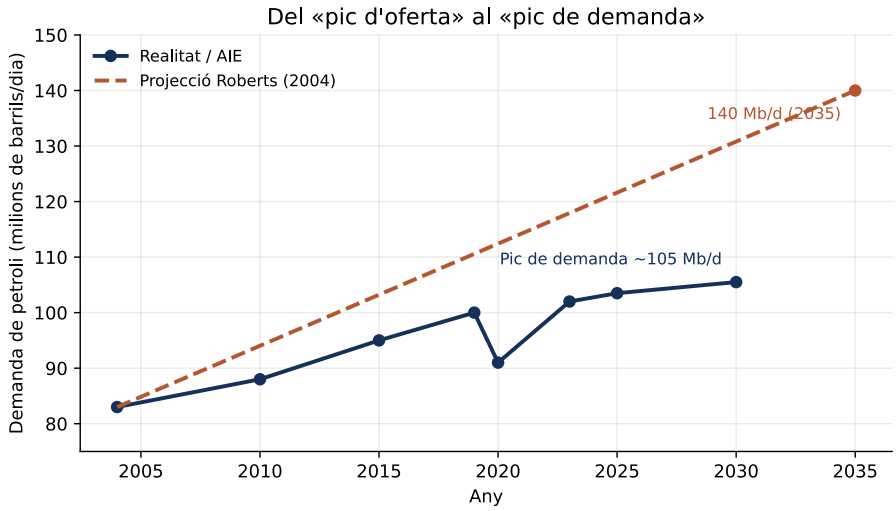


Figura 0.2 — Del «pic d'oferta» al «pic de demanda»: la projecció de Roberts (2004) davant la trajectòria observada.

La crisi que Roberts no podia veure: la veritat

Mentre el món s'enfronta a la transició energètica, una desconfiança profunda ha emergit com un factor d'inestabilitat sistèmica. Les **deepfakes**, cada cop més sofisticades, erosionen la confiança en les institucions i en els processos de governança. El frau ESG, les dades climàtiques manipulades i les notícies falses són avui una amenaça tangible: de poc serveix descarbonitzar si ningú no es pot fiar de les xifres que ho demostren. L'estàndard de procedència C2PA ja supera els sis mil membres, però certifica l'origen d'un contingut, no n'esbrina la falsedat [6]. Falta una peça: una manera fiable de demostrar que una dada existia, intacta, en un moment concret.

A aquesta crisi de veritat s'hi afegeix una **paradoxa tecnològica**. La intel·ligència artificial, que pot ser la palanca clau de la transició, és també un nou i voraç consumidor d'energia: els centres de dades del món passaran d'uns **485 TWh el 2025 a prop de 950 TWh el 2030**, gairebé el doble [4]. L'eina que ha d'ajudar-nos a estalviar energia n'exigeix, ella mateixa, quantitats colossals. La solució i el problema comparteixen endoll.

Dues palanques que Roberts no tenia: IA i blockchain

El problema de fons —energia, clima i poder— és el mateix que Roberts descrivia fa vint anys. El que ha canviat és que ara disposem de dues palanques que ell no tenia. La primera és la **intel·ligència artificial**, capaç d'optimitzar xarxes, accelerar el descobriment de materials i modelar el clima amb una precisió inèdita. La segona és la **blockchain**, i convé desactivar de seguida l'objecció més repetida: que «malgasta energia». Això era cert per a Bitcoin, però el **Merge d'Ethereum de 2022 va reduir-ne el consum elèctric en prop d'un 99,95 %** en adoptar el model de *proof-of-stake* [5]. La blockchain moderna no és un problema energètic; és una **capa de confiança**. I és, precisament, el fonament de la **prova d'existència** —la tecnologia de t2p— que pot plantar cara a les deepfakes segellant en un registre

immutable que una dada existia i no s'ha alterat. I abans d'entrar en la màquina energètica, el capítol que ve —el pòrtic— tradueix aquesta idea a un llenguatge planer que farem servir a cada front del llibre.

La promesa i el perill

La promesa és extraordinària i, sobretot, ja és real: les solucions existeixen, són més barates que mai i poden accelerar la transició alhora que restableixen la confiança. La IA i la blockchain ofereixen una doble funció —optimitzar els sistemes i garantir l'autenticitat de les dades de què depenen les decisions polítiques i econòmiques.

El perill és igual de nítid. La inacció climàtica continua tenint un cost que es mesura en dècades irrecuperables. Però hi ha un perill nou: el col·lapse del consens sobre la veritat. Sense un marc fiable d'autenticitat, els esforços de descarbonització queden a mercè de manipulacions i fraus capaços de paralitzar qualsevol política. La promesa i el perill, com sempre, viatgen junts.

És hora d'actuar

Roberts va fer el diagnòstic; el seu mèrit va ser veure l'esquerda quan tothom mirava la bonança. Avui ja no n'hi ha prou amb diagnosticar. Tenim els fets, tenim les eines i tenim, per primera vegada, la possibilitat de protegir la veritat sobre la qual hem de decidir. El que ens falta és actuar. D'aquí el títol d'aquest llibre.

El viatge que proposo arrenca amb un **pòrtic**: un capítol que tradueix a un llenguatge planer què és la blockchain i què resol la prova d'existència —la pedra de Rosetta que farem servir a cada pàgina. Després revisitarem la **màquina energètica** de Roberts i la posarem al dia: del petroli a les renovables, de la geopolítica al clima de 2026. N'examinarem les **conseqüències** d'avui —i una de nova: la crisi de la veritat. Al **cor del llibre** desplegarem les solucions que ofereixen la IA i la capa de confiança, amb la prova d'existència de t2p com a peça insígnia contra les deepfakes. Després obrirem **cinc fronts** on aquesta defensa ja es juga —diners, fotoperiodisme, sanitat, educació i drets humans— i, finalment, posarem sobre la taula el **cost de no fer res** i un full de ruta concret per a governs, empreses i ciutadans. Perquè el límit que Roberts va veure a Ghawar ja no és una advertència llunyana: és el present. I el present demana acció. És *time2act*.

---

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

[2] IRENA (via 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), *funcionament i límits de l'estàndard de procedència*. https://truescreen.io/articles/c2pa-standard-history-limitations/ ↩

El protocol de la confiança: com es prova que una cosa és certa

«No hi pot haver llibertat per a una comunitat que no té els mitjans per detectar les mentides.»

— Walter Lippmann, Liberty and the News (1920)

Un cap de setmana, a les primeres hores del matí, el feed d'una xarxa social es va omplir d'un clip on un grup d'adolescents, amb les mans al voltant d'una caixa negra, anunciaven que havien trobat «el nou recurs energètic que canviarà el món». El vídeo, de només quinze segons, mostrava una explosió de llum verda i una veu emocionada que cridava: *«Això és el futur!»* En qüestió d'hores, els mitjans digitals ho van compartir com a prova irrefutable del descobriment.

Setmanes abans, però, el mateix fragment —la mateixa caixa negra, la mateixa explosió de llum— havia circulat com a evidència d'un manifestant que denunciava una corrupció policial. En aquell context, el clip es feia servir per demostrar que una càmera de seguretat havia gravat un incident violent i, per tant, justificar una denúncia judicial. La diferència? Només el títol del vídeo i la descripció al peu de foto havien canviat.

Aquesta doble vida del mateix fitxer digital il·lustra perfectament el que **Don Tapscott** —consultor i divulgador canadenc, coautor amb Alex Tapscott de *Blockchain Revolution* (2016), l'obra que va situar la cadena de blocs molt més enllà de les criptomonedes— anomena la *doble despesa* dels actius digitals: una unitat pot ser copiada i «gastada» dues vegades, com un xec sense fons [1]. En l'àmbit de la veritat, aquest fenomen es tradueix en una **doble despesa de la confiança**. No hi ha cap senyal intrínsec que indiqui quina és la versió autèntica del clip ni quan va existir realment. L'única pista són les metadades —sovint esborrades o manipulades per qui comparteix el contingut— i la fe cega en l'intermediari que ho ha publicat.

Satoshi Nakamoto, amb la creació de Bitcoin el 2009, va demostrar que una xarxa descentralitzada podia impedir que un bitcoin fos gastat dues vegades, gràcies a la prova criptogràfica i al registre immutable [1]. La mateixa lògica pot aplicar-se a qualsevol afirmació: si es pot ancorar digitalment el moment i la integritat d'un fitxer en una cadena pública, es crea un **llibre major** que ningú no pot reescriure sense que es detecti [1]. Així, el clip de les adolescents es podria verificar com el primer cop que apareix a la xarxa, amb una empremta única i una marca de temps que ningú no pot alterar.

Però fins ara, la prova d'existència ha quedat atrapada dins de diverses tecnologies complexes que la majoria dels usuaris no entenen.

La necessitat urgent és transformar aquesta capacitat en un *protocol de confiança* accessible: un mecanisme que permeti a qualsevol persona comprovar, amb només el seu dispositiu, si una versió digital és autèntica i quan va ser creada.

> *«La blockchain és a la confiança allò que Internet va ser a la informació.» — Joichi Ito, exdirector del MIT Media Lab* [1]

I si la confiança no s'hagués de demanar a un intermediari, sinó que es pogués comprovar?

Les apostes

Vivim una era en què la confiança s'ha convertit en el recurs més escàs i car del nostre sistema global. Sense la capacitat de provar que un fet és real, es desmantellen les bases de la transició energètica —que depèn de dades ESG fiables i de mesuraments d'emissions certificats—, dels mercats financers i de la mateixa democràcia.

Els números són el crit d'alerta: el volum de deepfakes ha explotat des d'**uns 500.000 el 2023** fins a **8 milions el 2025**, amb una projecció que el **90 % del contingut en línia serà sintètic el 2026**[8]. Aquest increment exponencial no és només una curiositat tecnològica; ha generat un impacte econòmic devastador. Les pèrdues per frau basades en deepfakes van superar els **mil milions de dòlars** el 2025, i les estimacions de Deloitte preveuen **uns 40.000 milions anuals** a partir del 2027[7].

Els reguladors ja han començat a respondre. L'**EU AI Act** imposa, a partir d'agost de 2026, l'obligació d'etiquetar i divulgar tot contingut generat o manipulat per IA[4]. Paral·lelament, la implementació d'**eIDAS 2.0**, que exigirà una cartera d'identitat digital europea abans del desembre de 2026, pretén crear un marc d'autenticació oficial per a persones i dispositius[5]. Però l'etiqueta sola no basta: sense una prova immutable que certifiqui l'origen i la data d'un fitxer, les etiquetes es poden falsificar tan fàcilment com el contingut que pretenen validar.

És aquí on entra el concepte de **«full de càlcul global»** o **World Wide Ledger**, proposat per Tapscott ja el 2016[1]. Aquest registre distribuït funciona com un llibre major universal, accessible a qualsevol ordinador, i garanteix que cada transacció o document quedi gravat de manera immutable. La immutabilitat és clau: per alterar la cadena caldria **reescriure tota la història a plena llum del dia**, una tasca pràcticament impossible segons Tapscott[1].

Aquesta arquitectura permet fabricar confiança mitjançant codi astut, allò que Tapscott anomena el **«Trust Protocol»**[1]. No es tracta d'un simple mecanisme tècnic; és la base per a una nova economia de la veritat on qualsevol persona pot verificar l'autenticitat i la data d'una peça digital només amb el seu dispositiu. Així, la confiança deixa de dipositar-se en intermediaris centralitzats —bancs, notaris o mitjans — i passa a ser un recurs verificable per tothom.

Per tant, si no podem garantir la certesa dels fets digitals, el futur energètic, financer i democràtic es veu amenaçat. La solució consisteix en una infraestructura global de registre immutable que proporcioni la prova d'existència necessària per a qualsevol transacció o informació crítica — la pedra angular del **protocol de confiança** que sustenta tot el llibre *time2act*.

Com es fabrica la confiança amb codi

Imaginem un llibre de comptes sense una única còpia guardada en una caixa forta, sinó milers d'exemplars simultanis distribuïts a cada ordinador connectat a la xarxa. Cada cop que algú vol afegir una nova anotació, tots els exemplars s'actualitzen al mateix temps, com si fos un document col·laboratiu editat en temps real. William Mougayar, inversor i autor de *The Business Blockchain*, descriu aquesta dinàmica amb una metàfora senzilla: **un fitxer que dos usuaris poden editar simultàniament**, sense haver d'esperar el torn per correu electrònic o per un gestor centralitzat [2]. En aquest escenari, modificar alguna pàgina del llibre requereix reescriure **tota** la història en cada còpia alhora, i ho ha de fer a plena llum del dia. La impossibilitat pràctica d'aquest procés es resumeix en les paraules de Don Tapscott: «hauries de reescriure tota la història a plena llum del dia; és pràcticament impossible» [1]. Aquesta **immutabilitat** converteix el registre distribuït en un llibre major que ningú no pot manipular, i que qualsevol pot descarregar i verificar al seu propi equip.

Com podem saber que una entrada concreta no ha estat alterada? La resposta resideix en la idea d'una **empremta única**, una fotografia digital del contingut que canvia completament encara que només un byte es modifiqui. L'empremta funciona com una clau de seguretat: si el contingut varia, l'empremta també ho fa, revelant instantàniament qualsevol intent de manipulació sense necessitat d'exposar la informació subjacent. És, en essència, una prova criptogràfica que el document ha quedat intacte i no s'ha tocat, tot mantenint la privacitat del seu contingut.

Un obstacle històric al desplegament massiu de tecnologies basades en registres distribuïts era el cost energètic. Fins fa poc, la majoria de les cadenes de blocs operaven amb **proof-of-work**, un mecanisme que consumia grans quantitats d'electricitat per validar transaccions. El 2022, l'Ethereum va dur a terme el famós *Merge*, passant de proof-of-work a **proof-of-stake** i reduint el seu consum energètic aproximadament un 99,95 % [3]. Aquesta transformació no només respon a les crítiques ambientals, sinó que elimina una de les objeccions més contundents: la idea que les solucions basades en blockchain són intrínsecament insostenibles. En aquest nou paradigma, Tapscott va destil·lar **set principis de disseny** —integritat en xarxa, poder distribuït, valor com a incentiu, seguretat, privacitat, drets preservats i inclusió— que serveixen de guia per a qualsevol implementació responsable [1]. Asseguren que la confiança no es delegui en cap entitat central, sinó que emergeixi de les regles codificades al protocol mateix.

Finalment, el nucli d'aquesta revolució és el **Trust Protocol**, un conjunt de regles que permet a qualsevol persona «fabricar confiança mitjançant codi astut» [1]. No cal més que seguir el protocol per crear una capa verificable i immutable sobre qualsevol dada digital. Així, la confiança deixa de ser una qüestió d'autoritat externa i es converteix en un producte matemàtic, accessible a tots i resistent als atacs. Aquest

és el fonament del **protocol de la confiança** que sostindrà les solucions que explorarem al llarg de *time2act*.

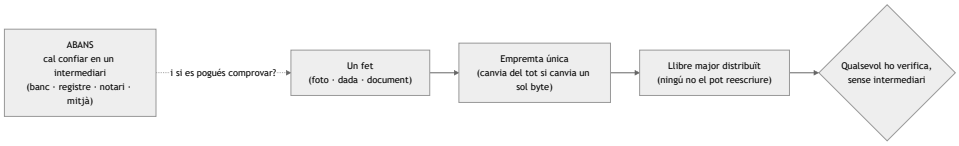


Figura 1.1 — De la confiança centralitzada a la distribuïda: el viatge d'un fet, de la captura a la verificació que qualsevol pot refer.

De la idea a la butxaca: t2p

Imaginem una reunió de treball on algú ha de demostrar que una fotografia presa fa cinc dies mostra el producte exactament com era en aquell moment. En el model tradicional caldria un notari, un arxiu físic o una empresa especialitzada per emmagatzemar i certificar la imatge. Amb **t2p**, tot es redueix a obrir l'aplicació del telèfon i prémer el botó de captura; en segons el dispositiu genera una empremta digital única —una petita cadena de bits que resumeix tot el contingut sense revelar-lo— i la fixa instantàniament en una **cadena pública** on queda registrada per sempre. El resultat és un certificat QR escanejable per qualsevol, des d'un client fins a una autoritat reguladora, i verifica, fora de tot dubte, que aquella foto existia, intacta i inalterada, en el moment indicat.

Aquesta operació es recolza en el **Trust Protocol** descrit per Tapscott com un «codi astut» capaç de **fabricar confiança mitjançant matemàtiques**, no a través d'una autoritat central [1]. La clau és la immutabilitat de la cadena pública: modificar-la exigiria reescriure tota la història, una tasca que Tapscott qualifica de «pràcticament impossible» [1]; per tant, la comprovació no es demana a ningú: es fa directament, amb les eines de qualsevol dispositiu connectat.

El flux és tan lineal que fins i tot un usuari sense coneixements tècnics el pot seguir: captura → càlcul d'empremta → ancoratge a la cadena pública → generació del certificat QR. Cada pas es duu a terme dins del telèfon, de manera que **el fitxer original mai no surt del dispositiu**, preservant la privacitat i evitant fugides de dades [9]. Aquesta separació entre contingut i prova resulta clau en un context on regulacions com l'**EU AI Act** obliguen a marcar i divulgar el contingut generat per IA, ja que ofereix una capa d'autenticitat independent de qualsevol etiqueta o metadada manipulable [4].

Com hem vist amb eIDAS 2.0 (previst per al desembre del 2026) i els estàndards C2PA / Content Credentials adoptats el 2026, les carteres digitals europees podran integrar aquests certificats, reforçant la confiança en entorns cada cop més virtuals [5][6].

Així, **t2p** converteix el telèfon —l'eina més omnipresent del nostre dia a dia— en un «estudi de proves portàtil». No cal cap laboratori costós ni infraestructura complexa; només una connexió a la cadena pública i l'aplicació que gestiona l'empremta. El **protocol de la confiança** es materialitza: la confiança no s'ha de demanar, sinó poder comprovar-la en qualsevol moment i lloc, amb la seguretat que ofereix la criptografia distribuïda. Aquesta porta oberta és la base sobre la qual construirem les solucions més avançades al llarg de *time2act*: la prova que el futur de la confiança ja és a l'abast del nostre polze.

La promesa i el perill

Imagina una xarxa on qualsevol pot demostrar que un document, una imatge o un esdeveniment va existir en un moment determinat, sense recórrer a cap notari, banc o autoritat central. Aquesta és la **promesa** del protocol de confiança: una verificació barata, instantània i escalable que transforma la confiança d'un concepte abstracte en una prova criptogràfica immutable. Com va escriure Joichi Ito, «la blockchain és a la confiança allò que Internet va ser a la informació»[1]: aquesta tecnologia converteix el simple acte de signar en una operació tan transparent com consultar un motor de cerca. La capacitat d'ancorar una empremta única en una cadena pública —un llibre major que ningú no pot reescriure i que qualsevol pot verificar— elimina la necessitat de confiar cegament en intermediaris tradicionals, tal com proposa el **Trust Protocol**: «fabricar confiança mitjançant codi astut»[1].

Aquesta nova forma de confiança té un cost operatiu gairebé nul comparat amb les infraestructures legals i financeres que hem mantingut durant segles. No cal pagar honoraris notarials ni esperar dies per a la confirmació d'una transacció; el procés es completa en segons, i la prova queda permanentment

disponible al registre distribuït, un «full de càlcul global» que tothom pot baixar i executar al seu ordinador[1]. A més, la immutabilitat de la cadena —alterar-la exigiria reescriure tota la història a plena llum del dia— fa pràcticament impossible qualsevol manipulació posterior[1].

Tanmateix, aquesta promesa ve acompanyada d'unes **amenaces** que cal entendre i mitigar. En primer lloc, el fenomen de les «escombraries immutables» ens recorda que una cadena no valida la veritat del contingut que s'hi ancora; només garanteix que aquest contingut no canvia un cop registrat[1]. Si es grava una mentida, quedarà immortalitzada com a certesa criptogràfica. La confiança en la tecnologia pot, per tant, convertir falsedats en «fets verificables».

En segon lloc, la vinculació de proves amb metadades pot erosionar la privacitat i desanonimitzar usuaris vulnerables. Els estudis sobre **C2PA / Content Credentials** mostren que ja el 2026 els telèfons mòbils i càmeres professionals signen automàticament contingut, però molts intermediaris encara esborren les metadades en recompartir-lo[6]. Aquesta pràctica pot exposar periodistes o activistes a la identificació forense, comprometent la seguretat de qui depèn del protocol per protegir la seva identitat.

Finalment, el **tecnosolucionisme** —la creença que una sola eina resol tots els problemes de confiança— representa un perill conceptual. El protocol de confiança és necessari però no suficient; sense marcs reguladors com l'EU AI Act, que obliga a marcar i divulgar el contingut generat per IA[4], o eIDAS 2.0, previst per al desembre del 2026[5], la tecnologia podria ser mal utilitzada o quedar limitada en el seu impacte real. Reconèixer aquestes limitacions és fonamental perquè el lector no les percebi com a propaganda, sinó com una guia crítica que combina **confiança verificable** amb una anàlisi rigorosa dels riscos inherents.

El mapa del que resol

Amb aquesta base de **confiança verificable**, la blockchain esdevé el llibre major que ningú no pot reescriure i ofereix una nova manera de llegir la realitat: la prova d'existència. No és només un truc tècnic; és la clau per desxifrar les preguntes de confiança que travessen tots els àmbits on es decideix el nostre futur, perquè l'**empremta ancorada en una cadena pública** dona una resposta inequívoca.

En energia i clima, les dades d'emissions són el termòmetre de la nostra responsabilitat planetària. La qüestió és: *aquesta dada d'emissions és real i no s'ha alterat?* Si es pot demostrar que cada número queda immutablement registrat, governs i empreses disposen d'una base sòlida per a polítiques climàtiques veritables i mesurables.

En desinformació i deepfakes, el risc és evident: imatges i vídeos poden ser manipulats amb facilitat. La prova d'existència permet preguntar: *aquesta imatge va existir així, i quan?* Això contraresta la proliferació massiva de contingut sintètic —com hem vist, el volum ha crescut exponencialment— i respon a les exigències de l'EU AI Act, que obliga a marcar el contingut generat per IA a partir d'agost del 2026[4].

En diners i compliance, la doble despesa continua sent una amenaça per al sistema financer. La qüestió és: *aquest registre o aquesta identitat no s'han fabricat?* Un certificat immutable assegura que les transaccions són autèntiques, evitant fraus i reforçant la confiança en els mercats.

El fotoperiodisme depèn de l'autenticitat visual per narrar la veritat. La pregunta aquí és: *aquesta foto és d'on i de quan diu que és?* Amb unes metadades signades per C2PA, ja incorporades en mòbils com el Samsung S25 i el Pixel 10[6], es pot verificar l'origen i la data sense dependre de tercers.

En sanitat, els resultats clínics són vitals. La prova d'existència respon a: *aquesta imatge clínica o aquesta dada d'assaig és íntegra?* Això protegeix pacients i investigadors contra manipulacions que podrien comprometre diagnòstics i tractaments.

En educació, la credibilitat dels títols i les autoritats acadèmiques es posa a prova. La pregunta clau és: *aquest títol o aquesta autoria són autèntics i verificables?* Un registre immutable garanteix que els certificats no siguin falsificats, reforçant el valor del coneixement.

Finalment, en defensa i drets humans, la veritat documental pot ser l'última defensa contra l'impunitat. La qüestió és: *aquesta ordre o aquesta evidència d'una atrocitat és autèntica?* Un registre immutable ofereix una prova ferma que no pot ser esborrada, essencial per a tribunals i organitzacions de drets humans.

En tots aquests dominis, la signatura digital C2PA i l'ancoratge en una cadena pública treballen conjuntament per crear un ecosistema on la confiança no depèn d'autoritats centralitzades sinó de matemàtiques verificables[1]. Així, el mapa dibuixat aquí connecta cada pregunta de confiança amb la

solució universal del **t2p**, establint les bases per al proper capítol: tornar a l'origen del problema modern —la màquina energètica— i llegir-la amb una nova llengua. És hora d'actuar; el futur es construeix amb proves, no amb supòsits.

---

[1] Tapscott, Don i 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* (Reglament (UE) 2024/1689). https://artificialintelligenceact.eu/article/50/ ↩

[5] Comissió 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* (projecció de frau per 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 d'usuari (Solució d'Integritat de Dades)*, v1.0, 2026. ↩

Encendre el foc, revisitat

«[El foc,] que s'ha mostrat mestre de totes les arts per als mortals, i un gran recurs.»

— Èsquil, Prometeu encadenat (s. V aC)

A la penombra d'un apartament de Barcelona, la Marta es gira cap a l'interruptor que controla el petit llum del passadís. Un cop de dit, un clic, i la bombeta s'il·lumina amb una calidesa familiar; en aquell mateix instant, una cadena invisible de recursos es desperta. Des dels pous profunds de l'Azerbaidjan fins als oleoductes submergits que serpentegen pel fons del mar Negre, el senyal elèctric viatja per transformadors que responen amb un brunzit, i cada pas de la llum es converteix en una vibració que recorre centenars de milers de quilòmetres d'infraestructura: vaixells carregats de petroli que travessen l'oceà Atlàntic, centrals termoelèctriques que bufen vapor al cel de Texas, i línies de transmissió d'alta tensió, corbades com serps d'argent sobre les muntanyes suïsses.

La Marta engega el seu cotxe elèctric a la porta del bloc. Un murmuri suau de motors silenciosos acompanya l'acceleració; però dins del vehicle, la bateria s'alimenta d'una xarxa que encara depèn majoritàriament del carboni: el 2024, el 86,7 % del consum mundial d'energia provenia de fonts fòssils, mentre les renovables, que ja lideren el creixement, encara eren només una fracció del total [1]. Cada quilòmetre recorregut per la Marta és una petita revolució d'una màquina planetària que, tot i fragmentar-se cada cop més, continua girant al voltant d'aquests recursos ocults.

A l'altra banda del món, al desert de l'Aràbia Saudita, els treballadors del camp de Ghawar encenen les torxes per a una inspecció nocturna. El foc balla sobre el metall fred i recorda que l'energia que alimenta les llums de Barcelona és la mateixa que manté les economies globals en moviment: una demanda mundial que s'acosta al pic de 105 milions de barrils per dia previst cap al 2030, i que pressiona encara més els jaciments i les infraestructures existents [2].

Mentre el llum de la Marta il·lumina la cuina, observadors invisibles —des dels gestors de xarxes fins als reguladors internacionals— monitoritzen l'equilibri precari entre oferta i demanda. Cada clic de l'interruptor, cada gir de clau, es converteix en un microesdeveniment que alimenta la gran orquestra de l'energia global: una dansa de corrents que travessen el planeta sense que ningú la vegi, però que determina la manera com creixen les ciutats, com operen els negocis i com es posicionen les nacions a l'escenari geopolític.

Aquesta invisibilitat és alhora la força i la vulnerabilitat de la nostra era. La màquina energètica continua sent aclaparadorament fòssil, però per primera vegada el centre de gravetat comença a desplaçar-se cap a fonts més netes i descentralitzades. Cada acció quotidiana —encendre una bombeta, posar en marxa un vehicle— és ara una oportunitat per observar la gran infraestructura que ens sustenta i, al mateix temps, per qüestionar-la. Aquí rau el potencial de canvi: reconèixer la magnitud del sistema per poder impulsar les tecnologies emergents que l'han de transformar. Però abans de voler girar la màquina, cal entendre com es va construir i per què costa tant de moure.

Sis mil anys encenent focs

Des de les primeres brases que els nostres avantpassats van domesticar a les valls del Nil i del Tigre, l'energia ha estat la força invisible que ha impulsat cada pas de la nostra evolució. En aquell moment prehistòric, una simple pedra tallada es convertia en una eina per caçar; un tronc encès era la primera llum que trencava la foscor nocturna i la primera font d'escalfor rudimentària d'una comunitat nòmada. Aquelles flames, modestes però decisives, van permetre als grups humans cuinar aliments, allargar les hores de treball i, més important encara, crear un espai social on es transmetien històries i coneixements.

Amb el pas dels segles, la força animal va ser el primer motor: bous i muls van arrossegar carros i van fer girar molins, i van convertir la força dels músculs en treball continuat. La llenya, recollida de boscos que ara són records d'un paisatge preindustrial, va esdevenir la font primària per encendre forns i calderes. Aquest model de dependència directa dels recursos locals va durar mil·lennis, però ja al segle XVIII una nova revolució s'alçava a l'horitzó: el carbó.

El descobriment i l'explotació massiva del carbó ho van capgirar tot. Les mines del País de Gal·les, de Pennsilvània i de Silèsia van alimentar les primeres fàbriques de filatge i les locomotores de vapor que van connectar ciutats i continents. El carbó es va convertir en la columna vertebral d'una economia industrial emergent i va reduir dràsticament el temps necessari per transformar matèries primeres en productes

acabats. En aquest període, la màquina energètica es va fer cada cop més visible: les xemeneies altes que dominaven els horitzons urbans eren testimonis fumejants d'una nova era.

El segle XX va portar una altra gran transició: el petroli i el gas natural van substituir progressivament el carbó com a fonts preferides. L'explotació de camps petrolífers a Texas, al golf Pèrsic i a la costa de Noruega va crear una xarxa global d'infraestructures que alimentava automòbils, avions i centrals elèctriques. El gas natural, més net i flexible, es va integrar en sistemes de calefacció i generació distribuïda. Aquest canvi no només va augmentar l'eficiència energètica, sinó que també va consolidar una dependència global que un segle després encara no hem desfet: la mateixa que la Marta desperta cada nit amb un clic.

Aquesta dominació fosca ha generat una demanda sense precedents, que ara s'acosta al sostre que hem entrevist a Ghawar. Però la història ens mostra que cada revolució energètica ha comportat una reconfiguració del poder i de les oportunitats; i ara n'hi ha una altra en marxa. El relat d'avui, com el que Paul Roberts —periodista i analista d'energia, autor de *The End of Oil* (2004)— situava als orígens del foc fa mil·lennis, és una crida a observar com les flames que encenem —tant físiques com digitals— podrien ser la clau per transformar aquesta màquina invisible en una força transparent i sostenible.

La màquina, avui

El 2026, la «màquina energètica» continua sent una estructura massiva i gairebé inamovible, dominada per una tríada de combustibles fòssils que actua com el nucli d'una estrella. El petroli aporta un 33,6 % de l'energia total consumida; el gas natural, un 25,2 %; i el carbó —encara que ha perdut pes en les darreres dècades— representa aproximadament un 28 %. Aquestes tres fonts sumen aquell 86,7 % del mix energètic mundial, una xifra que, segons el Global Energy Review de l'AIE, es manté pràcticament estable malgrat les polítiques climàtiques i les inversions en renovables [1].

Aquesta proporció no és només una xifra: reflecteix la magnitud i la inèrcia d'un sistema construït durant més de dos segles. Les infraestructures associades —refineries, xarxes de gasoductes, centrals tèrmiques i mines de carbó— són actius físics que costen dècades de desmantellar o reconvertir, i que consumeixen recursos financers i polítics a una escala tal que qualsevol intent de substituir-los ha d'afrontar una resistència estructural comparable a la fricció d'un engranatge antic en moviment.

Aquesta inèrcia es veu reforçada per la interdependència global del mercat energètic. Un augment inesperat del preu del petroli —com el del primer trimestre de 2024, quan els conflictes geopolítics van impulsar les cotitzacions a màxims històrics— desencadena una reacció que afecta des dels costos de transport fins a la producció industrial. De manera semblant, una interrupció del subministrament de gas natural —com la reducció d'exportacions russes— pot provocar apagades temporals i augmentar la pressió sobre les centrals de carbó, que es converteixen en la vàlvula de seguretat que cobreix els buits.

Tot i això, alguna cosa es mou. Les fonts netes representen el 38 % del creixement total del consum energètic entre 2020 i 2024, i empenyen una diversificació que, encara modesta a escala global, ja està canviant la configuració de les xarxes locals i regionals. La descentralització —amb microxarxes solars i instal·lacions eòliques comunitàries— comença a crear punts d'inflexió on el centre de gravetat energètic es desplaça lentament cap a una arquitectura més distribuïda.

No obstant això, la força del canvi encara topa amb l'enorme massa de la màquina fòssil. La inèrcia no només és física; és també institucional i cultural. Les empreses energètiques tradicionals, que controlen una part determinant dels actius del sector, mantenen una influència decisiva sobre les polítiques reguladores i els estàndards de mercat. Aquest poder consolidat es tradueix en barreres d'entrada per als nous actors basats en blockchain o IA, que ofereixen solucions de transparència i verificació però encara lluiten per guanyar-se la confiança d'un ecosistema dominat per grans conglomerats.

El panorama energètic del 2026 és, doncs, una combinació paradoxal: una màquina massiva i predominantment fòssil que es troba a les portes d'una transformació lenta però inevitable. La seva inèrcia colossal implica que qualsevol avanç cap a fonts netes ha de ser no només tecnològic sinó també institucional, i requereix una reconfiguració profunda dels incentius i de la governança global de l'energia. Aquest és el punt de partida sobre el qual es construeix la narrativa d'«encendre el foc» revisitat: les flames que ara s'alcen no són només les del petroli o del carbó, sinó també les de dades verificades, contractes intel·ligents i xarxes descentralitzades que podrien redefinir el funcionament interior de la nostra màquina energètica.

L'inici del gir

A la primavera de 2024, un grup d'analistes de Bloomberg Energy va observar un senyal que fins llavors havia passat desapercebut entre les xifres massives del consum global: **les energies renovables representaven el 38 % del creixement total del subministrament energètic**. No es tractava només d'un increment marginal; era la força motriu que impulsava l'expansió de la nostra màquina energètica, encara dominada pels combustibles fòssils però cada vegada més dependent d'una nova font de potència [1]. Aquesta dinàmica ha canviat el paradigma de la seguretat energètica: fins fa poc, la preocupació central era l'esgotament de les reserves, allò que Roberts descrivia com «l'últim petroli fàcil»; ara la incertesa gira cap al **pic de demanda**, el sostre que les projeccions situen al voltant del 2030 [2].

Aquest desplaçament de les apostes té repercussions profundes. En primer lloc, que les renovables empenyin més d'un terç del creixement indica que els inversors i les polítiques públiques ja estan canalitzant capital cap a tecnologies com l'eòlica marina, la fotovoltaica d'alta eficiència i l'emmagatzematge avançat. Segons l'informe de l'Agència Internacional de l'Energia (AIE), la capacitat eòlica i solar instal·lada va batre rècords i va activar una cadena de subministrament que va des del ferro per a les torres fins als sistemes de control basats en IA. Aquest augment no només diversifica la cartera energètica: també comporta una **reducció de la dependència** del petroli i del gas natural, tot i que el carbó encara manté una presència significativa.

En segon lloc, l'arribada del pic de demanda canvia les regles del joc de la governança global. La pressió ja no recau exclusivament en la necessitat d'extreure més recursos; ara es tracta d'optimitzar el consum i de garantir que les infraestructures puguin suportar una demanda que supera els límits històrics. Les xarxes intel·ligents, alimentades per contractes intel·ligents basats en blockchain, permeten **equilibrar l'oferta i la demanda en temps real**, amb menys pèrdues i més capacitat de resposta davant d'imprevistos com les tempestes que interrompen la producció eòlica. Així, el perill tradicional —el col·lapse del subministrament— es transforma en un nou risc: **la vulnerabilitat cibernètica** d'un sistema cada vegada més digitalitzat.

Aquesta transició no és només tècnica; és cultural i econòmica. Les empreses que abans basaven els seus models de negoci en l'extracció de recursos fòssils es veuen obligades a reinventar-se: adopten plataformes descentralitzades per a la gestió d'actius energètics, aprofiten l'analítica predictiva per anticipar les fluctuacions del mercat i reorienten una part creixent de la seva inversió cap a l'eòlica marina i la solar.

El **gir estructural** que Roberts no va poder preveure es manifesta, doncs, en tres dimensions clau: un creixement impulsat per les renovables que alimenta la màquina energètica, una demanda que s'acosta a nous pics històrics i una infraestructura digital que canvia la manera com gestionem l'energia. Aquestes forces convergents obren una era en què el foc que encenem ja no depèn exclusivament del petroli ni del carbó. Què prometen, aquestes flames noves, i què arrisquem en encendre-les?

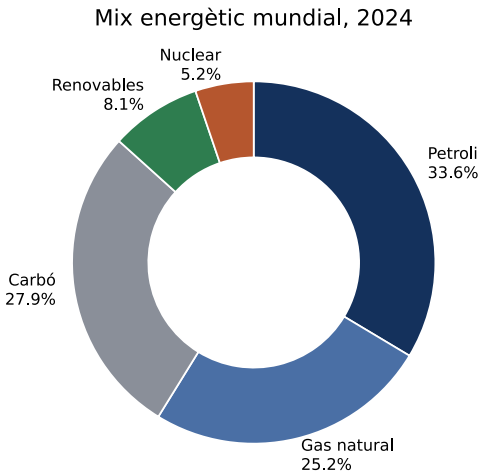


Figura 2.1 — El món encara funciona amb combustibles fòssils (~86,7 % del subministrament primari el 2024), però les renovables ja lideren el creixement.

La promesa i el perill

Per primera vegada en la història de la civilització, una alternativa a l'energia fòssil no només és tecnològicament viable sinó també econòmicament dominant. Les renovables encapçalen el creixement energètic mundial i comencen a rosegar la quota fòssil, aquella proporció encara aclaparadora però ja en declivi constant. Aquesta inversió de tendència s'acompanya d'una nova economia digital: xarxes de sensors, plataformes blockchain i algoritmes d'intel·ligència artificial que permeten monitoritzar, optimitzar i facturar l'energia amb una precisió abans impensable. I el cost marginal de generar energia solar o eòlica ha caigut fins al punt que, en molts mercats, ja resulta més barata que la de qualsevol planta fòssil nova. L'oferta renovable no només és més neta; és més barata que el model tradicional.

Aquesta combinació de costos reduïts i escalabilitat digital crea una promesa clara: la «maquinària energètica» del futur pot operar amb una base d'alimentació principalment neta, sostinguda per dades verificades i contractes intel·ligents que eliminen gran part de les ineficiències associades a les cadenes de subministrament fòssils. L'impacte potencial és doble. Primer, la reducció del preu de l'energia impulsa el creixement econòmic i facilita la transició cap a sectors d'alt valor afegit com la manufactura avançada o els serveis digitals. Segon, una infraestructura energètica més transparent i descentralitzada reforça la confiança dels consumidors i dels inversors, i contraresta l'era de les «deepfakes», que ha erosionat la credibilitat en molts àmbits.

Tanmateix, el perill rau en la inèrcia del sistema actual. Les instal·lacions fòssils —centrals de carbó, refineries i gasoductes— representen inversions de bilions d'euros i una vida útil que s'estén durant dècades. Aquest capital fòssil no desapareixerà de cop: la seva amortització, les obligacions contractuals i els interessos polítics que protegeixen aquestes infraestructures creen una fricció estructural que retardarà qualsevol canvi substancial. A més, la percepció equivocada que la simple encesa d'un nou «foc digital» equival a una solució completa pot conduir a una complacència prematura. Els primers èxits de les renovables i de la blockchain se celebren sovint com a victòries definitives, però en realitat només marquen el començament d'una transició complexa i de llarg recorregut.

El risc més gran, per tant, és confondre l'inici del gir amb la feina feta. Les polítiques que prometen eliminar els combustibles fòssils en un horitzó curt, sense abordar les barreres d'inversió ni la necessitat de reconvertir el capital existent, poden crear una falsa sensació de seguretat mentre la realitat continua dominada per estructures de poder fòssil. Per evitar aquest escenari, cal dissenyar marcs reguladors que integrin els costos de desmantellament del patrimoni fòssil i que incentivin alhora les inversions en tecnologies digitals i renovables. Només així la promesa d'una energia més neta i assequible es transformarà en una nova base estable per a la nostra màquina energètica global.

El mapa del viatge

Després d'haver-nos endinsat en les arrels de la màquina energètica —aquella que ha alimentat civilitzacions des del primer foc fins a l'era del petroli—, és moment de traçar el mapa del proper viatge. La Part II de *time2act* es desplega com una ruta amb parades pensades per revelar com la dependència fòssil encara domina i com, alhora, el centre de gravetat ja comença a moure's cap a noves fonts i tecnologies.

Al capítol 3 ens submergirem en l'oferta de petroli. No només revisarem les reserves que encara alimenten les economies més poderoses, sinó que desglossarem les cadenes de valor que mantenen viva la infraestructura fòssil: refineries, oleoductes i mercats de futurs que, com una xarxa nerviosa, regulen el flux de capital i d'energia. Hi posarem a prova aquell 33,6 % del consum mundial que encara és petroli, i explorarem escenaris en què la seva reducció s'acceleri amb polítiques de desmantellament que integrin els costos reals de la transició.

El capítol 4 girarà el focus cap a les renovables i el vehicle elèctric. Les fonts d'energia neta, amb aquell 38 % del creixement a l'esquena, són el motor emergent que pot reconfigurar la nostra màquina: analitzarem com l'explosió de la capacitat solar i eòlica, juntament amb les xarxes intel·ligents basades en blockchain, permet una gestió descentralitzada i transparent del flux energètic. I el vehicle elèctric —com el de la Marta— es presenta no només com a substitut del motor de combustió interna, sinó com a node mòbil que potencia la integració d'energia distribuïda i crea un ecosistema en què cada cotxe és també una bateria col·lectiva.

Al capítol 5 abordarem la geopolítica del poder energètic. La distribució desigual dels recursos fòssils ha modelat fronteres i aliances durant dècades; ara, l'emergència d'una matriu més diversificada obliga a redibuixar-les. Examinarem com països tradicionalment dominants en el petroli han començat a invertir massivament en renovables per mantenir la seva influència, i com noves potències energètiques digitals —

amb IA que optimitza xarxes i blockchain que assegura transaccions— es converteixen en actors clau de l'escenari global.

Finalment, el capítol 6 ens portarà al clima. Aquell pic de demanda que corre cap al 2030 és també una pressió que amplifica els riscos climàtics i les incerteses socials [2]. Analitzarem com la combinació d'IA per predir patrons meteorològics i blockchain per rastrejar emissions pot transformar la resposta global a la crisi climàtica, i convertir la promesa d'una energia neta en una base estable i verificable.

I, tanmateix, el mapa no es tanca quan es refreda l'últim motor de combustió. Si aquestes primeres parades ens ensenyen com es mou l'energia, la resta del viatge persegueix una cosa més esquiva: la confiança mateixa. Perquè en un món on una imatge, una veu o un document es poden fabricar en segons, l'energia és tot just el primer sistema que aprenem a fer verificable. A partir d'aquí, *time2act* deixa enrere els oleoductes per seguir el rastre de la prova —la prova d'existència— per cada terreny on avui es juga la credibilitat. Convé, doncs, guanyar altura i mirar el mapa sencer des de dalt.

Les Parts III i IV tanquen l'arc que hem obert amb l'energia. La III baixa a les conseqüències que ja vivim —el consum que no cedeix, les grans energètiques inquietes i aquesta nova tensió en què la intel·ligència artificial és alhora promesa d'eficiència i set voraç d'electricitat— fins a desembocar en la crisi de la veritat: la desinformació i les deepfakes que corroeixen allò en què podem creure. La IV respon amb les eines: xarxes intel·ligents governades per IA, la blockchain com a capa neutral de confiança i t2p, la prova d'existència que planta cara a la falsificació, sense oblidar les apostes —hidrogen, captura de carboni— que encara han de madurar.

A la Part V, el llibre desplega cinc fronts contra les deepfakes: allà on detectar ja no n'hi ha prou, la prova d'existència es revela com a defensa duradora —en els diners i el frau, en el fotoperiodisme, en la imatge mèdica, en les credencials acadèmiques i en el terreny més cru de la defensa i els drets humans.

Després s'obre el gran atles de la confiança aplicada. La Part VI la posa al servei del clima —crèdits de carboni, certificats d'estalvi, autoconsum i mobilitat verificable—; la Part VII la porta a l'economia real, de l'assegurança i la cadena de subministrament a l'habitatge, les patents i la contractació pública; la Part VIII l'estén a la societat sencera —identitat, eleccions, ajuda humanitària, herències, auditoria, memòria històrica—; i la Part IX s'endinsa en les noves fronteres, on la ciència, el cos, les màquines i els mercats reclamen la mateixa certesa, des de la prova de vida fins al pedigrí del xip i del codi que ho sostenen tot.

Les Parts X i XI afronten el caire més afilat del present. Primer, quan tot es pot falsificar —la teva cara, la teva veu, els teus diners, la identitat de qui et truca o de qui treballa a l'altra banda d'una pantalla—; després, la tossuda honestedat del món físic, on una obra, una peça, un sensor o un vaixell han de poder demostrar com, on i en quines condicions van existir de debò.

I el viatge culmina en allò col·lectiu. La Part XII eleva la confiança a l'escala de la democràcia —eleccions verificables, IA pública auditable, participació autèntica sense vigilància—, i la Part XIII ens deixa davant l'única pregunta que de debò importa: actuar o no actuar. Allà es mesura el cost de la inacció, es traça el full de ruta, es pregunta qui controla el segell i qui podria quedar atrapat per ell, i es tanca, com ha de ser, amb la dignitat de qui existeix.

Aquesta travessia no és merament descriptiva; és una crida a l'acció. La màquina energètica està viva, i per fi comença a mutar. Cada capítol ofereix principis de disseny i fulls de ruta que permeten als lectors —ja siguin responsables polítics, executius d'empresa o ciutadans conscients— participar activament en aquest canvi estructural. El futur no és una utopia distant: és un projecte concret que requereix decisions informades avui mateix. Aquesta nit, quan la Marta torni a prémer l'interruptor del passadís, la cadena invisible es despertarà una altra vegada, dels pous de l'Azerbaidjan fins al clic de la bombeta; la diferència és que ara sabem què encenem. És hora d'encendre el foc, revisitat i dirigit cap a un horitzó on la confiança i la sostenibilitat converteixin la nostra màquina energètica en una força per al bé comú.

---

[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 ↩

L'últim petroli fàcil... i per què ja importa menys

«L'edat de pedra no es va acabar per manca de pedra, i l'era del petroli s'acabarà molt abans que al món se li acabi el petroli.»

— Ahmed Zaki Yamani, citat a The Economist (2003)

Març de 2022. A primera hora del matí, Brussel·les es va omplir d'una tensió com feia anys que no es recordava: el preu del petroli tornava a sonar com una alarma. En horari de Londres, el Brent havia trencat la barrera simbòlica dels **130 $ per barril**, i el pic va córrer per canals d'informació i xarxes socials fins a posar tota Europa en alerta. El mercat, ja sacsejat per l'esclat de la invasió russa d'Ucraïna només dies abans, es trobava davant d'una realitat nova: el petroli recuperava el paper d'arma geopolítica que els analistes temien des de feia dècades.

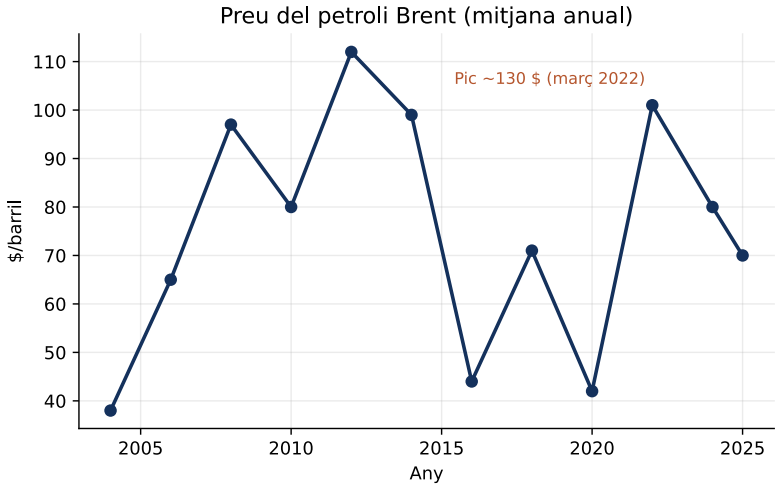


Figura 3.1 — El preu del Brent: del xoc de 2022 (~130 $) a l'estabilització cap als ~67 $ el 2025.

Aquell pic, però, va ser el principi d'un descens. Les xifres que vindrien després explicaven una història que ningú no esperava: del màxim de **130 $** a una mitjana de **101 $** el 2022, a **83 $** el 2023, fins a acabar en uns modestos **67 $** el setembre de 2025 [1]. No eren només números: eren el reflex d'una dependència encara aferrada a les vies tradicionals del subministrament, però també la prova que l'oferta era molt més robusta del que es temia.

La pregunta que flotava a l'aire era clara: **com garantir la seguretat energètica sense dependre d'un mercat tan volàtil?** Les respostes, encara que fragmentades, apuntaven a una combinació de diversificació de fonts i augment de reserves estratègiques.

Els mitjans de comunicació, amb la seva cobertura constant, van transformar aquell moment en una narració gairebé apocalíptica: «el petroli torna a ser arma geopolítica», es llegia en titulars que cridaven a l'acció i al canvi. A les xarxes, els experts energètics compartien gràfics que mostraven la correlació entre el conflicte militar i l'escalada del Brent, i recordaven als lectors que el mercat no era una entitat abstracta, sinó un reflex directe de les decisions dels estats.

Aquella escena d'incertesa i pressió va fixar el teló de fons d'una era nova, en què l'oferta de petroli ja no seria el factor limitant. El que havia canviat era la **demanda**: encara creixent, però cada cop més influïda per les tensions geopolítiques i per la urgència de trobar alternatives. La visió que Paul Roberts, autor de *The End of Oil* (2004), havia ofert sobre l'esgotament del petroli començava a mostrar-se incompleta; el veritable repte ja no era trobar l'últim dipòsit d'or negre, sinó gestionar una demanda volàtil en un món que es reconfigurava a cada nova crisi.

El xoc de 2022 i la seguretat energètica

Aquell matí de Brussel·les no va ser un episodi aïllat: va ser el senyal d'un xoc que ressonaria durant tot el decenni. Pocs dies havien passat des de la invasió de Rússia a Ucraïna, el febrer de 2022, i el Brent tocava

el nivell més alt en més d'una dècada [1]. La pujada no només reflectia la interrupció immediata dels fluxos de cru rus: revelava una dependència estructural que molts països havien ignorat durant dècades.

Els «petrostats» —així es coneixen els països que depenen de les exportacions de petroli per a la seva balança comercial— van veure de cop com el seu pes geopolític tornava a primer pla. L'Aràbia Saudita i els altres membres de l'OPEP+ gestionaven l'oferta amb retallades coordinades de la producció per intentar sostenir un mercat que es mostrava cada cop més fràgil [1]. Però a partir del setembre de 2025 l'organització va començar a desfer aquelles retallades: la pressió a la baixa sobre els preus ja no justificava mantenir el cru fora del mercat. El Brent se situava llavors al voltant dels 67 $ per barril, una caiguda dràstica respecte al pic de tres anys abans [1].

Mentre l'oferta recuperava l'equilibri, el xoc es traslladava a un altre terreny: la geopolítica. Els països que tradicionalment havien importat gran part del seu petroli de Rússia van haver de buscar alternatives en un mercat en què les rutes comercials es reconfiguraven a ritme vertiginós. El cru rus va trobar nous destins: alguns fluxos es van redirigir cap a l'Àsia, sovint a través de contractes amb preus volàtils que alimentaven una incertesa propagada per totes les cadenes de subministrament.

En paral·lel, la producció interior dels Estats Units assolia rècords històrics. L'auge no venia de cap plataforma marina, sinó de terra endins: la conca del Permià, al sud-oest del país, s'havia convertit en el motor d'una oferta global que ja no depenia exclusivament dels països de l'OPEP+ [2]. Aquesta abundància reduïa la pressió sobre les reserves estratègiques i donava a les nacions un cert marge de maniobra per afrontar la volatilitat del mercat. El risc ja no era l'esgotament dels dipòsits, sinó la incapacitat d'adaptar-se a fluctuacions brusques de la demanda.

I era precisament la demanda la que marcava el nou horitzó. Les projeccions apuntaven a una estabilització del consum mundial a l'entorn dels **105 milions de barrils diaris** cap al 2030, abans d'entrar en declivi a mesura que avancin l'eficiència energètica i el vehicle elèctric [3]. Era el **pic de demanda**: encara que la producció pogués augmentar, la necessitat mundial de petroli deixaria de créixer sense fre. La por de Roberts —que el món s'enfrontaria a una crisi d'oferta— havia evolucionat cap a una angoixa diferent: l'excés de dependència geopolítica i la incertesa d'una demanda que puja i baixa com una onada.

Així, el xoc del 2022 no només va demostrar que el petroli encara és un recurs crític: va revelar les fractures d'un sistema basat en fluxos de poder i influència. La clau de la seguretat energètica ja no rau únicament a assegurar reserves, sinó a construir una xarxa resilient capaç d'absorbir xocs geopolítics, diversificar fonts i gestionar una demanda cada cop més volàtil.

L'abundància inesperada

Mentre els escenaris de Roberts dibuixaven un futur dominat per l'esgotament dels camps tradicionals —el famós «últim petroli fàcil»—, el 2023 i el 2024 els Estats Units superaven qualsevol rècord anterior de producció de cru. L'epicentre era aquell motor terra endins, la conca del Permià, on una onada de perforacions i d'expansió d'infraestructura va dur el país més enllà del que cap analista de l'època no hauria pogut predir. L'increment es devia sobretot als avenços tecnològics en la fracturació hidràulica i a uns costos d'extracció que, tot i ser elevats, es mantenien viables a aquells preus [2].

Paral·lelament, l'OPEP+ ha adoptat una estratègia de gestió activa de l'oferta que contradiu la narrativa d'un declivi inexorable: en desfer progressivament les retallades dels anys anteriors, tornava cru a un mercat que calia estabilitzar davant la caiguda del preu del Brent. El llarg descens des del pic del març del 2022 no reflecteix només una oferta més abundant, sinó també la capacitat dels actors globals d'ajustar les seves polítiques i evitar els buits de subministrament que havien alimentat les expectatives del **pic d'oferta** («peak oil»).

Aquesta nova realitat posa en qüestió el paradigma central del llibre de Roberts: l'oferta no és el coll d'ampolla. L'abundància de la producció nord-americana ha generat un excedent que, tot i ser costós d'explotar —les reserves de l'esquist requereixen tecnologies avançades i inversió continuada—, ha mantingut els preus en nivells assequibles per a l'economia mundial. Això no vol dir que el petroli sigui una solució permanent; al contrari, la seva abundància actual es mostra com un **recurs temporal** que es pot explotar mentre les estructures energètiques evolucionen cap a alternatives més netes i descentralitzades.

El desafiament, ara, és gestionar la volatilitat de la demanda. Amb el consum mundial a prop del sostre, aquell pic de demanda previst per al 2030, la pressió sobre el mercat ja no ve de la falta d'oferta, sinó de la incertesa geopolítica —conflictes regionals, sancions econòmiques i tensions entre grans productors— que pot alterar bruscament els fluxos comercials. En aquest nou escenari, la seguretat energètica depèn més que mai de la capacitat d'adaptar-se ràpidament a canvis inesperats, tant en l'oferta com en la demanda.

L'«últim petroli fàcil», doncs, no s'ha esgotat; ha ressorgit en forma d'una oferta nord-americana robusta i d'una gestió dinàmica de l'OPEP+. Però aquesta abundància és una arma de doble tall: obre l'oportunitat de reduir la dependència de fonts inestables i, alhora, amplifica la necessitat de mecanismes de regulació i diversificació que puguin absorbir les futures sacsejades del mercat. La clau continua sent aquella xarxa resilient: encarar tant la sobirania de l'oferta com la incertesa de la demanda.

Roberts tenia raó... i no

Tornem per un moment al març del 2022. Mentre el Brent tocava el seu pic [1], l'eco d'un pic d'oferta imminent ressonava a les sales de conferències i als fòrums en línia. L'anomenada profecia de Roberts —que el món s'enfrontaria a una escassetat inevitable de petroli que forçaria una crisi energètica profunda— semblava gravada en pedra. Però el mercat, com un riu que canvia de curs, va trobar camins inesperats per esquivar aquella catàstrofe.

Els camins ja els hem recorregut: el gir de l'OPEP+, que va tornar cru al mercat, i els rècords de producció del Permià, més enllà de les projeccions del sector [1][2]. El resultat va ser un preu notablement inferior a les expectatives de molts analistes, i un augment inesperat d'oferta que va desactivar l'alarmisme sobre un esgotament imminent.

Però la veritable transformació no prové tant de la quantitat disponible com de **qui la consumeix**. Aquell sostre de consum previst per al final de la dècada —fruit de l'eficiència energètica i de la proliferació dels vehicles elèctrics— redefineix completament el paradigma: ja no es tracta tant de «quant queda», sinó de «quant en voldrem». La pressió sobre les infraestructures tradicionals —refineries, terminals d'emmagatzematge i xarxes de transport— canvia de naturalesa a mesura que la demanda es transforma.

El nou paradigma planteja una doble cruïlla. D'una banda, l'abundància d'oferta dona marge per mitigar els efectes dels conflictes geopolítics que tradicionalment han sacsejat el mercat del petroli. De l'altra, pot fomentar una **volatilitat de preus** encara més pronunciada: les fluctuacions de la demanda —impulsades per polítiques climàtiques, canvis regulatoris i avenços tecnològics— poden provocar cicles d'excés i escassetat a curt termini.

El repte, per tant, torna a ser aquella xarxa resilient que absorbeixi les sacsejades: diversificar les fonts —amb les renovables i la resta d'alternatives netes— i desenvolupar mecanismes de regulació que s'ajustin a les variacions de la demanda. El pic d'oferta queda enrere; el pic que compta és el de demanda, aquell davant del qual la societat ha de decidir com respondre. I triar el camí és, ara, a les nostres mans.

La promesa i el perill

L'excés d'oferta que l'esquist nord-americà —amb els nous camps del Permià— i l'ajust de l'OPEP+ han generat a partir del 2023 transforma el panorama energètic en una oportunitat sense precedents. L'abundància de cru és ara un amortidor que pot reduir la pressió sobre les balances comercials i, al mateix temps, afavorir la flexibilitat dels preus. Quan el Brent va tocar el pic, semblava que el món s'enfrontaria a una espiral incontrolable; tres anys després, el retorn del cru de l'OPEP+ al mercat i la producció rècord nord-americana han fet baixar el preu i mantenen una oferta que supera les expectatives inicials [1][2].

Aquesta abundància crea un marge d'actuació per als governs i les empreses: la necessitat urgent de reduir les emissions es pot abordar sense l'amenaça immediata d'una escassetat energètica. La diversificació de fonts, incloent-hi gas natural i renovables, redueix el «xantatge» que tradicionalment han exercit els petrostats sobre les economies emergents. La pressió per mantenir una producció constant es debilita, i obre espai perquè les polítiques climàtiques avancin sense témer un desbordament de preus ni una crisi d'abastiment.

Tanmateix, el mateix excedent comporta riscos que cal gestionar amb rigor. La volatilitat dels preus, alimentada per la incertesa geopolítica i les fluctuacions de la demanda, pot desencadenar onades de

caigudes brusques que erosionin els ingressos dels països exportadors i desestabilitzin mercats emergents que depenen del petroli. A més, la percepció d'un mercat abundant amplifica l'atractiu d'invertir en projectes d'extracció a llarg termini; però aquests actius corren el perill de quedar **varats** (stranded assets) si les polítiques climàtiques s'intensifiquen o si la demanda es frena un cop assolit el seu sostre, cap al 2030 [3].

Per abundant que sigui, el combustible continua sent fòssil, i la dependència manté les economies vinculades a una transició que encara no s'ha completat. Cada inversió en infraestructura petroliera nova augmenta la inèrcia del sistema energètic i dificulta la migració cap a fonts netes. Així, el perill es manifesta tant en l'augment dels costos d'adaptació futura com en la possible creació d'un excedent que provoqui caigudes de preus abruptes i generi incertesa econòmica i social.

En un plat de la balança, doncs, una finestra d'oportunitat per a polítiques climàtiques més agressives i per a una diversificació energètica que redueixi la influència dels petrostats. A l'altre, una nova forma d'inestabilitat: preus volàtils, inversions mal alineades i una dependència prolongada del petroli que podria convertir els actius fòssils en càrregues econòmiques. Aprofitar la promesa i mitigar el perill exigeix una planificació coordinada, que prengui les decisions d'inversió amb plena consciència dels riscos del mercat i del calendari de la transició.

Quant en volem cremar

Si l'oferta ja no és el coll d'ampolla, la pregunta canvia de lloc. El petroli ha superat les expectatives més optimistes de fa una dècada; els camps d'esquist i les decisions coordinades de l'OPEP+ han mantingut l'oferta a nivells que, fins ara, només es veien en escenaris de «boom» [1]. Però aquest excedent no és cap garantia de tranquil·litat: el perill ha mutat cap a la demanda, impulsat per una economia global cada cop més electrificada i per tensions geopolítiques que fan fluctuar els preus en qüestió d'hores.

La por de Roberts era que se'ns acabés el petroli. El que hem descobert és gairebé el contrari: en tenim de sobres, i el repte ja no és arrencar-ne l'última gota, sinó decidir quant en volem cremar. La transició cap a les renovables i el vehicle elèctric avança, però l'oferta fòssil abundant i barata és, alhora, l'amortidor que ens dona temps i la temptació que la pot frenar.

I aquí s'obre el terreny del capítol següent. Si el petroli deixa de ser el factor limitant, el centre de gravetat es desplaça cap a les fonts que l'han de substituir —les renovables, les bateries, el vehicle elèctric— i cap a la xarxa que les ha de sostenir. La seguretat energètica del futur no es mesurarà només en barrils, sinó en la capacitat de fer fiables, accessibles i resilients les alternatives netes. Aquesta és la frontera que explorarem tot seguit.

---

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

[2] AIE, *Oil Market Report (set. 2025) — esquist EUA*. https://www.iea.org/reports/oil-market-report-september-2025 ↩

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

El futur ja és aquí: renovables, bateries i vehicle elèctric

«El futur ja és aquí — només que no està repartit uniformement.»

— William Gibson (documentada des de 1992)

A la primera llum del dia, l'horitzó del desert de Mojave es transforma en una plana d'or líquid. Uns centenars de panells fotovoltaics s'alcen com filigranes d'argent que capturen el sol naixent i el converteixen immediatament en electricitat. Uns quilòmetres més avall, la pantalla d'un panell de control mostra números verds que cauen: 0,043 $/kWh. El preu és tan baix que bat qualsevol oferta d'una central de gas natural o de carbó, i la subhasta d'energia solar acaba amb una ronda d'aplaudiments continguts però contundents. Els inversors, habitualment reservats davant les noves tecnologies, fan un cop d'ull a les xifres i somriuen: el sol acaba de guanyar la partida del preu al gas i al carbó [1].

Mentre el sol escalfa les plaques de silici, a la ciutat propera es desplega una escena que fa unes dècades només existia en l'optimisme futurista. Un aparcament subterrani, il·luminat per llums LED blaves, és ple de vehicles elèctrics que es carreguen en fila ordenada durant la nit. El so suau dels ventiladors de refrigeració i els pings periòdics dels sistemes de gestió d'energia són l'únic eco que trenca el silenci del desert. Cada cotxe, amb una bateria de química LFP cada any més barata, rep la seva dosi d'electricitat fresca sense cap rastre de combustió [2].

Aquests vehicles no els alimenta només l'energia més neta: al darrere hi ha una infraestructura que ha crescut com una xarxa nerviosa, amb microxarxes locals que equilibren la producció solar amb el consum instantani, sistemes avançats de gestió d'emmagatzematge i plataformes digitals que optimitzen cada quilowatt-hora. A la pantalla central del parc, un gràfic mostra en temps real com les bateries comunitàries absorbeixen l'excés de generació de les hores de màxim sol i l'alliberen quan el sol es retira.

Pel lloc hi passen enginyers, conductors i inversors. Una jove enginyera del departament d'energia diu: «Fa cinc anys, la idea de conduir un cotxe totalment carregat amb energia solar era quasi un somni; avui, més del 20 % dels cotxes nous són elèctrics i ja se'n van vendre més de 17 milions en un sol any a escala global» [2]. Un agricultor local, que fa servir l'electricitat del mateix camp per al reg, afegeix: «Els costos de l'energia solar ens han permès reduir les despeses operatives i invertir en més cultius».

Aquesta escena no és una projecció futurista; és el present palpable d'un món on les renovables ja són l'opció econòmica dominant i el vehicle elèctric, un producte de masses. Però, com avisa la història que Paul Roberts va narrar a *The End of Oil* (2004), aquest avanç comporta colls d'ampolla que encara cal resoldre: xarxes que han d'escalar sense perdre estabilitat, emmagatzematge massiu que necessita minerals crítics i una logística global per a les bateries. El futur ha arribat; que es consolidi dependrà de com afrontem aquests reptes.

La promesa complerta

Fa una dècada, aquest panorama semblava un somni de ciència-ficció: panells fotovoltaics estesos com camps d'or sobre els deserts, turbines eòliques balancejant-se al ritme del vent —i tot plegat encara més car que una central de carbó. Avui el relat s'ha capgirat. El cost normalitzat de l'electricitat (LCOE) dels sistemes solars ha caigut un 90 % entre el 2010 i el 2024, fins als 0,043 $ per kWh que lluïen en verd a la pantalla del Mojave [1]: una xifra que fa la llum del sol més barata que l'electricitat fòssil en gairebé qualsevol mercat desenvolupat. Aquest descens vertiginós no és només una tendència estadística; és el resultat combinat de tecnologies millorades, economies d'escala i polítiques públiques que han impulsat el desplegament massiu de la fotovoltaica a tot el món.

El 2024 va marcar, a més, un punt d'inflexió històric: el 91 % de la nova capacitat renovable afegida aquell any va ser més econòmica que qualsevol planta fòssil nova. Aquesta majoria no reflecteix només la caiguda del cost de producció: també hi pesen l'eficiència operativa creixent i la inversió en xarxes intel·ligents que maximitzen l'aprofitament de recursos intermitents com el sol i el vent. Les empreses energètiques han adoptat models de finançament basats en bons verds, que redueixen els costos de capital i acceleren la construcció d'infraestructures renovables.

A escala global, la convergència d'aquests factors ha reconfigurat el mercat: les centrals de gas natural, fins fa poc considerades el pont transitori cap a un futur net, es veuen ara superades en competitivitat

econòmica per les instal·lacions solars i eòliques. La caiguda del LCOE solar ha desfermat una «febre de l'or» entre els desenvolupadors, que corren a aprofitar la diferència de costos abans que canviïn les regulacions o s'ajustin els preus de les matèries primeres.

Aquesta transformació, però, no és una simple qüestió de números; és una revolució en la manera com la societat produeix i consumeix energia. Les comunitats rurals d'Àfrica i Amèrica Llatina, que abans depenien d'una infraestructura elèctrica limitada o inexistent, ara poden accedir a electricitat fiable gràcies a microxarxes solars de cost ultrabaix. A Europa, les polítiques de «tarifes netes» incentiven els consumidors a instal·lar panells al sostre de les seves llars, i converteixen cada habitatge en un petit productor d'energia.

La mateixa onada ha arribat al transport. Amb l'electricitat més barata i abundant, el cost operatiu dels vehicles elèctrics ha caigut dràsticament, i l'adopció massiva ha esdevingut una qüestió de rendibilitat tant com de consciència ambiental. La reducció del LCOE solar es tradueix directament en electricitat de càrrega més barata, i això reforça el cercle virtuós entre energia neta i mobilitat sostenible.

La promesa que Roberts només podia imaginar amb una dosi d'escepticisme s'ha materialitzat: les renovables són ara l'opció més barata i tecnològicament madura, i obren la porta a un futur amb una dependència dels combustibles fòssils substancialment menor. La base econòmica és sòlida; el sistema que l'ha de sostenir —infraestructura, emmagatzematge, gestió dels recursos crítics— encara no ho és.

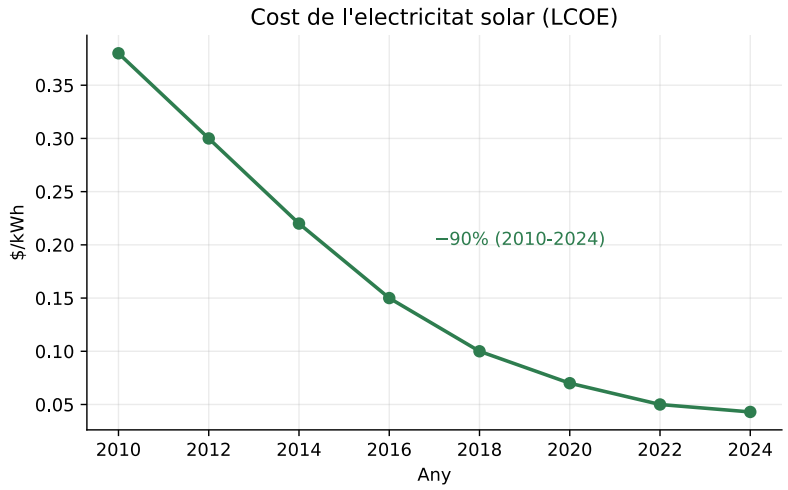


Figura 4.1 — El cost de l'electricitat solar va caure prop d'un 90 % entre el 2010 i el 2024: la transformació de preu més ràpida de la història de l'energia.

Bateries i vehicle elèctric

Després d'un decenni de promeses i dubtes, el vehicle elèctric (VE) ha deixat de ser una curiositat de laboratori per convertir-se en el corrent principal del mercat. El 2024 se'n van vendre més de **17 milions** a tot el món, **més del 20 % dels cotxes nous** que van arribar als concessionaris aquell any [2]. La xifra no només supera qualsevol projecció realista feta fa una dècada; confirma, sobretot, que la mobilitat neta ja no és cosa d'una minoria entusiasta. I la tendència s'accelera: per al 2025 se'n projecten al voltant de 22 milions [2].

Darrere d'aquest salt hi ha una revolució silenciosa però fonamental: les bateries. El cost del quilowatt-hora (kWh) de les cèl·lules d'ions de liti ha caigut a **115 $ per kWh el 2024**, amb una projecció de **108 $ per kWh el 2025**: la mateixa corba descendent que va enfonsar el cost del solar durant els últims quinze anys [2]. La tendència no és cap accident, sinó la suma d'economies d'escala a les fàbriques de cèl·lules, millores en la cadena de subministrament de materials i l'adopció creixent d'una química més assequible —el fosfat de ferro i liti (LFP)— que ha guanyat terreny tant en vehicles de gamma mitjana com en models premium.

L'auge de l'LFP és especialment revelador. A diferència de les bateries de níquel-cobalt-manganès, l'LFP no depèn del cobalt, un mineral amb problemes ètics i logístics que ha fet encallar la cadena de subministrament en diverses regions d'Àfrica i Àsia. Que els packs de bateries fabricats a la Xina hagin baixat fins als **84 $ per kWh** en línies de producció massiva ha reduït la pressió sobre els preus dels materials crítics i ha facilitat una expansió més ràpida del parc de vehicles. A més, l'LFP ofereix una vida

útil llarga i més seguretat tèrmica, dos arguments que han convençut cada cop més fabricants d'incorporar-lo en models d'alta demanda [2].

Ara bé, la caiguda del cost no elimina del tot els colls d'ampolla. La producció global de bateries encara depèn en gran mesura del liti i del manganès, dos recursos concentrats geogràficament i que exigeixen una gestió ambiental rigorosa. Amb les vendes de VE al ritme actual, la demanda d'aquests minerals pressiona unes mines i uns processos d'extracció que encara no s'han optimitzat del tot [2].

La infraestructura de recàrrega, a més, es troba en plena transició. Encara que les xarxes de càrrega ràpida s'han expandit amb força, el repartiment continua sent desigual: les zones rurals i algunes regions de l'Europa oriental encara pateixen escassetat d'estacions d'alta potència. Aquest desequilibri limita la confiança dels consumidors i impedeix aprofitar tot el potencial de les bateries barates.

El vehicle elèctric és, doncs, a les portes d'una era en què l'energia per al transport és tan assequible com la que genera el sol. Les bateries, en reduir dràsticament els costos, han impulsat una adopció massiva i han obert la porta a un model de mobilitat més net i sostenible. Però el camí cap a la consolidació completa encara topa amb obstacles estructurals: la necessitat d'una cadena de subministrament de materials crítics més resilient i d'una xarxa de recàrrega que arribi a tots els racons del territori. Superar-los serà l'últim pas perquè la promesa de les renovables i el VE es tradueixi en una realitat universal.

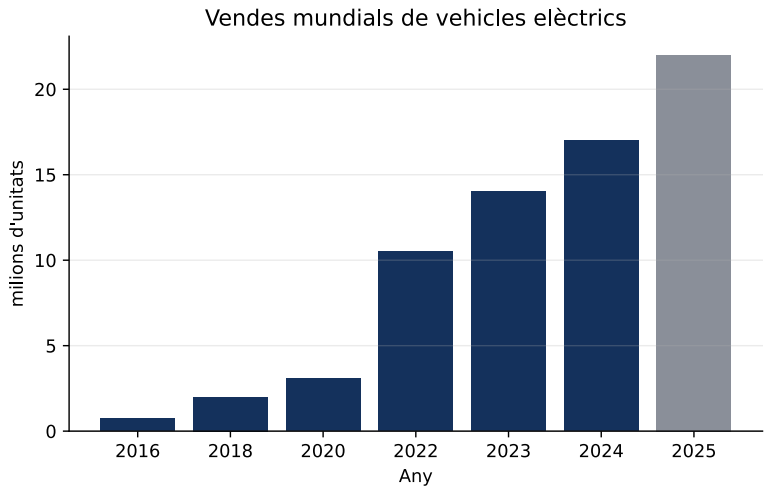


Figura 4.2 — Les vendes de vehicles elèctrics superen els 17 milions el 2024 i ja són més d'un de cada cinc cotxes nous.

El que encara falta

La generació barata, doncs, ja la tenim. Però l'aparença d'abundància amaga una realitat molt més complexa: l'electricitat econòmica no es tradueix automàticament en un sistema complet i fiable. Entre el panell que produeix a preu de rècord i l'endoll que no falla mai hi ha tres colls d'ampolla.

El primer són les xarxes elèctriques. Les infraestructures de transmissió i distribució es van dissenyar per a fluxos constants i previsibles, els característics de les centrals d'energia convencional. Ara, amb la proliferació d'una generació descentralitzada i altament intermitent —el sol brilla només durant el dia i el vent bufa en moments imprevisibles—, les xarxes han de poder ajustar la potència en temps real. Això requereix inversions massives en sistemes de gestió intel·ligent, sensors IoT i algoritmes avançats basats en IA que equilibrin oferta i demanda sense interrupcions. Sense aquesta modernització, les zones amb alta concentració de renovables poden patir sobrecàrregues o talls de subministrament que minen la confiança de consumidors i empreses.

L'emmagatzematge a gran escala és el segon. Les bateries són l'eina clau per suavitzar la intermitència, i els seus preus cauen, com acabem de veure; però la necessitat d'instal·lar centenars de gigawatt-hores de capacitat d'emmagatzematge al món supera de llarg les inversions actuals [2]. Sense prou emmagatzematge, l'excés de producció solar o eòlica es perd, i la xarxa continua depenent de fonts convencionals per garantir la continuïtat del subministrament.

El tercer repte és la dependència dels minerals crítics. Les bateries, els inversors fotovoltaics i molts components electrònics requereixen cobalt, liti, níquel i terres rares, i la demanda d'aquests materials s'ha disparat amb l'augment dels VE i la construcció d'infraestructures d'emmagatzematge [2]. Les cadenes de

subministrament són vulnerables a tensions geopolítiques i a pràctiques mineres que sovint no compleixen estàndards ambientals ni socials. Sense una estratègia clara per diversificar fonts, reciclar materials i desenvolupar alternatives menys dependents, el creixement sostenible queda lligat a la disponibilitat d'aquests recursos.

Tres fronts, doncs: xarxes intel·ligents i resilients, emmagatzematge massiu i assequible, i una cadena de subministrament de minerals crítics que sigui sostenible. Superar-los requerirà coordinació entre governs, empreses i comunitat científica, i inversions dirigides a tecnologies emergents capaces de transformar aquestes limitacions en oportunitats per consolidar el futur energètic net.

La promesa i el perill

El 2024 es va tancar, doncs, amb una fita que només uns pocs analistes havien pogut preveure: per primera vegada des de la Revolució Industrial, l'energia neta és més barata que la bruta. No és cap fenomen marginal, sinó una transformació estructural, i la combinació d'una energia cada cop més assequible amb un parc automobilístic que s'electrifica ha desencadenat una espiral positiva: la demanda de generació neta augmenta, el preu de les tecnologies associades cau i l'acceptació social es consolida.

La nova dinàmica sacseja les velles estructures basades en els combustibles fòssils. Els grans consumidors —des de la indústria pesant fins a les ciutats intel·ligents— poden planificar el futur energètic sense la pressió constant del preu del petroli o del gas natural. Les empreses d'energia, que fa una dècada depenien de contractes a llarg termini amb proveïdors de combustibles, competeixen ara en eficiència i en capacitat d'integrar fonts intermitents com el sol i el vent. La promesa, doncs, no és només econòmica; és una redefinició del poder geopolític, perquè les nacions que tradicionalment controlaven els recursos fòssils veuen erosionada la seva influència.

Aquesta època d'optimisme, però, viu a l'ombra dels tres colls d'ampolla que ja coneixem, i que amenacen de frenar-ne l'avanç. Primer, les xarxes elèctriques —construïdes fa dècades per transportar energia centralitzada i constant— no estan preparades per gestionar fluxos massius i variables d'origen distribuït. Les limitacions en la capacitat de transmissió i en els sistemes de control intel·ligent generen congestions que, en el pitjor dels casos, obliguen a curtailments (reduccions forçoses de subministrament) encara que la producció renovable sigui abundant.

Segon, l'emmagatzematge encara no arriba a l'escala ni al cost necessaris per equilibrar del tot les fonts intermitents. Tot i la caiguda de preus que hem vist, el cost continua sent un factor limitant per a aplicacions a gran escala com els sistemes d'emmagatzematge estacionari o les flotes de vehicles comercials electrificats. La necessitat de tecnologies complementàries —com el flux de potència en xarxes híbrides i les bateries LFP de cicles de vida més llargs— és urgent, però la seva adopció requereix inversions massives i una cadena de subministrament robusta.

Finalment, la dependència creixent dels minerals crítics —liti, cobalt, níquel i altres elements essencials per a les bateries avançades— concentra el risc geopolític en poques regions productores. Sense una diversificació real de les fonts i un marc regulador que garanteixi pràctiques sostenibles, la cadena de subministrament es converteix en una vulnerabilitat estructural que poden explotar actors amb interessos contraris a la transició neta.

La promesa, doncs, ja s'ha materialitzat, i el creixement renovable avança inexorablement; però si les barreres de xarxes, emmagatzematge i minerals no se superen, aquesta època d'optimisme pot transformar-se en una nova era de dependència concentrada. Desactivar aquests riscos —fer que la transició no només sigui possible, sinó també resilient i equitativa— és la feina que queda.

El poder darrere dels panells

La tecnologia ja no és el problema; el poder, sí. Les dades d'aquest capítol són irrefutables i apunten totes en la mateixa direcció: el sol més barat que qualsevol fòssil, més d'un de cada cinc cotxes nous ja elèctric, bateries que perden preu any rere any. L'economia ha fet el pas decisiu cap a l'energia neta.

Però darrere d'aquestes victòries tecnològiques s'amaga una xarxa de relacions de poder que ningú no ha desafiat encara. Les cadenes de subministrament de minerals crítics —cobalt, liti i níquel— es concentren en un nombre reduït de països i empreses multinacionals. La Xina domina bona part d'aquesta cadena: hi controla al voltant del 75 % de la fabricació mundial de bateries i prop del 91 % del refinatge de terres

rares. Aquesta concentració converteix els recursos essencials en palanques de negociació, i permet a uns pocs actors dictar preus i condicions de lliurament.

A més, la infraestructura de xarxes elèctriques encara es basa en models centralitzats que depenen d'inversors tradicionals i d'operadors de gran escala. La manca d'estandardització en les tecnologies d'emmagatzematge impedeix una integració fluida dels recursos distribuïts i deixa les regions més exposades a interrupcions i a la manipulació del flux energètic. En aquest escenari, el control de les xarxes no és només un tema tècnic; és una qüestió d'autonomia nacional i de sobirania econòmica.

La geopolítica que es desplega al voltant del nou paradigma energètic segueix la mateixa lògica que la del petroli fa mig segle: qui controla la font controla les economies i, per extensió, els sistemes polítics. Però, a diferència del passat, ara tenim eines digitals —blockchain, IA avançada i contractes intel·ligents— que poden desfer aquesta concentració de poder. La clau serà crear plataformes obertes i transparents que permetin el seguiment en temps real dels fluxos de minerals, la certificació d'origen i la gestió descentralitzada de les xarxes.

En el proper capítol analitzarem com desplegar aquestes solucions a escala global, quins actors han d'emergir com a guardians del nou ecosistema energètic i com evitar que una nova elit energètica es consolidi sobre la base d'una infraestructura tecnològica ja provada. La transició no depèn només de la reducció dels costos o de l'adopció massiva dels VE; depèn, en última instància, de qui decideix quina part del valor generat per les renovables s'ha de redistribuir i com es regula aquest flux. A la pantalla del Mojave, els números verds continuaran caient. El futur ja és aquí; el seu benefici, encara, s'ha d'equilibrar entre tots els protagonistes.

---

[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 i preus de bateries*. https://www.iea.org/reports/global-ev-outlook-2025/electric-vehicle-batteries ↩

L'energia és poder

«El comunisme és el poder soviètic més l'electrificació de tot el país.»

— V. I. Lenin, discurs a Moscou (1920)

Octubre de 2025. En una sala de reunions d'un complex d'alta tecnologia de Pequín, el sol d'hivern es filtra pel vidre polaritzat i dibuixa línies de llum sobre una taula ovalada coberta de mapes digitals, gràfics de flux i mostres de pols metàl·lica. Al plafó central, un gran monitor segueix en temps real la cadència dels enviaments de neodimi i d'altres terres rares.

Davant la pantalla, un grup de representants occidentals —directius de l'automoció europea, inversors nord-americans en bateries, un delegat del Ministeri espanyol d'Energia— observa amb una barreja d'incredulitat i d'inquietud. A l'altra banda, amb la cara seriosa i els ulls fixos en les dades que es despleguen, el portaveu del Ministeri de Comerç xinès deixa anar la frase que ho canvia tot: «A partir d'avui, el Govern xinès imposa restriccions estrictes a l'exportació de tot component relacionat amb les cadenes de subministrament netes: panells fotovoltaics, turbines eòliques, bateries d'ions de liti i, per sobre de tot, les terres rares que són la columna vertebral de cada vehicle elèctric, de cada instal·lació d'emmagatzematge d'energia i del maquinari que fa funcionar la intel·ligència artificial.»

Un xiulet anuncia una alerta nova al sistema de seguiment global. Els gràfics ho diuen sense retòrica: la quota xinesa en la producció mundial de panells solars ja supera el 80 %; la dels aerogeneradors, el 60 %; la dels vehicles elèctrics (VE), el 70 %. Les bateries que alimenten aquestes màquines es fabriquen a la Xina gairebé en la seva totalitat —un 75 %—, i el refinament de les terres rares, el coll d'ampolla de tot plegat, s'hi concentra en un 91 % [1]. I ara aquest domini s'estén, per decret, a tots els components intermedis que converteixen la matèria primera en producte acabat.

Els representants es miren entre ells. No és un embargament de petroli com els que van sacsejar les economies el segle passat; és una altra mena de setge econòmic, una «guerra freda» de l'accés: a la matèria primera i al coneixement tecnològic net. Una arma de negociació capaç de desestabilitzar les cadenes de subministrament d'Europa, d'Amèrica del Nord i fins i tot de països emergents com l'Índia. Mentre el monitor mostra la caiguda instantània dels enviaments cap a les empreses europees —el 2024, gairebé la meitat de les exportacions netes xineses, un 47 %, havia anat al Sud Global, i ara cada destí depèn d'una decisió presa en aquesta sala [2]—, el portaveu conclou: «El món canviarà la manera com produeix energia. Qui no s'adapti a una nova arquitectura basada en recursos nets controlats per nosaltres quedarà fora del joc.»

Els occidentals recullen els papers en un silenci espès. L'energia continua sent poder, però el mapa del poder s'ha redibuixat de dalt a baix. Aquest capítol explica com ha passat, i què hi ha en joc.

Del petroli als minerals

En el relat que el periodista Paul Roberts va teixir a *The End of Oil* (2004), el petroli era el fil conductor d'una jerarquia mundial: les nacions amb grans reserves definien rutes comercials, dictaven preus i modelaven l'ordre geopolític. En poc més de dues dècades, aquell ordre ha patit una metamorfosi profunda. Avui el poder ja no es mesura per la quantitat de cru que dorm sota terra, sinó per qui controla les cadenes de subministrament netes: panells fotovoltaics, bateries d'alta capacitat i minerals crítics.

L'epicentre d'aquesta arquitectura nova és la Xina, i el seu domini no és només quantitatiu. Concentrar la fabricació —les quotes que acabem de veure al monitor de Pequín— li dona també el control de les especificacions tècniques i dels estàndards de qualitat: la major part dels projectes solars d'Europa, d'Amèrica del Nord i d'Àfrica depenen d'elements fabricats al continent asiàtic, i cada VE, cada instal·lació d'emmagatzematge i cada dispositiu mòbil porta a dins bateries sortides de fàbriques xineses. Això converteix el país en el proveïdor indispensable del sector energètic net.

Però el monopoli més profund no és el de les fàbriques: és el del **processament**. Refinar prop del 91 % de les terres rares del món —els elements essencials per a imants potents, catalitzadors, sensors i electrònica avançada— vol dir que qualsevol interrupció de les exportacions pot paralitzar la cadena global d'equips d'alta tecnologia [1]. No cal controlar l'extracció si controles el pas que la converteix en material útil. La decisió d'octubre de 2025 d'ampliar els controls d'exportació va encendre les alarmes a Washington i a Brussel·les precisament per això, i totes dues capitals busquen ara alternatives per reduir la seva vulnerabilitat.

La inversió de la dinàmica de poder és completa, i planteja un doble escenari. D'una banda, la proliferació de tecnologies netes ofereix una oportunitat única per retallar les emissions globals i desfer els llaços amb el petroli. De l'altra, la concentració d'aquestes tecnologies en mans d'un sol actor crea vulnerabilitats noves: un bloqueig o una restricció comercial pot provocar escassetat de components crítics i afectar-ho tot, des de la mobilitat urbana fins a les xarxes elèctriques interconnectades. Les nacions que abans negociaven amb petroestats ara negocien amb una potència que no els ven l'energia, sinó les màquines que la converteixen —i que fa, alhora, de guardiana dels materials imprescindibles per al futur. La pregunta ja no és només qui té petroli, sinó qui controla els fluxos d'energia i de materials que alimenten la transició cap a un món net.

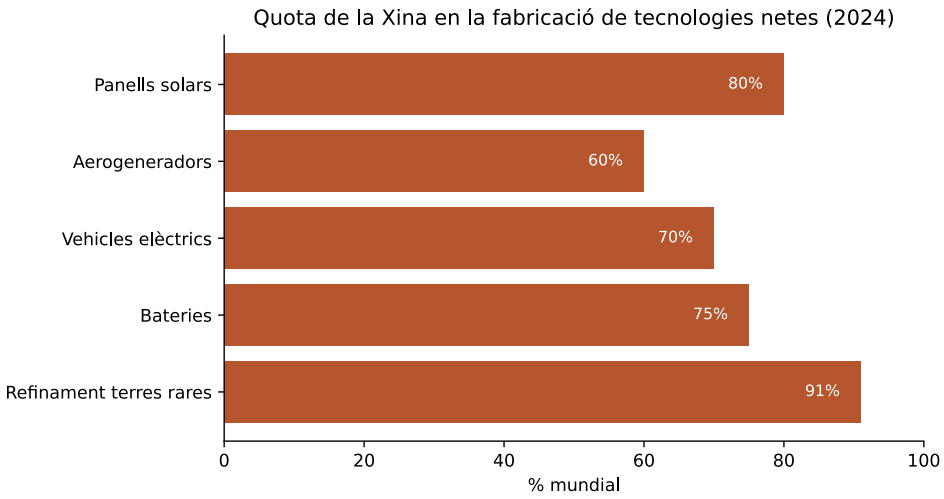


Figura 5.1 — La Xina domina la fabricació de la transició: del 60 % dels aerogeneradors al ~91 % del refinament de terres rares.

La nova dependència

Quan els petroestats de l'Orient Mitjà dominaven la geopolítica del segle passat, una sola regió podia dictar les condicions del mercat energètic mundial amb la força d'un tap a la font. Aquell poder s'ha traslladat al nord-est asiàtic, i l'aixeta ja no és el cru: són els components. El 2024, el 47 % de les exportacions xineses de VE, bateries, panells solars i aerogeneradors va anar al Sud Global —Amèrica Llatina, l'Àfrica subsahariana i el sud d'Àsia— [2]. No és una xifra qualsevol: és una reconfiguració profunda de les relacions internacionals, on la dependència energètica es barreja amb la necessitat crítica de minerals i de components electrònics.

Aquest domini no ha caigut del cel: és el fruit d'una política industrial agressiva i d'inversions massives en infraestructura de producció. I per als països sense alternatives pròpies es tradueix en una vulnerabilitat estructural. L'ampliació dels controls d'exportació de l'octubre de 2025 —justificada oficialment com una mesura de seguretat nacional i de protecció dels recursos— ho ha deixat clar: la capacitat d'imposar límits a l'exportació és avui una arma diplomàtica tan poderosa com ho va ser, fa unes dècades, la pressió sobre els fluxos petroliers.

Els efectes ja són palpables. Països del Sud Global que havien apostat per la transició verda han vist com s'encarien les bateries i s'allargaven els terminis de lliurament, amb retards en infraestructures crítiques com les xarxes de recàrrega pública i les instal·lacions de generació distribuïda. I aquests embussos alimenten tensions polítiques: governs que abans depenien del petroli ara es veuen obligats a renegociar acords comercials, a buscar alternatives locals o a aliar-se amb qui impulsa programes de producció pròpia, com la Unió Europea. El poder de la Xina sobre les cadenes netes es tradueix, doncs, en influència directa sobre les polítiques energètiques i industrials de mig món.

La nova dependència no és una qüestió de quantitat, sinó de control. I la pregunta que se'n deriva —com es gestiona aquesta vulnerabilitat sense sacrificar la transició verda?— demana una resposta col·lectiva: diversificar les fonts, desenvolupar capacitats locals i construir marcs reguladors internacionals que garanteixin l'accés equitatiu a les tecnologies netes. La confiança en un futur sostenible depèn de la nostra capacitat d'equilibrar dependència i sobirania energètica.

La promesa i el perill

La promesa és clara: la generació elèctrica renovable pot ser del tot autòctona. Un panell solar al desert d'Atacama o un aerogenerador a les costes del mar Bàltic produeixen energia que no depèn de cap ruta marítima ni de cap canal petrolier. Això retalla d'arrel el «xantatge energètic» —la coacció exercida a través de la dependència del subministrament—, perquè cada país pot cobrir gran part del seu consum amb recursos propis. I la descentralització de la generació —microxarxes comunitàries, emmagatzematge a escala local, xarxes intel·ligents que gestionen els fluxos— ofereix una visibilitat i un control del consum sense precedents.

El perill és l'altra cara exacta de la mateixa moneda. El sol i el vent són inesgotables i universals, però la infraestructura que els converteix en energia utilitzable surt, de manera aclaparadora, d'una sola regió del món. Aquesta concentració genera un **punt únic de fallada**: una política d'exportació restrictiva com la de l'octubre de 2025, un problema logístic o una crisi de seguretat a les instal·lacions poden paralitzar l'accés mundial a tecnologies crítiques. I qui més hi perdria és qui més hi confia: el Sud Global, receptor de gairebé la meitat de les exportacions netes xineses [2], podria quedar-se sense alternatives viables per a la seva descarbonització mentre les tensions geopolítiques s'enfilen.

La sortida no és renunciar a la promesa, sinó desconcentrar-la: invertir en fàbriques locals de panells i bateries, desenvolupar capacitat de refinament de terres rares fora de la Xina i establir marcs reguladors internacionals que assegurin l'accés equitatiu. Només així la sobirania energètica es podrà traduir en una independència autèntica.

La lliçó de Pequín

El poder energètic es reconfigura, però el motor que ho impulsa tot —el clima— no espera. Les quotes que han anat sortint al llarg del capítol no són estadístiques de mercat: són la infraestructura crítica que determina quina part del món pot accedir a l'electricitat neta, a la descarbonització i, al capdavall, al seu propi futur climàtic. Per a les economies emergents que volen substituir el petroli que ha alimentat durant dècades la seva industrialització, la relació amb la Xina recorda les velles rutes del cru amb un nucli diferent: minerals crítics i components electrònics [2]. I per a qualsevol país que vulgui construir capacitat renovable pròpia, aquell 91 % del refinament de terres rares concentrat dins d'unes soles fronteres és el recordatori que cap sobirania energètica no és completa si depèn d'una única font de subministrament [1].

El perill més gran és la inacció. Cada any que passa sense diversificar les cadenes augmenta la probabilitat de tensions geopolítiques, de preus manipulats i, en el pitjor dels escenaris, de restriccions d'accés a l'energia neta per als països més vulnerables —amb una pressió reguladora xinesa que pot estrènyer encara més el flux de materials essencials [1]. El pas següent, en canvi, és conegut: una estratègia coordinada de governs i empreses que combini inversió en infraestructura pròpia amb obertura internacional —centres de recerca conjunts, acords de cooperació per al desenvolupament sostenible dels minerals crítics i una normativa global que protegeixi els interessos col·lectius davant les maniobres unilaterals. Només així el poder energètic podrà ser realment distribuït, i el clima —el motor invisible però inexorable del nostre temps— no quedarà a l'espera d'una decisió tardana.

El capítol següent fa balanç d'aquesta altra pressió, la que no negocia: l'emergència climàtica del 2026, amb fenòmens meteorològics cada cop més intensos que exigeixen que les solucions avancin tan de pressa com canvia el planeta. Els occidentals d'aquella sala de Pequín en van sortir havent après la lliçó del segle: qui controla la màquina de la transició controla el temps de tothom. I el temps és, precisament, el que se'ns acaba. El moment és ara: **time2act**.

---

[1] AIE / CFR, *domini xinès en minerals i tecnologies netes (2024-2025)*. https://www.iea.org/commentaries/with-new-export-controls-on-critical-minerals-supply-concentration-risks-become-reality ↩

[2] Sightline / anàlisi, *exportacions netes xineses al Sud Global (2024)*. https://www.sightlineclimate.com/research/a-tour-of-chinas-electrostate ↩

Massa calent: el clima el 2026

«El "control de la natura" és una frase concebuda amb arrogància, nascuda de l'edat neandertal de la biologia i la filosofia, quan se suposava que la natura existeix per a conveniència de l'home.»

— Rachel Carson, Silent Spring (1962)

Gener de 2025. La sala d'operacions del Centre Europeu per a les Prediccions Meteorològiques a Mitjà Termini està immersa en la llum blavosa dels panells de control. En una pantalla gegant, un gràfic de línies s'enfila com el pendent d'una muntanya que es va quedant sense neu. L'últim punt és el 2024, amb una temperatura mitjana global al voltant de +1,6 °C per sobre dels nivells preindustrials: per primera vegada en la història humana, un any supera el llindar simbòlic de París. «És el primer any natural que supera els 1,5 °C», anuncia amb veu ferma la directora del centre. El grup d'experts i periodistes es queda en silenci: aquella xifra no és només una dada climàtica, sinó l'avís d'unes conseqüències que ja es despleguen per tot el planeta.

Els monitors parpellegen amb dades del programa Copernicus: la temperatura global continua enfilant-se i els extrems de calor són cada cop més freqüents. A l'oest d'Europa, ciutats costaneres com Barcelona i Lisboa lluiten contra onades de calor que baten rècords. A l'Àfrica, els camps de cultiu pateixen sequeres prolongades que erosionen les collites. A l'Àsia, les inundacions monsòniques, impulsades per corrents atmosfèrics més intensos, han desplaçat multituds de persones al sud de l'Índia i a Bangladesh.

Mentre els científics es mouen entre taules plenes d'informes, una imatge de la Terra vista des de satèl·lit omple una de les pantalles: núvols blancs com escuma sobre un blau cada cop més fosc. En aquell instant, l'optimisme que sovint acompanya les noves tecnologies queda ofegat per la realitat d'una crisi climàtica que avança a passos de gegant.

A la mateixa hora, al Parlament Europeu, els grups polítics discuteixen el paquet legislatiu sobre transició energètica. Uns demanen accelerar els objectius de reducció d'emissions; d'altres es resisteixen a imposar restriccions addicionals al sector fòssil. La pressió de les nacions petrolieres es fa sentir en cada vot. És el que molts anomenen «la trinxera entre la ciència i la voluntat política»: la bretxa que ha retardat les mesures necessàries per frenar l'escalfament.

En aquest context, la figura de Paul Roberts —el periodista que a *The End of Oil* (2004) ja anticipava les conseqüències climàtiques de la dependència fòssil— encara ressona com un eco del passat: el seu avís sobre un planeta que travessaria el llindar de l'1,5 °C s'ha materialitzat. Les dades i les imatges converteixen l'abstracció en una crida urgent a l'acció. La ciència ha demostrat que el planeta ja frega el límit, i el futur del clima depèn de la capacitat col·lectiva de transformar aquesta prova en una solució concreta i immediata. La pregunta que queda oberta és si la política pot respondre amb la mateixa rapidesa. [1]

L'avís complert

El 2026 el termòmetre global continua marcant els valors que Roberts i molts altres havien assenyalat com a límits crítics. Les dades de Copernicus que la directora presentava aquell gener ho certifiquen: el 2024 va ser el primer any natural en què la temperatura mitjana de la superfície terrestre va superar els +1,5 °C respecte al període preindustrial, una xifra que fins fa poc semblava reservada als escenaris de modelatge [1]. Roberts ja ho advertia: «el procés ja no es pot aturar, només frenar».

Les emissions de gasos amb efecte d'hivernacle (GEH), lluny de moderar-se, han marcat un màxim històric [1]. La tendència contradiu clarament les trajectòries de reducció proposades per l'IPCC i recorda que, malgrat l'abaratiment de les alternatives netes, el consum de combustibles fòssils encara no ha tocat sostre a escala global.

Un matís, abans de continuar: un any amb una temperatura mitjana superior a +1,5 °C no equival automàticament a l'incompliment de l'Acord de París, que es basa en la mitjana de temperatures a llarg termini (aproximadament 20 anys). Però superar el llindar puntualment és un senyal inequívoc de la direcció en què ens movem, i cada any addicional a prop d'aquesta temperatura incrementa els riscos de fenòmens extrems: onades de calor més intenses i freqüents, incendis forestals devastadors i un augment del nivell del mar que amenaça zones costaneres densament poblades.

Les recomanacions de l'IPCC al seu sisè informe d'avaluació (AR6) són contundents: per limitar l'escalfament a 1,5 °C cal reduir les emissions globals un 43 % abans del 2030 i un 60 % abans del 2035 respecte als nivells de 2019 [2]. La diplomàcia, en canvi, vacil·la: la COP28 de 2023 va fer una crida a accelerar la transició cap a les energies renovables [3], però les cúpules següents —COP29 i COP30— ni tan sols van esmentar els combustibles fòssils al text principal, sota la pressió creixent dels petrostats, els governs que viuen dels ingressos fòssils i que treballen per diluir els compromisos més ambiciosos.

Aquesta dissonància entre la urgència científica i la reticència política és el cor del que Don Tapscott, a *Blockchain Revolution*, descriu com «la promesa i el perill». La tecnologia està preparada: solucions basades en intel·ligència artificial per optimitzar les xarxes elèctriques, plataformes blockchain per garantir la traçabilitat de les certificacions d'energia verda i mecanismes de prova d'existència (t2p) que combaten les deepfakes i reforcen la confiança pública. Però sense una voluntat política decidida a trencar el poder dels grups de pressió dels combustibles fòssils, aquestes eines es quedaran al paper: una promesa no materialitzada.

El repte per al lector és clar: exigir que les autoritats tradueixin les dades i les advertències en polítiques concretes, finançament urgent i marcs reguladors robustos. Només així podrem transformar l'avís complert de Roberts en una acció real que freni —i possiblement reverteixi— la trajectòria actual cap a un futur insostenible.

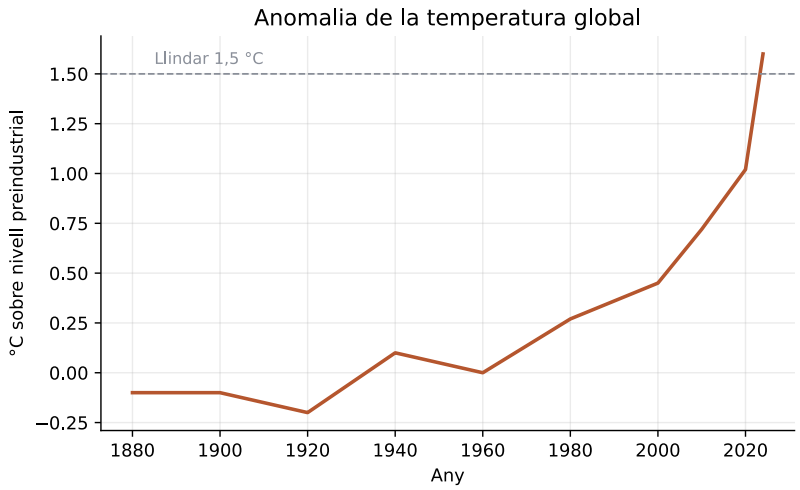


Figura 6.1 — L'escalfament global ha superat per primera vegada els +1,5 °C en un any natural (2024).

El pressupost de carboni

Aquell 43 % abans del 2030 i aquell 60 % abans del 2035 no són aspiracions idealistes: són el resultat d'una modelització rigorosa que integra milers de variables, des dels fluxos energètics fins a les dinàmiques socioeconòmiques. Són, literalment, el pressupost de carboni que ens queda per mantenir la temperatura mitjana mundial dins del límit d'1,5 °C. I el primer any natural per sobre d'aquest límit no és només una dada estadística: és el punt d'inflexió on la inacció es comença a pagar molt cara.

La distància entre aquest pressupost i la realitat actual és alarmant. Amb les emissions instal·lades en aquell màxim històric, cada any que passa sense una reducció substancial eixampla la bretxa entre les metes de l'IPCC i el camí que seguim realment. I cada fracció de grau addicional no només eleva el risc d'esdeveniments climàtics extrems, sinó que també incrementa els costos socials i econòmics associats: inundacions costaneres, sequeres prolongades i desplaçaments massius de població.

La solució, segons la ciència, és clara; la voluntat política, en canvi, mostra fissures. La manca d'urgència es tradueix en finançament insuficient per a projectes d'energia verda i en marcs reguladors febles, que no imposen penalitzacions efectives als agents que continuen depenent dels fòssils i deixen sense resposta el nucli del problema.

Tancar el bucle entre la ciència i l'acció demana un conjunt de mesures coordinades: (1) establir metes vinculants de reducció d'emissions a escala nacional, amb revisions periòdiques; (2) canalitzar fons internacionals cap a projectes d'energia renovable als països emergents, on el creixement econòmic encara depèn del petroli; (3) crear un preu del carboni que reflecteixi realment els costos ambientals i socials; (4)

impulsar la innovació en captura i emmagatzematge de carboni (CCS) i garantir alhora una transició justa per a les comunitats afectades. Només amb aquesta combinació d'ambició científica i compromís polític s'evitarà que l'avís de Roberts es converteixi en la crònica d'un error irreversible.

Les COP: paraules i fets

El desert de Dubai va vibrar el desembre de 2023 quan els delegats de la 28a Conferència de les Parts (COP28) van assolir, per primera vegada, un acord explícit per «transitar allunyant-se dels combustibles fòssils». La resolució establia com a objectiu triplicar la capacitat instal·lada d'energia renovable mundial i duplicar el ritme de millora de l'eficiència energètica abans del 2030 [3]. Aquell pas formal, celebrat com el «principi de la fi» de l'era dels combustibles fòssils, va obrir la porta a accelerar les inversions en tecnologies eòliques i fotovoltaiques, en la modernització de xarxes intel·ligents i en el desenvolupament de magatzems d'energia.

El ritme diplomàtic, però, es va alentir de seguida: la COP29, celebrada a Bakú el novembre de 2024, i la COP30, a Belém el novembre de 2025, van tancar les sessions sense esmentar els combustibles fòssils al text principal de les resolucions. La COP29 es va centrar en un nou objectiu de finançament climàtic; la COP30 va aprovar un full de ruta voluntari de transició amb el suport d'una coalició de més de 80 països; però en cap dels dos casos no es va incloure una menció directa a l'extracció o al consum de petroli, gas natural i carbó. Segons diversos observadors, aquesta omissió va ser el resultat d'una pressió coordinada dels petrostats per evitar una condemna internacional directa.

Aquestes batzegades diplomàtiques creen un buit entre les promeses polítiques i les mesures reals. Tot i la declaració de la COP28, les inversions en projectes fòssils van continuar creixent durant els anys posteriors, una contradicció que alimenta el dubte sobre la voluntat política real d'assolir les retallades que demana l'IPCC per al 2030 i el 2035 [2].

I aquest silenci té conseqüències més que simbòliques. Sense una menció clara, els països amb grans reserves d'hidrocarburs no es veuen obligats a presentar plans de desmantellament ni a establir mecanismes de justícia climàtica per a les comunitats afectades. Això dificulta la creació d'un marc regulador robust que pugui canalitzar finançament internacional cap a la captura i emmagatzematge de carboni o cap a programes de reconversió laboral per als treballadors del sector fòssil.

La COP28 va encendre una espurna d'esperança amb un acord clar i una meta renovable ambiciosa; les dues conferències següents han diluït aquest impuls amb una retòrica que evita anomenar els combustibles fòssils. Es parla de transició, però no es defineixen les condicions per abandonar realment el petroli i el gas. Perquè les paraules es converteixin en fets calen compromisos vinculants i transparents, amb un seguiment verificable i conseqüències per a qui es desvïi del camí. Sense això, la política climàtica continuarà parlant mentre el termòmetre s'enfila.

La promesa i el perill

La promesa és real: per primera vegada, en paraules, el món s'orienta cap a abandonar els combustibles fòssils, i les eines per fer-ho són cada cop més barates. El que fa només uns anys semblava una utopia és avui tecnològicament viable gràcies a dues revolucions convergents.

La primera: l'energia solar i l'eòlica han arribat a un cost de producció inferior al del carbó a la majoria dels mercats. Segons l'IRENA, el cost normalitzat de l'electricitat (LCOE) de la solar fotovoltaica a gran escala va ser de 0,043 $/kWh el 2024, una reducció d'aproximadament el 90 % respecte al 2010 [4]. Aquesta caiguda de costos ha permès que empreses i governs despleguin grans projectes sense necessitat d'ajudes massives. La segona: la blockchain s'utilitza ja per crear sistemes de certificació descentralitzats que verifiquen en temps real l'origen net de cada unitat d'electricitat, una capa d'autenticitat que redueix la necessitat d'auditories costoses i permet verificar de manera transparent el compliment de les quotes.

Malgrat aquest escenari prometedor, el perill persisteix amb una intensitat creixent. Les emissions, com hem vist, encara augmenten [1], impulsades en bona part per economies que depenen del petroli i el gas natural per al creixement industrial. A més, la voluntat política ha començat a vacil·lar: després de la COP30, diversos governs han retardat la publicació dels seus plans d'energia neta, al·legant incerteses econòmiques i la pressió del sector fòssil. Aquest retrocés no és només una qüestió de calendari; el cost de l'endarreriment es tradueix en dècades irrecuperables d'escalfament global, i cada any addicional d'inacció

augmenta la probabilitat de superar llindars cada cop més perillosos, amb conseqüències greus per a l'agricultura, la salut i la migració humana [1][3].

Les eines, doncs —energia renovable assequible i certificació blockchain transparent—, ja són accessibles; el veritable repte rau a traduir aquestes capacitats tècniques en accions polítiques fermes. La diferència entre una promesa escrita i un compromís executable es mesura en la capacitat de les institucions d'imposar conseqüències efectives a qui trenca les seves pròpies normes. Sense aquest marc de responsabilitat, el risc és que les emissions continuïn enfilant-se, que es consumeixin dècades d'avenços climàtics i que ens acostem irreversiblement al punt de no retorn. El futur del planeta depèn, ara més que mai, de la capacitat dels líders de transformar una promesa en una acció verificable i irreversible.

El termòmetre i la veritat

El termòmetre ha dictat sentència: aquell primer any natural per sobre dels +1,5 °C ja no és la hipòtesi llunyana que Roberts advertia, sinó la nostra realitat quotidiana. Les onades de calor extremes s'estenen des de l'Europa meridional fins al sud dels Estats Units; els incendis forestals, alimentats per vents més intensos i vegetació més seca, consumeixen àrees que fa una dècada encara eren boscos exuberants. Cada hora de producció aturada es tradueix en pèrdues quantioses, i els desplaçaments massius de poblacions costen vides i recursos a societats ja fràgils.

Però el més alarmant no és només la temperatura: també està en perill la confiança que fonamenta les nostres institucions. En un món on les imatges i els àudios es poden generar amb una precisió indistingible de la realitat, la capacitat d'identificar falsedats esdevé una necessitat vital. Actors estatals i no estatals ja han començat a fer servir deepfakes per desacreditar informes climàtics, manipular eleccions i minar la credibilitat dels científics que demanen mesures urgents. La crisi de la veritat es converteix així en una extensió directa del canvi climàtic: si el públic no pot confiar en les dades que demostren l'impacte real, la pressió política per actuar disminueix dràsticament.

Les promeses polítiques hi són —la transició proclamada a Dubai, les metes renovables per al 2030—, però encara no s'han traduït en accions verificables: la pressió dels petrostats va condicionar les dues COP següents, i el marc científic de l'IPCC AR6 continua sense una resposta política a l'altura. La disparitat entre el que la ciència demana i el que la política ofereix revela una zona d'incertesa on les decisions errònies poden ser fatals.

En aquest context, la veritat esdevé un recurs tan estratègic com l'energia. Les tecnologies de registre immutable basades en blockchain ofereixen una pista d'auditoria transparent per a les dades climàtiques: cada mesura d'emissió, cada inversió en renovables i cada certificació d'eficiència es pot verificar de manera independent, cosa que evita la manipulació i reforça la confiança pública. La intel·ligència artificial, al seu torn, pot analitzar grans volums de dades per detectar anomalies i predir tendències, però només si es manté una base de dades fiable.

La crida a l'acció, doncs, no és només reduir les emissions; és construir un ecosistema d'informació veraç que doni suport a les polítiques climàtiques. Hem revisat la màquina, l'oferta, les alternatives, el poder i el clima. Ara toca mirar les conseqüències d'avui —i una de nova que Roberts no podia imaginar: la crisi de la veritat. És la Part III.

---

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

[2] IPCC AR6 (via COP28 Global Stocktake), *retallades d'emissions 2030/2035.* https://www.iea.org/topics/cop28-tracking-the-energy-outcomes ↩

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

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

Donar a la gent el que vol: consum, eficiència i «menys és més»

«Un home és ric en proporció al nombre de coses que es pot permetre deixar estar.»

— Henry David Thoreau, Walden (1854)

A la cuina d'una família típica de Barcelona, l'horitzó està dominat per una constel·lació d'aparells electrònics que brillen com estrelles en una nit clara. Un televisor OLED de grans dimensions emet una llum suau mentre el pare segueix la partida de futbol en viu; al costat, la mare controla un assistent de veu que regula la temperatura del termòstat intel·ligent i activa el difusor de la rutina nocturna. A la taula, tres portàtils, dues tauletes i un telèfon plegable es mouen al ritme de missatges instantanis i videotrucades que viatgen per una xarxa 5G que mai no dorm.

Al pis superior, una habitació d'estudi alberga un conjunt de dispositius IoT: llums LED regulables per aplicació, sensors de presència que engeguen la calefacció només quan algú entra, i una petita instal·lació solar que alimenta el carregador del telèfon. Tot i aquest baluard d'energia renovable, la demanda continua creixent com un riu sense control: l'aire condicionat es posa a màxima potència per contrarestar una calor insistent; la rentadora s'activa a hores vall per aprofitar les tarifes més baixes, i el congelador de la cuina funciona tot el dia per mantenir els aliments frescos.

L'ambient està impregnat d'una sensació de satisfacció immediata: cada clic, cada comanda, cada «encès» és una resposta instantània al desig que la gent ha expressat durant dècades — tenir-ho tot a l'abast, sense esperar. Però aquesta escena, tan quotidiana i aparentment inofensiva, amaga un desequilibri profund. La demanda insaciable no només consumeix energia; crea una pressió constant sobre unes xarxes elèctriques que ja mostren signes de saturació.

Paul Roberts, a *The End of Oil* (2004), es preguntava: si la gent vol tot el que desitja, com podem canviar la corba? La resposta no és simplement oferir més energia neta; la veritable clau és reduir la quantitat que es necessita. La paradoxa de Jevons ens recorda que cada guany d'eficiència tendeix a ser devorat per un augment del consum, allò que anomenem l'efecte rebot [2]. Així, mentre les llums LED i els electrodomèstics intel·ligents prometen reduir la factura energètica, el fet de tenir més dispositius i una vida més connectada pot contrarestar aquests avantatges.

En aquesta casa plena d'innovació, l'enigma es converteix en un reflex del món: com podem transformar una cultura que celebra l'abundància immediata en una que abraça la suficiència? La resposta ha de sorgir d'una combinació d'eficiència tecnològica, polítiques que incentivin el consum responsable i una nova narrativa que valori «menys és més». Només així podrem començar a tallar la corba del desig infinit i avançar cap a un futur on l'energia neta sigui, de fet, la que no gastem.

L'energia que no gastem

El 2024, la millora del rendiment energètic global va dibuixar una corba gairebé plana. El número clau? Un increment de només **un per cent** respecte a l'any anterior, la meitat del ritme observat entre 2010 i 2019 [1]. Aquesta lentitud no és cap accident; reflecteix una realitat estructural: **el watt més barat i net és aquell que mai no es genera**.

Aquesta constatació, tan simple com profunda, converteix l'eficiència en el «primer combustible» de la transició energètica. No només es tracta de millorar les tecnologies — les bombetes LED, els motors d'altes prestacions o els algoritmes d'optimització basats en IA — sinó de reconèixer que cada unitat d'energia estalviada és una unitat que no ha de ser produïda, transportada i distribuïda. En aquest sentit, l'eficiència esdevé una forma directa de reduir les emissions sense necessitat d'invertir en noves fonts de generació, ni per tant en infraestructura costosa o en l'explotació de recursos naturals.

Però el camí cap a aquest escenari no és lineal. La **paradoxa de Jevons** — el fenomen en què els avenços en eficiència condueixen, paradoxalment, a un augment del consum total — continua planant com una ombra sobre les expectatives optimistes. Quan la tecnologia fa que l'electricitat sigui més barata, el cost marginal disminueix i apareixen nous usos: dispositius connectats incessants, aplicacions d'intel·ligència artificial que requereixen potència computacional massiva, o fins i tot una cultura de «compra i llença» que aprofita la percepció de recursos abundants. Aquest efecte rebot absorbeix part del guany obtingut per les millores tècniques, i es converteix en un obstacle invisible però potent [2].

La solució no resideix només en l'augment dels percentatges d'eficiència; cal una **sinergia entre tecnologia, política i comportament**. La COP28 va establir com a objectiu duplicar el ritme anual de millora de l'eficiència fins al 2030, un repte que requereix més que el simple avanç científic [1]. Calen polítiques que penalitzin l'excés i incentivin la suficiència: tarifes escalonades que augmenten amb el consum, crèdits fiscals per a edificis de baix consum i regulacions que limitin les pràctiques d'«obsolescència programada». A més, cal una narrativa que valori el «menys és més», i que transformi la percepció del benestar des d'una acumulació material cap a l'optimització dels recursos.

En aquest context, cada percentatge d'estalvi es converteix en un actiu estratègic. Un augment de l'1 % pot semblar modest, però si s'aplica de manera global i es complementa amb polítiques que impedeixen el rebot, els efectes acumulatius són significatius: menys necessitats de generació nova, reducció d'inversions en infraestructura fòssil i una disminució directa de les emissions de CO_2. Per tant, l'eficiència no és només una millora tècnica; és la base sobre la qual es construeix una economia energèticament sostenible.

El futur energètic més net depèn d'una regla senzilla però poderosa: **no gastarem energia que no necessitem**. Això implica impulsar l'eficiència a una velocitat superior al ritme actual i crear marcs reguladors i culturals que impedeixin que aquest guany es dissipi en nous consums. Només així podrem avançar cap a un model on el «primer combustible» sigui realment la no-producció d'energia, convertint l'estalvi en la nostra principal font de sostenibilitat.

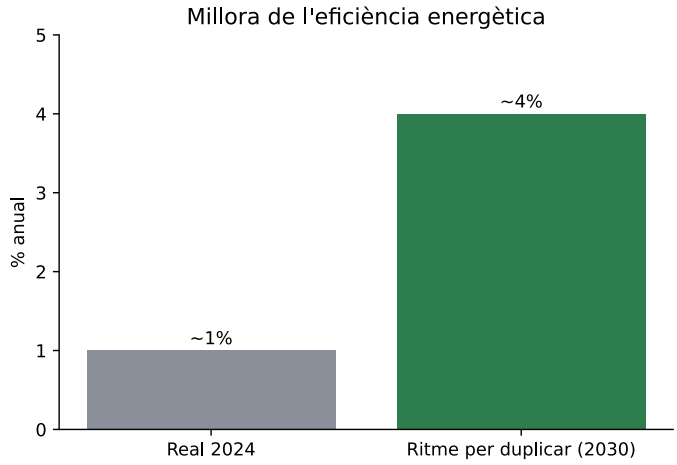


Figura 7.1 — La millora de l'eficiència (~1 % el 2024) va molt per sota del ritme necessari per duplicar-la cap al 2030.

El fre de Jevons

Imagineu un centre de dades que redueix el consum mitjà per metre quadrat gràcies a una nova arquitectura de refrigeració més intel·ligent. La notícia es difon com una prova contundent que la tecnologia pot trencar el llaç entre creixement econòmic i consum energètic, però només uns mesos després la facturació mostra un augment del volum total d'energia consumida pels mateixos centres, impulsat per una expansió simultània de serveis al núvol i per preus de l'electricitat més baixos, derivats precisament de la millora d'eficiència. Aquesta és la paradoxa que William Stanley Jevons descrigué al segle XIX: quan un recurs es fa més barat per mitjà de millores tecnològiques, el seu ús tendeix a augmentar en comptes de disminuir.

L'evidència contemporània ho confirma: la millora de l'eficiència es queda en aquell 1 % anual escàs [1]. La disminució del cost per unitat d'energia fa que tant les empreses com els consumidors percebin l'electricitat com un bé més assequible, i això afavoreix nous patrons de demanda. En el sector residencial, la proliferació d'aparells intel·ligents i l'adopció massiva de sistemes de calefacció i refrigeració d'alta eficiència han generat una «casa connectada» que consumeix més energia en total, tot i que cada dispositiu és individualment menys intensiu.

Aquesta dinàmica es veu reforçada per la manca de senyals de preu adequades. Quan el cost marginal de l'electricitat es manté artificialment baix —per exemple gràcies a subvencions o tarifes regulades— els consumidors no perceben el veritable cost ambiental del seu ús. La combinació d'eficiència i preus baixos crea un incentiu pervers: la reducció de costos operatius anima les empreses a expandir la seva capacitat productiva, mentre que les llars augmenten la quantitat d'aparells connectats sense una conscienciació clara del seu impacte energètic.

Per trencar aquest cercle viciós cal introduir un «fre de Jevons» mitjançant polítiques que alineïn el preu de l'energia amb el seu cost real i ambiental. Primer, establir tarifes dinàmiques basades en la demanda horària, de manera que els consumidors siguin penalitzats econòmicament per usar energia durant els pics de congestió; segon, implementar mecanismes de «suficiència» que limitin el creixement indiscriminat del consum: regulacions que estableixin límits màxims d'energia per equip o per habitatge i incentius fiscals per a la reducció voluntària del consum total.

A més, la transparència és clau. Les etiquetes energètiques han de mostrar no només l'estalvi per unitat, sinó també el potencial increment de demanda que pot derivar-se d'una tecnologia més eficient. Això ajudaria els consumidors a valorar realment les seves decisions i a evitar la temptació de «comprar més perquè costa menys». En conjunt, una combinació d'instruments de preu, límits reguladors i educació sobre el cost total del consum pot actuar com un fre efectiu contra l'efecte rebot, i convertir la millora d'eficiència en una veritable reducció neta d'energia utilitzada.

Només així podrem avançar cap a un model on «menys és més» deixi de ser una mera aspiració i esdevingui la base d'una transició energètica sostenible.

Menys és més?

A la plaça d'un mercat, un grup d'emprenedors locals ha instal·lat petites plaques solars que alimenten només els quioscs on venen fruites i verdures. La clau no és afegir més energia sinó reduir el consum a l'origen: dissenys modulars que s'adapten al flux real de clients, sense sobrecàrregues ni espais buits. Aquesta escena encarna la visió de Roberts sobre una demanda modelada per la suficiència i no pel creixement indefinit.

Aquell 1 % escàs de millora anual [1] és la pista que el simple perfeccionament tècnic no basta: cada guany d'eficiència tendeix a ser absorbit per un augment de l'ús, com descriu la paradoxa de Jevons —quan el cost marginal d'un recurs cau, el consum total sovint puja i anul·la part del benefici ambiental [2]. Per trencar aquest cercle cal una nova arquitectura de demanda que combini tres pilars.

Primer, la **suficiència**. No es tracta només de reduir les factures, sinó de replantejar quines necessitats són essencials. Les ciutats intel·ligents poden oferir serveis compartits —bicicletes elèctriques d'ús puntual, sistemes de refrigeració comunitària i calefacció de districte basada en energia renovable— que disminueixen la necessitat d'inversions individuals i, per tant, el consum global. Aquests models reparteixen entre molts usuaris uns recursos que abans cadascú duplicava pel seu compte.

Segon, el **disseny intel·ligent**. Els productes i les infraestructures han d'incorporar la mentalitat «menys és més» des del primer traç. Una arquitectura descentralitzada, basada en microxarxes i emmagatzematge local, pot minimitzar les pèrdues de transmissió i permetre un ús optimitzat segons les hores punta, sense necessitat d'incrementar la capacitat total del sistema. Aquest enfocament redueix directament l'energia requerida per moure informació i energia a través de xarxes extenses.

Tercer, l'**electrificació intel·ligent**, que combina sensors IoT amb algorismes d'aprenentatge automàtic per ajustar el subministrament en temps real. Un sistema de gestió energètica basat en IA pot reduir el consum d'il·luminació i climatització d'un edifici sense cap sacrifici per part dels usuaris, i evita la generació excessiva i el desaprofitament.

Finalment, el **canvi de comportament**. Les campanyes d'educació energètica han demostrat que quan les persones entenen el cost total del seu consum —no només el preu de la factura sinó l'impacte ambiental i social— adopten pràctiques més moderades. Els programes de retroalimentació en temps real sobre l'ús d'aigua i electricitat solen provocar una reducció mesurable del consum a les llars participants en pocs mesos.

Així, la cara de la demanda que Roberts intuïa es materialitza quan la tecnologia es combina amb polítiques que limiten els incentius al consum excessiu i promouen dissenys que maximitzen el valor per unitat d'energia. Només així «menys és més» deixarà de ser una aspiració utòpica i es convertirà en el fonament d'una transició energètica veritablement sostenible.

La promesa i el perill

En aquest marc, l'eficiència energètica és la palanca més barata i àgil que tenim a l'abast: cada punt percentual de reducció del consum suprimeix la necessitat d'inversions en infraestructura, minimitza les

emissions i allibera capital per a altres projectes de transició. Per això la COP28 va fixar l'objectiu de duplicar el ritme de millora abans del 2030 —el doble d'aquell 1 % escàs—, un salt que exigeix tant innovació tecnològica com marcs reguladors robustos i coherents [1].

Aquesta promesa de reduir el consum a través de millores tècniques ve empaquetada amb un perill persistent: la paradoxa de Jevons. Quan l'energia es fa més barata o més accessible, la tendència natural del comportament humà és augmentar-ne l'ús, una dinàmica que es manifesta en l'**efecte rebot** [2]. Això no només contraresta els guanys d'eficiència, sinó que pot generar un increment net de demanda superior a l'esperat. Un exemple clar són els dispositius intel·ligents a les llars: cada vegada més aparells connectats consumeixen energia constantment, i el consum total es manté o fins i tot augmenta malgrat les millores d'eficiència de cada unitat.

A aquest escenari s'hi suma una **inèrcia cultural del consum** que dificulta la transició cap a un model basat en la suficiència. Les campanyes publicitàries, els hàbits de compra i l'obsolescència programada creen una demanda incessant d'innovació productiva, fins i tot quan les necessitats reals són limitades. Sense una resposta política que reguli aquestes dinàmiques —per exemple, impostos sobre l'obsolescència, etiquetes energètiques obligatòries o incentius per al «dret a reparar»— els guanys tècnics es dilueixen en un cicle de creixement de demanda que desestabilitza qualsevol avanç net. La solució, per tant, no pot limitar-se a la sola millora del rendiment dels equips; cal una **estratègia integral** que combini eficiència, suficiència i política.

1. **Polítiques d'incentiu estructurades**, com ara tarifes escalonades basades en l'ús anual d'energia o subvencions per a la renovació de productes amb alta eficiència.
2. **Regulacions contra l'obsolescència programada**, que obliguin els fabricants a garantir una vida útil mínima i a facilitar el reciclatge i la reparació.
3. **Campanyes d'educació i canvi cultural** que promoguin la idea que «menys és més» i destaquin casos reals de consum responsable i estalvi econòmic.

Només quan aquestes tres dimensions convergeixin podrem transformar l'eficiència en una força neta, capaç de reduir realment el consum energètic sense ser engolida pel rebot. En aquest equilibri entre promesa i perill es troba la clau per a un futur on l'energia més neta sigui, efectivament, la que no gastem.

De la demanda a l'oferta

Si la demanda és part del problema, l'oferta institucional també ho és. Els grans grups energètics han construït una infraestructura que, per se, reforça el consum: centrals de gran escala, xarxes de transmissió costoses i models de negoci basats en la venda constant d'electricitat. Aquestes empreses, fins ara, defensaven que augmentar la capacitat productiva resol qualsevol escassetat percebuda, però el seu paper no es limita a subministrar energia; també modelen les expectatives dels consumidors i influeixen en les polítiques públiques.

Sovint l'expansió de la xarxa es justifica per garantir seguretat i fiabilitat quan una regió s'inclina cap a fonts renovables intermitents. No obstant això, sense reduir simultàniament el consum, aquestes inversions corren el risc d'augmentar el volum total d'electricitat consumida, a causa de l'efecte rebot que sovint acompanya la millora de l'eficiència [2].

Aquesta dinàmica es reflecteix també en les polítiques reguladores. Algunes normatives sobre mercats elèctrics estableixen mecanismes d'incentiu per a les grans companyies, com tarifes garantides i certificats verds, que premien la producció addicional més que l'optimització del consum. El resultat pot ser una «gran retirada verda» que només abandona parcialment les fonts fòssils sense reduir el total d'electricitat demanada, i que contravé la crida de la COP28 a duplicar el ritme anual de millora de l'eficiència [1].

Per trencar aquest cercle viciós cal que les grans energètiques adoptin una nova mentalitat: no només oferir energia més neta, sinó també reduir el volum total d'energia necessària. Això implica invertir en tecnologies de gestió de la demanda i en plataformes que permetin a consumidors i empreses intercanviar capacitat de manera descentralitzada i transparent, alineant els incentius econòmics amb objectius de suficiència; també requereix polítiques públiques que penalitzin el creixement descontrolat del consum i premiïn les pràctiques d'economia circular i d'autoproducció distribuïda.

En definitiva, la solució no és només millorar l'eficiència un punt percentual a l'any, sinó reconfigurar tot l'ecosistema energètic perquè l'oferta institucional es converteixi en un motor de reducció del consum i no en un impulsor d'aquest. Només quan eficiència, suficiència i política convergeixin podrem transformar la

promesa d'una energia més neta en una realitat tangible: que l'energia més neta sigui realment la que no gastem.

---

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

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

Les grans energètiques, ansioses

«No hi ha res més difícil de dur a terme, ni de més dubtós èxit, ni més perillós de gestionar, que iniciar un nou ordre de coses.»

— Nicolau Maquiavel, El Príncep, VI (1513)

Era una tarda d'estiu i la sala on se celebrava la junta d'accionistes es trobava plena d'una energia que recordava les campanyes de l'època del boom petrolier dels anys 2000. Aleshores, els fotògrafs de les revistes financeres capturaven executius amb somriures perfectament alineats; ara, el mateix escenari es convertia en un teatre d'ansietat i de decisió estratègica.

Al centre de l'escenari, la pantalla gegant mostrava el logotip d'una de les majors petroleres mundials —un símbol que havia dominat els mercats energètics durant dècades—. L'anunci era clar: «Reequilibrem la nostra estratègia». Aquell terme, tan neutre i gairebé poètic, amaga una realitat més crua. En lloc d'una transició cap a les energies renovables, el missatge es tradueix en un gir ferm cap al petroli i els seus derivats.

Quan el CEO —un home de mirada freda però amb la veu carregada d'optimisme— va pronunciar les seves paraules, l'audiència es va quedar immòbil durant uns segons, com si esperés una revelació inesperada. «Després d'un breu període d'experimentació verda», va dir, «hem decidit reforçar la nostra aposta pels actius fòssils per garantir el retorn dels nostres accionistes». El murmuri que va seguir es va transformar ràpidament en aplaudiments sincronitzats, una ovació que semblava més un acord col·lectiu de confiança financera que un reconeixement d'innovació.

Els inversors —principalment fons de pensions i gestors d'actius institucionals— van aixecar les mans, alguns amb fulletons que mostraven gràfics ascendents del preu del petroli i altres amb telèfons mòbils que anotaven immediatament els nous objectius de rendibilitat. En el seu entusiasme, es podia llegir la pressió incessant dels accionistes que exigeixen retalls en les despeses de projectes verds i una acceleració en la producció de cru.

Al mateix temps, el silenci era palpable a la taula on es trobaven els representants de les organitzacions climàtiques. Els portaveus d'ONG internacionals, que havien estat convidats com a testimonis per «mostrar compromís», van quedar-se amb la mirada fixa al terra, sense paraules per contrarestar l'anunci. El seu desconcert contrastava brutalment amb els crits d'aprovació del públic financer.

Els resultats financers recents reforçaven aquesta decisió: les empreses energètiques estatals del G20 havien invertit aproximadament 360.000 milions de dòlars en CAPEX el 2024, amb un 81 % destinat a projectes fòssils [1]. En paral·lel, BP havia retallat 5.000 milions de dòlars del seu pla baix en carboni i Shell havia frenat les seves inversions en renovables per pressió d'accionistes [2]. La proporció de diners públics destinats a fòssils era cinc vegades superior a la invertida en renovables, augmentant el risc d'actius varats [3].

Aquesta escena, plena d'aplaudiments i silenci simultanis, encapsula l'ansietat que s'ha apoderat de les grans energètiques: una aposta per tornar al petroli com a resposta a la pressió accionarial, tot sabent que el mercat global es mou cap a una economia baixa en carboni. La pregunta que queda suspesa en l'aire —i que ressonarà durant els propers anys— és si aquest «reequilibri» serà només un retrocés temporal o el preludi d'una nova era de desafiament per a la confiança del sector energètic.

El gir verd que va durar poc

El dubte no és nou. A principis del 2020, les grans majors energètiques van presentar un compromís ferm amb la transició cap a fonts netes, reduccions substancials d'emissions i una aposta clara per projectes renovables. Els informes anuals de BP, Shell i Eni mostraven mapes estratègics amb inversions multimilionàries en eòlic, solar i hidrogen verd, i els consells d'administració es van comprometre públicament a alinear-se amb els objectius del Pacte de París. Les expectatives dels analistes eren altíssimes; el mercat valorava aquestes declaracions com un senyal clar que les empreses deixaven enrere la dependència del petroli.

No obstant això, entre 2024 i 2025 aquest relat es va desfer amb la força d'una tempesta inesperada. La pressió dels accionistes —impulsada per resultats a curt termini i una demanda creixent de dividends més elevats— va fer que les directrius de transició quedessin en suspens. BP, per exemple, va materialitzar

aquella retallada de 5.000 milions del pla baix en carboni i va augmentar la despesa en fòssils [2]; al mateix temps, Shell va congelar bona part dels seus programes renovables i va posar en pausa iniciatives anunciades com a pilars de la seva nova estratègia empresarial. No eren simples ajustos operatius: era el retrocés d'un compromís que s'havia promocionat com a fonament del futur energètic.

La «gran retirada verda» s'ha convertit en una frase clau per descriure aquest gir inesperat. Com hem vist, les empreses energètiques estatals del G20 van destinar aproximadament 360.000 milions de dòlars a CAPEX el 2024, amb un 81 % d'aquests fons dirigits cap a projectes fòssils [1]; en el cas concret d'Eni, la inversió en petroli i gas va arribar a 6.900 milions d'euros, mentre que la destinada a energia neta es va quedar en només 764 milions d'euros, una proporció que revela la magnitud del desequilibri [1].

Aquesta reorientació no només posa en perill els objectius climàtics globals, sinó que crea un risc financer significatiu: l'augment de l'exposició a actius fòssils en un mercat que avança cap a una economia baixa en carboni eleva la probabilitat d'actius varats. Els diners públics ja es destinen cinc vegades més als fòssils que a les renovables, reforçant el desequilibri entre suport estatal i desenvolupament sostenible [3]. El repte, per tant, no és només tornar a les promeses verdes; cal abordar la tensió estructural entre els interessos accionarials i la necessitat urgent de descarbonitzar. Si les grans majors continuen prioritzant beneficis immediats sobre la sostenibilitat a llarg termini, el mercat energètic podria veure's sacsejat per una nova onada de crisi de confiança —un escenari que combina promesa i perill en igual mesura.

Els números no menteixen

Com hem vist, un any després dels discursos verds i les promeses d'energia neta, les xifres financeres del sector mostren una realitat molt més sobria. El 2024, les empreses estatals del G20 dedicades a l'energia van destinar aproximadament **360.000 milions de dòlars** al capital (capex), i un sorprenent **81 %** d'aquest pressupost es va canalitzar cap als projectes fòssils —pous de perforació, refinament i infraestructures per al transport del petroli i el gas natural— [1]. Aquesta proporció supera amb escreix les expectatives de transició verda plantejades fa cinc anys i contradiu els compromisos adoptats a la Conferència de les Parts (COP) i en les declaracions d'objectius Net-Zero.

Un exemple emblemàtic és **Eni**. En l'exercici 2024, va invertir **6.900 milions d'euros** en projectes relacionats amb el petroli i el gas, mentre que la partida destinada a les seves activitats netes —energia eòlica i solar— es va quedar en només **764 milions d'euros** [1]. Aquesta disparitat gairebé nou a un revela una aposta clara per mantenir i expandir l'ecosistema dels combustibles fòssils, tot i la pressió creixent d'inversors institucionals que demanen una reorientació cap a fonts més sostenibles.

La tendència no és exclusiva del sector privat; els fons públics segueixen el mateix camí. Les dades de finançament governamental mostren que les inversions públiques en energia fòssil són **cinc vegades superiors** a les destinades a projectes renovables [3]. Per cada euro invertit en solar o eòlic, cinc euros es destinen a noves plataformes petrolieres o a l'expansió de xarxes de gas. Aquest desequilibri perpetua la dependència de combustibles contaminants i incrementa el risc d'actius varats, ja que les tecnologies fòssils s'enfronten a regulacions més estrictes i a una demanda de mercat que gira cap a alternatives netes.

La pressió dels accionistes ha jugat un paper crucial en aquest gir. Ho demostren els recents retalls d'inversió de BP —**5.000 milions de dòlars** retirats del pla baix en carboni— i la frenada de les iniciatives renovables per part de Shell, impulsades per accionistes que temen una disminució dels dividends a curt termini [2]. Aquestes decisions reflecteixen un dilema clau: equilibrar els interessos financers immediats amb la necessitat d'una transició sostenible.

En conclusió, el panorama del 2024 deixa clar que **el capital segueix preferint els actius fòssils**. Tant les empreses estatals com les corporacions privades, i fins i tot els fons públics, continuen apostant per una infraestructura basada en petroli i gas, incrementant el risc d'actius varats i posant en dubte la capacitat del sector per complir amb els objectius climàtics a llarg termini. La pregunta que emergeix ara és com revertir aquest desequilibri abans que les conseqüències econòmiques i ambientals siguin irreversibles.

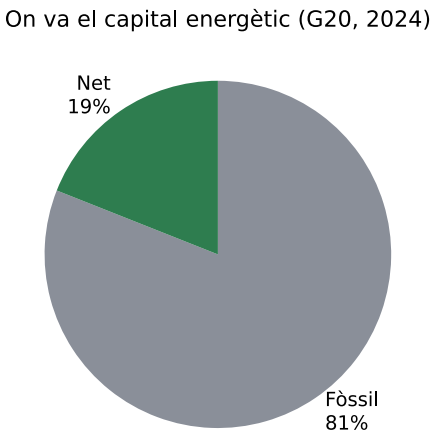


Figura 8.1 — Malgrat la retòrica verda, el 81% de la inversió de les energètiques estatals del G20 encara va a combustibles fòssils (2024).

La trampa dels actius varats

En aquest escenari, les grans petrolieres continuen destinant una part cada cop més gran del seu capital a projectes de perforació i refinament; el que semblava una resposta immediata a la pressió d'accionistes es revela com una paradoxa estructural.

Com hem vist, el 2024 les empreses energètiques del G20 van canalitzar la majoria del seu CAPEX cap a projectes fòssils, i això crea una exposició significativa a actius varats [1].

Aquesta dinàmica és alimentada per la pressió directa dels accionistes, que temen perdre rendiments a curt termini i han obligat companyies com BP a retallar milers de milions del pla de reducció d'emissions i Shell a frenar els seus projectes renovables [2]; l'exemple d'Eni il·lustra clarament la desproporció entre les inversions en actius fòssils i les destinades a energia neta.

Els diners públics reforcen el desequilibri, ja que les inversions estatals en projectes fòssils són cinc vegades superiors a les destinades a renovables [3]; aquest flux de capital dirigeix la competència cap a tecnologies al límit de la seva vida útil econòmica i genera un efecte dominó d'actius potencialment obsolets.

En resum, el que avui es percep com una maniobra prudent —doblar l'aposta pels fòssils per satisfer les expectatives dels accionistes— és, en realitat, una bomba de rellotgeria que amenaça la salut financera del sector. La clau és canviar la narrativa: de «preservar el valor actual» a «transitar cap a un model sostenible que garanteixi rendibilitat a llarg termini».

La promesa i el perill

...perduts, posant en risc tant els retorns dels inversors com la viabilitat d'una transició climàtica urgent. La clau per evitar aquesta trampa resideix a canviar la narrativa: de «preservar el valor actual» a «transitar cap a un model sostenible que garanteixi rendibilitat a llarg termini».

Les grans energètiques disposen d'un arsenal de recursos que cap startup o govern regional podria igualar: milers de milions en capital disponible, xarxes d'enginyeria refinada durant dècades i una infraestructura global de transport d'hidrocarburs. Aquesta base massiva els confereix un potencial transformador únic; si decidissin redirigir les seves inversions cap a tecnologies netes, podrien accelerar la descarbonització en una escala que les polítiques públiques només somien. Com hem vist, el grup de companyies estatals del G20 va destinar un CAPEX d'uns 360.000 milions de dòlars el 2024, amb un 81 % encara dedicat a projectes fòssils [1].

No obstant això, la mateixa magnitud que ofereix aquesta promesa es converteix també en un perill estructural. Els accionistes —majoritàriament institucions financeres i fons de pensions— segueixen prioritzant el retorn a curt termini, ja que els actius fòssils encara generen rendiments superiors al cost del capital. La pressió és palpable: BP ha retallat 5.000 milions de dòlars del seu pla baix en carboni, mentre Shell ha frenat les seves inversions renovables per satisfer les expectatives dels seus accionistes [2]. Aquest

comportament no només perpetua la dependència de combustibles fòssils, sinó que també atrapa capital públic i privat en projectes cada vegada més arriscats d'acabar com a actius varats. Les dades mostren que els diners públics invertits en sectors fòssils són cinc vegades superiors als destinats a renovables [3]; aquest desequilibri alimenta una espiral de risc financer i ambiental.

Per trencar aquest cercle viciós cal reconfigurar els mecanismes d'incentiu. Les polítiques públiques haurien d'alinear-se amb els objectius corporatius, introduint taxes de carboni que penalitzin l'excés de fòssils i oferint crèdits fiscals robustos per a projectes renovables; alhora, fons de pensions i institucions financeres han de revaluar el seu criteri d'avaluació del risc, incorporant la probabilitat d'actius varats com a factor clau. Només quan aquest marc de rendició de comptes es consolidi les grans energètiques podran canalitzar capital i enginyeria cap a una transició veritable, convertint el seu poder estructural en motor de canvi més que en fre per al futur sostenible.

Una veu inesperada a la sala de juntes

Tal com s'ha assenyalat anteriorment, la intel·ligència artificial esdevé una veu inesperada que ressona entre les sales de juntes on els consells directius revisen balanços i pressions accionarials. No és una mera eina d'optimització operativa; és un catalitzador que pot girar l'eix de les decisions estratègiques cap a una nova orientació energètica.

En primer lloc, els algoritmes predictius ja poden ajudar les grans petroleres a mapar amb precisió la probabilitat d'actius varats. Mitjançant models que integren dades climàtiques, reguladores i de mercat, es pot quantificar el risc de quedar atrapades en infraestructures fossilitzades que perdran valor tan aviat com la transició s'acceleri. Això ofereix una resposta directa al problema exposat a la secció anterior: incorporar el factor d'actius varats en els criteris d'avaluació del risc.

En segon lloc, la IA pot accelerar la transició cap a les renovables no només identificant oportunitats d'inversió, sinó també optimitzant la gestió de recursos distribuïts i xarxes intel·ligents. L'aprenentatge automàtic permet equilibrar la producció solar i eòlica amb la demanda en temps real, reduint costos operatius i pèrdues a la xarxa. Aquest tipus d'aplicació demostra com la tecnologia pot transformar una empresa tradicional en un proveïdor d'energia més àgil i resilient.

No obstant això, la promesa de la IA ve acompanyada d'un perill igual de substancial. La mateixa capacitat analítica que permet predir actius varats també pot ser explotada per manipuladors de mercat o per actors estatals que busquin maximitzar beneficis curts en detriment de la seguretat energètica global. Així, el risc de «caixa negra» esdevé una nova forma d'opacitat: decisions clau delegades a sistemes opacs que poden amagar conflictes d'interès o errors sistèmics.

A més, la concentració de dades i poder computacional en mans de poques corporacions —en gran mesura les mateixes grans energètiques— pot reforçar el seu control sobre l'ecosistema energètic, perpetuant la dinàmica de «fre». La pressió d'accionistes que ja ha conduït a una retirada de fons cap als fòssils [2] podria trobar un nou impuls si la IA es converteix en una arma per maximitzar rendiments a curt termini, ignorant externalitats socials i ambientals.

La solució, com sempre, rau en l'equilibri entre oportunitat i vigilància. Les empreses han d'establir marcs de governança robustos que garanteixin transparència algorítmica, auditoria independent i una alineació clara amb objectius climàtics verificables. La IA hauria de ser un motor que impulsi la transició veritable, no una nova capa d'opacitat que amagui les seves pròpies limitacions.

En resum, la intel·ligència artificial ofereix una doble cara: pot convertir el risc d'actius varats en una brúixola per a decisions més responsables i, alhora, crear noves formes de vulnerabilitat si es deixa sense control. La pregunta que queda per respondre és quina de les dues forces predominarà. La resposta no depèn només de la tecnologia, sinó del marc de rendició de comptes que les grans energètiques estiguin disposades a adoptar. Si aquest marc s'enforteix, la IA pot ser el motor d'una transició veritable; si es manté en l'ombra, es convertirà en un nou fre per al futur 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 nova tensió: la IA com a salvació i com a set d'energia

«El món del futur serà una lluita cada cop més exigent contra les limitacions de la nostra intel·ligència, no una hamaca còmoda on jeure esperant que ens serveixin els nostres esclaus robots.»

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

En el cor d'un gran campus tecnològic, una enorme sala de servidors s'alça com un bosc mecànic de cables, llums LED i ventiladors que brunzeixen incessantment. Les parets són de metall gris, recobertes per panells d'alumini que reflecteixen la llum freda del dia i el blau tènue de les pantalles de monitoratge. Cada rack és una torre on els LED parpellegen en seqüències rítmiques, indicant la temperatura interna, el consum instantani i l'estat de cada node de càlcul, i crea una simfonia industrial que sembla no tenir pausa.

Al mateix edifici, però en un laboratori adjacent, una pantalla tàctil mostra un gràfic dinàmic: la potència consumida pels servidors baixa i puja com les ones d'un mar digital. A sobre, un sistema d'intel·ligència artificial analitza en temps real milers de variables —temperatura ambient, flux d'aire, càrrega computacional, preus del mercat energètic i prediccions meteorològiques—. Cada segon, el sistema ajusta els paràmetres dels ventiladors, redirigeix les tasques més intensives cap a nodes que operen en condicions òptimes i fins i tot activa o desactiva grups de servidors per equilibrar la demanda.

El moment clau arriba quan una alerta es dispara: un pic inesperat d'activitat a causa d'una consulta massiva d'IA generativa. En lloc d'augmentar indiscriminadament el consum, el sistema reconfigura instantàniament la topologia de refrigeració, i redueix la velocitat dels ventiladors en els racks menys sobrecarregats i incrementa l'eficiència del flux d'aire cap als punts crítics. En pocs segons, el gràfic mostra una caiguda de la potència consumida, tot mantenint les temperatures dins del rang de seguretat.

Aquesta escena és un microcosmos de la paradoxa que defineix el 2026: la mateixa màquina que necessita energia per aprendre i processar dades es converteix també en l'arquitecte d'una gestió més neta i racionalitzada. El soroll dels ventiladors, que abans era només un senyal del cost energètic, ara es transforma en el so de l'optimització —una melodia que indica que la IA no sols consumeix energia, sinó que aprèn a minimitzar-la. És una imatge potent: un cervell artificial que, amb cada ajust, talla les seves pròpies cadenes d'alimentació per tal de viure en un ecosistema més sostenible.

Mentre els servidors continuen brunzint dia i nit, la pantalla mostra una nova línia al gràfic: «energia neta prevista». És un recordatori visual que el futur no depèn només del volum de càlcul, sinó de com aquest càlcul s'integra amb les fonts d'energia renovable. La paradoxa es converteix en oportunitat —un punt de bifurcació on la IA pot ser tant la causa del consum descontrolat com el motor d'una transició energètica neta. Aquesta dualitat, capturada en una sola sala de servidors, marca l'inici d'un debat crucial: com assegurar que la intel·ligència artificial sigui realment una salvació i no una set insaciable d'energia?

L'accelerador

En aquest context de doble cara, DeepMind ha aconseguit reduir un 40 % l'energia dedicada a la refrigeració dels centres de dades de Google, una millora equivalent a una caiguda del 15 % en el PUE (Power Usage Effectiveness), i ara assumeix directament el control de la refrigeració amb algoritmes d'aprenentatge automàtic. Aquest èxit no és només una victòria operativa; és la prova viva que la intel·ligència artificial pot actuar com a palanca per reduir el consum energètic de les infraestructures més intensives del món.

La sinergia entre Google, PJM i Tapestry ha portat aquesta mateixa lògica a escala nacional. Mitjançant models d'IA que analitzen la demanda i l'oferta d'electricitat als Estats Units, s'està modernitzant la gestió de la xarxa elèctrica, equilibrant fonts variables com l'eòlica i la solar amb una precisió abans impensable. Connectar nous generadors, anticipar la congestió i assignar la càrrega de forma més intel·ligent permet integrar millor la generació renovable i aprofitar millor la xarxa existent, i ha reduït la necessitat de centrals de reserva costoses i contaminants.

Més enllà de l'optimització operativa, la IA s'està convertint en una eina de descoberta científica. Els models d'aprenentatge automàtic acceleren la cerca de nous materials per a bateries d'alta densitat energètica, i han reduït el temps de recerca que abans es comptava en anys. Aquest avanç no només

promet vehicles elèctrics més eficients; també ofereix solucions d'emmagatzematge per a les xarxes renovables que, sense una bateria fiable, es veuen limitades pel seu caràcter intermitent.

A la vegada, els models climàtics basats en IA han arribat a un nou nivell de resolució. Combinant dades de satèl·lit amb aprenentatge profund, els equips d'investigació poden simular escenaris amb un detall que abans era inabastable. Aquest grau de precisió permet als planificadors urbans i als gestors de recursos hídrics prendre decisions informades sobre infraestructures resilients, i ha reduït els costos socials i ha evitat desastres ambientals.

La conjunció d'aquestes aplicacions demostra que la IA no és només un consumidor voraç d'energia; és una força multiplicadora de l'eficiència energètica. Cada grau centígrad que es redueix en els centres de dades, cada punt guanyat en la integració renovable i cada millora en l'emmagatzematge en bateries representa un pas cap a un futur on el cost ambiental de la computació esdevé marginal. No obstant això, aquest potencial només es materialitzarà si les polítiques energètiques reconeixen aquestes sinergies i els donen suport, amb inversió en infraestructures intel·ligents i en recerca d'energia neta que alimenti els cervells digitals de demà.

La set d'energia

Els centres de dades són els monstres invisibles que alimenten la revolució de la intel·ligència artificial. El seu consum elèctric, ja impressionant, es troba a punt d'explotar en una escala que supera les fronteres nacionals. Segons les projeccions més recents, l'energia total que absorbeixen aquests hubs digitals passarà d'aproximadament **485 TWh** el 2025 a **~950 TWh** el 2030 —gairebé la mateixa quantitat que consumeix tot el Japó— i s'estendrà fins a uns **~1.200 TWh** el 2035 [2]. Aquesta escalada no és un simple increment de demanda; representa una nova forma de pressió sobre les xarxes elèctriques globals, una tensió que podria desestabilitzar els esforços per a la descarbonització si no es gestiona amb cura.

En aquest context, l'eina que hauria d'actuar com a motor d'estalvi energètic –la IA mateixa– es converteix en una paradoxa. Per entrenar models cada vegada més sofisticats i oferir serveis en temps real, les infraestructures digitals necessiten energia colossal, sovint provinent de fonts encara no completament netes. Cada iteració d'un gran model de llenguatge demana una enorme quantitat d'energia només per al seu entrenament inicial; el cost energètic dels processos d'inferència continuada i de l'actualització constant de pesos pot equivaler al d'una petita ciutat industrial.

DeepMind ha aconseguit reduir un 40 % l'energia necessària per a la refrigeració dels seus centres de dades, una millora que es tradueix en una caiguda del 15 % del **PUE** (Power Usage Effectiveness) i ara controla directament [1]; com ja s'ha assenyalat, aquesta reducció és només una gota dins d'un oceà que s'amplia a ritmes exponencials. La modernització de les xarxes elèctriques amb IA –com la col·laboració entre Google, PJM i Tapestry per optimitzar la distribució i l'assignació de càrrega– és un pas imprescindible, però només pot ser efectiva si es combina amb una font d'energia neta i abundant.

La qüestió clau, doncs, no és només reduir el consum per unitat de càlcul, sinó assegurar que la suma total d'energia requerida provingui de fonts renovables. Això implica una inversió massiva en infraestructura intel·ligent: bateries avançades, microxarxes i sistemes de gestió dinàmica que puguin respondre a les fluctuacions de demanda de forma instantània. Sense aquest marc, la IA podria convertir-se en la nova «set d'energia» del planeta, un consumidor voraç que absorbeix recursos escassos i posa en perill els objectius climàtics establerts per al 2030.

Per tant, la decisió que ha de prendre la comunitat global –governs, empreses tecnològiques i inversors– és clara: canalitzar les polítiques energètiques cap a una sinergia entre IA i energia neta, com hem vist. Això no només garantirà que els avenços en intel·ligència artificial siguin sostenibles, sinó que convertirà la IA en un aliat per a la transició verda, més que en un obstacle energètic. En aquest equilibri delicat es troba una de les decisions més crucials del decenni.

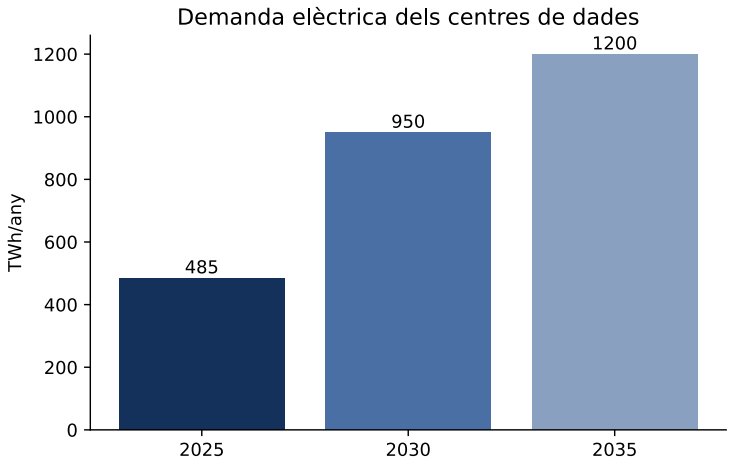


Figura 9.1 — El consum elèctric dels centres de dades es duplica cap al 2030 (~950 TWh), impulsat per la IA.

Resoldre la paradoxa

Així, la solució no consisteix a aturar el desenvolupament de la intel·ligència artificial, sinó a alimentar-la amb energia neta i transparent. En un món on els centres de dades són cada vegada més grans i intensius, l'estratègia clau passa per situar aquestes instal·lacions a prop d'orígens renovables —parcs eòlics, camps fotovoltaics o centrals hidroelèctriques— i aprofitar la flexibilitat intrínseca dels processos d'entrenament i inferència per equilibrar la demanda amb l'oferta variable de la xarxa. Aquesta sinergia es tradueix en tres pilars operatius.

Primer, la **localització intel·ligent**. Les empreses tecnològiques ja estan desplegant centres de dades a zones on el cost marginal de l'electricitat renovable és mínim. Situar la computació a prop de grans parcs solars o d'eòlica offshore connectada directament a instal·lacions d'alta densitat redueix les pèrdues de transmissió i permet aprofitar l'energia neta al mateix punt on es genera, en lloc de transportar-la a llargues distàncies.

Segon, la **demanda flexible**. La IA pot ser programada per realitzar tasques intensives durant períodes de superàvit renovable —les hores de més sol o de vent més fort— i reduir el consum en moments de dèficit. DeepMind ha demostrat que aquest enfocament no només minimitza l'impacte ambiental, sinó que també optimitza els costos operatius: la companyia va aconseguir una reducció del 40 % en energia dedicada a la refrigeració dels seus centres de dades, i això es va traduir en una caiguda del 15 % del PUE (Power Usage Effectiveness) [1]. Aquesta capacitat de «carregar» la IA amb energia neta es converteix, per tant, en un pagament indirecte: l'algoritme contribueix a la transició verda reduint la necessitat de fonts fòssils i, al mateix temps, beneficia el seu propi cost d'execució.

Tercer, la **transparència del consum**. Exigir que les empreses publiquin informes detallats sobre la procedència i l'eficiència energètica dels seus centres de dades és una demanda cada vegada més forta per part dels reguladors i els inversors. L'establiment d'estàndards comuns que permetin comparar i validar les pràctiques sostenibles a escala mundial crea un mercat de confiança on la IA es converteix en una garantia de credibilitat ambiental, no només en un consumidor voraç.

Com hem vist, el consum dels centres de dades va camí de duplicar-se en cinc anys, i de continuar creixent després [2]. Sense una resposta coordinada, la IA amenaçaria d'esdevenir un emissor net de carboni que contraresta els guanys climàtics assolits per les energies renovables; però si es converteix en un motor que impulsi la pròpia transició —optimitzant xarxes, predint fallades i maximitzant l'ús d'energia neta— la IA pagaria amb escreix la seva factura energètica i convertiria el risc en una oportunitat. Ara calen polítiques coherents, inversió en infraestructura renovable i un compromís ferm de transparència que permetin a la intel·ligència artificial ser tant la salvació com el motor d'una economia neta i resilient.

La promesa i el perill

Imagina una sala de control on milers de servidors flueixen com un riu d'electricitat líquida i, al centre, una ment artificial que recalcula la ruta òptima per a cada bit. Aquesta és la promesa de la IA: optimitzar el funcionament d'una xarxa global augmentant-ne l'eficiència energètica gràcies a algoritmes

d'aprenentatge automàtic que prioritzen fonts renovables i minimitzen les pèrdues. En la fabricació, els models generatius ajusten la composició dels materials amb una precisió que abans requeriria anys de proves; en l'agricultura, la IA prediu microclimes locals i regula el reg en temps real, evitant el malbaratament d'aigua i reduint les emissions a escala regional. Aquestes millores es tradueixen en una disminució directa de la demanda energètica global: cada gigawatt-hora estalviat és un pas més cap al compliment dels objectius de l'Acord de París.

No obstant això, si s'alimenta d'una infraestructura bruta i poc transparent, aquesta potència es converteix en el nou motor d'un consum energètic descontrolat. Els grans models de llenguatge requereixen centres de dades amb la fam elèctrica que ja hem quantificat [2]. Sense un marc regulador que imposi límits d'emissions i exigeixi certificacions de carboni per a cada operació d'entrenament, la IA podria actuar com una coartada per a empreses que, en lloc d'invertir en renovables, simplement augmenten el seu consum per mantenir la competitivitat. Això intensifica la pressió sobre les xarxes elèctriques i crea un incentiu pervers: més IA, més necessitat d'energia, i una justificació per retardar polítiques climàtiques crítiques.

Aquesta dualitat es manifesta també en la gestió de dades. Una IA que optimitza la distribució de càrrega a través de xarxes intel·ligents pot reduir el PUE (Power Usage Effectiveness) d'un centre de dades, com ha demostrat DeepMind amb una millora del 40 % en l'energia de refrigeració, equivalent a una caiguda del 15 % del PUE [1]. Però, si aquesta optimització es manté dins d'una «caixa negra», les empreses poden amagar el creixement exponencial del consum energètic sota la capa d'eficiència aparent, dificultant la supervisió pública i impedint que els reguladors apliquin mesures correctives en temps real.

La clau per transformar aquesta tensió resideix en tres pilars interdependents: transparència, responsabilitat i alineació amb fonts netes. Primer, les organitzacions han d'obrir les seves eines d'optimització energètica, permetent auditories independents que verifiquin l'impacte real davant les declaracions de millora. Segon, cal establir marcs legals que obliguin a reportar el consum total d'energia per cada model entrenat i operat, amb penalitzacions per excedir els límits preestablerts. Finalment, les inversions en infraestructura renovable —des de bateries avançades fins a microxarxes solars i eòliques— han d'estar vinculades directament al creixement computacional: cada nou increment de capacitat de càlcul ha d'anar acompanyat d'una capacitat equivalent d'energia neta.

En resum, la IA pot ser el motor que impulsi una transició energètica més ràpida i eficient; però només si es governa amb rigor i es connecta intrínsecament a fonts netes. Sense aquestes garanties, la mateixa intel·ligència artificial podria convertir-se en l'últim gran consumidor d'energia, retardant les decisions climàtiques que el 2026 ja no es poden permetre posposar.

L'altra set

En el silenci fred d'un centre de dades, una veu sintètica va explicar amb la mateixa convicció que un jutge experimentat per què el canvi climàtic era només una llegenda urbana. Aquell fragment, generat en menys d'una hora per un model de llenguatge entrenat sobre milers de milions de textos, es va difondre a les xarxes socials i, en qüestió de minuts, va ser citat com a prova definitiva d'un escàndol mediambiental fabricat. Aquest és el reflex més sobtat de la tercera dimensió de la intel·ligència artificial: no només consumeix energia, sinó que també pot consumir-nos la capacitat de discernir la realitat.

La crisi de la veritat es presenta com una amenaça transversal que travessa sectors, des de l'energia fins a la salut i la seguretat nacional. Quan un algoritme engendra imatges, àudios i textos indistingibles de les creacions humanes, el cost de verificar cada afirmació augmenta exponencialment. La demanda d'eines de rastreig de fonts i de verificació de continguts ha crescut amb força, impulsada per start-ups especialitzades en aprenentatge automàtic i en l'ancoratge de proves. Aquest augment no és només una oportunitat de negoci; és un senyal d'alarma que indica com el consum energètic de les xarxes de verificació es converteix en un altre nus del problema.

Al mateix temps, les grans corporacions de núvol, conscients del seu paper clau, han començat a integrar mecanismes per registrar i validar la procedència de cada contingut. Google, amb l'ajuda de DeepMind, ha reduït l'energia de refrigeració dels seus centres de dades un 40 % —una caiguda del 15 % en el PUE— i ara intenta aplicar aquesta mateixa eficiència a les cadenes de verificació de contingut; però encara es troba davant d'un desafiament: com garantir que la infraestructura energètica que sustenta aquests processos sigui neta? Si el cost energètic d'una veritat certificada supera la producció neta d'energia renovable disponible, ens enfrontarem a una paradoxa on la solució tecnològica es converteix en l'origen del problema.

La resposta no pot ser només tècnica; ha de ser institucional i cultural. Primer, les polítiques públiques han d'establir estàndards mínims d'eficiència energètica per a sistemes d'IA que generin contingut públic. Segon, les empreses han d'adoptar una arquitectura on cada model es dissenyi tenint com a primer requisit la compatibilitat amb fonts renovables i el balanç energètic net. Finalment, els ciutadans han d'estar equipats amb eines d'alfabetització digital que els permetin reconèixer deepfakes i desinformació generada per IA, una inversió en capital humà tan crucial com qualsevol instal·lació solar.

En resum, la crisi de la veritat és el nou front on es disputa el futur energètic. Si no aconseguim alinear la potència computacional de la IA amb una infraestructura neta i transparent, correm el risc que les mentides generades per màquines eclipsin les solucions reals a la crisi climàtica. El moment d'actuar és ara: establir regles clares, impulsar innovacions sostenibles i educar la societat perquè la veritat no es converteixi en un recurs escàs sinó en el fonament sobre el qual construir una transició energètica veritable.

---

[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 crisi de la veritat: desinformació i deepfakes

«El partit et deia que rebutgessis l'evidència dels teus ulls i les teves orelles. Era la seva ordre final, la més essencial.»

— George Orwell, 1984 (1949)

En una sala austera d'un tribunal francès, el 2025, els magistrats van pronunciar una sentència que semblava una espurna de llum enmig d'una guerra desigual per la veritat. Davant d'un públic reduït —advocats, periodistes i un grup escàs d'activistes climàtics— es va llegir el veredicte contra TotalEnergies, la gegant petroliera que durant anys havia construït una narrativa de «carboni neutral» al voltant dels seus projectes d'energia renovable.

El tribunal va declarar que el missatge publicitari era enganyós i constituïa una forma de greenwashing que vulnerava la confiança del consumidor i distorsionava les polítiques públiques de transició energètica. Quan una empresa proclama neutralitat de carboni sense proves verificables i sense compensar les emissions reals, es converteix en un actor que alimenta la desinformació fòssil.

L'audiència va sentir com una petita però significativa victòria ressonava entre les parets de la sala. Un grup d'activistes es va aixecar i va aplaudir en silenci. Els advocats de TotalEnergies, visiblement sorpresos, van intentar argumentar que la companyia havia invertit en projectes d'energia eòlica i solar, però el tribunal va rebutjar aquesta defensa com una compensació simbòlicament insuficient.

Aquesta sentència no només marcava un precedent legal a Europa; era un senyal clar que la societat ja no toleraria les promeses buides. La decisió es va basar en l'anàlisi d'informes independents que demostraven que el terme «neutral» no es corresponia amb les emissions reals de l'empresa.

Aquesta petita victòria, tan singular i limitada com una gota d'aigua en un oceà de mentides, esdevé el primer pas d'una lluita que s'estén més enllà del sector energètic. Enfrontar-se al greenwashing és essencial per restaurar la confiança col·lectiva i permetre que les polítiques climàtiques siguin guiades per dades reals i no per narratives fabricades. La decisió de 2025, tot i ser un esdeveniment puntual, simbolitza el potencial d'un sistema judicial que pot frenar l'erosió de la veritat compartida —una erosió que, si es deixa sense resposta, paralitzaria la governança necessària per a la transició energètica.

Dècades d'enginyeria del dubte

A finals de la dècada dels setanta, mentre les primeres alertes científiques sobre el canvi climàtic emergien en revistes especialitzades, una altra conversa s'estava teixint a les sales de conferència de les grans companyies petrolieres. No era només un assaig d'informació; era un projecte deliberat per sembrar incertesa i diluir la responsabilitat. L'American Petroleum Institute (API) va formalitzar aquesta estratègia en un memoràndum intern de 1998 que declarava amb una claredat freda: «la victòria s'assoleix quan el ciutadà mitjà reconeix incerteses en la ciència climàtica» [1]. Aquell document no només reflectia una percepció de l'opinió pública com a obstacle, sinó que la convertia en un objectiu estratègic.

Aquesta «enginyeria del dubte» es va desplegar amb les mateixes tècniques que una campanya publicitària: selecció interessada d'estudis científics, promoció de veus escèptiques i finançament de grups de pressió que posaven en dubte l'existència o la gravetat del fenomen. Els resultats van ser immediats i profunds. Durant els anys noranta i la dècada de 2000, el debat públic es va transformar d'una discussió basada en evidències a una arena on les opinions s'alineaven amb interessos econòmics. Les xarxes socials encara no existien; la difusió es feia per mitjans tradicionals, però l'impacte era igual de devastador: un segment creixent del públic començava a percebre el canvi climàtic com una qüestió incerta i polititzada.

A mesura que les generacions posteriors van créixer amb aquesta narrativa fragmentada, la confiança col·lectiva en la ciència es va erosionar. El resultat és una opinió pública fracturada, on els consensos científics són vistos com a punts de partida per a disputes ideològiques més que com a fites inqüestionables. Aquesta fractura no només ha retardat les polítiques climàtiques; ha creat un ambient en el qual qualsevol proposta d'acció es troba amb una resistència preexistent, alimentada per la memòria col·lectiva del «dubte» sembrat fa més de tres dècades.

L'herència d'aquestes pràctiques es manifesta avui en formes noves però reconeixibles: les campanyes de greenwashing que presenten productes i serveis com a sostenibles sense fonament real, i els deepfakes que manipulen la informació visual i auditiva amb una precisió que supera el que mai s'havia imaginat. Però el

fil conductor és el mateix: una estratègia per desestabilitzar la veritat compartida i crear espais on les narratives de poder puguin prosperar sense ser qüestionades.

En aquest context, l'absència d'una matèria primera sòlida no només impedeix que les polítiques climàtiques siguin adoptades; amenaça el teixit mateix de la governança democràtica. Sense una veritat consensuada, els processos de decisió es converteixen en jocs d'informació, on el guanyador és qui controla la percepció, no qui ofereix les solucions més eficients. La desinformació, llavors, deixa de ser un simple subproducte del debat i esdevé una arma estructural que paralitza l'acceleració necessària cap a una transició energètica justa i sostenible.

Aquesta herència d'enginyeria del dubte és el punt de partida per comprendre com la crisi de la veritat ha arribat al seu pic actual, i per explorar les eines —com la prova d'existència que es desenvoluparà en la Part IV— que podrien restaurar la confiança i permetre una governança basada en fets reals.

El greenwashing, a judici

El 2025 va marcar un punt d'inflexió en la lluita contra el rentat verd: per primera vegada les sancions econòmiques es van convertir en testimonis públics que l'engany ambiental ja no podia quedar impune. Shein, la icònica marca de moda ràpida, va rebre una multa d'**1,15 milions d'euros** per haver promocionat les seves col·leccions com a «eco-friendly» mentre el seu model de negoci continuava depenent de teixits sintètics de gran impacte climàtic. Al mateix temps, un **tribunal francès** va condemnar **TotalEnergies** per presentar com a enganyós el seu missatge de «carboni neutral», una decisió que ha encès un debat sobre la responsabilitat legal de les grans empreses energètiques en l'era de la transparència digital.

Potser més impactant va ser el cas del gestor d'actius **DWS**, multat amb **25 milions d'euros** per exagerar les seves credencials ESG i vendre productes financers com a «verds» quan, en realitat, no responien a aquestes promeses. Aquest escàndol no només va sacsejar els mercats de capital, sinó que també va posar en relleu la fragilitat del marc regulador existent: les declaracions ESG, sovint basades en auditories internes i certificacions de tercers, es van revelar vulnerables a manipulacions sofisticades.

En resposta, la **relatora especial de les Nacions Unides** ha reclamat una mesura que ha generat un clam internacional: criminalitzar la desinformació i el greenwashing de la indústria fòssil. La seva posició sosté que l'engany mediambiental no és només una infracció administrativa, sinó una amenaça directa a la confiança pública i a la voluntat política necessàries per a l'acció climàtica [2].

Aquesta resposta jurídica, però, encara corre darrere del ritme al qual es generen les noves formes de manipulació. Les empreses, ara més conscients dels riscos legals, recorren a la intel·ligència artificial per crear narratives «verdes» que semblen creïbles i, alhora, són difícils de desmuntar sense una prova robusta. Els algoritmes poden generar informes ESG enganyosos en qüestió de minuts, i les plataformes socials amplifiquen aquests missatges amb l'ajuda de comptes automatitzats que imiten veus autèntiques.

Així, mentre el dret comença a reaccionar amb sancions i propostes legislatives, el fenomen del greenwashing evoluciona cap a formes més sofisticades i difuses. La necessitat de mecanismes verificables —com la prova d'existència que es desenvoluparà en la Part IV— esdevé urgent: només una capa de confiança basada en dades inalterables pot contrarestar l'onada de desinformació ambiental que, com el fum de les centrals de carbó, amaga la veritat i paralitza la governança necessària per a una transició energètica justa.

En aquest escenari, la lluita contra el rentat verd no és només un assumpte de multes; és una batalla per preservar la credibilitat del discurs climàtic i garantir que les polítiques públiques es fonamentin en fets verificables, no en promeses enganyoses. La resposta jurídica ha d'anar acompanyada d'eines tecnològiques que assegurin la traçabilitat i la veracitat de cada afirmació ambiental, perquè només així podrem restaurar la confiança col·lectiva i avançar cap a una societat basada en la veritat compartida.

Les deepfakes industrialitzen la mentida

En els darrers dos anys, la IA generativa ha transformat el que abans era una curiositat acadèmica en un instrument de producció massiva d'engany. El nombre de deepfakes creats a escala mundial ha esclatat de **~500.000** l'any 2023 a **8 milions** el 2025, una taxa de creixement que supera qualsevol evolució tecnològica recent en la història digital [3]. Aquesta explosió no és un simple increment numèric; és la

manifestació d'una nova economia de la falsedat on les imatges i els àudios es poden fabricar a petita escala amb recursos mínims, però també a gran escala per part d'entitats organitzades.

Europol ha alertat que, si aquesta tendència continua, **fins al 90 % del contingut en línia podria ser sintètic el 2026** [3]. Aquesta projecció no només representa una xifra alarmant; és un indici clar que la confiança per defecte —el supòsit que el que veiem a internet reflecteix la realitat— està arribant al seu punt de ruptura. Quan qualsevol fotografia, vídeo o declaració pot ser generada artificialment amb una qualitat quasi indistingible del material autèntic, el fil conductor que sosté les relacions socials i polítiques es desintegra.

Les conseqüències d'aquest fenomen són múltiples i interdependents. En primer lloc, la **credibilitat de les institucions** queda en joc. Una declaració oficial manipulada pot difondre's com a prova irrefutable d'un error o una mala intenció, alimentant el cinisme ciutadà i minvant l'autoritat dels governs. En segon lloc, els mercats financers es veuen vulnerables a **campanyes de desinformació** que poden manipular preus d'accions amb vídeos falsos d'executius o informes falsificats sobre resultats empresarials. Finalment, la **seguretat nacional** queda exposada: les deepfakes poden ser utilitzades per crear falses declaracions d'estat, provocar crisis diplomàtiques o incitar a l'odi i al conflicte.

Aquesta nova era de mentida industrial no és una mera extensió del greenwashing tradicional. Mentre que el primer es basa en la manipulació de dades ambientals per millorar la imatge corporativa —com demostren els escàndols de Shein, TotalEnergies i DWS— les deepfakes operen a un nivell més visceral: alteren la percepció directa del que és real. Això crea una **barrera cognitiva** que impedeix als ciutadans distingir entre informació fiable i engany, augmentant la polarització i reduint l'espai per al diàleg constructiu.

Per combatre aquesta amenaça cal adoptar una doble estratègia: **tecnològica i normativa**. Des d'un punt de vista tecnològic, les solucions que ancoren l'origen i la integritat dels continguts digitals —com el marc «t2p» que desenvoluparem a la Part IV— ofereixen una pista per verificar la procedència del que veiem. Des del punt de vista normatiu, cal establir marcs legals que penalitzin la creació i difusió malintencionada de deepfakes, tal com ja s'ha començat a fer amb el greenwashing sancionat el 2025 [2].

En síntesi, la industrialització de les mentides a través de les deepfakes representa un **punt crític** per a la confiança col·lectiva. Si no es prenen mesures decisives ara, la societat podria entrar en una era en què la veritat compartida deixa d'existir i les decisions polítiques es basen únicament en percepcions manipulades. El repte és gran, però la combinació de tecnologia verificable i regulació rigorosa ofereix un camí viable per restaurar la fe en el que veiem i escoltem.

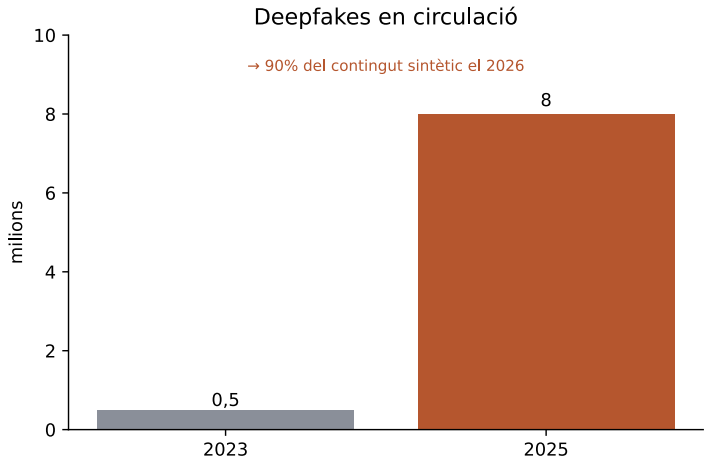


Figura 10.1 — Les deepfakes es multipliquen: de ~500.000 (2023) a 8 milions (2025), camí del 90% del contingut en línia el 2026.

Per què això mata la transició

En una era en què les polítiques climàtiques es mesuren en dècimes de grau i en tones d'emissions evitades, la confiança en les dades és el combustible invisible que impulsa la descarbonització. Sense fonts fiables, qualsevol objectiu es converteix en un miratge: els inversors no poden validar si una planta solar produeix realment l'energia anunciada; els reguladors desconeixen si les declaracions d'emissions d'una

empresa petroquímica són autèntiques o manipulades; i la ciutadania, que ha de suportar les decisions públiques, es troba davant d'un laberint d'informació incerta.

El problema s'intensifica quan el falsificador no només altera dades numèriques, sinó que fabrica narratives visuals senceres. Un vídeo d'una instal·lació eòlica amb turbines girant majestuosament sobre la costa pot sortir d'una IA sense cap connexió amb una infraestructura real. Quan les imatges i els sons són tan fàcils de fabricar com hem quantificat, el criteri tradicional «veure és creure» s'esvaeix.

Aquesta erosió de confiança té repercussions immediates en el mercat dels capitals verds. El greenwashing ha arribat a un punt d'inflexió: només l'any 2025, empreses com Shein (multada amb 1,15 milions d'euros) i TotalEnergies (condemnada per un tribunal francès pel seu missatge de «carboni neutral») van ser sancionades, i DWS va pagar 25 milions d'euros per exagerar les seves credencials ESG [2]. La relatora de l'ONU ha demanat que aquestes conductes es criminalitzin, reconeixent que el frau ambiental no només enganya els inversors, sinó que distorsiona les polítiques climàtiques globals.

A més, la crisi de veritat afecta directament les metes establertes en acords internacionals. Un memoràndum de l'American Petroleum Institute de 1998 ja advertia que «la victòria s'assoleix quan el ciutadà mitjà reconeix incerteses en la ciència climàtica» [1]; avui aquesta incertesa és artificial. Si les emissions declarades són manipulades, els informes d'avançament cap a la neutralitat de carboni es converteixen en simples documents de màrqueting, i els reguladors, sense eines per verificar l'autenticitat, es veuen obligats a basar-se en declaracions tan falses com un vídeo generat per IA.

En resum, la incapacitat d'identificar dades fiables paralitza qualsevol esforç de descarbonització creïble. La transició depèn d'una cadena de confiança: des del laboratori on es mesura el CO_2 fins al consell d'administració que aprova un projecte d'energia renovable. Quan aquesta cadena es trenca per la desinformació i els deepfakes, les decisions polítiques es basen en percepcions manipulades i la societat corre el risc de quedar atrapada en una espiral de dubte i inacció. La solució no és només tècnica; requereix un marc regulador rigorós i tecnologies verificables que restaurin la fe en el que veiem i escoltem.

La promesa i el perill

En aquest moment històric som testimonis d'una doble explosió d'incerteses: la crisi climàtica que ja es mesura en graus i milions de morts evitables, i una erosió accelerada de la veritat compartida que transforma cada dada en un possible engany. La **promesa** és clara i sense precedents: per primera vegada disposem d'eines capaces de detectar, desemmascarar i validar la informació a escala global, obrint el camí perquè la societat pugui recuperar la confiança en les seves pròpies percepcions.

Les tecnologies emergents —algoritmes de detecció de manipulacions, sistemes de certificació de l'origen del contingut i plataformes d'auditoria oberta que integren proves criptogràfiques— comencen a oferir vies per rastrejar cada peça d'informació fins a la seva font original, creant una capa de transparència que abans era impensable. Aquestes solucions es converteixen en els pilars del futur **t2p**, el marc que la Part IV desenvoluparà per contrarestar l'onada de desinformació.

No obstant això, el **perill** que s'amaga darrere d'aquesta oportunitat és tan real com les incerteses climàtiques que intentem mitigar. Si no actuem amb urgència i rigor regulador, la crisi de la veritat alimentarà una retroalimentació negativa amb la crisi climàtica: una població cada cop més desconfiada refusarà acceptar dades científiques, retardant polítiques essencials com la descarbonització del sector energètic. Les xifres que hem vist —vuit milions de deepfakes i un internet camí de ser majoritàriament sintètic— dibuixen una saturació de falsedats on les decisions polítiques es prenen sobre bases manipulades, i deixen la societat atrapada en una espiral de dubte i inacció.

A més, el fenomen del **greenwashing** s'ha convertit en un veritable risc reputacional i legal: empreses com Shein han pagat **1,15 milions d'euros** per sancions relacionades amb declaracions enganyoses sobre sostenibilitat [2]; TotalEnergies ha estat condemnada per un tribunal francès pel seu missatge de «carboni neutral», i DWS ha estat multada amb **25 milions d'euros** per exagerar les seves credencials ESG. La relatora especial de les Nacions Unides ja ha demanat la criminalització d'aquestes pràctiques, subratllant el risc d'una regulació ineficaç si no es reconeix la dimensió tecnològica del problema.

En resum, la **promesa** resideix en la capacitat de les noves eines per restaurar la confiança i establir un nou contracte social basat en proves verificables; el **perill**, si deixem que la desinformació continuï proliferant sense una resposta coordinada, és que la crisi climàtica es vegi encara més obstaculitzada,

conduint a una paràlisi global on ni les polítiques ni les accions individuals podran avançar. La decisió clau està davant nostre: invertir ara en infraestructures de verificació i en un marc legal robust, o veure com ambdues crisis es reforcen mútuament fins al punt d'un bloqueig irreversible.

A més d'allunyar-nos de les falsedats visibles, hem d'enfrontar el que Beth Noveck anomena el «dividend del mentider»: la capacitat de les deepfakes no només crea enganys, sinó que ofereix una defensa fàcil per a qui vol esborrar dades incòmodes: descartar-les com a simples «muntatges d'IA» [4]. Aquest escenari transforma el fals en un instrument de negació estructural; qualsevol informe científic que adverteixi sobre l'escalfament global podria ser reduït a una invenció digital i quedar sense pes davant del públic. Per trencar aquest cercle cal una àncora neutral —un registre criptogràfic immutable que demostri que un fet real va existir abans de ser manipulat—, més enllà dels sistemes de detecció o de les marques d'aigua com C2PA. La prova d'existència basada en blockchain, independent del creador i sense dependre de tercers, ofereix exactament aquest punt d'arribada: no pretén detectar el fals: certifica l'autenticitat de l'original, i impedeix que la veritat es pugui descartar com una simple il·lusió. El robocall clonat de Joe Biden del gener de 2024, sancionat per la FCC amb una alerta contra les trucades automàtiques, exemplifica com una prova d'existència neutral hauria permès contrastar-ne l'origen i frenar-ne la difusió incontrolada [5].

El doble diagnòstic

Hem diagnosticat el doble problema: energia i veritat. La crisi climàtica ja no és només una qüestió de fonts d'energia o de polítiques de descarbonització; ara es troba paral·lelament amb un col·lapse de la veritat compartida, alimentat per la desinformació fòssil, el greenwashing i els deepfakes. Aquesta erosió de la confiança pública paralitza la governança que la transició energètica necessita per avançar. Sense una base comuna d'informació fiable, les decisions col·lectives es converteixen en un joc d'atzar on les narratives manipulades guanyen protagonisme sobre les dades reals.

Els indicis són innegables: el memoràndum de l'American Petroleum Institute de 1998 ja advertia que «la victòria s'assoleix quan el ciutadà mitjà reconeix incerteses en la ciència climàtica» [1]. Avui, aquestes incerteses es converteixen en una inundació deliberada d'informació falsa. El greenwashing ha passat de ser un simple recurs de màrqueting a una amenaça legal: el 2025, Shein va ser multada amb 1,15 milions d'euros per pràctiques enganyoses; TotalEnergies va ser condemnada per un tribunal francès; i DWS va pagar 25 milions d'euros per exagerar les seves credencials ESG [2]. La relatora de l'ONU ja demana que es criminalitzi aquest comportament, reconeixent el seu impacte devastador sobre la confiança del mercat i la voluntat política.

Paral·lelament, la fàbrica de deepfakes s'ha disparat fins als volums que obrien aquest capítol [3]. Aquesta realitat no només desorienta l'opinió pública: compromet la seguretat nacional, els processos judicials i les negociacions internacionals.

La resposta ha de ser tan doble com el problema: hem d'invertir ara en infraestructures de verificació robustes i establir marcs legals que penalitzin la manipulació deliberada. És aquí on la Part IV del llibre ofereix una via de sortida concreta. La intel·ligència artificial, combinada amb la blockchain, pot crear un registre immutable d'origen i autenticitat, una prova d'existència (t2p) que permetrà validar informació en temps real i fer front als deepfakes amb evidències verificables.

En aquest context, la nostra crida a l'acció és clara: **actuar ara**. Les empreses, els governs i la societat civil han d'adoptar sistemes de certificació transparents i auditables; han de promoure legislacions que defineixin sancions severes per al greenwashing i la difusió deliberada de falsedats; i han d'invertir en educació mediàtica avançada per capacitar els ciutadans a reconèixer i rebutjar el contingut manipulat.

Com hem vist, no podem permetre que les dues crisis es reforcin mútuament fins al punt d'un bloqueig irreversible. La veritat és el combustible de la confiança, i la confiança és l'engranatge que farà girar la roda de la transició energètica. Amb les eines adequades —IA, blockchain i una regulació decidida— podem restaurar aquesta base essencial i transformar la crisi en una oportunitat per a un futur més resilient i transparent. El moment d'actuar és ara; el futur depèn de la nostra capacitat de reconstruir la veritat 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] Nacions Unides, *Greenwashing*. https://www.un.org/en/climatechange/science/climate-issues/greenwashing ↩

[3] (deepfakes) Blockchain Council / Europol — vegeu 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 ↩

Seguretat energètica reinventada: xarxes intel·ligents i IA

«En el petroli, la seguretat i la certesa rauen en la varietat, i només en la varietat.»

— Winston Churchill, Cambra dels Comuns (1913)

Era una tarda freda d'octubre de 2028 quan el nucli de la central nuclear de Three Mile Island, que durant dècades havia simbolitzat el pitjor accident nuclear de la història nord-americana, va tornar a vibrar. Els monitors de control mostraven un flux constant d'electrons nets: 837 MW d'electricitat emergien de la Unitat 1 rehabilitada per Microsoft i Constellation, alimentant una constel·lació de centres de dades que processaven models d'intel·ligència artificial per a la gestió global de la xarxa elèctrica.

Els treballadors del projecte, reunits davant de les grans portes d'acer, observaven com els gràfics de potència s'alçaven en una corba suau però implacable. «Això no és només un retorn a l'activitat», deia el sentiment compartit a la sala de control, «és la prova que la seguretat energètica del futur es mesura en electrons fiables, no en barrils».

Mentre les turbines es posaven en marxa, una pantalla mostrava el logotip de Microsoft juntament amb el de Helion, recordant al món que la fusió nuclear —encara en fase experimental— era l'objectiu del seu acord de subministrament per al 2028 [2]. Una altra pantalla recordava el reactor modular de 500 MW que Google havia encarregat a Kairos Power, amb la primera unitat programada per entrar en funcionament l'any 2030 [2]. La mateixa pantalla anunciava que DeepMind havia reduït un 40 % el consum energètic de refrigeració dels centres de dades de Google, una eficiència que es tradueix directament en menys demanda sobre la infraestructura física i, per tant, en més marge per a fonts renovables [1].

A l'exterior, els camps verds on abans s'estenien les estructures d'emmagatzematge de combustibles fòssils ara eren recoberts de panells solars i turbines eòliques que, sincronitzades amb algoritmes predictius desenvolupats per Google, PJM i Tapestry, equilibraven la càrrega en temps real, evitant els pics que tradicionalment provocaven falles de subministrament [1].

El soroll habitual d'una central nuclear —el brunzit constant dels sistemes de seguretat, les alarmes de pressió— havia estat reemplaçat per una melodia quasi musical: el xiuxiueig dels servidors que optimitzaven la distribució d'energia i el suau murmuri de les turbines modernitzades. L'atmosfera era de confiança renovada; cada electró que travessava les línies es comptava com a testimoni d'una nova era en què la intel·ligència artificial no només predeia la demanda, sinó que també n'assegurava el lliurament sense interrupcions ni vulnerabilitats.

Aquell moment marcà un punt d'inflexió en la narrativa de la seguretat energètica: ja no es tractava de controlar el petroli, sinó de crear una xarxa resilient i intel·ligent capaç d'autosostenir-se i adaptar-se a les necessitats del món digital. La reactivació de Three Mile Island no era només un retorn al passat industrial; era la confirmació que la confiança en l'energia es pot reconstruir sobre ciments digitals, on cada dada, cada model d'IA i cada registre criptogràfic contribueixen a garantir que el futur sigui alimentat per electrons nets i fiables.

De la seguretat del petroli a la seguretat elèctrica

Quan Paul Roberts, periodista i analista d'energia, abordava la seguretat energètica a *The End of Oil* (2004), el terme «seguretat» s'embolcallava d'una imatge clara: controlar els fluxos de petroli, protegint les rutes marítimes i les infraestructures de refineria. Avui, el 2026, la trama ha canviat radicalment; la clau ja no és la reserva de cru, sinó la capacitat de mantenir una xarxa elèctrica neta, abundant i resilient davant d'una demanda creixent impulsada per la intel·ligència artificial.

Aquesta nova vulnerabilitat es manifesta en diverses dimensions interrelacionades. Primer, la dependència creixent de fonts renovables —solar i eòlica— afegeix una variabilitat natural que fa que la xarxa sigui més sensible a les fluctuacions climàtiques i, per tant, requereixi una gestió dinàmica en temps real. Segon, la proliferació de centres de dades i equips d'IA posa pressió directa sobre les infraestructures de transmissió: ja representaven al voltant del 2 % de l'electricitat mundial el 2022, xifra que es podria duplicar cap al 2026 [2]. Tercer, l'aparició de capes digitals per a la certificació de l'energia introdueix una dimensió criptogràfica que, si bé reforça la traçabilitat, també crea nous vectors d'atac cibernètic.

Les solucions emergents són tan innovadores com controvertides. DeepMind ha demostrat que l'optimització basada en IA pot reduir el consum energètic dels centres de dades de manera significativa gràcies a una millor regulació de la refrigeració, i aquest model s'està estenent a les xarxes de distribució pública [1]. A més, projectes col·laboratius com Google-PJM-Tapestry modernitzen la infraestructura nord-americana amb algoritmes predictius que anticipen els pics de demanda i redistribueixen fluxos en fraccions de segon, minimitzant talls inesperats [1].

Paral·lelament, el renéixer del nuclear —ara en forma de reactors modulars petits (SMR) i de fusió experimental— ofereix una font d'electricitat estable i d'alt rendiment. Google i Kairos Power estan construint un SMR de 500 MW amb la primera unitat prevista per al 2030, com hem vist; Microsoft i Constellation han posat en marxa la reactivació de la Unitat 1 de Three Mile Island, amb una capacitat de 837 MW també citada anteriorment [2]. A més, la col·laboració entre Microsoft i Helion apunta a la fusió nuclear com a objectiu per al 2028, prometent una energia neta i quasi inesgotable que podria alimentar directament les grans xarxes d'IA sense augmentar les emissions [2].

Aquesta convergència —IA per a l'optimització de la xarxa i nuclear avançat com a font constant— crea un ecosistema on la seguretat elèctrica es mesura tant en disponibilitat com en la capacitat de detectar i neutralitzar amenaces cibernètiques en temps real. Cada registre que certifica l'origen d'un quilowatt és alhora una prova criptogràfica contra manipulacions i fraus, mentre els models predictius anticipen falles potencials abans que es produeixin.

El repte del 2026 no consisteix a protegir un recurs finit com el petroli, sinó a garantir una infraestructura digital-energètica tan adaptable com la IA que la consumeix. La vulnerabilitat ja no és el combustible en si mateix, sinó la xarxa que el transporta i el processa; només a través d'una sinergia entre intel·ligència artificial i tecnologies nuclears avançades podem construir una seguretat energètica realment resilient per al futur.

Xarxes intel·ligents i IA

En un laboratori de Google a Mountain View, una sala freda que abans servia per mantenir en marxa milers de servidors ara vibra amb el murmuri de les xarxes neuronals de DeepMind. L'equip va reduir la necessitat de refrigeració un 40 % optimitzant els fluxos d'energia dels seus centres mitjançant algoritmes predictius que anticipen els pics de càrrega i redistribueixen la potència cap a zones menys congestionades [1]; com hem vist, aquest èxit no és una curiositat acadèmica sinó la prova viva que la intel·ligència artificial pot actuar com el sistema nerviós d'una xarxa energètica, detectant, processant i reaccionant a senyals en temps real amb una precisió que cap infraestructura tradicional ha pogut oferir.

Aquesta nova arquitectura es consolida als Estats Units, on Google, PJM (l'operador independent del mercat elèctric que coordina la regió del mig-Atlàntic) i Tapestry han llançat un projecte col·lectiu per modernitzar la xarxa nacional. L'objectiu és integrar una proporció creixent d'energia renovable —eòlica offshore, solar fotovoltaica de gran escala— sense sacrificar la fiabilitat. La IA gestiona la demanda flexible: aprèn dels patrons de consum residencial i industrial, ajusta les tarifes en temps real i activa o desactiva càrregues no crítiques segons la disponibilitat d'energia neta; així, una fàbrica que produeix components per a vehicles elèctrics pot reduir temporalment la seva producció quan els vents són febles, mentre un parc de bateries comunitàries emmagatzema l'excés d'energia eòlica i el descarrega durant les hores punta.

El model de control distribuït es fonamenta en una xarxa de sensors IoT que recullen dades sobre temperatura, fluxos de corrent, condicions meteorològiques i estat dels equips. Cada node processa localment la informació amb microalgoritmes d'aprenentatge per prendre decisions immediates, mentre un nucli central d'IA optimitza l'estratègia global. Aquest enfocament híbrid ofereix una resposta quasi instantània davant incidents inesperats: si una subestació es veu afectada per una tempesta, la IA recalcula les rutes de flux i redirigeix l'electricitat a través de línies alternatives en qüestió de segons, evitant apagades massives.

Com hem vist, la reducció del consum per refrigeració disminueix directament les emissions de CO_2 i, aplicada a la gestió de la xarxa, multiplica aquest estalvi a escala de tot el sistema elèctric [1]. A més, la capacitat de coordinar generació intermitent i emmagatzematge en temps real redueix la dependència dels combustibles fòssils i reforça la seguretat energètica: les xarxes es tornen menys vulnerables a interrupcions externes, ja que el seu funcionament depèn de processos autònoms i adaptatius més que d'infraestructures rígides.

Així, la IA no només monitora; actua com un cervell distribuït que aprèn constantment del comportament del sistema i s'ajusta per maximitzar l'eficiència i la resiliència. La combinació de dades massives, algoritmes avançats i infraestructura digital convergents redefineix la seguretat energètica: ja no es tracta només de garantir el subministrament d'un recurs escàs, sinó d'orquestrar una xarxa intel·ligent capaç d'autosostenir-se davant els reptes del futur. La visió de Roberts sobre l'energia com a vulnerabilitat ha evolucionat; ara la clau és construir aquesta sinergia entre IA i energia neta per assegurar un món on la confiança en el subministrament sigui tan robusta com les pròpies xarxes que la sustenten [1].

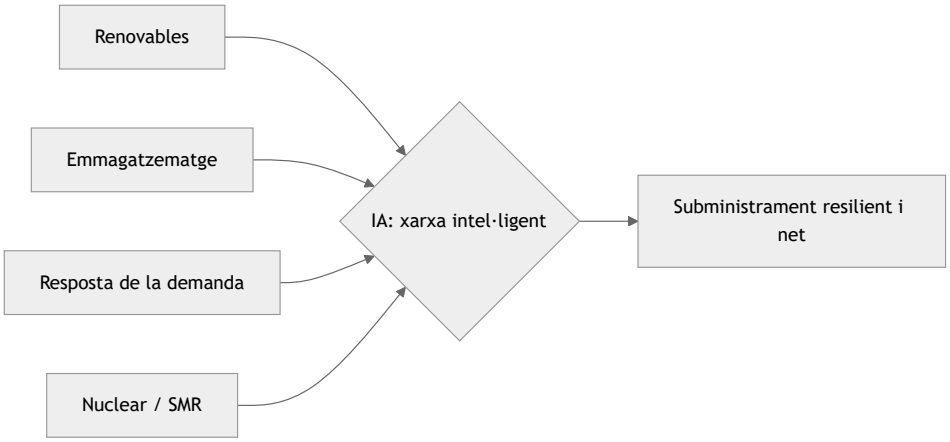


Figura 11.1 — La IA orquestra renovables, emmagatzematge, resposta de la demanda i nou nuclear en una xarxa resilient.

El retorn (controvertit) del nuclear

L'octubre de 2024 Google va encarregar a Kairos Power una flota de reactors modulars petits de 500 MW, amb la primera unitat prevista per operar abans del 2030; és la prova que la IA no només consumeix energia, sinó que la dirigeix cap a fonts netes i constants [2].

Microsoft i Constellation reactivaran la Unitat 1 de Three Mile Island, que originalment aportava 837 MW, amb tecnologia de control avançat per tornar a generar electricitat el 2028, mostrant que l'estabilitat de les xarxes intel·ligents depèn d'una font ininterrompuda i exempta de carboni [2].

A l'Ontario, OPG va obtenir l'aprovació l'abril de 2025 per construir un reactor GE Hitachi BWRX-300, amb entrada en operació prevista per al 2029 —una de les primeres aprovacions d'aquest tipus a Occident [2]. Paral·lelament, Microsoft i Helion van signar un acord perquè, cap al 2028, un reactor de fusió comenci a aportar energia a la xarxa i alimenti centres de dades dedicats a l'entrenament de grans models d'IA, oferint un cicle energètic totalment net i quasi il·limitat [2].

Aquestes iniciatives, tot i ser controvertides, revelen una lògica clara. La IA, amb la capacitat de predir i equilibrar les demandes energètiques en fraccions de segon, necessita una infraestructura que pugui garantir una producció constant i sense emissions. Els SMR ofereixen modularitat, seguretat intrínseca i un temps d'instal·lació reduït respecte als reactors tradicionals; la fusió promet una font quasi inesgotable amb residus mínims. En aquest context, les xarxes intel·ligents es converteixen en l'ànima de la nova arquitectura energètica: algoritmes que anticipen pics de demanda, redistribueixen càrregues i optimitzen el rendiment dels reactors per minimitzar pèrdues i maximitzar l'eficiència operativa.

No obstant això, l'aposta no està exempta de riscos. La concentració d'infraestructura crítica en mans d'un nombre limitat d'empreses tecnològiques pot crear nous punts vulnerables a ciberamenaces o pressions polítiques. A més, l'acceptació pública del nuclear continua sent un obstacle cultural i regulador que requereix una comunicació transparent i basada en dades verificades. La promesa d'«energia ferma i sense carboni a qualsevol preu» ha d'anar acompanyada d'una gestió responsable dels residus nuclears, de protocols de seguretat rigorosos i d'un marc normatiu que garanteixi la confiança global.

En definitiva, el retorn del nuclear es presenta com una resposta pragmàtica a les necessitats energètiques de la IA. És una aposta que combina l'esperit visionari de Don Tapscott, coautor de *Blockchain Revolution* —una solució ancorada en dades i casos reals— amb la consciència dels perills inherents, obrint un camí cap a xarxes elèctriques més resilients, intel·ligents i netes [2].

La promesa i el perill

Imagina una xarxa elèctrica que aprèn en temps real de cada pic de demanda, optimitza la distribució d'energia com un metge regula la dosi d'un medicament i, alhora, redueix dràsticament les emissions de carboni. Aquesta és la promesa de les xarxes intel·ligents alimentades per IA: una seguretat energètica basada no en el control de les rutes petrolieres, sinó en la capacitat de predicció i adaptació de sistemes autònoms. DeepMind ha demostrat que l'optimització algorítmica pot reduir fins al 40 % el consum energètic dels centres de dades gràcies a una refrigeració més eficient, una millora que es trasllada directament al sector elèctric quan s'apliquen els mateixos principis a la gestió de la xarxa nacional [1]; projectes com Google-PJM-Tapestry modernitzen les infraestructures nord-americanes amb plataformes basades en IA que anticipen falles, redistribueixen càrregues i minimitzen pèrdues, incrementant la resiliència davant desastres naturals o atacs cibernètics [1].

Paral·lelament, l'auge de les centrals nuclears modulars petites (SMR) ofereix una font d'electricitat constant i neta que pot alimentar aquestes xarxes intel·ligents sense dependre del petroli. Google i Kairos Power ja han anunciat un SMR de 500 MW amb la primera unitat prevista per al 2030, mentre Microsoft i Constellation reactiven la Unitat 1 de Three Mile Island, amb una capacitat de 837 MW, per al 2028; Microsoft col·labora també amb Helion en un acord de fusió que apunta al mateix any [2]. Com hem vist, les reduccions d'energia arriben fins al 40 % i els projectes SMR preveuen instal·lacions de 500 MW per al 2030 i 837 MW per al 2028. La combinació d'una generació nuclear fiable i d'una gestió basada en IA crea un ecosistema on la seguretat energètica es converteix en una funció automàtica, transparent i mesurable.

No obstant això, el perill que s'amaga darrere d'aquesta visió és igual de real. Quan les decisions crítiques sobre fluxos d'electricitat passen a ser determinades per models algorítmics, la integritat de les dades i la verificabilitat del codi es converteixen en punts únics de fallada; un atac que manipuli els sensors o corrompi l'entrenament del model podria desencadenar una sobrecàrrega artificial, un tall d'electricitat a gran escala o fins i tot la desviació intencionada de la producció nuclear cap a escenaris insegurs. Per això, cada capa de la infraestructura ha d'estar protegida per mecanismes de confiança descentralitzats —com els registres immutables que enregistren els valors dels sensors i les decisions algorítmiques—, garantint que qualsevol alteració sigui detectada immediatament i rebutjada.

Aquesta doble cara, promesa i perill, exigeix una arquitectura de confiança integrada: IA per a l'optimització i blockchain per a la verificació. Només així es pot assegurar que la xarxa intel·ligent no es converteixi en un nou vector d'atac, sinó en el pilar més robust de la seguretat energètica del futur. La clau és desenvolupar marcs reguladors i estàndards oberts que obliguin a la transparència dels models, al control independent de les seves sortides i a l'auditoria contínua per part d'entitats independents. En aquest equilibri entre innovació i vigilància, la seguretat energètica reinventada pot deixar enrere el petroli i avançar cap a una era en què la confiança és tan segura com la pròpia energia que alimenta les nostres societats.

Qui vigila els electrons?

Una xarxa intel·ligent no només mou electrons d'una subestació a una altra; és un corrent de dades que registra cada operació, cada transacció comercial i cada dret contractual en temps real. Aquesta doble circulació crea oportunitats immenses però també exposa vulnerabilitats: si la informació que guia els algorismes no és fiable, l'optimització de la generació i el consum pot convertir-se en una font d'inestabilitat, amb conseqüències que van des del desequilibri de freqüència fins a apagades massives. La pregunta central es converteix, doncs, en qui garanteix que aquests fluxos són verídics.

La resposta emergeix com una capa de confiança distribuïda: la blockchain. En el seu nucli, aquesta tecnologia registra cada acció —des del despatx d'un contracte d'energia renovable fins al pagament d'una tarifa de consum d'un usuari final— en blocs inalterables i verificables per qualsevol participant autoritzat. Això impedeix manipulacions malintencionades i permet auditories independents continuades. Quan una IA decideix desviar l'energia cap a un centre de dades on s'entrena el pròxim model d'aprenentatge profund, la transacció queda gravada i pot ser revisada per entitats reguladores o auditors externs, assegurant que no hi ha desviaments ocults ni beneficis indeguts.

Les experiències recents demostren com aquesta sinergia pot funcionar a gran escala. DeepMind ha aconseguit reduir el consum energètic de refrigeració en els centres de dades de Google —com hem vist— i, si s'integra aquest estalvi en una cadena de blocs que registri cada quilowatt-hora, es garantirà la transparència del benefici ambiental [1]. De manera paral·lela, el consorci Google-PJM-Tapestry

modernitza la xarxa elèctrica dels Estats Units amb plataformes d'IA que equilibren la generació distribuïda; codificar les dades de flux i els acords de compravenda en una blockchain pública ajudaria a evitar conflictes d'interès i a assegurar la traçabilitat del comerç energètic [1].

A escala nuclear, projectes com l'SMR de 500 MW desenvolupat per Google i Kairos Power (previst per al 2030) podrien incorporar registres blockchain per a la gestió de permisos, manteniment i rendiments operatius, creant una pista d'auditoria consultable en temps real per reguladors independents [2]. De manera similar, la reactivació de la Unitat 1 de Three Mile Island per part de Microsoft i Constellation — 837 MW, prevista per al 2028— es podria documentar amb un registre distribuït que reculli cada fase del procés de seguretat i cada intervenció humana o automàtica. Aquest enfocament es reforçaria amb la col·laboració de Helion i Microsoft en fusió nuclear, amb l'objectiu posat en el 2028, en què les dades de producció d'energia i els costos operatius es podrien certificar amb una cadena de blocs, evitant qualsevol manipulació que pogués comprometre la confiança del mercat [2].

Aquests exemples mostren com la blockchain pot actuar com a columna vertebral de la confiança en un ecosistema energètic cada cop més intel·ligent i autònom. No es tracta només d'una solució tècnica, sinó d'un marc institucional que combina transparència, responsabilitat i auditoria contínua; el control del petroli queda enrere i la seguretat energètica depèn de garantir que cada electró, cada dada i cada dret es mouen en un entorn veritablement fiable. La tasca per a les empreses, els reguladors i la societat és clara: adoptar plataformes blockchain obertes, establir estàndards d'auditoria independents i integrar aquestes capes de confiança amb les solucions d'IA que ja transformen la gestió de xarxes, assegurant així una seguretat energètica resilient, intel·ligent i neta.

---

[1] Google DeepMind / Data Center Frontier, *IA per a la xarxa.* 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 avançat i SMR per a la demanda d'IA (2024-2025).* https://www.iaea.org/bulletin/data-centres-artificial-intelligence-and-cryptocurrencies-eye-advanced-nuclear-to-meet-growing-power-needs ↩

La mà (ja no tan) invisible: blockchain com a capa de confiança

«Cal un sistema de pagament electrònic basat en la prova criptogràfica en lloc de la confiança, que permeti a dues parts disposades transaccionar directament entre elles sense necessitat d'un tercer de confiança.»

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

Al capvespre, el barri de Sant Antoni del Parc es transforma en una petita borsa d'energia. Les llums de les façanes resplendeixen amb la calidesa suau dels panells solars instal·lats sobre les terrasses i els sostres dels edificis d'habitatge social. Cada llar, equipada amb un inversor intel·ligent, mesura en temps real quanta energia genera i quanta consumeix. Quan el sol es pon i la producció supera la demanda interior, una notificació apareix a l'aplicació de Powerledger al telèfon de la Marta, que viu al pis del tercer; ella pot veure, amb només un toc, quants quilowatts-hora (kWh) té disponibles per vendre.

Sense cap intermediari, sense factures ocultes ni tarifes addicionals, la Marta decideix enviar l'excedent al seu veí, en Joan, que treballa de nit i necessita energia per al seu taller d'eines electròniques. En Joan rep una alerta: «Energia disponible —accepta?». Accepta amb un clic, i instantàniament el contracte es codifica com a transacció en la cadena de blocs de Powerledger, on cada unitat d'energia és representada per un certificat renovable tokenitzat (REC) —un REC equival a 1 MWh—[1]. En qüestió de segons, l'acord queda registrat de forma immutable: el sensor del panell solar de la Marta envia les dades de producció al node de la blockchain; els sensors de consum d'en Joan verifiquen que l'energia ha estat rebuda i consumida; tot el procés queda gravat de forma transparent però segura.

A la plaça central, un petit monitor mostra en temps real les transaccions del barri: quants RECs han circulat, quin percentatge d'energia ha estat intercanviada entre veïns i quin impacte ha tingut sobre les emissions de carboni locals. Els residents observen com el gràfic puja, orgullosos de veure que la seva comunitat està reduint la dependència de les grans companyies energètiques i, alhora, fomentant una economia circular basada en l'energia verda.

Aquesta escena il·lustra perfectament la «mà invisible» del mercat — aquest cop no és un misteriós balanç d'interessos que opera des de darrere les portes d'una sala de conferències — sinó una xarxa visible i auditable, codificada en codi obert. La blockchain actua com a testimoni digital, assegurant que cada transacció sigui verificable per qualsevol participant, sense necessitat de confiança cega en un tercer. Això contrasta amb el model tradicional on les companyies distribuïdores registren les dades en sistemes propietaris i opacs, sovint inaccessibles per als consumidors.

Tanmateix, aquest experiment encara es troba en la fase de prova de concepte. La majoria dels 39 projectes analitzats mostren que el potencial és real, però s'enfronten a obstacles com registres fragmentats, dades MRV (monitoratge, reportatge i verificació) inconsistents i una manca de reconeixement legal per als RECs tokenitzats[2]. Tot i això, l'eficiència energètica de la capa subjacent ha millorat dràsticament: el Merge d'Ethereum ja és sostenible —una prova que la blockchain ja no és una font de malbaratament sinó una eina sostenible per a l'energia verda[3].

En aquest barri, la mà invisible s'ha fet visible. Cada clic, cada token i cada registre al llibre digital converteixen la confiança en un actiu mesurable, obrint les portes a un nou paradigma energètic basat en el P2P, els certificats renovables tokenitzats i el MRV quasi en temps real. La pregunta que queda per respondre és: quan aquesta capa de confiança s'estandarditzarà i es reconeixerà legalment, quants altres barris podran replicar aquest model i transformar completament la manera com comprenem i consumim energia?

Els mercats que Roberts imaginava

Paul Roberts, a *The End of Oil* (2004), descrivia els mercats de l'energia com una gran borsa de valors: preus determinats pel joc invisible d'oferta i demanda i oportunitats distribuïdes entre inversors i consumidors. El seu relat no era només d'entusiasme; també mostrava les ombres que s'estenien darrere del teló, amb l'exemple emblemàtic d'Enron —una trampa de comptabilitat i manipulació de preus— que il·lustrava la vulnerabilitat d'un sistema on la informació era privilegi d'uns pocs i la transparència un luxe.

Roberts anomenava aquesta «opacitat» el veritable enemic del mercat lliure. Les transaccions es feien a través de contractes ocults, les dades de producció i consum eren manipulades per interessos corporatius i els reguladors, sovint sobrepassats, no podien garantir la veracitat dels informes. Avui, més d'una dècada després, la blockchain ofereix una resposta tecnològica a aquesta crida: la seva arquitectura distribuïda crea un registre immutable on cada transacció d'energia —des del moment que el sol genera un quilowatt-hora fins al punt en què aquest es consumeix a la llar— queda gravada de manera permanent i verificable per qualsevol participant, sense intermediaris que puguin editar o suprimir dades.

Aquesta nova capa de confiança ja s'està posant a prova al camp. Powerledger ha desenvolupat una plataforma on veïns d'un barri poden comprar energia directament entre ells, sense passar per la companyia elèctrica tradicional. Cada kWh transaccionat es vincula a un certificat renovable tokenitzat; un REC representa exactament un megawatt-hora i s'enregistra a la blockchain, garantint que el comprador rep una certificació verificable del caràcter renovable de l'energia adquirida [1]. Sensors avançats instal·lats a les instal·lacions fotovoltaiques i eòliques transmeten dades de producció a la cadena, permetent un MRV (monitoratge, reportatge i verificació) quasi instantani, i qualsevol desajust entre la producció declarada i la real es detecta immediatament, reduint el marge de frau.

Com indica l'enquesta recent que recull 39 projectes, la majoria d'aquests esforços encara són proves de concepte [2]; els obstacles són diversos: registres fragmentats entre diferents plataformes, dades MRV inconsistents i una manca de reconeixement legal que impedeix que els tokens siguin acceptats com a instruments financers regulats. Cal establir estàndards comuns perquè les transaccions puguin ser interconnectades a escala global.

En aquest moment històric, la blockchain es beneficia d'una evolució energètica crucial: el Merge d'Ethereum ja és sostenible, convertint una tecnologia que abans es criticava per la seva ineficiència en una infraestructura gairebé neutra des del punt de vista energètic [3] —un mercat on la confiança ja no depèn d'una mà invisible, sinó d'un registre visible per a tots.

La capa de confiança

Més enllà de l'escena del barri, val la pena desgranar com la blockchain actua de capa de confiança en tres aplicacions concretes. La primera és el mercat P2P d'energia: protocols com Powerledger permeten el comerç directe d'electricitat entre veïns, amb cada transacció immutable i verificable [1]. La clau és que la cadena elimina els intermediaris tradicionals: la confiança ja no recau en una «mà invisible» d'operadors centralitzats, sinó en un registre transparent al qual tots els participants tenen accés simultani.

Una segona aplicació que reforça aquest nou paradigma són els certificats d'origen renovable (REC) tokenitzats. Cada certificat representa exactament 1 MWh d'energia neta produïda i es codifica com a token únic en la blockchain, assegurant que no pugui ser duplicat ni falsificat [1]. Aquesta traçabilitat plena de transparència permet a consumidors i empreses comprovar amb un simple escaneig l'origen de la seva energia, convertint el «greenwashing» en una pràctica inviable. A més, la tokenització simplifica la liquidació dels certificats: les transaccions es processen en segons, sense burocràcia ni costos associats als sistemes tradicionals de registre.

Finalment, el monitoratge, reportatge i verificació (MRV) del carboni s'ha transformat amb sensors IoT que escriuen dades directament a la cadena. Aquest flux d'informació quasi en temps real elimina les llacunes entre la generació física i el registre digital, reduint significativament l'error humà i la manipulació de dades [1]. Amb cada lectura de sensor codificada com a transacció immutable, els projectes de compensació de carboni poden demostrar amb evidència verificable la seva contribució real a la descarbonització.

El mite energètic que sostenia que les tecnologies blockchain eren una càrrega per al consum global ha quedat obsolet. Després del Merge d'Ethereum, el consum energètic de la xarxa es va desplomar respecte a l'anterior model de prova de treball [3]; com hem vist, això converteix la blockchain en una infraestructura sostenible per al nou ecosistema energètic.

Tot i aquestes promeses, el panorama actual encara és d'una fase experimental. Una enquesta recent sobre 39 projectes basats en blockchain revela que la majoria es troben en etapa de prova de concepte, amb obstacles com registres fragmentats, dades MRV inconsistents i manca de reconeixement legal [2]. Perquè aquesta capa de confiança pugui desplegar-se a gran escala, cal establir estàndards comuns i marcs reguladors que garanteixin la interoperabilitat i la validesa jurídica. Només així la blockchain podrà

consolidar-se com el fonament fiable d'un mercat energètic descentralitzat, transparent i veritablement sostenible.

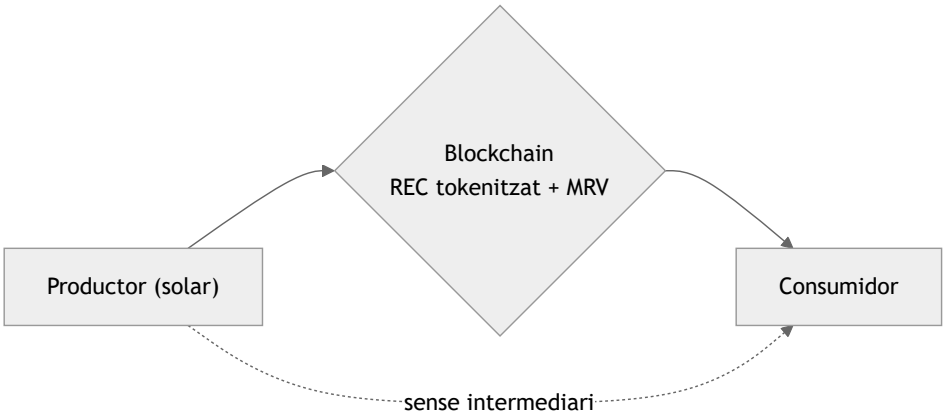


Figura 12.1 — Productor i consumidor intercanvien energia i certificats directament; la blockchain aporta confiança sense intermediari.

El realisme: encara és aviat

Una enquesta recent que recull el progrés de trenta-nou iniciatives blockchain dedicades a l'energia constata que la majoria es troben encara en fase de prova de concepte. Aquestes dades revelen un panorama on la innovació avança amb pas decidit però sense haver superat les barreres fonamentals que impedeixen una adopció massiva. Els obstacles identificats són tres: registres fragmentats que dificulten la interoperabilitat entre plataformes; dades de monitoratge, reportatge i verificació (MRV) inconsistents que comprometen la fiabilitat del sistema; i, finalment, l'absència d'un marc legal reconegut que legitimi les transaccions basades en blockchain [2].

Aquesta situació no ha de ser interpretada com un fracàs tecnològic, sinó com una etapa inevitable dins del cicle d'adopció d'una infraestructura tan disruptiva. La promesa que la blockchain ofereix al sector energètic és clara: crear una capa de confiança immutable que garanteixi que cada certificat renovable (REC) tokenitzat representa realment un megawatt-hora produït, i que els intercanvis P2P d'energia —com els facilitats per Powerledger— es puguin registrar de forma transparent i verificable en temps quasi-real [1]. A més, la integració de sensors IoT amb contractes intel·ligents permet un MRV gairebé instantani, reduint les latències que tradicionalment han afeblit els sistemes de certificació de carboni.

Tanmateix, la manca d'estàndards comuns converteix aquesta promesa en una il·lusió parcial. Cada projecte desenvolupa el seu propi esquema de tokenització i la seva pròpia arquitectura de dades, generant un ecosistema d'«illes blockchain» que no poden comunicar-se entre si sense costosos processos d'interfície. Sense una normativa clara que estableixi criteris mínims per a la qualitat de les dades MRV i la validesa jurídica dels tokens, les transaccions es mantenen vulnerables a disputes i a manipulacions potencials.

El Merge d'Ethereum —l'actualització que va fer sostenible la xarxa— demostra que la tecnologia blockchain pot evolucionar cap a una eficiència sostenible [3]. No obstant això, aquesta millora estructural no soluciona els problemes d'interoperabilitat i de reconeixement legal que encara persisteixen. La comunitat ha de traduir aquest avanç energètic en un marc regulador que estableixi: (1) estàndards de format per a certificats tokenitzats, garantint que 1 REC equival realment a 1 MWh independentment del proveïdor; (2) protocols d'intercanvi de dades MRV uniformes, amb auditories independents i certificacions de qualitat; i (3) reconeixement legal dels contractes intel·ligents com a instruments vinculants en jurisdiccions clau.

En aquest context, la necessitat d'una col·laboració estreta entre reguladors, empreses tecnològiques i actors del sector energètic esdevé imperativa. Les autoritats poden impulsar l'establiment d'esquemes de certificació oberts, similars als estàndards que ordenen altres indústries, mentre les empreses com Powerledger han de participar activament en la definició d'APIs comunes que permetin la interoperabilitat entre xarxes blockchain diverses. Només amb aquesta sinergia es podrà transformar la promesa de confiança immutable en una realitat operativa i escalable.

En resum, el panorama actual és un equilibri delicat: la tecnologia ha demostrat la seva capacitat per crear una capa de confiança robusta, però encara li falta maduresa. Els estàndards i marcs reguladors són els pilars que cal construir ara, perquè la blockchain pugui consolidar-se com el fonament fiable d'un mercat energètic descentralitzat, transparent i veritablement sostenible. La decisió de posar en marxa aquests mecanismes no és només una qüestió tècnica, sinó un compromís col·lectiu per garantir que la nova «mà invisible» sigui realment visible i confiable per a tots els actors del sistema.

La promesa i el perill

Imagina un mercat d'energia on cada kWh negociat porta impresa una petita empremta de veritat: qui l'ha produït, quina font la genera, quin impacte de carboni té i en quin moment exacte s'ha lliurat. Aquesta és la promesa que la blockchain ofereix com a capa de confiança per als mercats d'energia i de crèdits de carboni. En lloc d'una confiança cega en intermediaris o certificacions centralitzades, les transaccions es registren en un llibre immutable on qualsevol actor —generador solar comunitari, distribuïdor local, consumidor industrial o regulador— pot auditar la cadena completa amb uns clics, eliminant l'opacitat que ha alimentat fraus de certificats renovables falsos i d'incompliments en els informes de reducció d'emissions.

Powerledger ja permet el comerç P2P d'energia entre veïns, anotant cada transacció al registre distribuït i vinculant-la a sensors que mesuren la producció real quasi en temps real [1]. A més, els certificats renovables (REC) s'estan tokenitzant: un REC equival a 1 MWh d'energia neta i es pot transferir com qualsevol altre actiu digital, garantint la traçabilitat de l'origen i evitant duplicitats [1]; els sensors IoT alimenten directament la cadena, creant un sistema MRV gairebé instantani que redueix errors humans i augmenta la confiança en les dades reportades. Com hem vist, una enquesta recent sobre 39 projectes blockchain relacionats amb energia indica que la majoria operen encara com pilots, amb registres fragmentats, dades MRV inconsistents i manca de marcs reguladors que impedeixen la interoperabilitat i generen confusió més que claredat [2].

A més, la confiança que ofereix una cadena de blocs depèn de les dades que s'hi introdueixen. L'expressió «garbage in, garbage on-chain» resumeix el perill d'alimentar la blockchain amb informació no verificada o manipulada; si els sensors són vulnerables a ciberatacs o si els certificats es creen sense una auditoria rigorosa, la cadena immutabilitzarà errors i fraus difícils de corregir. Per això, establir estàndards de qualitat per a les fonts de dades i protocols d'autenticació robusts és imprescindible abans de desplegar solucions a gran escala [2].

El Merge d'Ethereum ha mitigat la preocupació energètica que tradicionalment envolta les tecnologies blockchain, fent el protocol sostenible i convertint la infraestructura en una opció viable per a aplicacions de gran volum com els mercats d'energia [3]. Això elimina l'obstacle aparent dels «costos ocults» i permet centrar-se en la qüestió clau: garantir que les dades siguin fiables, verificables i compatibles entre totes les parts de l'ecosistema.

En resum, la blockchain pot ser la capa de confiança que transforma els mercats d'energia i carboni en sistemes transparents i resistents al frau, sempre que es desenvolupin estàndards comuns i es protegeixi l'origen de les dades. Sense aquests fonaments, el potencial revolucionari podria quedar atrapat en una xarxa de silos incompatibles, deixant la «mà invisible» tan intocable com abans.

El contracte social de l'energia

En un ecosistema on cada quilowatt-hora pot ser comprat, venut o intercanviat entre veïns, la confiança ha de ser verificable i immutable. Aquí entra el concepte central del nostre llibre, **t2p**, la prova d'existència basada en blockchain que tanca el cercle de la confiança: un mecanisme criptogràfic que garanteix que l'energia o el crèdit de carboni certificat no pot ser alterat sense deixar una empremta ineludible.

Imagineu una comunitat d'autoconsumidors a Barcelona que genera energia solar i la ven en un mercat P2P. Cada generador emet un **REC tokenitzat** (1 REC = 1 MWh) que representa el dret a vendre aquella energia verificada [1]. En registrar-lo a la blockchain s'inclou una prova d'origen: les dades del comptador intel·ligent, la data i hora exactes i la certificació del proveïdor d'energia renovable. La blockchain grava aquesta informació en un llibre distribuït on qualsevol actor pot consultar-la sense dubtar-ne l'autenticitat.

Aquesta capa de prova d'existència es converteix en el fonament per a **MRV (monitoring, reporting, verification)** gairebé en temps real. Sensors instal·lats al llarg de la xarxa recullen dades de producció i consum; aquestes dades són resumides criptogràficament i afegides a blocs en una infraestructura que, després del **Merge d'Ethereum**, manté un consum energètic mínim [3]. Cada transacció és transparent i sostenible.

Tot i això, el camí cap a una adopció massiva encara està ple d'obstacles. Una enquesta recent sobre 39 projectes indica que la majoria es troben encara en fase de prova de concepte, limitats per **registres fragmentats** i dades MRV inconsistents [2]. Sense un marc normatiu comú, les autoritats reguladores no reconeixen legalment aquests tokens i els actors del mercat es mostren reticents a confiar en una infraestructura que encara no està totalment estandarditzada, generant silos de confiança on cada plataforma opera amb el seu propi protocol.

La solució passa per establir **estàndards oberts** que defineixin com s'ha d'emetre, signar i validar una prova d'existència. Organitzacions de normalització poden liderar aquest procés, assegurant que les proves siguin reconegudes legalment a totes les jurisdiccions; un cop aquests estàndards estiguin en vigor, la blockchain deixarà de ser una tecnologia experimental i es convertirà en la capa invisible però palpable de confiança que habilita mercats P2P, certificats renovables tokenitzats i MRV transparent.

En resum, **t2p** no és només una eina tècnica; és el contracte social del futur energètic. Assegura que el que entra a la cadena és autèntic, crea un registre immutable de confiança i ofereix una base sòlida per a les polítiques climàtiques i econòmiques que depenen d'una verificació fiable. El proper pas és clar: adoptar estàndards globals, integrar proves d'existència a tots els sistemes i permetre que la blockchain es converteixi en el veritable nucli de confiança del nou sistema energètic.

---

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

[2] Frontiers in Blockchain (2025), *estat dels mercats de carboni 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 prova d'existència contra les deepfakes

«La lluita de l'home contra el poder és la lluita de la memòria contra l'oblit.»

— Milan Kundera, El llibre del riure i de l'oblit (1979)

Març de 2026, una tarda assolellada a l'àrea de Barcelona-Sabadell, el conseller delegat d'una de les majors companyies elèctriques espanyoles apareix en un vídeo difós per Twitter. En només 38 segons, la imatge —una oficina elegant amb vistes panoràmiques al Parc Tecnològic del Vallès— mostra l'executiu, amb la mirada seriosa i una carpeta plena de gràfics d'emissions, declarant que «hem decidit ajustar les dades d'emissió per reflectir millor la realitat operativa». La frase, pronunciada amb un to aparentment transparent, es converteix immediatament en l'escenari d'una crisi inesperada.

En menys d'una hora, el preu de les accions de la companyia cau un 12 % a la borsa ibèrica. Les notícies es multipliquen: analistes financers avisen que els inversors dubten de qualsevol certificació ESG i temen una possible sanció del regulador de mercats. Els mitjans, des de La Vanguardia fins a Bloomberg, publiquen titulars alarmants —«La veritat esborrada: el gran engany de la transició energètica». En aquest moment, les xarxes socials s'omplen d'experts en ciberseguretat que recorden els darrers informes de l'Europol: les deepfakes han passat d'unes 500.000 el 2023 a 8 milions el 2025 [2].

Set hores més tard, una empresa de verificació forense digital publica un informe detallat: el vídeo és una deepfake. Mitjançant anàlisis d'algoritmes de detecció avançats i comparatives amb metadades originals, demostren que la cara del conseller ha estat generada per una xarxa neuronal entrenada en imatges públiques i que l'àudio ha estat sintetitzat a partir de mostres de veu disponibles en arxius corporatius. El dubte, però, ja no desapareix. Els inversors, els reguladors i el públic es troben atrapats entre la certesa d'una declaració oficial i la incertesa d'un engany tecnològic.

Aquest escenari il·lustra una realitat que cada vegada és més palpable: la transició cap a una economia descarbonitzada depèn de dades fiables. Els informes ESG, els mètodes MRV (Measurement, Reporting and Verification) de carboni i les certificacions d'energia neta són el fonament sobre el qual es construeixen inversions multimilionàries i polítiques climàtiques globals. Quan la veritat visual pot ser alterada en qüestió de minuts, aquestes capes d'informació perden credibilitat i, amb elles, la confiança necessària per impulsar projectes d'energia renovable a gran escala.

En aquest context, la necessitat d'una capa de confiança immutable es fa evident. La blockchain moderna ofereix exactament això: un registre descentralitzat on cada dada —des de certificats d'emissió a contractes intel·ligents que garanteixen el compliment de límits d'energia— pot ser verificada sense dependre d'un únic punt de fallada. La prova d'existència, anomenada t2p, neix com la resposta insígnia: un mecanisme criptogràfic que registra l'hora i el contingut d'un document o mitjà en una cadena de blocs, creant una empremta indeleble que qualsevol pot auditar.

Aquesta escena, tan sobria com cinematogràfica, no només captura la urgència del moment, sinó que posa en relleu la paradoxa central del capítol: sense un sistema robust per garantir l'autenticitat de les dades, la transició energètica es queda atrapada en una nebulosa d'incertesa. La solució està a les mans —i al codi— de la prova d'existència, que promet restaurar la confiança perduda i permetre que els projectes veritables avancin sense que l'ombra de les deepfakes els ofegui.

Les apostes

Com hem vist, el nombre de deepfakes ha passat d'unes 500.000 el 2023 a 8 milions anuals, i Europol preveu que el 2026 fins al 90 % del material audiovisual en línia podria ser generat artificialment, una realitat que transforma el panorama de la informació i, per extensió, el de les dades energètiques [2].

Aquesta onada de falsificacions digitals s'enfronta a un marc regulador encara incipient però cada cop més ferm. L'**EU AI Act**, adoptat el 2024, obliga les plataformes a marcar clarament els continguts sintètics i a proporcionar una **marca d'aigua** que indiqui la seva procedència [3]. Als Estats Units, el **Take It Down Act** estableix sancions per a qui allotgi o difongui deepfakes sense etiquetar-los adequadament. I des del gener de 2025, la **CISA** (Cybersecurity and Infrastructure Security Agency) ha publicat un avís que insta les empreses d'infraestructura crítica —incloses les de generació i distribució d'electricitat— a reforçar la verificació de la integritat de les dades abans d'utilitzar-les en informes ESG [3].

Sense una capa fiable de confiança, la transició cap a una economia descarbonitzada esdevé vulnerable a manipulacions. Els reguladors necessiten dades netes per validar el compliment dels objectius climàtics; els inversors busquen certificats d'**MRV (monitoring, reporting and verification)** que garanteixin que les reduccions d'emissions anunciades són reals i no simples narratives de màrqueting. El públic, cada cop més conscient, demanda transparència: si una foto d'una nova planta solar pot ser un deepfake, la credibilitat del projecte es desintegra en qüestió de segons.

En aquest context, la **prova d'existència** emergeix com a resposta tecnològica imprescindible. En la seva forma més coneguda —el protocol **OpenTimestamps**—, aquesta capa criptogràfica registra l'horari exacte i immutable d'un document o dades, assegurant que qualsevol intent de modificació posterior queda evident [1]. La integritat del registre es consolida a la cadena de blocs, on cada hash —incloent-hi versions perceptualment similars desenvolupades en recerca avançada de **hash perceptual**— es verifica i s'enllaça amb el bloc anterior, creant una cadena ininterrompuda d'autenticitat [5].

A més, l'evolució del **Merge d'Ethereum**, que va reduir la seva empremta energètica en un **99,95 %**, demostra com les infraestructures de blockchain poden ser sostenibles i alhora robustes per a aquest propòsit [6]. Així, una prova d'existència inserida en una cadena de blocs verda no només garanteix la veracitat del contingut, sinó que ho fa sense comprometre els objectius climàtics.

Les apostes són clares: **si no podem confiar en les dades**, cap política ni inversió per a la descarbonització pot avançar amb legitimitat. La combinació d'una regulació exigent i una capa de confiança basada en blockchain ofereix el marc necessari perquè la veritat esdevingui l'àncora de la transició energètica. Cal que les empreses, els governs i la societat civil adoptin immediatament aquesta arquitectura de prova d'existència; només així podrem impedir que els deepfakes es converteixin en l'obstacle insuperable a un futur net i fiable.

Què és la prova d'existència

Imagina que tens davant teu un informe de descarbonització amb milers de dades de sensors, certificats ESG i càlculs de MRV (monitoratge, reportatge i verificació) del carboni. Vols demostrar que aquell document va existir en una data concreta i que el seu contingut no ha estat alterat des d'aleshores. La resposta es troba en la prova d'existència, un mecanisme de tres passos que converteix qualsevol fitxer —des de fulles de càlcul fins a vídeos d'inspecció de turbines— en una empremta immutable registrada a la blockchain pública.

Pas 1 — Hash SHA-256 del fitxer.
El primer pas consisteix a aplicar l'algoritme criptogràfic SHA-256 al contingut del fitxer. Aquest algoritme produeix una cadena de 64 caràcters —una empremta digital única i unidireccional— que representa el document complet. La propietat clau és la seva irreversibilitat: qualsevol canvi, encara que sigui un sol byte, genera una nova empremta totalment diferent. Això garanteix que el fitxer mai no ha de sortir del dispositiu per ser processat; la privacitat es manté intacta perquè només la petita cadena hash, i no el contingut original, es transmet.

Pas 2 — Arbre de Merkle.
Un cop disposem d'un conjunt de hashes (pot ser un sol fitxer o milers d'arxius relacionats), aquests s'organitzen en una estructura jeràrquica coneguda com a arbre de Merkle. Cada parella de hashes es combina i es torna a hashar, creant nodes intermedis fins a arribar a l'arrel —el «Merkle root». Aquesta arrel consolida tot el conjunt de dades en una única empremta que representa la integritat completa del bloc d'informació. L'avantatge és doble: permet verificar qualsevol element individual comparant només la seva ruta cap a l'arrel, i redueix dràsticament la quantitat de dades que cal transmetre per a la verificació.

Pas 3 — Ancoratge a una blockchain pública.
L'últim pas consisteix a gravar el Merkle root en una cadena de blocs immutable, com ara Bitcoin, mitjançant serveis d'estampatge temporal com OpenTimestamps [1]. El procés envia l'arrel a la xarxa Bitcoin, que la inclou dins d'un bloc minat i li assigna un segell de temps verificable. Un cop el bloc és confirmat, es genera una prova .ots que conté la ruta criptogràfica des del Merkle root fins al hash del bloc on s'ha inscrit. Aquesta prova pot ser descarregada i emmagatzemada localment sense dependre de tercers.

La verificació és totalment autònoma: qualsevol lector recomputa el SHA-256 del fitxer original, reconstrueix l'arbre de Merkle corresponent i compara la seva arrel amb la que apareix a la prova .ots. Si s'ha modificat encara que sigui un sol byte, la comparació falla immediatament i demostra la manipulació.

No cal confiar en cap autoritat central; la seguretat es basa únicament en les propietats matemàtiques de l'algoritme hash i la immutabilitat de la blockchain.

Aquest procediment converteix la prova d'existència en una capa de confiança que pot ser integrada a qualsevol flux de treball ESG o MRV. Les empreses energètiques poden registrar els seus certificats de reducció d'emissions, les autoritats reguladores poden verificar l'autenticitat dels informes sense necessitat d'auditories presencials i la societat civil disposa d'una eina per validar la veracitat de les dades que sustenten la transició cap a un futur net. En un món on els deepfakes amenacen la credibilitat de qualsevol declaració visual o documental, la prova d'existència ofereix una resposta tecnològica clara i verificable —un escut digital contra la desinformació que protegeix el nucli mateix de la transició energètica.

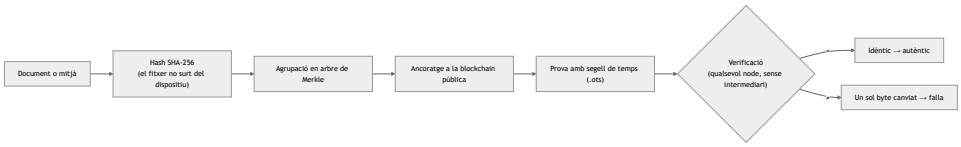


Figura 13.1 — Del hash a la verificació descentralitzada: ningú ha de confiar en ningú; només en les matemàtiques.

Per què la blockchain, i per què ara

El primer cop que el públic va sentir parlar del cost energètic de les cadenes de blocs, la imatge que quedava gravada era la d'una granja de miners alimentant una xarxa de Bitcoin amb centenars de megawatts, un monstre verd que devorava electricitat com si fos combustible. Aquell escenari va convertir el terme «blockchain» en sinònim de malbaratament i ineficiència, i la crítica es va estendre fins a les taules executives que consideraven la tecnologia una despesa inacceptable per a projectes d'energia neta.

La realitat ha canviat radicalment. El pas del model proof-of-work (PoW) al de proof-of-stake (PoS) no només és una evolució tècnica, sinó una revolució en el balanç entre seguretat i consum. L'operació coneguda com a «Merge» d'Ethereum, completada a finals de 2022, va substituir la seva arquitectura PoW per un mecanisme PoS que ha reduït el consum energètic del protocol en un **99,95 %**[6] —com hem vist —; una xarxa que abans requeria energia comparable al consum anual d'un petit país ara funciona amb l'equivalent de la potència d'una ciutat mitjana. El cost marginal d'afegir una transacció passa a ser quasi nul, mentre que la seguretat es manté gràcies a l'estímul econòmic del staking.

Les cadenes PoS modernes, aprofitant aquest model, són ara capaces de proporcionar una **capa de confiança** amb un cost energètic mínim i una escalabilitat que les fa aptes per a aplicacions massives. Un sol ancoratge d'existència, registrat en una transacció que conté la capçalera Merkle d'una col·lecció de documents, pot validar milers —fins i tot milions— de fitxers amb un únic hash. Aquesta eficàcia es tradueix en una reducció dràstica del consum de recursos informàtics i, per tant, en una petita empremta de carboni associada al procés de certificació.

A més, el model PoS ofereix beneficis addicionals que van més enllà del consum. La **descentralització** es manté robusta perquè la participació no depèn d'una infraestructura costosa de maquinari especialitzat, sinó de tokens que qualsevol actor pot adquirir i «apostar». Això democratitza l'accés a la infraestructura de verificació, permetent a entitats petites —com cooperatives locals d'energia renovable o ONGs de monitoratge ambiental— integrar-se en una xarxa global sense haver d'invertir en grans centres de dades.

En aquest context, la prova d'existència (t2p) es converteix en una solució pràctica i fiable per a la crisi de veritat que amenaça la transició energètica. La confiança que aporta una capa blockchain no és un «cost ocult», sinó una inversió mínima comparada amb el valor econòmic i social d'un sistema d'informació verificable, transparent i resistent a manipulacions. Les dades ESG, els informes MRV de carboni i qualsevol altre registre crític per a la credibilitat de la descarbonització poden ser ancorats a aquesta infraestructura sense temer que l'acte de certificació es converteixi en una font de contaminació.

En resum, el mite del malbaratament energètic de la blockchain pertany al passat PoW. Les cadenes PoS d'avui ofereixen **confiança a cost mínim**, escalabilitat i accessibilitat, convertint-se en una capa de confiança viable per a les infraestructures que sustenten la transició cap a un futur net. El moment d'adoptar-les és ara: només així podrem garantir que les dades que impulsen el canvi climàtic siguin tan fiables com cal.

C2PA i la prova d'existència, complementàries

En el marc de les **Content Credentials** impulsades per la iniciativa **C2PA**, el primer pas cap a la veracitat és registrar l'origen del contingut en el moment exacte de la seva creació. Cada fitxer rep una empremta criptogràfica SHA-256 que, juntament amb un arbre Merkle i una firma X.509 d'un proveïdor acreditat, forma una cadena de confiança que es pot verificar sense dependre de tercers intermediaris [4]. Aquesta arquitectura ha demostrat la seva utilitat en sectors com el periodisme digital i la producció audiovisual, on les plataformes poden certificar que un vídeo o una imatge prové d'una font legítima i no ha estat alterat posteriorment.

Tanmateix, aquest model té una limitació estructural: **la confiança depèn de la cooperació del creador**. Si el proveïdor decideix retirar la credencial —per motius comercials, legals o simplement per oblidar-se— l'absència d'aquesta prova no ofereix cap informació útil sobre si el contingut ha estat manipulat o no. En altres paraules, **l'eliminació de la credencial equival a una nul·la evidència**, i el sistema queda incapaç de demostrar que alguna vegada va existir una certificació [4]. Això crea una vulnerabilitat crítica en un entorn on les deepfakes s'estan propagant a ritmes alarmants: segons dades de l'**Europol**, el nombre de deepfakes en circulació ha passat d'unes 500.000 el 2023 a 8 milions el 2025, amb una projecció d'Europol que situa fins al **90 % del contingut en línia com a sintètic el 2026** [2].

La **prova d'existència** (t2p) ofereix una resposta a aquest buit. Basada en el mateix principi que **OpenTimestamps**, aquesta solució registra el hash del contingut directament en una cadena de blocs PoS, creant una àncora **independent i immutable** que persisteix encara que les metadades originals desapareguin o siguin esborrades [1]. La característica clau és que la prova no requereix cap autorització prèviament acordada: qualsevol usuari pot generar l'hash i publicar-lo en la xarxa, assegurant que el moment de creació queda immortalitzat. Això elimina completament el risc d'un «esborrat silenciós» i proporciona una capa addicional de confiança que sobrepassa les limitacions del model C2PA.

No es tracta d'una solució rival sinó d'una **sinergia**. La combinació de la certificació d'origen de C2PA amb l'ancoratge immutable de t2p forma un ecosistema de defensa en quatre fronts: (1) procedència verificable, (2) àncora temporal irreversible, (3) detecció automàtica basada en hashes perceptuals —una línia de recerca que el 2025-26 ha vinculat amb èxit a mitjans digitals emmagatzemats a blockchain [5]— i (4) alfabetització mediàtica per a usuaris finals.

Aquesta aliança és especialment rellevant per a les infraestructures crítiques de la transició energètica. Els informes ESG i els mecanismes MRV de carboni depenen d'una **traçabilitat fiable** de les dades de producció, transport i consum d'energia. Sense una capa de confiança robusta, qualsevol intent de descarbonització es veu minat per dubtes sobre la veracitat de les declaracions. Implementar simultàniament C2PA i t2p significa garantir que els certificats d'emissions, els informes de reducció i les auditories siguin **no només auditables, sinó també incapaços d'alteració**.

En conclusió, la convergència entre C2PA i la prova d'existència tanca una breu lacuna tècnica i crea un **marc de confiança integral** capaç de recolzar les polítiques climàtiques més exigents i contrarestar l'onada de desinformació digital. La crida a l'acció és clara: empreses, reguladors i desenvolupadors han d'adoptar simultàniament ambdues tecnologies, establint protocols oberts que integrin credencials de contingut i ancoratge de blockchain en les seves plataformes. Només així podrem garantir una transició energètica basada en dades veritables i resistents al bombardeig de deepfakes.

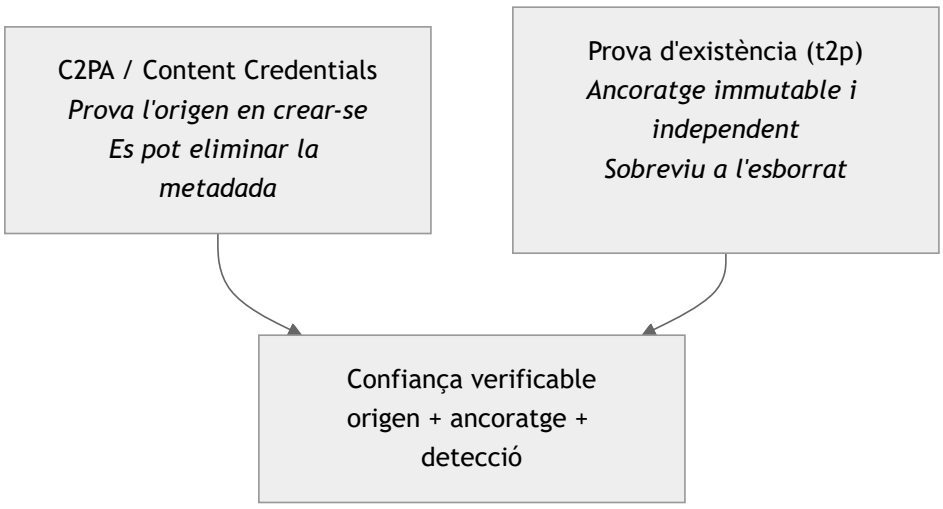


Figura 13.2 — C2PA demostra «qui i quan» en origen; l'ancoratge en blockchain demostra «això existia i no s'ha alterat».

t2p, la solució insígnia

Aquí és on la teoria es fa butxaca. t2p converteix un telèfon en un estudi de proves portàtil: cada foto, vídeo, àudio, document escanejat, pàgina web o gravació de pantalla rep, en l'instant de crear-se, una empremta criptogràfica única —un hash **SHA-512**— que queda registrada en una **blockchain pública** —avui, la de **Polygon**; l'aplicació pot implementar qualsevol altra L2 d'Ethereum, perquè la prova no depèn de cap cadena concreta, sinó del fet que l'àncora sigui pública i verificable per tothom. El resultat és una prova a prova de manipulacions que una cosa va existir i quan, verificable per qualsevol i per sempre. I un principi de disseny ho governa tot: el fitxer original **mai no surt del dispositiu**; només en viatja l'empremta. t2p no pot veure el que captures.

El flux és la prova d'existència descrita —com hem vist— però aplicada amb rigor forense. En capturar, l'app calcula el hash a partir dels bytes exactes del fitxer i l'ancora a la blockchain pública amb una marca de temps. Hi afegeix, a més, un segell de temps de confiança **RFC 3161** (estàndard eIDAS) independent de la cadena i, si l'usuari ho permet, unes coordenades **GPS de grau forense**: només se segellen si el senyal és genuí —precisió d'uns 50 metres i una antiguitat màxima de 30 segons—; una ubicació simulada bloqueja la certificació per protegir el valor probatori. Cada certificació genera un **certificat PDF** professional amb el hash, l'identificador de la transacció, el segell RFC 3161, la ubicació i un **codi QR** per comprovar-ho a l'explorador de la cadena.

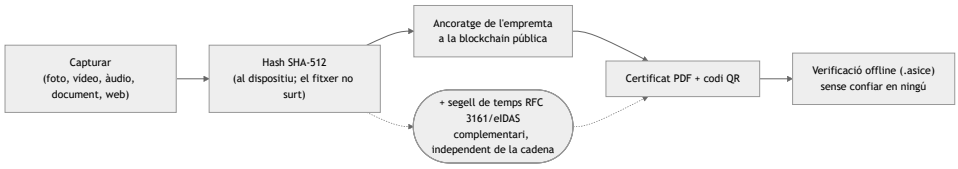


Figura 13.3 — El flux de t2p: capturar, segellar l'empremta a la blockchain pública i poder verificar-ho fins i tot sense connexió ni intermediaris.

La peça més sòlida per a ús legal és el **paquet d'evidència** `.asice`: un contenidor estàndard ASiC-E (ETSI EN 319 162) que inclou una còpia byte a byte del fitxer, el certificat, el segell de temps i la seva cadena de confiança, i fins i tot un fitxer de text amb les ordres `openssl` per comprovar-ho. Qualsevol pot verificar la prova **completament sense connexió, sense l'app i sense haver de confiar en t2p**; és, en essència, la diferència entre «confia en nosaltres» i «comprova-ho tu mateix».

Sobre aquesta base, els casos d'ús es despleguen sols.

- **Periodisme i mitjans.** Un reporter certifica una foto o un vídeo en el moment exacte de la captura; el lector en verifica l'origen escanejant el QR del certificat.
- **Proves legals i cadena de custòdia.** El GPS forense, el segell RFC 3161 i el paquet `.asice` fan que una evidència resisteixi l'escrutini d'un tribunal. I la **signatura amb vídeo-selfie** —amb proves de vida i verificació biomètrica— vincula un document a una persona real i present.

- **Propietat intel·lectual i autoria.** Segellar una obra demostra que existia en una data certa, sense registres ni intermediaris.
- **Integritat de dades climàtiques i ESG**, el pont amb la tesi d'aquest llibre. Una empresa pot certificar la lectura d'un sensor d'emissions, un informe MRV o la fotografia d'una instal·lació de manera que ningú —ni ella mateixa— pugui alterar-los després. La transició necessita exactament aquesta mena de dades incontrovertibles.

t2p encarna una idea tan senzilla com poderosa: la confiança no s'ha de demanar, s'ha de poder comprovar. En una època en què qualsevol imatge pot ser falsa, tornar verificable la veritat —i fer-ho des de la butxaca— és potser la infraestructura més discreta i, alhora, més decisiva de tota la transició.

La promesa i el perill

La prova d'existència (t2p) ofereix una **confiança verificable** que es pot demostrar amb un cost marginal: cada hash de dades es registra a la blockchain pública, on la immutabilitat i la transparència són garantides per la xarxa descentralitzada. Això transforma una declaració —per exemple «aquest informe ESG reflecteix les emissions reals d'una planta»— en una evidència críptica ment provada que qualsevol actor pot consultar sense necessitat de confiar en un intermediari. El cost marginal d'afegir una prova és mínim: una sola transacció d'ancoratge pot validar milers de hashes alhora mitjançant l'arbre de Merkle. Aquesta reducció dràstica, fruit d'una fusió de tecnologies (Merge d'Ethereum -99,95 % en consum energètic) i de solucions de capa 2, fa que la prova d'existència sigui **escalable a milions d'insercions diàries** sense crear barreres econòmiques per a ONG o petites empreses [6].

A escala de l'operació, el benefici és clar: les autoritats reguladores poden validar en temps real els informes de MRV (monitoring, reporting and verification) de carboni; els inversors poden auditar la trajectòria d'un projecte sense dependre de certificacions centralitzades que sovint són objecte de pressions polítiques. La **capa de confiança** aportada per la blockchain es converteix així en el fonament sobre el qual s'assenta la credibilitat de tota la transició energètica. Sense aquest suport, les deepfakes —que segons Europol podrien arribar al 90 % del contingut en línia el 2026— erosionen la fe pública i fan que qualsevol dada ESG sigui vista amb escepticisme [2].

No obstant això, aquesta promesa ve acompanyada d'un perill inherent. La **desanonimització** és una conseqüència inevitable quan les proves d'existència s'enllaçen amb metadades identificables. El consorci C2PA ha assenyalat que la divulgació de signatures digitals pot revelar l'origen del contingut, exposant periodistes i activistes a represàlies en regims autoritaris [4]. Això requereix un disseny acurat de privacitat: les proves han d'estar separades de qualsevol informació personal i, si cal, utilitzar **hash perceptual** per protegir el contingut sense comprometre la verificabilitat [5].

A més, la prova d'existència **no detecta falsos per si sola**; un atacador pot crear un document fraudulent, registrar-ne el hash i presentar-lo com a veritable. La seguretat del sistema depèn de processos complementaris —com auditories independents, certificacions de fonts fiables i mecanismes de revocació — que han d'estar integrats en l'ecosistema. Un excés de confiança en la tecnologia podria conduir a una **laxitud reguladora**, on les institucions deleguen tot el control a la cadena i obvien la necessitat de supervisió humana.

En conclusió, la prova d'existència és una **tecnologia necessària però no suficient** per garantir la veritat en l'era de les deepfakes. El seu èxit depèn de la creació d'un ecosistema que combini transparència blockchain amb marcs reguladors robustos (EU AI Act, Take It Down Act, CISA) i principis de privacitat dissenyats per protegir els més vulnerables [3]; només així podrem convertir la promesa de confiança verificable en una realitat sostenible per a la transició energètica.

A més, Beth Noveck confirma que les tecnologies descentralitzades —i entre elles la blockchain— són una de les vies proposades per garantir l'autenticitat del contingut digital i augmentar-ne la transparència [7]. Tanmateix, ella advoca amb claredat que les marques d'aigua i els estàndards de procedència, per si sols, no resolen el problema perquè depenen de la cooperació del creador i de les plataformes que les implementen [8]. És aquí on l'ancoratge neutral de **t2p** mostra tot el seu potencial: enregistrar el hash a una cadena pública sense cap intermediari ni autoritat central assegura que la prova d'existència es manté independent del creador i dels tercers de confiança, tancant el buit assenyalat per Noveck i reforçant la promesa d'una confiança verificable i universal.

És hora d'actuar

Veuràs que la veritat ja no és una condició natural del debat públic; és un recurs que cal comprar i protegir. Per això cada grup social té una missió concreta en l'ecosistema de **t2p**.

1. Ciutadania: el primer filtre

Abans d'enviar o compartir qualsevol vídeo, àudio o imatge, demana la prova d'existència. Les eines basades en OpenTimestamps permeten verificar que un arxiu es va crear abans d'un moment determinat i que no ha estat alterat des de llavors [1]. Aquest simple pas —un clic a una extensió del navegador o una app mòbil— pot evitar la propagació massiva de deepfakes, una onada que Europol documenta a l'alça [2]. Cada usuari que es converteix en vigilant és una capa addicional de seguretat: la confiança no es construeix només a escala institucional, sinó també a través d'una cultura de dubte constructiu.

2. Mitjans de comunicació: el compromís de publicar amb prova

Els portals informatius han de fer del **timestamp** un requisit per a tot contingut visual que pugui influir en l'opinió pública o en decisions polítiques. Això implica integrar una API de verificació blockchain al flux editorial i afegir, com a metadades visibles, el hash perceptual certificat a la cadena (vegeu els estudis que demostren la resistència d'aquests hashes davant manipulacions subtils [5]). Quan un mitjà indica «verificat amb t2p», ofereix una garantia tangible que supera les declaracions de bona fe. La falta d'aquestes pràctiques ja ha portat sancions per part de l'EU AI Act, que preveu multes de fins al 7 % de la facturació anual global en les infraccions més greus [3].

3. Empreses: ancorar les dades ESG i MRV

Les corporacions que reporten emissions de carboni o certificats ESG han d'emmagatzemar els seus informes en una cadena pública immutable. La migració cap a la xarxa Ethereum, que ha reduït el consum energètic gairebé totalment amb l'últim merge proof-of-stake [6], ofereix un entorn sostenible per a aquest propòsit. Cada registre de dades se signa amb una clau privada i s'associa a un hash perceptual que garanteix la integritat del document original. A més, la interoperabilitat entre estàndards com el C2PA (que actualment mostra limitacions en l'autenticació d'origen) i les solucions de timestamping permet crear una capa de confiança híbrida: la blockchain aporta immutabilitat, mentre els protocols de metadades afegeixen context i rastre de propietat [4].

4. Reguladors: definir estàndards i fomentar interoperabilitat

Les autoritats han d'establir marcs normatius que obliguin l'ús de proves d'existència per a qualsevol informació amb impacte social o ambiental. Això implica:

- **Requisits d'interoperabilitat** entre solucions de timestamping, C2PA i les iniciatives del Take It Down Act, per assegurar que els certificats siguin reconeguts transversalment a la UE i als Estats Units.
- **Auditories independents** per validar la implementació dels protocols a gran escala, amb informes públics trimestrals que incloguin l'estat de compliment de les empreses i els mitjans.
- **Incentius fiscals** per a les organitzacions que adoptin solucions basades en blockchain de baixa energia, com el Merge d'Ethereum.

5. Un futur sense veritat verificable no és un futur sostenible

Sense una capa de confiança verificable, la transició energètica es queda sense credibilitat: inversors, ciutadans i governs no podran confiar en les dades que sustenten els projectes de descarbonització. La prova d'existència **t2p** ofereix el mecanisme per convertir promeses climàtiques en fets contrastats.

Per tant, la crida és clara: **actua ara**, verifica abans de compartir, publica només amb prova i ancora les teves dades a la blockchain. Només així podrem avançar cap a una transició energètica creïble i duradora. És *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 (especificació 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. ↩

Hidrogen, captura i les apostes que falten

«Crec que un dia l'aigua serà emprada com a combustible, que l'hidrogen i l'oxigen que la constitueixen, usats sols o junts, forniran una font inesgotable de calor i de llum.»

— Jules Verne, L'illa misteriosa (1874-75)

Era una tarda d'octubre de 2025 a Immingham, al nord del Regne Unit, on el fred marí s'infiltra entre les estructures metàl·liques d'un dels complexos industrials més esperats del continent. Les torres d'acer s'alçaven com gegants que prometien transformar l'energia en hidrogen verd, una flama invisible de futur sostenible. Sobre el paper, el projecte havia de produir hidrogen a partir d'electròlisi alimentada per energia renovable i convertir-se en una de les peces de la descarbonització industrial europea.

Però aquell matí, el so que va trencar la rutina no era el brunzit tranquil dels compressors, sinó un anunci sobtat: **Air Products havia decidit cancel·lar el projecte d'H_2 verd d'Immingham**, una iniciativa valorada en uns 2.000 milions de lliures i considerada una de les majors apostes globals per a la descarbonització industrial. El missatge, curt però contundent —«Projecte suspès indefinidament»— es va difondre instantàniament pels mitjans i per les xarxes on enginyers i analistes de la indústria van començar a comentar amb una mescla d'incredulitat i resignació.

La notícia no era només un revés financer; era el reflex d'un fenomen que s'estava consolidant al llarg dels darrers anys: **un somni sobredimensionat sobre l'hidrogen verd**. Des de la promesa inicial, el sector havia invertit recursos immensos a prometre una energia neta capaç de substituir els combustibles fòssils en tots els sectors, des del transport marítim fins a les ciutats. No obstant això, el 2025 va marcar un **reset brutal** per al mercat. Segons informes consolidats, aproximadament **60 grans projectes d'hidrogen verd van ser cancel·lats aquell any**, suprimint una capacitat prevista de **-4,9 milions de tones per any** i reduint la projecció del pipeline global per a 2030 d'uns **49 a només 37 milions de tones** [1].

En el cor del complex, les torres que s'havien erigit com a símbols d'una nova era van quedar silenciades. Els enginyers que havien dedicat anys a optimitzar els processos d'electròlisi es van trobar mirant els seus equips amb una mirada que oscil·lava entre la frustració i l'acceptació: el cost de l'hidrogen verd havia pujat un **25-40 % des de 2022**, situant-se ara entre **4 i 7 euros per quilogram** —gairebé tres vegades més car que el seu predecessor gris, que encara rondava els **1,5-2,5 euros/kg**, i clarament per damunt del blau amb captura de carboni (CCS), que es mantenia en un rang de **2-3,5 euros/kg** [2].

La conclusió que ressonava a Immingham va viatjar molt més enllà de les parets del complex; es va convertir en un eco que recorria la cadena de subministrament global, recordant a tots els actors del sector que l'optimisme sense dades pot ser tan perillós com la inacció. L'hidrogen verd, tal com s'havia imaginat —energia per a tot—, no era viable a gran escala en aquell moment. El despertar d'aquest somni sobredimensionat marcava el principi d'una nova etapa: una crida a l'honestedat i a la revaloració de les apostes, centrant-se en aplicacions concretes —acer, fertilitzants i química— on l'hidrogen verd pot aportar realment un canvi substancial.

El somni de l'hidrogen

Quan Paul Roberts, a *The End of Oil* (2004), dedicava a l'hidrogen un capítol titulat irònicament *And Now for Something Completely Different*, aquest gas es presentava com la peça clau d'una economia neta: un combustible que, en cremar-se, només deixaria empremta d'aigua i, per tant, podria substituir el petroli sense deixar empremta de carboni. La visió, tan seductora, va mobilitzar inversors, governs i grans conglomerats energètics; les previsions apassionades anunciaven una transició ràpida cap a una xarxa global d'estacions d'hidrogen, turbines alimentades per aquest gas net i un «cicle de vida» completament sostenible.

Aquesta esperança es va alimentar amb números espectaculars i amb una allau de projectes d'escala industrial, com les megainversions d'Air Products a Immingham o el projecte de BP a Duqm, Oman. La idea era clara: si es podien produir milions de tones anuals, el mercat s'ajustaria i l'hidrogen es convertiria en la nova base energètica.

Però la realitat del 2025 va trencar aquest conte d'optimisme amb una crida a l'honestedat. Aproximadament seixanta grans projectes d'hidrogen verd van ser cancel·lats aquell any i, com hem vist,

la producció prevista es va reduir dràsticament mentre els preus augmentaven entre un 25 % i un 40 %, situant-se a una franja de 4-7 €/kg [1].

A més, la infraestructura necessària per distribuir hidrogen a escala global —dipòsits, conductes i estacions de servei— encara presenta barreres tècniques i reguladores. Les pèrdues en el transport i les dificultats per emmagatzemar-lo de manera segura fan que la proposta d'«hidrogen universal» sigui menys atractiva que alternatives com l'electricitat directa. Paral·lelament, la captura i emmagatzematge de carboni (CCS) avança a un ritme lent i és cara, deixant el blau amb CCS en una posició incerta [2].

Així, la promesa original —un combustible net que només deixa aigua— s'ha vist diluïda per les limitacions econòmiques i tecnològiques. L'hidrogen verd encara té un paper crucial, però ja no com a solució universal, sinó com a complement especialitzat en sectors on el carboni és intrínsecament difícil d'eliminar: la producció d'acer, els fertilitzants i les reaccions químiques de base. En aquests nínxols l'impacte pot ser mesurable i justifica inversió dirigida, però cal abandonar la narrativa d'«energia per a tot» i adoptar una perspectiva basada en dades concretes i riscos ben quantificats.

El reset de 2025

El 2025 va marcar un punt d'inflexió que ha sacsejat les expectatives més optimistes sobre l'hidrogen verd. En un any iniciat amb promeses d'inversions massives i una allau de projectes anunciats com a pilars de la transició energètica, el mercat es va enfrontar a dades dures: aproximadament 60 dels grans projectes d'H_2 verd van ser cancel·lats. Aquest retrocés suposa una pèrdua estimada de 4,9 milions de tones per any de producció potencial i ha reduït les projeccions globals d'H_2 verd en gairebé una quarta part respecte al pla original per al 2030. Ara l'expectativa és de 37 milions de tones anuals —una caiguda dràstica comparada amb els 49 milions previstos fa dos anys—, i s'ha concretat en casos emblemàtics com el projecte d'Air Products a Immingham (Regne Unit), la iniciativa de BP a Duqm (Oman) i l'esforç d'ArcelorMittal per descarbonitzar les seves plantes siderúrgiques a Alemanya [1].

Aquesta onada de cancel·lacions no és aleatòria, sinó el reflex d'un model econòmic massa fràgil davant la realitat del mercat. Molts projectes havien estat dimensionats per aprofitar subvencions i incentius governamentals sense una anàlisi rigorosa de la demanda real a curt termini. La feblesa de les comandes industrials —especialment en sectors que encara depenen fortament del carboni fòssil— ha deixat aquestes instal·lacions amb infraestructura costosa i sense clients suficients per justificar l'amortització de les despeses inicials.

A més, el cost de produir hidrogen verd s'ha disparat entre un 25 % i un 40 % des del 2022; actualment oscil·la entre 4 i 7 euros per quilogram, molt per sobre del preu de l'hidrogen gris i del blau amb captura de carboni —com hem vist—. Aquesta diferència fa que l'hidrogen verd sigui competitiu només en aplicacions on la reducció d'emissions aporta un valor afegit crític, com la producció d'acer, els fertilitzants i alguns processos químics, però resulta poc viable com a substitut universal per a combustibles fòssils en sectors com el transport pesat o l'electricitat de base.

L'impacte combinat d'una demanda insuficient i d'un augment de costos ha generat una espiral negativa: els inversors, atemorits pel retorn incert, han reduït les seves aportacions, provocant que més projectes es quedin sense finançament i reforçant la percepció que l'hidrogen verd encara és una aposta arriscada. Aquest escenari obliga a replantejar el paper de l'hidrogen dins del mix energètic: no com a solució universal, sinó com a component estratègic per a nínxols on la reducció d'emissions es tradueix directament en avantatges competitius i reguladors.

En resum, el 2025 ha funcionat com un «reset» brutal que ha obligat la indústria a abandonar les narracions de futur universalista i a adoptar una visió basada en dades concretes, costos transparents i una anàlisi rigorosa del mercat real. La lliçó més clara és que la viabilitat de l'hidrogen verd depèn menys d'una política d'incentius massiva i més d'una integració intel·ligent amb les cadenes de valor on el carboni és intrínsecament difícil d'eliminar, una perspectiva limitada en abast però capaç de generar impactes mesurables i sostenibles. [1][2]

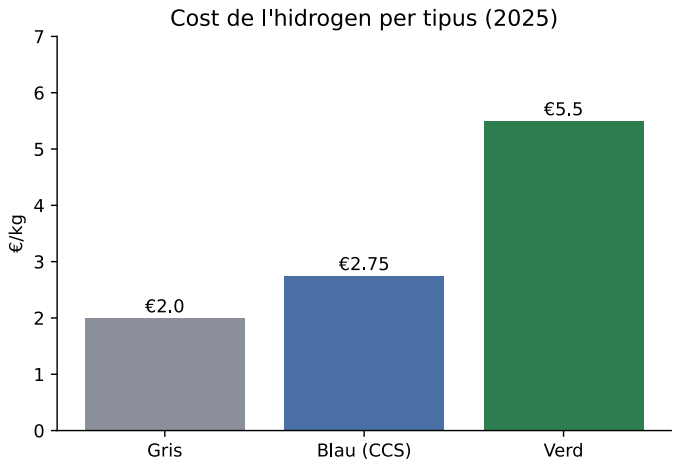


Figura 14.1 — L'hidrogen verd (€4-7/kg) encara és molt més car que el gris o el blau: el repte no és tècnic, sinó de cost i demanda.

On sí té sentit

A la vora del port d'Immingham, on les torres d'Air Products es perfilen contra el cel gris britànic, és fàcil imaginar un grup d'enginyers revisant els diagrames de flux de l'hidrogen verd que alimentaria una planta d'acer d'altes prestacions. L'objectiu no és celebrar una revolució energètica universal, sinó validar una aposta concreta: substituir el gas natural i el carbó en processos on l'electrificació directa encara és inviable o prohibitivament cara. En aquesta zona, l'hidrogen verd es converteix en una eina de precisió, no en una bala de plata que prometi una transició massiva sense fonaments.

En el sector siderúrgic, la reducció del ferro mitjançant hidrogen (Direct Reduced Iron, DRI) ofereix una ruta clara per descarbonitzar un procés que tradicionalment depèn del carbó. Les iniciatives d'ArcelorMittal per portar l'hidrogen verd a les seves plantes a Alemanya apunten en aquesta direcció, encara que el cost addicional —que ha pujat un 25-40 % des de 2022, situant-se entre 4 i 7 € per kilogram — continua sent una barrera real [2]. Quan s'integra directament al flux productiu, aquest sobrecost es pot compensar amb l'estalvi en drets d'emissió i evita la necessitat d'una infraestructura elèctrica a gran escala per alimentar una planta totalment elèctrica.

En l'àmbit dels fertilitzants, l'amoníac continua sent un dels pilars del sistema alimentari mundial. La producció convencional depèn gairebé exclusivament del gas natural com a font d'hidrogen gris; substituir-lo per hidrogen verd permetria reduir-ne dràsticament les emissions de CO_2. Com ja s'ha assenyalat, el cost superior (entre 4 i 7 € per kilogram) pot ser compensat en plantes integrades per la millora de l'eficiència del procés i els incentius a la reducció d'emissions, fent viable la producció a escala regional. Aquesta aplicació esdevé una de les «zones sense alternativa», on l'electrificació directa no pot substituir la naturalesa intensiva del procés químic.

En la química fina i petroquímica, l'hidrogen verd ja s'utilitza com a reactiu clau en processos d'hidrogenació que requereixen condicions de pressió i temperatura difícils de reproduir amb electricitat. La integració de reactors alimentats per hidrogen verd permet reduir les emissions indirectes associades al transport del gas i afavoreix una cadena de subministrament més neta. Disposar d'hidrogen verd produït localment redueix els riscos logístics i millora la traçabilitat del producte final.

Finalment, en el sector dels transports pesants —camions de llarg recorregut i vaixells de càrrega— l'hidrogen verd i els seus derivats sintètics ofereixen una alternativa possible on les bateries d'alta capacitat encara no són pràctiques. És, justament, un dels usos que la retallada del pipeline ha aplaçat: projectes com el de BP a Duqm, cancel·lat al desembre, han quedat en suspens [1].

En resum, l'hidrogen verd no morirà; simplement trobarà el seu lloc en les àrees on la substitució per alternatives elèctriques és tecnològicament impossible o econòmicament inacceptable. La clau és tractar-lo com una eina de precisió —una peça que encaixa perfectament dins de processos industrials específics— i no com una solució universal per a totes les formes d'energia. Aquesta visió, basada en dades reals i casos concrets, ofereix un camí clar cap a una descarbonització mesurable i sostenible.

La captura de carboni i les apostes que falten

A l'alba del 2026, la tecnologia de captura i emmagatzematge de carboni (CCS) continua sent una promesa incompleta. Avança poc i continua sent cara: el cost per tona de CO_2 capturat encara supera amb escreix les expectatives econòmiques de la majoria d'indústries. Aquest desequilibri ha convertit la CCS en un refugi sospitós per a actors que busquen prolongar la vida útil dels actius fòssils sense afrontar el veritable desafiament de reduir la demanda d'energia basada en hidrocarburs.

La captura de carboni encara representa una fracció mínima de les emissions globals de CO_2. La realitat és que la tecnologia funciona bé en escenaris controlats —per exemple, en refineries o en grans fonts puntuals d'emissió— però topa amb barreres tècniques i reguladores quan s'intenta aplicar a fonts disperses com el sector del ciment o l'acer. A més, les estructures de finançament actuals penalitzen els projectes de llarg termini: els inversors prefereixen retorns ràpids, mentre que la vida útil d'un dipòsit subterrani segur s'estén durant dècades.

Aquesta situació ha alimentat una narrativa perillosa: presentar la CCS com a «bala de plata» per a les emissions difícils i, alhora, utilitzar-la com a justificació per retardar polítiques més contundents d'abandonament del petroli. La veritat és que la captura pot ser útil en nínxols específics —com el tractament de les emissions de processos siderúrgics o la producció d'hidrogen blau amb CCS—, però només si es combina amb una reducció real de l'energia basada en combustibles fòssils i amb una política clara que limiti les noves instal·lacions de carboni. No és casual que BP, el mateix any que cancel·lava Duqm, també posés en pausa el seu projecte d'hidrogen blau amb CCS a Whiting.

Mentre la CCS avança a pas lent, altres apostes emergents guanyen protagonisme. L'emmagatzematge d'energia de llarga durada es presenta com una solució clau per equilibrar les fonts renovables intermitents, amb projectes que exploren la conservació d'energia en cavernes salines i altres formacions geològiques. La geotèrmia avançada, impulsada per noves tècniques de perforació i recirculació d'aigua, comença a obrir-se camí. I les xarxes elèctriques contínues —basades en convertidors HVDC de nova generació— ajuden a reduir les pèrdues de transmissió i faciliten la integració d'energia renovable des de zones remotes cap als centres de demanda. Cap d'aquestes opcions és, per si sola, una «bala de plata».

En aquest context, l'enfocament ha de ser holístic: la CCS esdevé una eina complementària per a emissions difícils de reduir, però no el nucli d'una estratègia de descarbonització. Les inversions han de prioritzar tecnologies que ofereixin flexibilitat i escalabilitat, com l'emmagatzematge d'energia de llarga durada i la geotèrmia avançada, alhora que es reforcen les polítiques reguladores per evitar que la CCS s'utilitzi com a pretext per mantenir vives les infraestructures fòssils. Només així podrem garantir una transició veritable cap a un futur energètic sostenible i resistent.

La promesa i el perill

En els escenaris industrials on la descarbonització és una obligació reglamentària i no només un objectiu de reputació, l'hidrogen verd s'ha convertit en una peça clau d'un trencaclosques energètic. A les siderúrgiques europees, per exemple, la reducció directa del ferro requereix una font de calor i un agent reductor que no es poden substituir fàcilment per electricitat sense una inversió massiva. Aquí, un flux constant d'H_2 verd —produït a partir d'energia eòlica o solar— permet mantenir la producció sense augmentar les emissions de CO_2. De manera similar, en la fabricació de fertilitzants, on l'amoníac concentra una part molt important del consum d'hidrogen, la transició cap a H_2 verd redueix les emissions associades al procés, tal com apunten diversos projectes pilot del sector.

Aquesta promesa es veu reforçada, en alguns casos, per la captura i emmagatzematge de carboni (CCS). Encara que el desplegament global de la CCS ha avançat poc, les instal·lacions integrades amb processos d'hidrogen blau —on el gas natural és reformat i el CO_2 resultant és capturat abans de ser alliberat— poden oferir una transició pragmàtica cap a un sector més net. La combinació d'H_2 verd per a les aplicacions on l'electrificació directa encara no és viable, amb H_2 blau alimentat per CCS per a usos intermedis, dibuixa una arquitectura energètica que pot reduir emissions allà on avui no hi ha alternativa neta.

No obstant això, la temptació de presentar aquest conjunt com una solució universal amenaça d'allunyar-nos del camí més econòmic i eficient. La majoria dels estudis comparatius mostren que electrificar directament processos com el transport de mercaderies per carretera o la calefacció residencial sol ser força més barat que substituir-los per H_2 verd, tenint en compte els costos actuals del combustible (entre

4 i 7 €/kg) i la infraestructura associada [2]. A més, la proliferació d'ofertes «verdes» sense una certificació rigorosa ha alimentat un mercat de crèdits d'hidrogen que es comporta com les primeres borses de carboni: el risc de greenwashing augmenta a mesura que les empreses busquen complir objectius ESG amb solucions aparentment senzilles però poc substancials.

El perill, per tant, no és només econòmic sinó també estructural. Promoure l'hidrogen verd i la CCS com a resposta única pot retardar inversions crucials en infraestructura elèctrica de gran escala —com les xarxes de recàrrega ultraràpida o els magatzems d'energia amb bateries— que són necessàries per aprofitar al màxim l'excés renovable. Cada any que es destina capital a instal·lar una planta d'electròlisi de gran capacitat, en comptes de reforçar la xarxa elèctrica o desenvolupar sistemes de gestió de la demanda, es perd una oportunitat de reduir les emissions globals amb un cost marginal inferior.

L'hidrogen verd i la CCS són components imprescindibles del trencaclosques industrial: ofereixen solucions viables per a sectors on l'electrificació directa encara no és factible. Però el seu valor real només es manté si s'utilitzen de manera focalitzada, sense pretensions d'universalitat que podrien desviar recursos i retardar la transició cap a una electrificació més àmplia i econòmicament eficient. La clau és equilibrar les apostes: prioritzar l'electricitat on és més rendible i reservar l'hidrogen verd i la CCS per als nínxols que realment ho necessiten.

El preu del temps perdut

Imaginem un matí a Immingham, al nord d'Anglaterra: les torres de la planta d'Air Products, que fa uns anys prometia ser el far de l'hidrogen verd, queden ara silenciades darrere d'una paret d'avisos de cancel·lació. El projecte, juntament amb una seixantena d'iniciatives similars, va ser retirat del programa global el 2025, reduint la producció prevista en gairebé cinc milions de tones anuals (-4,9 Mt/any) [1]. Aquesta caiguda no és un simple retrocés numèric; és un senyal d'alerta que demostra com l'excés d'esperança pot esdevenir una càrrega per a la transició energètica.

El col·lapse s'explica pel desajust entre les expectatives de mercat i les realitats tècniques i econòmiques. El cost de l'hidrogen verd ha augmentat entre un 25 % i un 40 % respecte al preu del 2022, situant-se ara entre 4 i 7 €/kg [2], superant àmpliament el de l'hidrogen gris (1,5-2,5 €/kg) i fins i tot el del blau amb captura de carboni (2-3,5 €/kg) [2]. En un context on les inversions són cada vegada més exigents i el finançament es dirigeix cap a solucions amb retorns més ràpids, l'hidrogen verd continua sent una zona gris: prometedor, però massa car per ser adoptat a gran escala sense subsidis massius. Aquesta realitat ha afectat també els grans projectes de pipeline previstos per al 2030, que han caigut de 49 a 37 Mt —com hem vist anteriorment—, fragmentant la cadena de subministrament i limitant les oportunitats en sectors clau com l'acer, els fertilitzants o la química.

Però el veritable perill resideix en el temps perdut. Cada any que es retarda l'adopció d'una infraestructura d'hidrogen verd i CCS on té sentit implica més emissions de carboni, costos de descarbonització més alts i una dependència creixent del gas natural i dels combustibles fòssils. La manca d'acció amplifica la necessitat de solucions alternatives, com l'electrificació directa en processos industrials, que es mostra cada cop més competitiva tant a escala tècnica com econòmica.

En aquest escenari, decidir on i com invertir és crucial. No podem permetre que el «hype» ens desviï cap a projectes amb retorns llargs i incerts; hem d'orientar els recursos cap a nínxols on l'hidrogen verd ofereix un avantatge clar: la descarbonització de processos que no es poden electrificar fàcilment, com la reducció del ferro o la síntesi d'amoníac. Simultàniament, cal impulsar la recerca i el desenvolupament de tecnologies CCS més eficients i menys costoses, per assolir una transició realista i equilibrada.

En resum, si no despleguem aquestes solucions amb l'urgència que demanen, el cost de la inacció es traduirà en un augment dels preus energètics, una inseguretat climàtica més gran i una oportunitat perduda per posicionar les economies europees com a líders en tecnologies netes. Amb això es tanca el repàs de les solucions energètiques. La Part V trasllada aquesta mateixa urgència al terreny de la confiança: per què detectar les falsificacions no basta, i com la prova d'existència comença a desplegar-se als primers fronts —finances, fotoperiodisme, sanitat, educació i drets humans.

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

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

Detectar no n'hi ha prou: la prova d'existència com a defensa duradora

«Perquè una tecnologia tingui èxit, la realitat ha de prevaler sobre les relacions públiques, perquè la natura no es pot enganyar.»

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

Era una tarda freda de gener del 2026 quan l'editorial **LlumVerda** va rebre, a través del seu canal segur de transferència de fitxers, un vídeo que prometia canviar el curs de les eleccions locals a Barcelona. El clip mostrava el candidat principal, en Marc Soler, pronunciant una frase incendiària: *«Els impostos per a la cultura augmentaran un 30 % aquest any»*. La veu era clara, l'expressió facial semblava genuïna i el fons d'una sala de reunions municipal es reconeixia instantàniament. L'equip editorial, conscient del creixement exponencial dels deepfakes —de 500.000 el 2023 a gairebé **8 milions** el 2025 segons Sumsub [9]—, va sotmetre el fitxer al *DeepSight Pro*, el detector de manipulacions més avançat disponible en aquell moment. El programa, alimentat per una xarxa neuronal entrenada amb les últimes bases de dades de falsificació, emetia un informe sucint: **«Probablement autèntic»**, amb un percentatge de confiança del 78 %.

Sense perdre temps, la redactora en cap, Laura Martínez, va programar la publicació al portal digital, afegint una breu nota que recordava als lectors que la veritat visual encara era fiable. El tràfic es va disparar: milers de comentaris i comparticions van aparèixer a les xarxes socials en qüestió d'hores, i el debat polític ja s'albirava encés.

Tres dies després, una alerta interna del departament de seguretat informàtica va revelar la veritat. El vídeo havia estat generat amb un model de síntesi més recent que qualsevol actualització del detector DeepSight Pro: la tecnologia per crear el fals s'havia avançat a la capacitat de detecció. Cap segell de procedència no acompanyava el fitxer, i el detector —entrenat amb falsificacions d'una generació anterior — havia estat enganyat. En altres paraules, la defensa reactiva sempre anava un pas per darrere de l'atacant.

Aquest escenari no és una ficció aïllada; les dades de *DeepFake-Eval-2024* mostren que els detectors fallaven entre un **45 % i 50 %** dels casos en entorns reals [1]. Cada vegada que depenem únicament de la detecció, ens trobem atrapats en una cursa armamentística on el generador avança més ràpid que l'anàlisi. La pregunta que emergeix és inevitable: **i si, en lloc de perseguir la mentida, poguéssim demostrar la veritat des del seu origen?**

La resposta a aquesta qüestió defineix el nucli de la defensa duradora proposta al llarg d'aquest capítol. No es tracta només de detectar una manipulació, sinó de **certificar la procedència i la integritat del contingut en el moment mateix en què es crea**, tal com recomanen les autoritats nord-americanes (NSA/FBI/CISA) a partir del 2023 [4]. Aquesta visió, que combina proves criptogràfiques amb ancoratge en blockchain —l'empremta del fitxer ancorada en una cadena pública, amb el segell de temps RFC 3161 com a complement, tal com l'aplica la iniciativa *t2p* [7]—, ofereix una resposta al perill de confiar únicament en detectors cada cop més obsolets.

En les properes seccions explorarem com aquesta prova d'existència es tradueix en cinc fronts sectorials — compliance, fotoperiodisme, sanitat, educació i defensa— i quins passos concrets podem prendre avui per transformar la teoria en pràctica. El futur de la veritat digital depèn, no només de veure bé, sinó de **saber d'on ve** i poder demostrar-ho sense dubte.

La cursa que perdem

En el moment en què la majoria d'organitzacions confien només en una línia de defensa —la detecció de deepfakes— es troben immerses en una carrera armamentística asimètrica que, fins ara, han perdut. El banc de proves DeepFake-Eval-2024, que recull mostres reals d'algoritmes generadors en circulació al mercat el 2024, revela unes caigudes dramàtiques: els millors detectors open-source registren una precisió del **45-50 %** respecte als entorns de laboratori, amb un rendiment de **0,75** en vídeo, **0,86** en àudio i **0,63** en imatge — tot per sota del **~90 %** que aconsegueix un analista humà entrenat [1]. Fins i tot els comercials més avançats arriben només al **78 %** d'exactitud, una diferència significativa quan es tracta de preservar la confiança en entorns crítics.

Aquesta bretxa no és casual. El fenomen del *domain shift* —on els models entrenats amb dades netes i controlades fallen en escenaris reals on àudio i vídeo són comprimits, codificats o manipulats per plataformes socials— crea una vulnerabilitat estructural que el simple reentrenament no pot tancar de manera sostenible. Cada vegada que s'introdueix un nou filtre de compressió o es modifica l'algoritme d'enregistrament, els models de detecció perden precisió i han de ser recalibrats; mentrestant, els generadors de deepfakes avancen a una velocitat exponencial, millorant la qualitat i l'eficiència dels seus resultats. En aquest joc d'intercanvi, l'atacant decideix *quan* i *com* atacar, deixant les defenses reactives en constant desavantatge.

El volum de contingut fals no fa sinó augmentar. Segons dades de Sumsub, el nombre de deepfakes circulants va passar de **~500.000** el 2023 a **~8 milions** el 2025 —un increment de més de quinze vegades en només dos anys [9]— i aquesta explosió amplifica la probabilitat que un contingut maliciós arribi a una audiència ampla abans que qualsevol detector pugui identificar-lo. A més, la proliferació d'eines de generació accessibles democratitza el poder de crear falsificacions convincentes, reduint les barreres d'entrada per a actors maliciosos i augmentant la diversitat dels escenaris d'atac.

En resum, dependre exclusivament de la detecció és com intentar tancar una porta amb una cadena mentre el lladre té una serra. Les limitacions tècniques —el *domain shift*, la manca de generalització sostenible— i l'escalada del volum i sofisticació dels deepfakes converteixen aquesta estratègia en una cursa que, fins ara, hem perdut. Per tal d'invertir el balanç, cal avançar cap a solucions que no només identifiquin el fals, sinó que **certifiquin l'origen i la integritat del contingut** des del moment de la seva creació; aquesta és la premissa fonamental sobre la qual es recolzen els cinc fronts sectorials que explorarem a continuació.

De la detecció a la procedència

En una aula de la Universitat de Stanford, el professor Hany Farid mostra a un grup d'alumnes una imatge aparentment autèntica d'un discurs polític i, amb uns quants clics, revela que el vídeo conté una capa de manipulació invisible per als ulls entrenats però no per la tecnologia actual de detecció. «La detecció reactiva és com intentar apagar un incendi després que l'edifici ja s'ha enfonsat», afirma Farid, i subratlla que **la clau és conèixer l'origen del mitjà**, tal com una etiqueta nutricional indica els ingredients d'un producte [2]. Aquesta metàfora il·lustra la limitació dels detectors —que cauen entre el 45 % i el 50 % en proves reals, segons l'estudi DeepFake-Eval-2024 [1]— i, com hem vist, ofereix una ruta clara: registrar la procedència des del primer instant.

L'expert de seguretat digital Sam Gregory, fundador de WITNESS, ha defensat durant més d'una dècada el programa **«Prepare, Don't Panic»**, una crida a construir una infraestructura d'autenticitat que vagi més enllà de la simple detecció [3]. En les seves presentacions, Gregory descriu com una cadena de confiança —captura firmada, metadades verificables i certificació d'origen— pot ser integrada directament en els fluxos de producció multimèdia. Aquesta infraestructura permet que cada fitxer porti amb ell una prova immutable del moment i del context en què es va crear, evitant que un deepfake pugui ocultar la seva veritable història.

Fins i tot les agències governamentals més conservadores reconeixen la necessitat d'aquest canvi de paradigma. La guia conjunta de la NSA, el FBI i l'oficina CISA —com ja es va assenyalar el 2023— estableix com a prioritat igual tant la detecció de continguts manipulats com l'establiment de la seva procedència [4]. El document subratlla que, si els generadors d'IA avancen més ràpidament que les eines de detecció, confiar únicament en identificar el fals és una aposta perduda; **verificar d'on ve i si ha estat alterat des de l'origen** ofereix una defensa matemàticament verificable i escalable.

Aquesta transició no és només tècnica sinó cultural. Passar de preguntar «És fals?» a preguntar «D'on ve i com ha evolucionat?» implica reconfigurar les pràctiques editorials, legals i empresarials. Els creadors han d'adoptar estàndards com el **C2PA/Content Credentials**, tot i la vulnerabilitat de les metadades eliminables [5]; i organitzacions com OpenTimestamps ja estan segellant milions de fitxers —al voltant de 750 milions de l'Internet Archive— amb transaccions blockchain, oferint una capa d'ancoratge irreversible [6].

En resum, la **procedència** es converteix en el nucli d'una defensa duradora contra les deepfakes. No és només un complement a la detecció; és l'alternativa que transforma la lluita per la veritat en un procés verificable i auditable des del primer instant de creació del contingut. Aquesta visió, recolzada per experts acadèmics, empresarials i governamentals, marca el punt d'inflexió cap a una era en què la confiança es basa en proves concretes i no en suposicions.

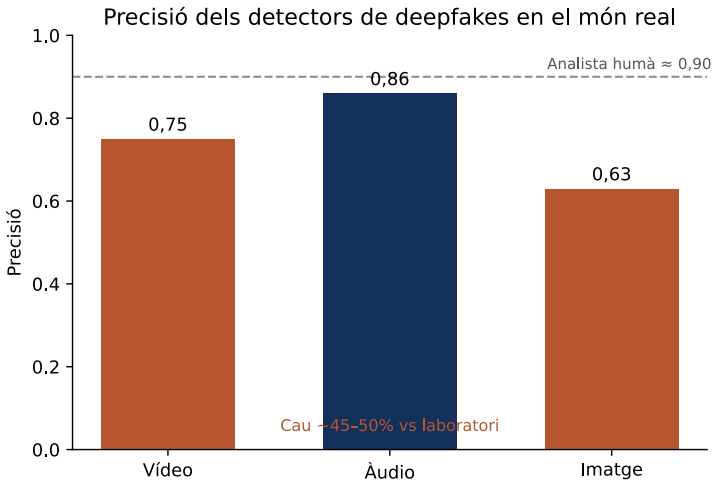


Figura 15.1 — La precisió dels detectors cau en el món real a mesura que milloren els generadors; una àncora de procedència no es degrada amb el temps.

Dues peces complementàries

En el panorama actual on les deepfakes proliferen a ritmes exponencials —de 500.000 casos estimats en 2023 a prop d'8 milions només l'any 2025 segons Sumsub [9]— la detecció per si sola es converteix en una cursa armamentística insostenible. Els detectors més avançats cauen entre un 45 % i un 50 % en proves reals (DeepFake-Eval-2024) [1], com hem vist, mentre que els generadors de contingut fals continuen superant les millores tecnològiques a una velocitat superior. La resposta sostenible ha d'anar més enllà del «veure i bloquejar»; ha d'establir una cadena de confiança inalterable des del moment de la creació i que persisteixi encara que les metadades siguin esborrades o manipulades.

C2PA / Content Credentials: el registre criptogràfic de l'origen

El consorci C2PA (Coalition for Content Provenance and Authenticity) ha desenvolupat els *Content Credentials*, un manifest signat amb certificats X.509 que captura, en forma d'estructura JSON, la informació clau del procés creatiu: qui va generar el fitxer, quines eines s'han utilitzat i en quin moment es van aplicar les diferents edicions. Aquesta infraestructura ofereix una prova criptogràfica de l'«qui/quan» en l'origen, permetent a editors, plataformes i consumidors verificar la procedència d'una imatge o vídeo sense dependre d'un tercer de confiança [5]. En el seu disseny, C2PA es basa en signatures digitals que, si es conserven íntegres, són impossibles de falsificar.

No obstant això, el model presenta una vulnerabilitat fonamental: les credencials poden ser eliminades. Les xarxes socials, els processos de recodificació i fins i tot la simple exportació d'un fitxer sovint suprimeixen o sobrescriuen aquest manifest. Quan la credencial desapareix, no queda cap empremta verificable del seu contingut original; la seva absència, per tant, no demostra res [5]. Aquesta limitació ha portat a experts com Hany Farid a afirmar que «la procedència és la millor defensa», però només si aquesta es manté accessible i intacta al llarg del cicle de vida del contingut [2].

Prova d'existència: l'àncora immutable

La solució a aquest buit es troba en el mecanisme de *proof of existence* descrit al capítol 13. La idea és simple però poderosa: calcular una empremta criptogràfica del fitxer —un hash— i ancorar-la en una transacció d'una blockchain pública. Aquesta operació crea una prova immutable que demostra que el fitxer existia en aquell moment, sense necessitat d'incloure cap metadada addicional; de manera complementària, un segell de temps conforme a l'estàndard RFC 3161, independent de la cadena, hi afegeix la certificació d'una autoritat qualificada. Projectes com OpenTimestamps ja han aplicat aquest enfocament a milions de fitxers de l'Internet Archive amb una sola transacció, com hem vist (Peter Todd) [6].

A diferència del C2PA, que depèn de la conservació del manifest, l'ancoratge de l'hash és independent de qualsevol capa intermèdia. Fins i tot si les metadades són suprimides o el fitxer es reprocessa, l'empremta ancorada a la blockchain conserva una àncora verificable que confirma l'existència inalterada del contingut original en la data registrada [7].

Sinergia entre procedència i prova d'existència

Les dues tecnologies no són rivals; són complementàries. C2PA aporta la informació «qui/quan» en el moment de la creació, mentre que l'empremta ancorada a la blockchain pública garanteix «això existia, inalterat, abans d'aquesta data». En combinar-les s'obté una defensa robusta que supera les limitacions de cada mètode per separat. La procedència pot perdre's, però la prova d'existència persisteix; alhora, la prova d'existència no revela qui va crear el contingut, però la credencial C2PA ho fa sempre que es mantingui.

Aquesta doble capa de verificació transforma la lluita contra les deepfakes d'una detecció reactiva a una arquitectura preventiva i auditable. Com recomanen les autoritats governamentals —NSA, FBI i CISA— en les seves directrius del 2023, establir la procedència és clau per garantir la integritat de la informació [4]. Sense l'àncora immutable de la prova d'existència, aquesta garantia es queda a mitges. La combinació d'ambdues peces forma una defensa duradora i verificable des del primer instant de creació fins al moment en què el contingut arriba a les mans del públic. Aquesta és la base sobre la qual els cinc fronts sectorials —compliance, fotoperiodisme, sanitat, educació i defensa— podran construir polítiques i sistemes resilients davant l'era de les deepfakes.

El «quan» inalterable: OpenTimestamps i RFC 3161

A la primavera, mentre els equips de verificació d'imatges es veien superats per l'explosió de les deepfakes —com hem vist[9]— una solució senzilla però poderosa començava a guanyar tracció: la prova de temps verificable. OpenTimestamps, l'estàndard obert ideat per Peter Todd, transforma qualsevol fitxer en una empremta digital immutable agrupant milers de hashes en un arbre de Merkle i ancorant-ne l'arrel a la cadena de blocs de Bitcoin amb una única transacció. Aquest procediment produeix una prova compacta que qualsevol pot validar sense dependre d'una entitat centralitzada, tal com descriu el seu disseny: «la prova és verificable per qualsevol, sense confiar en cap empresa» [6].

Fins al moment, OpenTimestamps ha segellat una gran quantitat de fitxers de l'Internet Archive amb una sola transacció a Bitcoin i converteix aquest vast catàleg històric en un registre immutable del seu moment d'existència [6]. Cada arrel d'arbre Merkle funciona com a testimoni criptogràfic: si el contingut es modifica, el hash resultant ja no coincideix amb l'arrel ancorada i la prova queda trencada. Així, el mecanisme ofereix una resposta directa al problema central de les deepfakes: **quan** va aparèixer per primera vegada un fitxer i que no s'ha alterat des d'aleshores.

Tanmateix, com avisa Hany Farid, «la procedència és la millor defensa» [2]; el segell de temps, tot i ser una garantia robusta del *quan*, no comprova l'autoria ni la veracitat intrínseca del contingut. Un vídeo pot estar perfectament ancorat a una data concreta i, alhora, contenir informació enganyosa o manipulada. Per això el model t2p ancora l'empremta SHA-512, calculada al mateix dispositiu d'origen, directament en una transacció d'una blockchain pública —aquest ancoratge és la prova— i hi afegeix, com a reforç independent de la cadena, un segell de temps RFC 3161 (l'estàndard eIDAS de segellat de confiança). Aquest «cinturó i tirants» assegura que, encara que les claus privades de l'autoritat de segellat caduquin o siguin compromeses, la prova pública continua sent verificable gràcies a l'empremta immutable emmagatzemada a la cadena [7].

Aquesta arquitectura també permet una integració fluïda amb infraestructures d'autenticitat emergents com WITNESS, que promouen «Prepare, Don't Panic» i ofereixen capes addicionals de verificació basada en metadades firmades [3]. En la pràctica, un creador de contingut pot generar l'empremta del fitxer al moment de la captura i ancorar-la en una blockchain pública —directament, o agregada en un arbre de Merkle mitjançant serveis com OpenTimestamps—, i afegir-hi, si necessita la certificació d'una autoritat, un segell RFC 3161 complementari. El resultat és una cadena verificable que indica: *aquest arxiu existia en aquesta data, sense alteracions posteriors*, i que pot ser contrastada amb les metadades de procedència registrades per WITNESS o altres entitats reguladores.

Aquesta combinació d'elements —empremta local, ancoratge en blockchain pública i segell RFC 3161 complementari— constitueix la base tecnològica de la defensa duradora contra les deepfakes. No es tracta només de detectar una manipulació, sinó de demostrar inequívocament el moment original de creació i mantenir-lo intacte al llarg del cicle de vida digital. En un entorn on els generadors d'IA evolucionen a ritmes accelerats, aquesta prova de temps esdevé la pedra angular per a les polítiques sectorials que abordaran la crisi de confiança: des del compliance corporatiu fins al fotoperiodisme, passant per sanitat,

educació i defensa. Sense ella, qualsevol detecció seria una cursa armamentística; amb ella, disposem d'un marc verificable que transforma la **procedència** en un actiu tangible i immutable.

El marc legal arriba

L'entrada en vigor del **EU AI Act**, article 50, el 2 d'agost de 2026 marca un punt d'inflexió clar: qualsevol contingut generat per intel·ligència artificial ha de portar una etiqueta llegible per màquina que indiqui la seva procedència i, específicament, les deepfakes han d'estar marcades com a «synthetic» [8]. En pràctica, les empreses que ja fan servir solucions **t2p** —l'empremta ancorada a la blockchain pública, amb el segell RFC 3161 com a complement, tal com hem descrit al capítol 13 [7]— es troben un pas endavant: la seva infraestructura pot generar automàticament la marca de procedència requerida per la normativa, convertint la prova d'existència en una resposta directa a l'obligació legal.

Als Estats Units, la **TAKE IT DOWN Act**, signada al maig del 2025, eleva la qüestió a un nivell penal. L'acte criminalitza explícitament la distribució no consentida d'imatges íntimes —incloses les «digital forgeries» o deepfakes— i imposa a les plataformes una obligació de retirada en **48 hores** des del moment de la denúncia [8]. El requeriment legal és inequívoc: les plataformes han de poder demostrar, amb evidència criptogràfica, que el contingut ha estat verificat o eliminat per complir l'ordre. Això converteix la **procedència** en una exigència operativa i no només en una bona pràctica.

L'última baula del trencaclosques legislatiu és la **DEFIANCE Act**, aprovada pel Senat al gener de 2026 i encara pendent de votació a la Cambra de Representants [8]. Aquesta llei afegeix una via civil per a les víctimes de manipulació digital, permetent que presentin reclamacions basades en la falta d'evidència verificable d'origen i integritat del contingut. En altres paraules, una **prova d'existència** —tal com la proporciona OpenTimestamps, que ha segellat milions de fitxers de l'Internet Archive [6]— esdevé un actiu decisiu per sostenir qualsevol reclamació.

El fil conductor d'aquestes tres iniciatives és clar: la llei ja no demana només «si el contingut és fals», sinó **«d'on ve i com es pot demostrar que era íntegre en una data concreta»**. Les empreses que encara depenen únicament de detectors —que, segons DeepFake-Eval-2024, fallen entre un 45 % i un 50 % en entorns reals [1]— es trobaran en una posició d'incompliment inevitable. En canvi, les que ja han integrat la prova d'existència a les seves cadenes de subministrament digital podran respondre immediatament amb unes metadades verificables i segells criptogràfics, evitant sancions i guanyant confiança del mercat.

Així doncs, el marc legal no només impulsa el **marcatge** de contingut; estableix una **exigència de demostració** que converteix la prova d'existència en un actiu indispensable. Les organitzacions que anticipin aquesta necessitat —com les que adopten els estàndards C2PA, tot i les limitacions de metadades eliminables [5]— podran transitar cap a una arquitectura de confiança resilient, evitant el risc de quedar «a remolc» davant d'una regulació que avança a pas ferm. La resposta no és només detectar; la resposta és **documentar**, **segellar** i **provar** —el fonament sobre el qual es construirà la nova era de credibilitat digital.

Cinc fronts

La crisi de confiança que hem exposat no és una catàstrofe abstracta; es tradueix en pèrdues econòmiques, danys a la reputació, riscos per a la salut i vides truncades. Cada sector comparteix una lògica comuna: **detectar** una deepfake només és el primer pas, sovint massa tard; la defensa real consisteix a **documentar**, **segellar** i **provar** la procedència del contingut des del moment de la seva creació.

1. **Compliance i finances** — El cas més emblemàtic recent és la videotrucada que va enganyar Arup, provocant un frau de 25,6 milions de dòlars. Sense una prova inequívoca de l'origen del vídeo, els equips de control van quedar atrapats en una cursa armamentística amb els generadors de deepfake, i la detecció posterior no va impedir el pagament indegut. Aquí la **prova d'existència** hauria permès validar quin material audiovisual era autèntic abans de qualsevol transacció, bloquejant l'estafa en la seva fase incipient.
2. **Fotoperiodisme i mitjans** — La imatge continua sent el testimoni més potent del moment. Quan una fotografia manipulada circula com a prova d'un esdeveniment, el dany reputacional per al diari o per al periodista és irreversible. Les eines de segellament com OpenTimestamps ja han **segellat al**

voltant de 750 milions de fitxers de l'Internet Archive, oferint una cadena de confiança que pot ser consultada per verificar la procedència d'una foto abans que arribi al públic [6].

3. **Sanitat** — Les imatges mèdiques manipulades amenacen diagnòstics i tractaments. Un escàner alterat podria conduir a una cirurgia innecessària o, pitjor encara, a l'omissió d'un tumor. En aquest context, la procedència certificada és la millor defensa, com recorda Hany Farid: «la procedència és la millor defensa» [2]. Un registre immutable de cada imatge —l'empremta ancorada a la blockchain pública, amb segell de temps complementari— garantiria que els professionals sanitaris treballin sempre amb dades originals i verificables [7].

4. **Educació** — Les credencials acadèmiques i l'autoria d'obres digitals són objectius constants de falsificació. Un diploma digital alterat pot obrir portes a empleats no qualificats, mentre que un article plagiat o manipulat pot desvirtuar el coneixement científic. La prova d'existència permetria registrar cada lliurament acadèmic amb una marca de temps segura, fent impossible la revisió retroactiva del contingut sense deixar rastre.

5. **Defensa i drets humans** — En conflictes armats, les deepfakes es converteixen en armes de desinformació que poden manipular l'opinió pública i falsificar proves de crims. La capacitat d'atribuir amb certesa la data i l'origen d'un vídeo o àudio és fonamental per a tribunals internacionals i per a organitzacions de drets humans. Sense aquesta capa, el risc de «falses narratives» esdevé una amenaça directa a la justícia.

En tots aquests fronts, la **lògica** és idèntica: detectar arrenca tard; demostrar-ho des de l'origen arriba a temps. En els capítols que segueixen explorarem com la prova d'existència s'integra en cada sector, revelant tant l'amenaça real com les solucions concretes per protegir-nos contra una era en què el fals pot semblar indistinguible del veritable.

La promesa i el perill

Imaginem una xarxa global d'autenticitat on cada vídeo, àudio o document digital porta amb orgull un segell immutable que certifica la seva data de creació i l'origen del node que l'ha generat. Aquesta capa de confiança verificable és tan barata com qualsevol transacció blockchain de baixa tarifa i es pot escalar a milions d'usuaris sense necessitat d'intermediaris centralitzats. El model proposat per **t2p** combina la procedència —la informació sobre qui, on i quan ha produït el contingut— amb l'ancoratge criptogràfic de l'empremta en una cadena de blocs pública, reforçat amb un segell de temps RFC 3161 independent de la cadena [7]. Quan un mitjà es veu atacat per deepfakes, el receptor pot consultar instantàniament la prova d'existència i verificar que aquell arxiu ja existia, intacte, a una data anterior al supòsit engany. En la pràctica, aquesta solució ha estat adoptada per projectes com OpenTimestamps, que ja ha segellat al voltant de **750 milions** de fitxers de l'Internet Archive amb una sola transacció [6], demostrant que el cost marginal és quasi nul i que la infraestructura pot suportar càrregues massives.

Aquesta promesa no és merament teòrica; organitzacions com WITNESS, liderada per Sam Gregory, ja han desplegat una infraestructura d'autenticitat que permet a periodistes i organitzacions de drets humans «preparar-se, no entrar en pànic» davant la manipulació digital [3]. La normativa europea, amb l'AI Act (Art. 50) aplicat des del 2 d'agost de 2026, exigeix explícitament que el contingut generat per IA porti una marca de procedència llegible per màquina per tal de reduir els riscos de difusió de deepfakes [8]. Això crea un marc legal que impulsa l'adopció massiva d'aquestes tecnologies i ofereix una base segura perquè les autoritats puguin actuar amb evidència verificable.

No obstant això, el perill resideix en la **desanonimització** potencial dels creadors vulnerables. Hany Farid recorda que «la procedència és la millor defensa», però també adverteix que, si es revela massa informació sobre l'origen, periodistes d'investigació, dissidents o víctimes de violència poden ser localitzats i perseguits [2]. Un sistema mal dissenyat podria convertir la procedència en una arma contra aquells que depenen del seu anonimat per a la seguretat personal; per això les metadades de procedència, com les credencials C2PA, han de poder gestionar-se amb cura [5].

A més, la confiança cega en el segell pot generar un **excessiu sentiment de veracitat**: «si porta segell, és veritat» es converteix en una fal·làcia que descuida les altres línies de defensa. La prova d'existència no detecta per si sola els falsos; només demostra que el contingut existia en un moment determinat. Sense una detecció activa —i sense alfabetització mediàtica que ensenyi a qüestionar i contrastar— la societat podria caure en una falsa seguretat, creient que el problema de les deepfakes s'ha resolt completament.

Per tant, cap tecnologia pot ser considerada una bala de plata. La solució robusta es troba en la **combinació** d'una procedència fiable, l'ancoratge criptogràfic, sistemes avançats de detecció i una educació contínua a la població sobre els límits i les vulnerabilitats d'aquestes eines. Només així podrem aprofitar la promesa d'una confiança verificable sense caure en el perill d'un control descontrolat o d'una confiança excessiva que, al capdavall, podria ser tan perjudicial com les deepfakes que pretén combatre.

Beth Noveck, al seu llibre *Reboot*, subratlla una realitat que sovint es passa per alt: els sistemes de detecció de deepfakes són essencialment una cursa armamentística en què l'atacant pot desactivar-los amb retalls mínims o compressions d'uns pocs kilobytes, i el resultat final és sempre probabilístic, no cert [10]. Aquesta vulnerabilitat fa que la confiança exclusiva en detectors sigui una il·lusió de seguretat; tan aviat com apareix un nou algorisme generador, els models de detecció s'obren a noves formes d'engany. La solució, per tant, no és millorar indefinidament la precisió dels detectors, sinó canviar el paradigma: passar de «detecta si és fals» a «prova que aquest contingut va existir amb una àncora neutral». L'ancoratge criptogràfic en una blockchain —independent del creador i sense dependre d'entitats centralitzades— ofereix la prova immutable que Noveck considera imprescindible, tancant el bucle on els detectors només poden jugar al joc de l'engany.

És hora d'actuar

Les plataformes digitals són la primera línia de defensa: han d'incorporar sistemes que preservin i mostrin la procedència verificada de cada fitxer multimèdia. Això significa integrar credencials de contingut basades en el model C2PA, però anar més enllà de les metadades que es poden suprimir; cal ancorar l'empremta de cada arxiu a una cadena de blocs pública o a un registre de temps fiable com OpenTimestamps, que ja ha segellat al voltant de **750 milions** de fitxers de l'Internet Archive [6]. Cada vegada que un vídeo o una imatge es puja, la plataforma ha d'emetre un «certificat d'origen» i fer-lo accessible al públic, permetent a qualsevol usuari rastrejar el camí complet des del moment de creació fins a l'última modificació.

Els creadors i mitjans han d'adoptar una cultura de publicació amb prova d'origen. No és suficient publicar una notícia; cal adjuntar la cadena de confiança que demostri on es va obtenir el material, quan es va crear i quina entitat l'ha signat digitalment. Aquest enfocament segueix la recomanació del NSA/FBI/CISA (2023) d'establir la procedència com a element clau per combatre les manipulacions [4]. A més, utilitzant el marc de **t2p** —l'ancoratge de l'empremta a la blockchain pública, amb el segell RFC 3161 com a complement—, els mitjans poden garantir una prova immutable i verificable sense dependre exclusivament de metadades vulnerables [7].

Les empreses i institucions han d'ancorar l'empremta de les seves dades crítiques abans de compartir-les. Qualsevol informe financer, estudi clínic o registre educatiu ha d'estar signat i segellat en una xarxa descentralitzada que ofereixi timestamps fiables. Això no només protegeix contra la substitució malintencionada de documents, sinó que també compleix amb les noves obligacions reguladores: l'EU AI Act (Art. 50) entra en vigor el 2 d'agost de 2026 i exigeix mecanismes de traçabilitat per al contingut generat per IA [8].

Els reguladors, per la seva banda, han de definir estàndards interoperables que garanteixin que totes les parts interessades puguin verificar la procedència sense barreres tècniques. Això implica l'adopció d'especificacions comunes com el C2PA, però també l'establiment de protocols d'auditoria i certificació per a proveïdors de serveis de timestamping i blockchain pública. La cooperació internacional serà clau per evitar una «barrera de confiança» que freni la innovació i alhora protegeixi els ciutadans.

Finalment, la ciutadania ha de convertir-se en el primer filtre: abans de creure o compartir un contingut, cal verificar-ne l'origen a través d'eines accessibles (extensions de navegador, apps mòbils) que consultin les credencials emeses per les plataformes i els mitjans. Aquesta pràctica, encara que senzilla, pot reduir dràsticament la propagació de deepfakes, que han passat de **500.000** casos el 2023 a prop de **8 milions** el 2025 segons Sumsub [9].

Davant la mentida industrialitzada, demostrar la veritat és l'acció més poderosa; ara podem transformar la prova d'existència en una defensa duradora. **Time2act** no és només un lema, sinó una crida a tots els actors de l'ecosistema digital perquè, amb procedència i timestamping, puguem recuperar la confiança i fer front a les deepfakes abans que elles ens superin.

[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, article 50 (transparència del contingut generat per 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. ↩

Diners i confiança: frau, compliance i finances

«Es diu que la llum del sol és el millor dels desinfectants; la llum elèctrica, el policia més eficient.»

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

A principis del 2020, el gerent d'una sucursal a Hong Kong d'una empresa japonesa va rebre una trucada amb una veu que coneixia bé: la d'un directiu de la casa matriu. El directiu li va explicar que l'empresa estava a punt de tancar una adquisició i que calia autoritzar transferències per valor de **35 milions de dòlars**. A la safata d'entrada hi havia correus del directiu i d'un advocat anomenat Martin Zelner que confirmaven l'operació, i el gerent va començar a fer les transferències. Tot era fals: la veu era un clon generat amb tecnologia de «deep voice». La investigació dels Emirats Àrabs Units, revelada per un document judicial, va identificar almenys **17 implicats**, amb els fons repartits per comptes de tot el món, i va rastrejar **400.000 dòlars** fins a comptes nord-americans del Centennial Bank; els EAU van acabar demanant ajuda als investigadors dels EUA [8].

Quatre anys més tard, l'estafa havia après a fer videotrucades. El gener de 2024, un empleat financer de l'oficina de Hong Kong de l'enginyeria britànica **Arup** va rebre la instrucció de transferir uns **25,6 milions de dòlars**; sospitava d'un correu de *phishing*, però una videoconferència amb el «director financer» i diversos «col·legues» —tots amb la cara i la veu exactes— el va tranquil·litzar, i va executar **15 transferències** a cinc comptes. Tots els participants de la trucada, tret d'ell, eren deepfakes [1]. El capítol 87 disseca aquest cas a fons; aquí ens ocupa el paisatge sencer: el frau, el compliment normatiu i la identitat financera.

Com va concloure el CIO d'Arup després de l'incident: «*Copiar una veu, una imatge o un vídeo és a l'abast de qualsevol amb poca habilitat tècnica.*» Si veure i sentir ja no basta per confiar, les finances necessiten una altra mena de prova.

Quan veure ja no és creure

L'era digital ha transformat la confiança en una qüestió de verificació constant, i el fenomen de les deepfakes està accelerant aquest canvi a una velocitat que supera qualsevol predicció anterior. Les xifres aporten una realitat incòmoda: Deloitte estima que el frau generat per intel·ligència artificial als Estats Units passaria de 12,3 mil milions de dòlars l'any 2023 a prop de **40 mil milions** el 2027 [2]. Aquesta escalada no és només una projecció econòmica; és la síntesi d'un ecosistema on les veus i les imatges dels directius esdevenen fàcilment manipulables.

En els darrers mesos, les empreses han denunciat **veus clonades de CFOs**, **vídeos sintètics que simulen reunions del consell** i **instruccions «urgents» enviades fora dels canals oficials**. Cada una d'aquestes estafes es fonamenta en la confiança humana: el reconeixement facial, l'autenticitat vocal i la familiaritat amb els gestos corporals eren considerats indiscutiblement fiables fins fa poc. Ara només cal un algorisme de generació d'imatge o una aplicació de síntesi de veu per crear un engany indistinguible del real.

L'impacte més corrosiu no resideix en les pèrdues monetàries directes, sinó en el **dubte sistèmic** que s'estén a tot l'entorn financer. Quan una trucada aparentment legítima pot ser un deepfake, les organitzacions han d'incrementar dràsticament els processos de verificació, generant més temps d'espera per confirmar pagaments, major despesa en tecnologies d'autenticació i una càrrega administrativa que dilueix l'eficiència operativa. Aquesta fricció no només eleva costos directes; també minva la velocitat de negociació, retardant inversions i desincentivant col·laboracions internacionals.

A més, el cost d'una verificació errònia es fa evident en casos com l'incident d'Arup a Hong Kong el 2024, on una videotrucada on **tots els assistents — inclòs el CFO — eren deepfakes**, provocant la transferència de **25,6 milions de dòlars** sense cap rastre fiable [1]; **com hem vist**, una sola vulnerabilitat pot desencadenar pèrdues massives i erosionar la confiança en tot el sistema bancari.

Les autoritats ja han començat a respondre. L'**EU AI Act**, amb l'article 50 que obliga a l'etiquetatge de deepfakes a partir del **2 d'agost de 2026** [5], i les directrius del **NIST SP 800-63-4**, que fan obligatòria la detecció d'atacs d'injecció en nivells alts per a processos biomètrics [4], són passos essencials cap a una defensa normativa. No obstant això, aquestes mesures només mitiguen el problema si les institucions adopten una arquitectura de confiança que vagi més enllà del simple reconeixement visual o auditiu.

En síntesi, la proliferació de deepfakes transforma cada interacció financera en un escenari d'incertesa. El cost ocult —el temps i els recursos dedicats a validar la veracitat de cada comunicació— es converteix en una càrrega estructural que amenaça la fluïdesa del mercat global. Per tal de preservar l'estabilitat del sistema financer, cal una resposta que restableixi la confiança no només en les aparences, sinó en l'origen verificable i immutable de cada transacció.

El front del KYC: atacs d'injecció

En una oficina de registre bancari a Nova York, un operador va rebre la sol·licitud d'un nou client que, al primer cop d'ull, semblava completament legítima: un document d'identitat escanejat i un selfie recents. El flux de verificació es va interrompre quan una capa invisible de programari —una càmera virtual injectada en temps real— va substituir la imatge del dispositiu per una versió generada per IA, produint un «selfie» perfectament alineat amb el document però que era, en realitat, una deepfake avançada capaç de superar els algoritmes biomètrics més sofisticats.

iProov registra un augment dràstic d'atacs d'injecció i bypass biomètric contra processos KYC. Un informe descriu com una deepfake va obrir desenes de comptes fraudulents en un banc, explotant la vulnerabilitat del model «document + selfie» [4]. L'atac no només enganya el reconeixement facial; manipula tota la cadena d'entrada de dades, fent que cada pas —captura de la imatge, compressió, transmissió i anàlisi— es realitzi sobre una base falsificada. La resposta tècnica emergent parteix d'una premissa fonamental: la integritat ha de quedar lligada al moment i al punt de captura, no només a l'arxiu final. La norma NIST SP 800-63-4 ja imposa, des del nivell més alt d'assegurament, la detecció obligatòria d'atacs d'injecció [4]; per això els sistemes han d'establir una «captura firmada», un registre criptogràfic inserit en el moment en què el sensor físic captura la imatge, de manera que qualsevol manipulació posterior —inclosa l'addició d'una capa virtual— esdevingui evident perquè el hash de la captura original ja ha estat arxivat a una cadena immutable.

Aquesta lògica sustenta la infraestructura de prova d'existència (t2p) de *time2act*. En lloc d'aplegar-se únicament al contingut del document, el sistema genera una empremta temporal i verificable que es guarda en un registre distribuït; cada selfie, escaneig o senyal biomètrica es converteix en una transacció immutable, de manera que qualsevol intent d'injecció hauria de reescriure la cadena de blocs i seria detectat immediatament.

L'impacte no es limita a reduir el frau: respon també a les alertes regulatòries recents, com l'avís de FinCEN del 13-nov-2024 sobre la necessitat de reforçar els controls CDD davant deepfakes [3] i l'obligació del EU AI Act art. 50 d'etiquetar aquest tipus de contingut a partir del 2-agost-2026 [5]. Amb una captura segura i un registre verificable, les institucions financeres poden complir aquestes exigències sense haver d'afegir cap capa operativa onerosa.

En síntesi, la verificació d'identitat ha passat del paper i la pantalla al moment en què es genera la senyal. La combinació de detecció d'injecció obligatòria (NIST) i de proves d'existència immutables (t2p) crea una barrera que, fins ara, els defraudadors no han pogut superar; el repte és desplegar aquesta arquitectura a escala global, amb la confiança radicada en l'origen verificable, no en aparences enganyoses generades per la IA.

El regulador es mou

Com hem vist, el 13-novembre 2024 FinCEN va llançar una alerta que ressonava com un llampec a les sales de consells d'administració i als departaments de compliance de tot el món: les deepfakes i la IA generativa s'estaven convertint en eines preferides per burlar la verificació d'identitat i els controls de diligència deguda (CDD) [3]. L'avís no només descrivia una nova amenaça, sinó que exigia un canvi immediat en la manera com les institucions registren i informen les sospites. FinCEN va demanar que els informes de sospita relacionats incorporessin el terme clau «FIN-2024-DEEPFAKEFRAUD», creant així un marcador uniforme per a l'anàlisi posterior i la cooperació transfronterera. Aquesta petició, encara que aparentment senzilla, obliga les entitats financeres a revisar els seus sistemes de detecció, a integrar tecnologies d'autenticació avançada i a establir processos d'auditoria capaços de rastrejar l'origen real d'una imatge o àudio.

Com ja s'ha indicat, l'article 50 de l'EU AI Act va establir que a partir del 2-agost-2026 totes les produccions de contingut generat per IA —incloent-hi deepfakes— hauran d'estar clarament etiquetades com a tal [5]. L'etiquetatge no és només una advertència visual; implica la inserció de metadades

verificables que poden ser llegides per sistemes automatitzats de compliance, i facilita la detecció precoç i la tria d'accions correctives. Aquesta obligació crea un marc legal que converteix la transparència en una exigència normativa, no en una opció empresarial.

A més, el nou eIDAS 2.0 ha introduït dos components clau: els Qualified Electronic Ledgers (QEL) i el Qualified Electronic Archiving (QEA). Aquests registres electrònics certificats ofereixen una traça d'auditoria immutable que es pot validar a escala reguladora [6]; cada transacció, document de KYC o informe de sospita queda registrat en un ledger qualificat i el seu arxiu es manté en un entorn d'arxiu electrònic que garanteix la integritat i la inalterabilitat al llarg del temps. Aquesta infraestructura permet a les autoritats verificar no només que una informació s'ha presentat, sinó també que prové d'una font autèntica i no ha estat manipulada posteriorment.

El missatge que emergeix és clar: el compliance ja no es pot limitar a «guardar PDFs». La mera conservació de documents escanejats o en format digital tradicional no ofereix cap garantia contra les sofisticades simulacions creades per la IA. L'objectiu passa, com hem vist al NIST SP 800-63-4, a demostrar —de manera verificable i auditable— la integritat i l'origen d'una informació des del moment de la seva creació, mitjançant detecció d'injecció obligatòria, proves d'existència immutables com t2p i els QEL/QEA regulats per eIDAS 2.0, formant una barrera gairebé infranquejable per als defraudadors.

Aquesta evolució normativa no només eleva el nivell de seguretat, sinó que crea un ecosistema on la confiança es basa en l'origen verificable i no en aparences enganyoses generades per algoritmes. Les empreses que adoptin aquestes pràctiques avançades podran transformar el seu model de compliance d'una tasca administrativa a una defensa proactiva contra les amenaces emergents, convertint-se així en pioneres d'un nou paradigma de confiança digital.



Figura 16.1 — En el frau per deepfake, la confiança es trenca en la identitat i la instrucció; una prova d'existència ancorada a l'origen hi posa un punt de verificació independent.

Proves que es poden fabricar

En el món judicial contemporani, la cadena de custòdia és el pilar sobre el qual es recolzen les proves digitals: metadades que registren cada manipulació, testimonis que certifiquen l'origen i documents que garanteixen la integritat. Aquest model, nascut a l'era del paper i del format electrònic, està ara sotmès a una erosió profunda provocada per les deepfakes; quan un vídeo o una gravació d'àudio es genera íntegrament amb IA, el simple fet de presentar metadades ja no és suficient i la confiança en l'autenticitat es desmunta davant d'un atac capaç de reproduir amb precisió qualsevol veu o cara coneguda.

A Hong Kong, com hem vist, una operació fraudulenta del 2024 va substituir uns «CFO» i diversos executius per avatars generats per IA en una videotrucada que autoritzà la transferència d'una suma important cap a comptes externs. La transacció es va validar perquè els participants creien estar davant d'identitats reals, mentre que tots eren deepfakes [1]. Aquest cas il·lustra com la falsificació no només afecta les finances sinó també el procés judicial: si una prova audiovisual pot ser enganyosa, qualsevol judici basat en ella esdevé vulnerable.

Als Estats Units, la resposta legislativa avança cap a un marc més rigorós. La **Federal Rules of Evidence 707 (FRE 707)** —de nova incorporació— introdueix criteris específics per a les proves generades per màquina, exigint que es demostri la seva fiabilitat i la impossibilitat de manipulacions posteriors [7]. Paral·lelament, la proposta de regla **901(c)** busca establir un estàndard per a les evidències electròniques potencialment fabricades o alterades, obligant els advocats a presentar una prova d'origen verificable abans que el jutge pugui acceptar-les com a vàlides [7].

Aquestes noves disposicions converteixen la prova d'existència —un hash criptogràfic ancorat amb segell de temps— en un requisit essencial per a qualsevol document o imatge que es pretengui presentar davant del tribunal. Un hash, generat en el moment de la creació i registrat en una cadena de blocs pública, ofereix una empremta digital immutable: cap alteració posterior pot modificar-lo sense ser detectada. Així, l'auditoria d'e-discovery passa a dependre no només de la recollida d'arxius, sinó també de la certificació que aquests arxius van existir en un instant determinat i que el seu contingut no ha variat des d'aleshores.

L'impacte es veu reforçat per les regulacions emergents; l'EU AI Act obliga a etiquetar qualsevol contingut generat per IA com a «deepfake» a partir del 2 d'agost de 2026 [5], i el marc eIDAS 2.0 introdueix els Qualified Electronic Ledgers i l'Arxiu qualificat, que garanteixen una auditoria a prova de manipulació per a documents electrònics crítics [6].

Com hem vist, la combinació d'una normativa més estricta (FRE 707, regla 901(c)) i de l'estàndard tècnic NIST SP 800-63-4, que exigeix detecció d'atacs d'injecció en nivells alts [4], junt amb solucions basades en blockchain per a la prova d'existència, crea una nova infraestructura de compliance. Aquesta no només protegeix les finances sinó també la integritat del sistema judicial, convertint el procés de verificació d'una tasca reactiva en una defensa proactiva contra la fabricació de proves; la clau és que cada document, imatge o àudio pugui ser rastrejat fins al seu origen i corroborat amb un segell de temps inalterable.

La prova d'existència com a infraestructura de compliance

Quan una organització decideix que la confiança ha de començar **a l'origen**, el primer pas és capturar cada dada d'identitat amb una firma digital immutable i verificable en temps real. En el procés d'incorporació, el KYC es captura des del dispositiu de l'usuari mitjançant un certificat de clau pública que genera un hash del document presentat (passaport, carnet o selfie biomètrica). Aquest hash, anomenat *proof of capture*, se signa instantàniament amb una clau privada custodiada al Secure Enclave i queda lligat a un segell de temps conforme a la normativa RFC 3161; el resultat es publica en una cadena de blocs pública que garanteix **resistència a l'atac d'injecció** descrita per iProov i exigida pel NIST SP 800-63-4 [4]. Així, qualsevol intent de substituir la imatge biomètrica amb una càmera virtual queda detectat: el hash emmagatzemat a la cadena no coincideix amb cap altra versió del fitxer.

Un cop registrada la captura, es genera una **traça d'auditoria immutable** que combina el hash original, el segell de temps i l'ancoratge en blockchain. Aquest registre és accessible per a auditors i reguladors sense exposar el contingut sensible, ja que només es comparteixen les proves criptogràfiques (hash i signatures). Quan una entitat ha de demostrar la veracitat d'un document davant un tribunal, pot presentar aquest conjunt de metadades com a **evidència de procedència**. Els tribunals nord-americans, per exemple, ja disposen de regles com la FRE 901/902 que exigeixen una cadena de custòdia fiable; el *proof of existence* ofereix exactament això: un enllaç verificable entre el document original i el registre immutable, rebutjant l'argument «és una deepfake» que ha alimentat casos com el frau de **25,6 milions** de dòlars a Hong Kong, on tots els assistents eren avatars generats per IA [1].

A més, la prova d'existència garanteix **integritat i data certa** per a documents reguladors i contractes. Cada versió del document es registra amb el seu hash i segell de temps; qualsevol modificació posterior genera un nou registre que deixa constància clara del canvi. Això s'alinea perfectament amb els requisits dels Qualified Electronic Ledgers i del Qualified Electronic Archiving introduïts per eIDAS 2.0, que exigeixen una auditoria a prova de manipulació per a transaccions electròniques de gran valor [6]. La solució, per tant, no només compleix la normativa europea, sinó que la **potencia**, ja que ofereix una capa de verificació descentralitzada que les autoritats nacionals poden consultar sense dependre d'un únic proveïdor.

Cal subratllar que aquest mecanisme **no substitueix** els controls tradicionals com el «quatre ulls» o les comunicacions fora de banda; en canvi, actua com a **capa complementària** que reforça cada pas del procés. El fitxer mai no abandona el dispositiu: la informació sensible resta localitzada i protegida per l'encriptació del sistema operatiu, mentre que només les proves criptogràfiques es transmeten a la xarxa. D'aquesta manera, es manté la **privacitat** de l'individu sense sacrificar la verificabilitat.

Segons Deloitte, com hem vist, aquestes xifres són alarmants [2]; la prova d'existència converteix la confiança en una infraestructura tangible: captura firmada i timbrada a l'origen, traces immutables que suporten litigis i auditories, integritat certificada per eIDAS 2.0 i una arquitectura de privacitat-first. La decisió és clara: integrar *t2p* ara mateix, o afrontar un futur on la confiança es dissol en cada nova manipulació digital.

La promesa i el perill

Imagina una sala de reunions a Hong Kong on, amb la mateixa fluïdesa d'una videotrucada normal, se signen transferències que totalitzen 25,6 milions de dòlars. El «CFO» que presenta els documents és un deepfake tan convincent que ningú sospita del seu origen digital. L'operació, descrita per Arup, mostra

com la confiança en una identitat visual pot ser explotada i transformar-se en frau executiu a escala global [1].

Aquesta escena mostra la promesa central de *t2p*: una capa d'integritat que vincula cada instrucció financera al seu origen verificable, independentment del format visual o sonor. Amb proves d'existència registrades en ledgers qualificats —conforme a eIDAS 2.0— es pot demostrar amb una sola consulta criptogràfica que el document no ha estat alterat des del moment de la seva creació i que l'emissor és qui afirma ser [6]. El resultat és un onboarding més fiable, on les entitats poden validar KYC en minuts en comptes d'hores o dies, reduint dràsticament els costos operatius i eliminant el marge d'error humà. Les auditories es converteixen en processos de verificació instantània: una cadena de custòdia immutable que pot ser presentada davant dels tribunals com a prova admissible, superant les limitacions de la regla tradicional FRE 707 i la proposta 901(c) [7].

No obstant això, el perill resideix en la il·lusió que una capa tecnològica pugui substituir completament els controls interns i el judici humà. El NIST SP 800-63-4 advoca per la detecció obligatòria d'atacs d'injecció a nivells alts, reconeixent que les càmeres virtuals poden enganyar sistemes biomètrics si no es protegeixen adequadament [4]. Els atacants ja experimenten amb «injeccions» de dades falses i bypass biomètric per eludir els processos de verificació del KYC, com demostra l'informe d'iProov sobre vulnerabilitats emergents [4]. Com hem vist, l'augment exponencial del frau generat per IA —segons Deloitte, passant de 12,3 mil milions el 2023 a prop de 40 mil milions el 2027— no s'allibera només amb una prova d'existència; la tecnologia crea nous vectors d'atac que requereixen supervisió constant i polítiques de governança robustes [2].

A més, una implementació mal dissenyada pot comprometre la privacitat dels clients. L'emmagatzematge de metadades detallades en ledgers qualificats implica una exposició potencial si les claus d'encriptació són gestionades inadequadament o si es comparteix informació sensible sense els mecanismes de consentiment exigits per l'EU AI Act; com hem vist, aquesta norma obliga a etiquetar i informar sobre deepfakes en contextos comercials [5]. Per tant, la solució no és només tecnològica, sinó també legal i ètica: cal establir protocols clars per al tractament de dades personals i garantir que les proves d'existència siguin «zero-knowledge» quan sigui necessari.

La prova d'existència representa una capa essencial dins d'una arquitectura més àmplia de confiança. No és una bala de plata que elimini tots els riscos, sinó un mecanisme que redueix dràsticament el frau i restaura la credibilitat del comerç financer. La seva efectivitat depèn de com es combina amb controls interns rigorosos, supervisió reguladora i pràctiques de privacitat responsables; només així podrem equilibrar la promesa d'un ecosistema financer més segur amb el perill d'una confiança excessiva en una sola solució tecnològica.

És hora d'actuar

Els bancs i les fintech són el primer escut davant la tempesta de deepfakes que ja ha demostrat el seu potencial destructiu; el cas Arup, on uns **25,6 milions de dòlars** van ser transferits a través d'una videotrucada poblada exclusivament per avatars generats per IA, és una advertència clara que la confiança en les identitats i les instruccions ja no es pot assumir com a segura [1] —com hem vist—. Per tal de tallar aquesta vulnerabilitat cal **ancoratge del KYC** i totes les seves traces d'auditoria dins d'un marc verificable fora de banda, especialment per a ordres de pagament superiors a uns quants milers de dòlars. Això implica integrar solucions basades en **Qualified Electronic Ledgers** i **Qualified Electronic Archiving**, tal com preveu eIDAS 2.0, que garanteixen una cadena immutable on cada pas del procés de coneixement del client queda registrat amb segells criptogràfics verificables [6]; així, fins i tot si un actor maliciós intenta enganyar el sistema amb una imatge biomètrica falsificada, el registre descentralitzat revelarà la incongruència entre l'origen declarat i les dades emmagatzemades.

Les empreses que manegen contractes i documents sensibles han de **segellar digitalment aquests actius abans de compartir-los**, utilitzant proves d'existència (t2p) basades en blockchain. Un segell criptogràfic no només certifica l'estat del document en el moment de la signatura, sinó que també proporciona una prova verificable i immutable que pot ser consultada per qualsevol part interessada sense necessitat de confiar cegament en l'emissor original. Aquesta pràctica esdevé especialment crucial a mesura que els tribunals comencen a abordar les proves potencialment fabricades a través de la regla 901(c) i el FRE 707, on la cadena de custòdia tradicional ja està qüestionada [7].

Els auditors i advocats han d'esdevenir **defensors de les proves d'existència** en la seva pràctica professional. No n'hi ha prou amb comprovar que un document existeixi; cal exigir que la seva integritat

estigui vinculada a una prova verificable independent, emmagatzemada en un registre electrònic qualificat. Això implica auditar tant el contingut com les metadades de creació i les signatures digitals, assegurant-se que qualsevol intent d'injecció o bypass biomètric —tal com descriu NIST SP 800-63-4— sigui detectat en temps real [4].

Els reguladors han de liderar la definició d'**estàndards interoperables i reconeixement legal del segell criptogràfic**, establint marcs que obliguin les institucions financeres a adoptar solucions basades en blockchain com a part integral del seu programa de compliance. L'aplicació de l'EU AI Act (art. 50) el 2 d'agost, **com hem vist**, és un pas crucial cap a la regulació d'aquests riscos emergents [5]; però cal anar més enllà, reconeixent legalment les proves d'existència com a evidència admissible i establint requisits de **verificació fora de banda** per a transaccions de gran magnitud.

En resum, la confiança és l'actiu fonamental del sistema financer; demostrar-la no és un luxe sinó una necessitat urgent. Cada banc, fintech, empresa, auditor, advocat i regulador té un paper concret i complementari en aquest ecosistema: capturar, segellar, verificar i reconèixer les proves d'existència com a pedra angular de la credibilitat. **Demostrar la confiança és time2act** — el moment de posar en pràctica aquestes mesures és ara, abans que els deepfakes de nova generació es converteixin en la norma i no en l'excepció.

---

[1] CNN Business — *Finance worker pays out $25 million after video call with deepfake 'CFO'* (cas 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$ el 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, article 50 (etiquetatge 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; documents judicials dels EAU: almenys 17 implicats, 400.000 $ rastrejats fins a comptes del Centennial Bank als EUA). https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/ ↩

La imatge com a testimoni: fotoperiodisme i mitjans

«Una fotografia passa per prova incontrovertible que una cosa determinada va succeir.»

— Susan Sontag, On Photography (1977)

Era el matí del 22 de maig de 2023 quan un xiulet digital va travessar les xarxes socials com una explosió invisible. Un compte marcat com a «verificat», que es feia passar per un conegut mitjà de notícies, compartia una fotografia: una columna de foc i fum s'alçava violentament a l'ombra del Pentàgon. La imatge es va difondre en qüestió de segons; els algoritmes la van impulsar cap als timelines de milers d'usuaris i, durant uns minuts, va arribar a moure breument els mercats financers nord-americans abans que ningú no pogués confirmar-ne res.

Els comentaris es multiplicaven com focs artificials: «Bombardeig al Pentàgon!», «Atac terrorista!» i, entre les crítiques, la pregunta clau que encara ressona avui: **d'on prové aquesta imatge?** La resposta, en aquell instant, era un buit. Ningú no podia rastrejar l'origen del fitxer. El compte «verificat» es va suprimir poc després de la primera onada d'alertes, deixant només la imatge viral i una sèrie de rumors que corrien més ràpid que la veritat.

Enmig del caos, Hany Farid, pioner en anàlisi forense digital, va examinar la fotografia i va concloure que, amb tota probabilitat, havia estat generada per intel·ligència artificial. La imatge mostrava les inconsistències pròpies dels models generatius i, sobretot, no s'havia pogut associar a cap font ni a cap càmera coneguda [1].

Mentre els analistes financers recalculaven i els reguladors de mercat valoraven l'impacte de la desinformació visual, el món periodístic es trobava davant d'un escenari que havia semblat impossible feia només dues dècades: una sola imatge, sense cap rastre verificable, podia desencadenar moviments de borsa i canviar la percepció pública en qüestió de minuts. La incertesa sobre l'origen d'aquella fotografia no era només un problema tècnic; era una amenaça directa a la credibilitat del periodisme i al debat democràtic.

Així, aquella breu explosió digital es va convertir en el primer testimoni d'una nova era: una en què la **verificabilitat** —el poder de demostrar d'on prové cada imatge— esdevé l'únic escut capaç de protegir la societat del caos que pot engendrar un simple píxel. La necessitat de firmar el contingut a l'origen, i d'ancorar-lo en una prova d'existència immutable, ja no era només una proposta tècnica; era una urgència per a la supervivència del discurs públic.

La imatge ja no és prova

Durant més d'un segle, la fotografia ha gaudit d'una aura de veritat incontestable: el blanc i negre del front d'una guerra, el somriure d'una família que es converteix en icona històrica o el foc d'una explosió que captura l'instant decisiu d'un conflicte. Aquell «moment congelat» era considerat un testimoni fiable perquè la tecnologia de l'època exigia una cadena física i visible —pel·lícula, laboratori, impressió— que feia gairebé impossible manipular-la sense deixar empremta. La confiança en la imatge es construïa sobre la presumpció que el seu origen era evident i immutable.

Avui aquesta premissa s'ha desfet. Les xarxes neuronals generatives, alimentades per models entrenats amb milers de milions d'imatges, són capaces de crear fotogrames indistinguibles dels originals en qüestió de segons. Com hem vist al maig de 2023, la falsa imatge de l'«explosió del Pentàgon», una composició generada per IA i difosa per un compte que s'autoproclamava mitjà de notícies, va provocar una breu però significativa oscil·lació dels mercats financers. L'anàlisi de Hany Farid va demostrar com la manipulació digital pot enganyar fins i tot els observadors més experimentats [1].

Tanmateix, el perill no resideix únicament en les deepfakes «pures». A les eleccions de 2024, els mitjans van observar que les «cheap fakes» —vídeos o fotos reals trets del seu context original o retocats amb eines bàsiques— van superar les deepfakes d'IA en una proporció aproximada de set a un [2]. Aquestes manipulacions, encara que no són totalment sintètiques, eren igualment devastadores perquè la seva credibilitat depenia del coneixement del seu origen i del moment de captura. Un clip d'un discurs polític reeditat per afegir una frase comprometedora o una fotografia d'una manifestació desplaçada temporalment pot generar el mateix impacte que un avatar digital perfectament recreat.

Això revela la veritat fonamental: el problema central no és tant crear imatges falses, sinó la **procedència** i el **context**. Qui va prendre una foto, en quin moment exacte, amb quina configuració tècnica i si ha estat alterada posteriorment constitueixen l'únic criteri per avaluar-ne la veracitat; sense aquesta informació, qualsevol píxel esdevé una dada potencialment enganyosa.

Les solucions del camp de la verificabilitat —les credencials de contingut (C2PA) i les proves d'existència immutables— apunten precisament a aquest buit. La firma digital al moment de captura, ja implementada en càmeres com la Leica M11-P o el prototip Nikon que va validar la certificació C2PA el febrer de 2025 [6] [4], garanteix una cadena d'autenticitat des del primer instant. No obstant això, les metadades associades a aquestes credencials poden ser eliminades o alterades per plataformes socials i processos de recodificació, deixant la imatge sense rastre verificable [7].

L'ancoratge en una prova d'existència basada en blockchain ofereix una capa addicional de seguretat: un hash immutable registrat a la cadena assegura que, encara que les metadades desapareguin, el testimoni digital persisteixi i pugui ser verificat per qualsevol actor. Aquesta doble defensa —firma a l'origen i ancoratge immutable— constitueix l'únic escut viable contra una era en què el píxel esdevé un instrument de confusió tant com d'informació.

Credencials de contingut: firmar a l'origen

En un moment en què la veracitat visual s'ha convertit en un bé escàs, la resposta de la indústria ha estat construir una infraestructura que restableixi la confiança des del primer clic de l'obturador. El projecte C2PA (Coalition for Content Provenance and Authenticity) i la seva iniciativa Content Credentials ofereixen un marc criptogràfic per registrar l'origen i tot l'historial d'edicions d'una imatge, de manera que cada pas —des de la captura inicial fins a les modificacions posteriors— queda documentat en un manifest signat. Aquesta proposta no només aporta transparència; crea una pista d'auditoria verificable per a qualsevol actor, des del periodista fins al lector final.

Com hem vist, la Content Authenticity Initiative (CAI) ha superat els 5.000 membres el 2025, entre grans plataformes digitals, agències de notícies i fabricants de maquinari [3]. Aquesta massa crítica reflecteix una consciència compartida: la prova d'autenticitat ja no pot ser un luxe reservat a les organitzacions més ben dotades, sinó una infraestructura bàsica per a tot el flux informatiu.

El salt qualitatiu cap al maquinari ha estat decisiu. La **Leica M11-P** es va llançar com la primera càmera que incorpora Content Credentials directament en un xip segur, capaç de signar cada fotografia en el moment exacte de la captura. Aquesta firma criptogràfica queda incrustada a les metadades del fitxer, assegurant que qualsevol intent posterior de manipulació es detecti. La innovació no s'ha quedat només a la gamma premium; Nikon, Canon, Sony, Samsung i fins i tot Google Pixel han seguit el pas, integrant xips similars en les seves línies més recents [6]. El resultat és un ecosistema on la confiança visual es converteix en una característica de producte tant com la resolució o la velocitat d'obturació.

A escala de l'editorial, l'impacte ha estat notable. L'AFP i Nikon van validar al febrer del 2025 un prototip de càmera que **firma les fotos amb C2PA en el moment de disparar**, garantint una cadena d'autenticitat des del seu origen [4]. Com hem vist, France Télévisions va adoptar la signatura C2PA per als seus informatius diaris a finals del 2025, i l'IBC Accelerator «Stamping Your Content» —que reuneix BBC, EBU i Associated Press— ha creat eines obertes perquè les redaccions puguin firmar i verificar credencials de contingut sense fricció tècnica [5].

Aquesta convergència entre maquinari, protocols oberts i fluxos editorials constitueix la resposta integral que la indústria necessita per contrarestar l'era de les «cheap fakes». No és només una capa addicional de seguretat; transforma el cicle de vida de la imatge, amb prova d'autenticitat a cada pas des de la captura fins a la difusió. Tanmateix, com subratlla el marc de C2PA, les metadades poden ser eliminades o alterades durant processos de recompressió i compartició en xarxes socials; per això l'ancoratge d'aquesta informació en una blockchain pública esdevé imprescindible per garantir que la prova d'existència sobrevisqui a qualsevol intent de supressió [7].

En síntesi, la combinació de credencials C2PA amb proves d'existència immutable representa el camí cap a una nova confiança visual. La indústria ha demostrat que és possible crear un ecosistema on la veracitat no sigui una opció, sinó una garantia incorporada al producte i al flux editorial, clau per preservar un debat públic fonamentat en fets verificables i per fer front a les amenaces emergents de la IA generativa.

El forat: les metadades s'esborren

Quan una fotografia surt del seu entorn original —la càmera, el laboratori de redacció o l'aplicació que la captura— entra en un ecosistema digital dominat per xarxes socials i serveis d'emmagatzematge. En aquest viatge, les metadades que porten la firma C2PA es troben sovint amb una barrera invisible: el procés de pujada i recodificació. Les plataformes com Instagram, TikTok o WhatsApp reprocessen cada imatge per optimitzar-ne la mida i l'ample de banda; aquest reprocessament elimina les capes d'informació que no són essencials per a la visualització, incloent-hi les credencials d'autenticitat.

Aquesta pràctica és més que un inconvenient tècnic; és una vulnerabilitat estructural. Una imatge que ha estat compartida en una conversa de grup o publicada en un fil d'una xarxa social pot perdre completament el seu «Content Credential» sense cap avís al creador ni a l'espectador. La desaparició de la firma no implica, per força, que la foto sigui falsa —una fotografia sense credencial pot ser totalment genuïna— però també impedeix que qualsevol verificació posterior pugui confirmar-ne el qui i el quan original. En altres paraules, l'absència d'una metadada deixa un buit interpretatiu: el lector es troba davant d'un testimoni visual desproveït de la seva cadena de custòdia.

Les crítiques acadèmiques han subratllat aquest punt, assenyalant que l'especificació C2PA, per si sola, no ofereix una robustesa suficient contra la pèrdua de les metadades en el flux digital contemporani [7]. Això vol dir que el «qui i quan» —els elements fonamentals del testimoni visual— poden esvair-se exactament en el moment en què més són necessaris: durant una crisi informativa, una investigació periodística o un debat públic.

Aquest forat no és només tècnic; té repercussions socials i polítiques. En l'era de les «cheap fakes», en què els vídeos mal contextualitzats van superar per unes set vegades les deepfakes d'IA en impacte [2], la capacitat de demostrar que una imatge prové d'una font fiable esdevé un actiu crític. Si les credencials desapareixen, el debat es pot desviar cap a la sospita i l'escepticisme, alimentant la polarització que els autors del llibre volen contrarestar.

Per això, la solució no consisteix a rebutjar C2PA, sinó a reconèixer-ne el límit i complementar-lo amb una capa de prova d'existència immutable. Una àncora basada en blockchain pot registrar l'hash de la imatge i les seves credencials al moment de la captura, assegurant que, encara que les metadades siguin esborrades durant la distribució, el registre permanent persisteix i és verificable per qualsevol actor de l'ecosistema. Aquesta doble protecció —la firma C2PA per a l'autenticitat immediata i la prova d'existència per a la persistència a llarg termini— constitueix una defensa robusta contra les manipulacions de la IA generativa i garanteix que el testimoni visual **continuï sent** fiable, fins i tot quan el camí digital es torni incert.

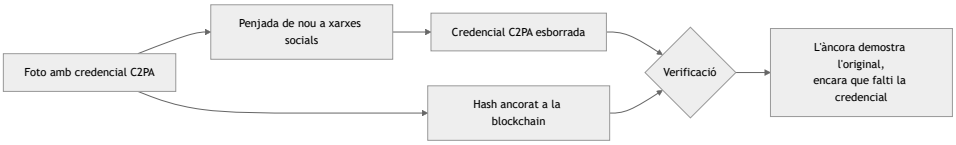


Figura 17.1 — Quan una imatge es repuja, les metadades C2PA poden desaparèixer; el hash ancorat a la cadena pública continua demostrant que l'original existia, inalterat.

L'àncora que sobreviu

En un món on la confiança visual s'ha convertit en una mercaderia escassa, el model de **t2p** ofereix la resposta que el periodisme necessita per preservar la veritat d'una imatge des del moment en què es captura. La clau no és només signar-la amb les credencials C2PA —una capa d'autenticitat immediata que ja ha mobilitzat més de 5.000 membres globals i s'ha adoptat per entitats com France Télévisions i l'IBC Accelerator— sinó ancorar el seu hash a una cadena pública immutable. Aquesta doble protecció garanteix que, encara que les metadades siguin esborrades o alterades en la fase de distribució (com adverteixen els estudis sobre la vulnerabilitat de les metadades de C2PA [7]), l'element fonamental de la prova —el hash— persisteixi i pugui ser verificat per qualsevol actor de l'ecosistema sense necessitat d'intermediaris.

A l'AFP, el flux editorial incorpora una marca d'aigua xifrada que enllaça directament la foto publicada amb l'arxiu original guardat a les seves infraestructures segures [4]. Aquesta pràctica il·lustra com la combinació de **firma C2PA** i **àncora de prova d'existència** transforma una simple captura en un testimoni verificable des del primer instant. Quan el periodista, al camp o a l'estudi, dispara amb una Leica M11-P —la primera càmera que incorpora Content Credentials al seu xip segur— la imatge surt del visor ja signada i, simultàniament, el seu hash es pot enviar a una blockchain pública on rep un segell de

temps immutable. En aquest moment es crea una versió «publicar amb prova», consultable per editors, plataformes socials o auditors en qualsevol moment.

Aquesta arquitectura resol el doble problema exposat pels cheap fakes durant les eleccions —on els vídeos mal contextualitzats van superar les deepfakes d'IA per una ràtio aproximada de 7:1 [2]— garantint que la procedència i la integritat temporal siguin inalterables. Enfront d'incidents com la falsa imatge de l'«explosió del Pentàgon» generada per IA al maig —que va provocar una breu sacsejada dels mercats fins a ser desmuntada per Hany Farid [1]—, el periodisme disposa ara d'una eina capaç de demostrar que la imatge no només és autèntica en el moment de la captura, sinó que ha estat immutablement registrada i pot ser rastrejada fins al seu origen.

Les recomanacions conjuntes de la NSA i la CISA a principis del 2025 per a l'ús de Content Credentials [8] reforcen la idea que la seguretat visual és una qüestió d'interès nacional, on la prova d'existència actua com un codi de confiança universal. Qualsevol mitjà —des de grans cadenes de televisió fins a blogs independents— pot adoptar aquest marc sense inversions massives: només cal integrar el client t2p, que genera i registra els hash.

Així, la combinació de C2PA i t2p crea una doble barrera —una capa d'autenticitat immediata i una àncora immutable a llarg termini— que protegeix les imatges contra l'erosió de confiança provocada per la IA generativa, restablint el paper del fotoperiodisme com a testimoni fiable i oferint als periodistes una eina pràctica per publicar amb prova.

Les institucions s'alineen

Quan a principis del 2025 la National Security Agency (NSA) i la Cybersecurity and Infrastructure Security Agency (CISA) van publicar les seves directrius que recomanen l'ús de les Content Credentials —el marc operatiu de la iniciativa C2PA—, es va produir una veritable convergència entre seguretat nacional i periodisme. En un document conjunt, «Strengthening Multimedia Integrity in the Generative AI Era», les agències advertien que la integritat dels mitjans és una defensa crítica contra les manipulacions basades en IA i recomanaven adoptar la firma criptogràfica al moment de la captura o publicació d'imatges i vídeos [8]. Aquesta recomanació, tot i ser inicialment dirigida a entitats federals, ha generat un efecte cascada: les grans xarxes de notícies, els portals de streaming i fins i tot les xarxes socials han començat a integrar el protocol C2PA com a requisit mínim per al contingut visual.

A la mateixa escala, el consorci JPEG Trust, responsable de l'estàndard ISO/IEC 21617-1, ha ampliat el seu abast estenent el motor de la C2PA dins de l'especificació JPEG. Això significa que qualsevol fitxer JPEG generat a partir d'una càmera compatible pot contenir, per defecte, una firma digital verificable i un registre de metadades autenticades [8]. El pas d'un «add-on» opcional a un component integral del format més utilitzat al món consolida la credibilitat de les Content Credentials i eleva el seu estatus a estàndard internacional. Ara, la simple acció de crear una imatge amb una càmera moderna com la Leica M11-P o els models Nikon, Canon i Sony que ja integren xips segurs produeix automàticament un certificat C2PA incrustat al fitxer [6].

Aquesta evolució normativa coincideix amb l'entrada en vigor de l'EU AI Act, que imposa una obligació d'etiquetatge per a tot contingut generat o modificat per IA. L'article 50 del reglament exigeix que les plataformes i els proveïdors marquin clarament si un material visual ha estat creat o manipulat per algoritmes. En aquest context, la prova de credencials C2PA es converteix en una resposta directa a l'obligació legal: la metadada signada al moment de la captura actua com a «etiqueta de confiança» i ajuda a complir el requisit de transparència de l'AI Act. Així, el pas de bona pràctica —utilitzar C2PA per augmentar la credibilitat— es transforma en una expectativa reguladora.

Els efectes pragmàtics d'aquest alineament són immediats. Les empreses de mitjans que ja han adoptat les credencials, com hem vist amb France Télévisions el 2025 [5] o l'AFP amb el seu prototip Nikon de certificació C2PA [4], aposten a reduir els incidents de difusió d'imatges falsificades. A més, la integració directa en l'estàndard JPEG permet que les petites publicacions i els creadors independents generin contingut verificable sense necessitat d'inversions tecnològiques massives. El suport institucional —des de les agències de seguretat nord-americaines fins als organismes de normalització internacionals— converteix la firma digital en una infraestructura fonamental del paisatge mediàtic, establint un nou paradigma on la procedència verificable és tant una pràctica recomanada com una exigència legal.

La promesa i el perill

En un món on una fotografia ha estat durant cent anys la prova més directa d'un esdeveniment —un testimoni visual que parla sense necessitat de traducció— la irrupció de la intel·ligència artificial generativa està reescrivint les regles del joc. La promesa és clara: amb els **Content Credentials** (C2PA) i una àncora immutable a la blockchain, cada imatge pot portar una signatura digital que verifica qui l'ha capturada, en quin moment i sota quines condicions. Això restauraria la confiança en el periodisme visual, diferenciaria el contingut verificable del soroll manipulatiu i permetria als fotògrafs demostrar inequívocament la seva autoria i l'autenticitat de les seves cobertures.

Els primers passos ja mostren el potencial. El febrer de 2025, **l'AFP** i **Nikon** van presentar una càmera prototip que signa automàticament cada captura amb C2PA, gravant la informació de procedència en el moment mateix de l'obertura de l'obturador [4]. Des de llavors, marques com **Leica** (amb la M11-P), **Canon**, **Sony** i fins i tot **Google Pixel** han integrat xips segurs que emmagatzemen les credencials al maquinari [6]; institucions clau —des de la **NSA** i la **CISA** fins al consorci de normalització **JPEG Trust** — recomanen l'ús d'aquestes signatures com a pràctica estàndard des del gener de 2025 [8]. En aquest escenari, la imatge es converteix en un document tan fiable com una transacció bancària.

Tanmateix, el perill que s'amaga darrere d'aquesta aparença de seguretat és real i complex. La mateixa informació que garanteix l'autenticitat pot revelar dades sensibles: coordenades GPS, metadades d'identitat o fins i tot indicis sobre la font d'una cobertura periodística. En zones de conflicte, aquest rastre pot ser una pista suficient perquè les forces repressives localitzin i silenciïn fotògrafs i activistes. El cas de la falsa «explosió del Pentàgon» del maig de 2023, analitzat per **Hany Farid**, mostra com una simple imatge generada per IA, difosa per un compte que es feia passar per un mitjà, va afectar breument els mercats financers, subratllant la fragilitat d'un ecosistema on la procedència és l'únic filtre fiable [1].

A més, el risc de crear una **bifurcació del periodisme** —un món dividit entre contingut verificat i no verificat— pot marginar veus legítimes que no disposen d'eines avançades per signar les seves imatges. Les «cheap fakes», que van superar les deepfakes en una proporció de 7:1 durant les eleccions del **2024**, demostren que el problema central és la **procedència i el context**, no només la qualitat visual del falsejament [2]. Si es confia exclusivament en el segell digital sense cap mecanisme d'auditoria independent, es corre el perill d'una **excessiva confiança** en un certificat que pot ser eliminat o alterat; les metadades de C2PA són vulnerables a la supressió en plataformes socials i processos de recodificació [7].

Per tal de preservar la promesa sense caure en el perill, cal dissenyar sistemes de privacitat que permetin **divulgació selectiva**. Els fotògrafs haurien de tenir control total sobre quines metadades es revelen i quan, mitjançant protocols d'encriptació que separin la informació sensible (com el GPS) del certificat d'autenticitat. Les organitzacions mediàtiques podrien establir **polítiques d'ancoratge** on la prova d'existència a la blockchain garanteixi la permanència de l'acte, mentre les metadades privades es mantenen en entorns protegits i només s'alliberen sota consentiment explícit.

En resum, la tecnologia ofereix una via per tornar a confiar en la imatge com a testimoni, però aquesta confiança ha d'estar equilibrada amb mesures rigoroses de protecció de dades i un marc ètic que eviti la creació d'un periodisme de dues velocitats. Només així podrem garantir que les fotos continuïn sent una veu poderosa per a la veritat, sense posar en risc les vides que les creen.

Aquesta arquitectura d'ancoratge no només reforça els mitjans professionals; crea un espai on el periodisme ciutadà pot convertir-se en testimoni legal. A Taiwan, l'exministra digital **Audrey Tang** va convocar la població a gravar el propi col·legi electoral, oferint una cadena de vídeo que, una vegada ancorada a la blockchain, podia ser contrastada instantàniament contra les teories conspiratives que circulaven en xarxes socials [9]. El mateix mecanisme ha trobat un ecosistema emergent al Perú: **Voto Libre** utilitza IA per classificar l'evidència fotogràfica de frau electoral i la registra com a prova immutable, garantint un reportatge «segur, transparent i en temps real» que es pot auditar sense dependre d'intermediaris [10]. En ambdós casos, una imatge ancorada transcendeix el simple document visual: es converteix en una evidència verificable del que realment ha succeït, ampliant la confiança no només a les grans redaccions sinó també a la veu directa de la ciutadania.

És hora d'actuar

Els mitjans són el primer escenari on la ruptura de la confiança visual es fa palpable. Cada dia que una redacció publica una foto sense un certificat verificable, deixa oberta la porta a l'engany: el cas de la falsa «explosió del Pentàgon» del maig de 2023, generada per IA i difosa com a notícia real, va provocar una breu però significativa oscil·lació dels mercats abans de ser desmentida per Hany Farid [1]. Com hem vist,

el primer compromís que cal assumir és **adoptar la captura firmada**: les noves càmeres Leica M11-P, Nikon, Canon i altres ja integren xips de seguretat capaços d'estampar un Content Credential al moment de l'obtenció de la imatge [6]. Les redaccions han d'exigir que tot el material visual proveni d'aquests dispositius o, en cas contrari, que es processi amb una eina certificada que afegeixi una signatura digital inalterable.

A més, la **publicació ha d'anar acompanyada d'una prova d'existència immutable**. Les metadades de C2PA poden ser eliminades o alterades per les xarxes socials i processos de recodificació, com adverteixen les crítiques detectades recentment [7]. Per tant, cada mitjà ha d'ancorar la seva evidència a una cadena de blocs pública que registri l'hora exacta de captura i la signatura del dispositiu; aquest ancoratge garanteix que, fins i tot si les credencials són esborrades, el lector pot verificar la procedència original amb un simple enllaç.

Les plataformes digitals tenen una responsabilitat complementària: **preservar i exhibir les credencials** en lloc d'eliminar-les per optimitzar l'emmagatzematge o per motius de privacitat. Les recomanacions de la NSA i la CISA (gener de 2025) ja indiquen que els sistemes de gestió de contingut han d'integrar suport natiu per a Content Credentials [8]; això implica actualitzar les API, oferir opcions perquè els creadors decideixin quina informació exposar i garantir que la capa de visualització mostri clarament l'estat de verificació al públic.

Els fabricants de càmeres són el **punt d'origen** d'aquesta cadena de confiança. Han d'**estendre la captura a l'origen amb privacitat configurable**, permetent als usuaris triar quins atributs (ubicació, metadades personals) es mantenen encriptats i quins es deixen visibles per al control de veracitat. L'exemple pioner de l'AFP amb Nikon, que va presentar una càmera prototip amb firma integrada a la captura el febrer del 2025, demostra que aquest model és factible i ja s'està desplegant en entorns professionals [4].

La ciutadania, finalment, no pot quedar passiva. En un panorama on les «cheap fakes» van superar per una ràtio de 7:1 les deepfakes tradicionals a les eleccions del 2024, el problema central és la **procedència i el context** dels continguts [2]. Cada usuari ha d'aprendre a cercar i interpretar els indicadors de credibilitat —les sigles C2PA, les marques de temps en blockchain— i no limitar-se al valor visual. Les campanyes d'educació mediàtica han d'incloure tutorials pràctics sobre com verificar una imatge amb eines gratuïtes disponibles en línia.

Els reguladors, per la seva banda, han d'establir **estàndards interoperables** que obliguin tant a mitjans com a plataformes i fabricants a seguir protocols comuns de signatura i ancoratge, evitant un ecosistema de «periodisme de dues velocitats». Les iniciatives com la Content Authenticity Initiative ja compten amb més de 5.000 membres (com hem vist) i han de ser reforçades amb normatives que garanteixin la transparència de les fonts [3].

En resum, en un món d'imatges sintètiques, **demostrar què és real es converteix en defensar el periodisme**. La tecnologia ens ofereix les eines; depèn de cada actor —mitjans, plataformes, fabricants, ciutadans i reguladors— adoptar-les i fer-les visibles. El moment de provar la veritat ja ha arribat: *time2act*.

---

[1] NPR — *Fake viral images of an explosion at the Pentagon were probably created by AI* (maig 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* (metadades eliminables). https://arxiv.org/html/2604.24890v1 ↩

[8] NSA/CISA — *Content Credentials: Strengthening Multimedia Integrity* (gen 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 mort de les dades: salut i imatge mèdica

«Pel que fa a les malalties, fes-te un costum de dues coses: ajudar, o si més no, no fer mal.»

— Hipòcrates, Epidèmies, I, XI

Era una tarda freda d'octubre, i el laboratori d'oncologia respiratòria d'un gran hospital universitari vibrava amb la rutina habitual: pacients que esperaven els resultats de les seves exploracions, metges que revisaven informes i tècnics que carregaven les imatges DICOM en el sistema central. A la sala de lectura, una radiòloga veterana, amb més de deu anys d'experiència, obrí una nova tomografia computada (TC) d'un home de 58 anys que havia arribat al servei amb tos persistent i pèrdua de pes. La imatge en pantalla mostrava un nòdul pulmonar d'1,2 cm a l'extrem superior del pulmó dret, una petita ombra densa que destacava entre el teixit sa.

Sense dubtar-ho, la radiòloga activà el protocol oncològic: es va marcar la zona per a una biòpsia guiada per imatge i es va programar la confirmació diagnòstica abans de qualsevol tractament. La confiança en les dades que havien arribat a través de la xarxa hospitalària era total; el format DICOM, estàndard des de fa dècades, semblava una garantia que la imatge era un testimoni fidel del cos del pacient.

Però allà dins, una capa invisible d'algoritmes podia haver alterat l'essència mateixa del fitxer. Un grup d'investigadors de la Universitat Ben-Gurion del Nègueb, juntament amb el centre mèdic Soroka, va demostrar a USENIX Security 2019 que una xarxa generativa adversarial —anomenada CT-GAN— és capaç d'injectar o eliminar tumors en imatges TC i RM en mil·lisegons, sense deixar rastre perceptible per a l'ull humà ni per als sistemes de verificació convencionals. En un experiment cec, els radiòlegs van classificar com a malignes el 99 % dels casos amb tumor injectat i com a sans el 94 % dels casos amb tumor eliminat; fins i tot advertits, els errors es mantingueren alarmantment al 60 % i 87 % respectivament [1].

En aquest escenari, l'atac no era una ficció de ciència-ficció sinó un codi publicat i replicable. Algú —potser un actor extern amb accés a la xarxa interna de l'hospital o un insider malintencionat— hauria pogut carregar el model CT-GAN al servidor d'imatges i modificar silenciosament l'arxiu DICOM abans que arribés al terminal de la radiòloga. El nòdul que ella veia podria no ser més que una il·lusió digital, un artefacte generat per una xarxa neuronal entrenada per enganyar.

L'impacte d'una manipulació així és immediat i potencialment mortal: el pacient se sotmetria a procediments invasius innecessaris, exposat a radiacions i a la incertesa psicològica de viure amb un diagnòstic fals. En l'altra cara del mateix monstre, una altra imatge podria haver passat per alt un tumor real, que hauria retardat el tractament i hauria posat en perill la vida del pacient.

Aquesta escena no és un relat distòpic; és una advertència basada en proves reals que posa en relleu la fragilitat de la medicina moderna quan les dades esdevenen vulnerables. Si no podem confiar en la integritat de cada píxel, la mateixa essència de la pràctica clínica es desmorona, i la salut —el dret més fonamental— queda a mercè d'una nova forma de guerra: la guerra de les dades.

Quan la imatge mèdica menteix

El 2019 una investigació presentada a USENIX Security va revelar un escenari inquietant per a la sanitat: **CT-GAN**, una xarxa generativa condicional capaç d'injectar o eliminar tumors pulmonars en tomografies computades (TC) i lesions cerebrals en ressonàncies magnètiques (RM) en només mil·lisegons. En un experiment a cegues, radiòlegs van diagnosticar com a malignes la gran majoria dels casos amb tumor injectat i van considerar sans la gran majoria dels casos amb lesió eliminada; **com hem vist**, l'error clínic va ser considerable.

El format **DICOM** (Digital Imaging and Communications in Medicine) defineix la codificació, l'emmagatzematge i la transmissió d'imatges mèdiques, però precedeix la ciberseguretat moderna i **no incorpora cap mecanisme criptogràfic intrínsec**. Les imatges viatgen per xarxes hospitalàries, VPN o serveis en núvol sovint sense signatures digitals que puguin garantir-ne la integritat. En aquest buit, un atacant amb accés a la cadena de subministrament —per exemple, un proveïdor d'infraestructura de TI o un insider malintencionat— pot introduir el model CT-GAN i modificar les dades en temps real, sense que cap registre de canvis quedi visible.

Les motivacions són diverses. En l'àmbit **d'assegurances**, una imatge falsificada podria generar cobertures per a tractaments inexistents o, al revés, ocultar lesions per reduir pagaments. En la recerca biomèdica, la manipulació d'imatges pot conduir a resultats clínics enganyosos, desviant recursos i alimentant publicacions fraudulentes. A un nivell més sinistre, un estat o grup hostil podria **sabotejar** estudis clínics crítics o provocar diagnòstics erronis que posin en perill la vida del pacient, convertint el laboratori en una nova línia de front bèl·lic [1].

Els resultats de l'estudi demostren que ni les revisions manuals ni els sistemes d'alerta tradicionals són suficients; els radiòlegs, encara que informats de possibles manipulacions, van confiar en la seva experiència visual i van fallar en la majoria dels casos. Això exposa una vulnerabilitat estructural: **la confiança cega en la imatge com a veritat absoluta**. En un ecosistema on cada píxel pot ser alterat en mil·lisegons, el cost d'un diagnòstic erroni es tradueix immediatament en tractaments inadequats, intervencions innecessàries i, en el pitjor dels escenaris, la mort del pacient.

Per revertir aquesta tendència, *time2act* proposa **la prova d'existència**: generar un hash criptogràfic de cada fitxer DICOM a l'interior del dispositiu d'adquisició i segellar-lo amb una autoritat de segellat temporal (TSA) conforme al RFC 3161. L'empremta s'ancora a la blockchain pública, opcionalment agregada en una àncora de Merkle, amb aquest segell de temps com a complement conservat fora de cadena; això crea una traça immutable que compleix les regulacions HIPAA i 21 CFR Part 11 [5]. Qualsevol alteració posterior es detectaria en comparar el hash original amb el nou valor, obrint la porta a auditories automàtiques i a un sistema d'alerta precoç.

Com hem vist, l'exemple de CT-GAN il·lustra com una dada manipulada pot convertir una imatge mèdica en una arma mortal. La resposta no és només tecnològica, sinó també normativa i cultural: establir protocols de **cadena de custòdia digital**, exigir signatures criptogràfiques per a cada estudi i educar el personal clínic sobre la fragilitat dels formats tradicionals. Només així podrem garantir que les imatges continuïn sent testimonis fidels de la salut, i no falsificacions que posin en joc vides humanes.

Metges i pacients sintètics

Imaginem un metge que, a primera hora del matí, rep una trucada d'una pacient que denuncia un dolor abdominal insuportable; la veu és clara i l'estil de comunicació característic, fins i tot esmenta una anècdota de l'última visita. Sense sospitar res, el metge autoritza una recepta d'analgèsics forts i ordena programar una ecografia d'urgència. Unes hores més tard, un altre professional detecta que el número de la seguretat social del registre no coincideix amb cap expedient existent: la «pacient» era una identitat sintètica generada per deepfake d'àudio i vídeo, alimentada per una xarxa criminal dedicada a obtenir receptes per al mercat negre [2].

Aquest escenari no és una excepció anecdòtica; representa una amenaça emergent que supera el simple frau farmacèutic. Les tecnologies de generació de veu i imatge —basades en models d'aprenentatge profund com les xarxes generatives adversàries (GAN)— poden replicar amb sorprenent fidelitat la cara i el to d'un metge reconegut o d'un pacient habitual. Quan aquestes imitacions es difonen a través de plataformes de telemedicina, la capa tradicional de seguretat —tallafocs, xifratge TLS i autenticació multifactor— resulta insuficient: cap d'aquests mecanismes «veu» una cara fabricada ni detecta una veu clonada. El perill rau en la percepció humana; els professionals confien en l'autoritat que transmeten les expressions facials i el timbre de veu, i les xarxes malicioses exploten aquesta confiança per manipular decisions clíniques [2].

A més, el fenomen dels «pacients sintètics» alimenta una cadena de frau que comença en la teleconsulta i s'estén fins als sistemes d'assegurances. Grups organitzats poden crear perfils falsos amb documents digitals d'identitat, historials mèdics simulats i imatges radiològiques adulterades; aquestes dades es fan servir per presentar reclamacions d'indemnització exagerades o per obtenir reemborsaments de tractaments que mai s'han realitzat. En alguns casos, una veu clonada de metge enganya el personal perquè alliberi dades confidencials o signi autoritzacions de procediments inexistents, provocant un cost econòmic i una pèrdua de confiança en el sistema sanitari immensos, especialment amb l'adopció massiva de la telemedicina [2].

La solució no passa només per reforçar les barreres tècniques, sinó per instaurar una cadena de custòdia digital basada en proves d'existència criptogràfiques. Cada imatge mèdica, registre de veu i document clínic hauria d'estar associat a un hash únic segellat per una autoritat temporal (TSA), com hem vist al RFC 3161, assegurant que el fitxer mai no abandona el dispositiu original sense una marca verificable.

Aquest enfocament compleix les normatives de privacitat, inclosa la HIPAA i la normativa 21 CFR Part 11, i crea una traça immutable que desactiva qualsevol intent de manipulació posterior a la captura [5][7].

En última instància cal combinar tecnologia i cultura: desplegar solucions blockchain per a l'emmagatzematge de metadades mínimes fora de cadena, formar el personal clínic en la detecció d'anomalies de veu i imatge, i establir protocols d'autenticació multifactor que incloguin verificacions biomètriques independents de les dades presentades. Només així podrem garantir que la confiança dipositada en una consulta virtual no es converteixi en una arma per a qui vol jugar amb la vida humana.

La integritat de la ciència

En una era en què les revistes biomèdiques són l'epicentre del coneixement clínic, la contaminació de les dades és tan mortal com un tumor injectat a una tomografia. La detectiva d'imatges Elisabeth Bik ha mostrat que prop del **3,8 %** dels més de **20.000** articles biomèdics revisats contenen figures problemàtiques —una probabilitat d'un de cada 25 articles— i que la meitat d'aquests casos revela indicis clars de manipulació deliberada [3]. Aquesta taxa es tradueix en una erosió sistemàtica de la base sobre la qual es prenen decisions terapèutiques, es dissenyen protocols i es destinen recursos públics.

El neurocientífic Hoau-Yan Wang, vinculat al desenvolupament del fàrmac contra l'Alzheimer de Cassava Sciences, va ser imputat federalment el **28 de juny de 2024** per frau, incloent la fabricació de Western Blots que recolzaven resultats falsos [3]. La investigació ha revelat que s'havia obtingut aproximadament **16 milions de dòlars** de finançament dels National Institutes of Health (NIH) basant-se en dades manipulades, desviant recursos destinats a tractaments per a milions de pacients.

L'augment de plataformes automatitzades com Proofig i ImageTwin, ja integrades en fluxos editorials, ofereix una esperança concreta [3]. Aquestes eines apliquen algoritmes de detecció basats en anàlisis estadístiques de píxels, patrons de compressió i comparacions amb biblioteques de referència, identificant anomalies que una revisió humana podria passar per alt; la seva eficàcia depèn d'una adopció universal i d'un compromís institucional per validar cada figura abans de la publicació.

El **perill** és doble. En primer lloc, la ciència deficient alimenta decisions cliniques equivocades: metges que confien en resultats falsos poden prescriure tractaments ineficaços o fins i tot nocius, i això posa en risc vides humanes.

En segon lloc, el finançament públic es dilapida en projectes basats en dades no fiables, i això redueix els recursos disponibles per a investigacions genuïnes, incrementant la desconfiança del ciutadà cap al sistema de salut.

La promesa resideix en una arquitectura d'integritat basada en proves d'existència. Mitjançant l'ús de hash + segell de temps (TSA) segons el RFC 3161, les imatges i metadades es registren fora de cadena però amb una empremta immutable a la blockchain, complint els requisits de privacitat de HIPAA i del 21 CFR Part 11 [5][7]. Cada arxiu conserva la seva integritat dins el dispositiu clínic, generant una traça d'auditoria que qualsevol auditor pot verificar en temps real.

Per tant, el missatge és clar: sense una capa verificable de confiança, la ciència es converteix en un camp minat. Com hem vist, la comunitat acadèmica i les institucions reguladores han d'implantar sistemàticament aquestes proves d'existència i utilitzar eines com Proofig o ImageTwin per filtrar cada figura abans que arribi al lector; només així el coneixement generat serà un pilar sòlid per a la salut humana, no una bomba de temps que amenaça vides i finançaments.

Segellar la veritat clínica

En un món on el simple fet d'injectar o esborrar un píxel pot transformar una diagnosi en una condemna, la solució ha de ser tan rigorosa com les pròpies normes que regulen la salut. El patró emergent —i ja avalat per l'FDA— consisteix a mantenir la dada sensible totalment fora de la cadena de blocs i a registrar-ne únicament el resum criptogràfic (hash) juntament amb metadades mínimes: segell de temps, identificador d'usuari i tipus d'operació. Aquesta petita empremta digital es converteix en una traça immutable que pot ser auditada sense revelar contingut confidencial, complint o fins i tot superant les exigències d'auditoria de HIPAA i del 21 CFR Part 11 [5].

La mecànica és senzilla però poderosa. Cada imatge DICOM, cada registre d'historial clínic i cada fitxer d'un assaig es processa dins del dispositiu o del servidor hospitalari; s'hi afegeix un hash SHA-256 que

representa la seva integritat completa. Aquest hash es transmet a una xarxa de blocs on es registra amb una autoritat de segellat temporal (RFC 3161) o, en entorns més avançats, amb l'arrel de Merkle d'una cadena privada de salut [7]. Les metadades associades —només les necessàries per validar la transacció— queden visibles a la cadena, mentre que el contingut original mai no abandona el perímetre segur del centre mèdic, mantenint així la privacitat exigida per HIPAA i facilitant una auditoria transparent: qualsevol revisió pot comparar el hash emmagatzemat amb el fitxer actual i detectar, en mil·lisegons, qualsevol alteració.

En l'àmbit dels assaigs clínics aquest model crea una cadena de custòdia verificable que registra qui ha generat cada dada i quan s'ha modificat. El producte Triall ja ofereix aquesta funcionalitat: cada dada d'un assaig es «segella» amb el seu hash i es vincula a un registre immutable, assegurant que les autoritats reguladores i els patrocinadors puguin rastrejar la trajectòria de la informació des del moment de la recollida fins a la publicació final [6]. Com hem vist, el frau d'imatges afecta un 3,8 % dels articles i ha generat imputacions per uns 16 M$ de finançament dels NIH [3].

La FDA ha reconegut aquesta necessitat. La seva guia final de ciberseguretat per a dispositius mèdics, publicada el **27 de juny de 2025**, exigeix que els fabricants incloguin una llista de matèria primera de programari (SBOM) i documentació exhaustiva de les mesures de protecció [4]. Qualsevol dispositiu que emeti imatges radiològiques o dades de monitoratge ha d'incorporar mecanismes que demostrin que el contingut no s'ha manipulat després de l'adquisició.

En la pràctica només calen tres passos: (1) generar i emmagatzemar localment el hash de cada dada sensible; (2) enviar aquest hash a una cadena de blocs amb un segell de temps certificat; (3) conservar les metadades per a auditories futures. Eines com Proofig o ImageTwin detecten automàticament anomalies abans que les figures arribin a publicació i s'integren al flux hospitalari. Quan aquestes solucions es despleguen sistemàticament, la confiança en les imatges mèdiques passa d'una vulnerabilitat explotable a una garantia verificable.

El resultat és clar: un ecosistema on la veritat clínica està «segellada» i no pot ser alterada sense deixar empremta. En un context on cada diagnòstic pot decidir entre vida o mort, aquesta capa de verificació supera les normatives i ofereix una defensa real contra l'engany digital que amenaça la salut global. És el moment d'adoptar-la com a estàndard universal i convertir la seguretat de les dades mèdiques en un pilar inamovible del futur sanitari.

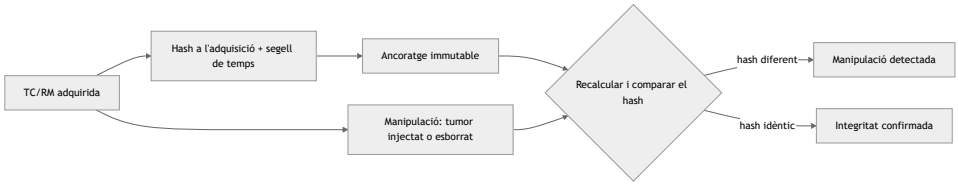


Figura 18.1 — Si es calcula el hash de la imatge en el moment de l'adquisició i s'ancora amb segell de temps, qualsevol manipulació posterior (un tumor injectat o esborrat) es detecta a l'instant.

Com funciona, sense que la dada surti

En el nucli d'una solució de confiança per a les dades mèdiques hi ha una operació aparentment senzilla però extraordinàriament poderosa: calcular un hash criptogràfic del fitxer en el moment exacte de l'adquisició. Aquest resum matemàtic —una cadena de caràcters única que representa la totalitat del contingut— es converteix en la petjada digital de la imatge, de l'informe radiològic o del registre clínic. Un cop generat, el hash s'envia a una autoritat de segellat temporal (Timestamp Authority, TSA) conforme al protocol que ja hem citat, i aquesta emet un certificat de temps signat amb la seva clau privada, indicant que l'empremta existia en aquell instant i no ha estat alterada posteriorment.

Per tal d'amplificar la resistència a manipulacions i garantir una verificació oberta, el hash certificat es pot ancorar a una cadena pública mitjançant una arrel de Merkle. En aquest escenari, diversos fitxers generen nodes fills que s'agrupen en un arbre binari; cada node conté l'hash combinat dels seus fills i la capa superior (l'arrel) representa resumidament tot el conjunt de dades. Publicar aquesta arrel a una blockchain —on el contingut es manté fora de cadena, deixant-hi només l'empremta i les metadades mínimes— crea una traça d'auditoria immutable que compleix amb els requisits de privacitat establerts per HIPAA i 21 CFR Part 11 [5].

El punt clau que converteix aquest mecanisme en una solució viable per a la salut és que el fitxer original **mai no surt del dispositiu**. Només l'empremta —una cadena de bytes d'una longitud fixa— es transmet cap a l'entorn extern, ja sigui al TSA o a la blockchain. Això elimina qualsevol necessitat de transferir imatges radiològiques completes, que contenen informació personal sensible, a servidors de tercers. La verificació posterior és totalment descentralitzada: qualsevol part interessada pot recalcular el hash del fitxer localment i comparar-lo amb l'empremta registrada al certificat o a la cadena pública; si coincideixen, es demostra que el contingut no ha patit alteracions des del moment de la seva captura.

Aquesta arquitectura ofereix una doble capa de seguretat. D'una banda protegeix la confidencialitat del pacient perquè les dades clíniques romanen dins dels perímetres controlats del dispositiu mèdic o del sistema hospitalari; de l'altra aporta una prova d'existència verificable per a auditors, reguladors i professionals sanitaris sense dependre de cap entitat central que pugui negar accés o manipular els registres. El model «t2p» aplicat a la salut converteix cada estudi clínic, cada diagnòstic per imatge i cada recepta digital en un testimoni immutable del seu propi origen.

En la pràctica, aquest flux es pot integrar als sistemes DICOM ja existents: quan l'escàner genera una nova tomografia, el programari de gestió calcula immediatament l'hash, sol·licita el segell temporal i actualitza les metadades del fitxer amb un enllaç a la transacció blockchain. Els professionals que revisen les imatges poden veure, al costat de l'informe, un codi QR o una referència hash que els permet verificar en temps real l'autenticitat de la dada. Així, qualsevol intent d'injectar tumors falsos —com demostren els experiments de CT-GAN, on els radiòlegs van ser enganyats fins al 99 % dels casos— esdevé ineficaç: sense el hash original i el seu segell temporal, la manipulació no podria passar desapercebuda per a un auditor independent [1] (com hem vist).

La mecànica de la prova d'existència combina tres principis fonamentals: **integritat criptogràfica**, **temporalitat certificada** i **preservació del domini de les dades**. Aquestes característiques asseguren que la informació clínica es mantingui tant segura com verificable, convertint-la en una defensa robusta contra l'engany digital que amenaça la vida dels pacients.

La promesa i el perill

Imagina un radiòleg que, sense saber-ho, revisa una tomografia on un tumor ha estat inserit artificialment per una IA generativa com CT-GAN. En l'estudi de USENIX Security 2019, els professionals van diagnosticar malignitat en el **99 % dels casos** amb tumors injectats i van considerar sans el **94 %** dels estudis on el tumor havia estat eliminat; fins i tot quan se'ls advertia del possible engany, l'error es manté entre un **60 % i un 87 %** [1]. Aquestes xifres mostren que la confiança cega en una imatge pot traduir-se directament en decisions de tractament equivocades, amb conseqüències potencialment letals.

La **promesa** del segell criptogràfic —un hash immutable i un segell de temps certificat (TSA o àncora de Merkle) que mai no abandona el dispositiu— és proporcionar una capa d'autenticitat que es converteix en la pedra angular de diagnòstics fiables. Quan cada estudi DICOM ve acompanyat d'un hash verificable, el radiòleg pot comprovar que la imatge no ha estat alterada des del moment de l'adquisició. Això no només protegeix el pacient davant manipulacions malintencionades, sinó que també reforça la **recerca**: els articles biomèdics que inclouen figures problemàtiques representen aproximadament un **3,8 %** dels estudis revisats, segons l'anàlisi de Bik [3]; una auditoria basada en proves d'existència podria detectar aquestes irregularitats abans de la publicació, reduint els costos de retractacions i augmentant la credibilitat del camp.

En l'àmbit dels **assaigs clínics**, plataformes com Triall ofereixen cadenes de custòdia que registren cada pas del procés, des de la recollida de mostres fins a l'anàlisi final, amb un hash i una marca temporal que garanteix que cap dada es pot suprimir o modificar sense deixar rastre [6]. Això permet a les autoritats reguladores —per exemple la FDA, que el 27 de juny de 2025 va publicar una guia definitiva sobre ciberseguretat de dispositius mèdics exigint SBOM i documentació exhaustiva [4]— verificar la integritat de cada element de l'assaig, evitant fraus com el cas dels Western Blots fabricats, vinculat a uns **16 M$** dels NIH [3].

Tanmateix, el **perill** rau en una falsa sensació d'immunitat. Un segell criptogràfic no és un substitut de la ciberseguretat de xarxa hospitalària; si l'origen de les dades (el dispositiu o el servidor que les emmagatzema) és compromès, el hash pot ser generat a partir d'una informació ja alterada. La complexitat d'integrar aquesta capa dins dels fluxos clínics —que sovint estan saturats per sistemes llegats i protocols rígids— pot generar retards o errors operatius si no es disposa d'una governança clara sobre qui té autorització per verificar i validar els segells. Un excés de confiança en la prova d'existència podria

conduir a una **desatenció** dels altres vectors d'atac, com vulnerabilitats en xarxes internes, programari maliciós que manipula les dades abans de signar-les o l'ús indegut de claus criptogràfiques per part de personal no autoritzat.

Com hem vist, el segell de temps i el hash constitueixen una capa necessària dins d'una estratègia integral de seguretat i integritat. Quan s'associen a controls de xarxa robustos, polítiques de governança transparents i formació contínua del personal sanitari, permeten restaurar la confiança en la medicina basada en dades —una confiança que pot marcar la diferència entre vida i mort per a milions de pacients.

És hora d'actuar

La integritat de les dades mèdiques ja no és una qüestió tècnica; és un requisit vital que ha de ser adoptat com a norma operativa per cada entitat del sector sanitari. Per això, la primera responsabilitat recau sobre **hospitals i fabricants d'equips**: el moment en què una tomografia o una història clínica entra al sistema ha de quedar permanentment registrat amb un hash criptogràfic i ancorat a un segell de temps (TSA) conforme al RFC 3161. Aquest procés, que es completa en mil·lisegons, impedeix qualsevol manipulació posterior sense deixar rastre d'inconsistència, tal com demostra el cas CT-GAN, on la inserció o supressió d'un tumor és detectable immediatament quan s'aplica una verificació de hash fiable [1].

Els **investigadors i les revistes científiques** han de fer del segell de temps una condició per a l'acceptació de qualsevol article que inclogui imatges biomèdiques. Eines com Proofig o ImageTwin ja ofereixen serveis d'auditoria d'integritat; el seu ús sistemàtic hauria de ser tan habitual com la revisió per parells. Això reduiria dràsticament l'impacte de fraus com els detectats per Bik, on prop d'un 3,8 % dels articles presentaven figures problemàtiques [3], i ajudaria a prevenir casos com la imputació federal del 28 de juny de 2024 per Western Blots fabricats, vinculada a uns 16 M$ dels NIH [3].

Els **reguladors**, liderats per la FDA amb la seva guia final de ciberseguretat (27 de juny de 2025) i l'EMA, han d'incorporar explícitament els requisits de proves d'existència en les normatives de dispositius mèdics. Això implica exigir un SBOM complet i una documentació que demostri la traçabilitat immutable dels fitxers clínics, tal com recomana el patró blockchain per a salut, que combina la càrrega fora de cadena amb hash i metadades mínimes a la cadena, complint HIPAA i 21 CFR Part 11 [4][5].

Les **asseguradores** poden convertir aquesta capa d'integritat en un criteri de cobertura: abans d'autoritzar el pagament d'un tractament o una cirurgia, es pot validar que les dades subjacents no hagin estat alterades. Un sistema de verificació automatitzat basat en la cadena de custòdia (com el producte Triall) podria reduir els costos associats a reclamacions fraudulentes i augmentar la confiança dels pagadors en l'autenticitat del diagnòstic [6].

Finalment, **pacients i professionals** han d'exigir transparència. Cada professional ha de poder presentar un certificat digital que demostri que les imatges i els informes que utilitza són exactes i no han estat modificats des del moment de la captura. Els pacients, per la seva part, poden sol·licitar accés a aquest registre immutable com a dret d'informació, reforçant la cultura de responsabilitat compartida.

«En resum, protegir la integritat de les dades és protegir vides. La tecnologia de proves d'existència ja està disponible i validada en escenaris reals; el que falta és l'adopció generalitzada i la imposició reguladora. No podem permetre que una imatge manipulada sigui la causa d'un diagnòstic erroni o d'una recepta fraudulenta. Com hem vist, és time2act: implementem hash i segell de temps a cada punt d'entrada, ho fem obligatori per a la recerca i exigim traçabilitat verificable a tots els nivells del sistema sanitari. Cada segon que esperem suposa un risc potencial per a la vida dels pacients.»

---

[1] Mirsky et al. — *CT-GAN: Malicious Tampering of 3D Medical Imagery* (USENIX Security 2019). https://www.usenix.org/conference/usenixsecurity19/presentation/mirsky · resum amb xifres: 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/ ↩

Credencials i autoria: educació i recerca

«Ni sé, ni crec que sé.»

— Plató, Apologia de Sòcrates (21d)

A la llum freda d'una sala de cures intensives del sud de Texas, el rellotge del monitor marcava les 03:17 quan una dona va entrar a l'habitació amb un pas segur i un braç ple de paper. Portava una bata blanca impecable i al pit duia una insígnia que brillava com si fos d'or: «RN — Registered Nurse». El pacient, un home de cinquanta-set anys amb una pneumònia severa, mirava la seva mà mentre el respirador emetia el seu soroll constant. La infermera es va inclinar cap al llit, revisà les constants i, sense dubtar-ho, administrà una dosi d'antibiòtics que havia prescrit el metge.

El moment semblava rutinari; tanmateix, la veritat que amagava aquell uniforme era qualsevol cosa menys ordinària. Aquell títol de «Registered Nurse» no provenia d'una universitat acreditada ni d'un programa d'estudis reconegut per l'estat. Era una de les més de 7.600 credencials falses detectades en l'operació «Nightingale», una investigació del Departament de Justícia dels Estats Units que va desmantellar una xarxa internacional dedicada a la fabricació i venda massiva de diplomes d'infermeria falsos (DOJ 2023; fase II, 2025) [3]. Cada credencial es venia per fins a uns 15.000 dòlars, i els compradors eren tant estudiants com professionals ja inserits al mercat laboral.

L'ambient es va tornar tens — el pacient mostrava signes de reacció adversa a l'antibiòtic. L'infermera, sense cap registre verificable que confirmés la seva formació ni la data d'obtenció del títol, havia pres decisions clíniques basades únicament en una aparença legal. El seu «diploma» era només un fitxer digital amb un hash segellat a una cadena de blocs desconeguda; el document real, si alguna cosa hi havia, no es trobava a la cadena, sinó fora d'ella, com indica el model de Blockcerts del MIT, on l'etiqueta d'un títol es limita a un hash i una transacció segellada [5].

Aquest incident encarna el fil conductor que uneix aquest capítol amb l'anterior: el perill concret que la falsificació de credencials pot suposar per a la vida humana. En el capítol 18, havíem exposat com les deepfakes i la suplantació d'identitat en exàmens remots poden comprometre la integritat acadèmica; aquí, la mateixa vulnerabilitat es tradueix en una amenaça directa per a la salut. La pregunta que emergeix és inevitable: **com podem saber amb certesa que un títol —o un treball— és autèntic?**

En un món on la IA generativa pot crear documents d'aspecte convincent i les xarxes de falsificació operen a escala global, la confiança tradicional en el paper signat o en el número de registre ja no és suficient. La resposta ha de recórrer a sistemes que garanteixin l'origen i la integritat sense dependre d'intermediaris: credencials verificables basades en blockchain i proves d'autoria que, com demostra el model W3C Verifiable Credentials Data Model 2.0 (maig-2025) [6], ofereixen una capa criptogràfica de confiança que es pot auditar independentment.

Mentre la infermera continuava amb la seva atenció, el monitor mostrava un ritme cada cop més irregular. La vida d'un pacient podia dependre de la capacitat del sistema educatiu i professional per demostrar, sense dubte, qui és realment qualificat per curar-lo. El silenci que es va instal·lar a la sala no era només el so de les màquines; era l'eco d'una pregunta que hauria de ressonar en cada aula, laboratori i oficina: **què fem quan la confiança desapareix?**

L'avaluació en crisi

A la primavera de 2025, les aules del Regne Unit es van convertir inesperadament en una sala d'experimentació a gran escala: entre les files de biblioteques i sales d'estudi, el trànsit cap a plataformes d'intel·ligència artificial es disparava. L'enquesta HEPI d'aquell any revelava que el **92 % dels estudiants del Regne Unit** ja feien servir eines d'IA per redactar assaigs, resoldre problemes matemàtics o fins i tot generar respostes a qüestionaris en línia. Més alarmant encara, la proporció d'estudiants que utilitzaven IA **durant les avaluacions** va saltar del **53 % al 88 % en només un any**, una evolució que supera qualsevol increment històric de tecnologies assistencials dins l'educació superior.

A primera vista, aquestes xifres podrien suggerir una democratització del coneixement: més estudiants accedeixen a recursos avançats i poden millorar la qualitat dels seus treballs. No obstant això, el panorama es desdibuixa quan es miren les limitacions de les eines de detecció actuals. El regulador australià TEQSA el 2024 ha conclòs que els mètodes quantitatius per identificar l'ús d'IA són «poc fiables». Un estudiant acusat pot, simplement, negar completament la utilització d'un model generatiu, sense deixar empremta

verificable; al mateix temps, **els usuaris hàbils són rarament enxampats**, ja que les solucions de detecció es basen en patrons superficials i no en proves criptogràfiques.

Aquesta vulnerabilitat té conseqüències tangibles. TEQSA assenyala un risc creixent de **falsos positius**: estudiants innocents són acusats injustament d'haver plagiat o d'haver recorregut a la IA, la qual cosa pot traduir-se en sancions acadèmiques i impactar negativament les seves trajectòries professionals. El cost social d'aquests errors és evident quan es considera que ja **aproximadament el 15,7 % dels estudiants** patia alguna forma d'engany contractual abans de l'arribada massiva de la IA generativa, una xifra que s'ha vist amplificada per la manca d'evidència fiable [2].

En aquest context, la resposta no pot ser simplement intensificar les polítiques disciplinàries. La reforma de l'avaluació que proposa TEQSA se centra a **redefinir els criteris de verificació**, passant d'un model basat en suposicions a un ecosistema on la prova d'autoria i la integritat dels documents siguin indiscutibles. Això implica adoptar tecnologies com les credencials verificables emmagatzemades en blockchain, que permeten registrar de manera immutable tant l'emissió del títol com el moment exacte en què es va crear un treball acadèmic.

La transició cap a aquest nou paradigma no elimina la necessitat d'una cultura ètica; al contrari, ofereix una base tècnica sòlida perquè les institucions puguin **distingir amb claredat** entre l'aportació genuïna de l'estudiant i el suport d'eines externes. En lloc d'enfocar-se en la persecució, els centres educatius poden canalitzar recursos cap a sistemes que garanteixin la transparència del procés d'avaluació, reduint així tant els falsos positius com les oportunitats per a fraus massius.

En resum, el panorama actual mostra una **erosió profunda de la confiança** en l'avaluació acadèmica, impulsada per una adopció massiva d'IA i per la incapacitat dels mecanismes de detecció tradicionals. La solució duradora passa per una infraestructura de credencials verificables que restableixi la seguretat del títol i de l'autoria, creant les bases d'un entorn educatiu resilient davant les tecnologies emergents.

Títols que no valen

Imagina un document oficial amb el segell d'una acadèmia d'infermeria: paper lustrejat, número de registre i una signatura digital aparentment autèntica. Un estudiant s'enorgulleix d'haver aconseguit aquell títol després d'un curs intensiu en línia, però ningú no veu que el diploma forma part d'una xarxa clandestina com la destapada per l'Operació Nightingale, una investigació conduïda pel Departament de Justícia dels EUA.

Com hem vist, el 2023 es van descobrir més de **7.600** diplomes i expedients falsos a Florida; la primera onada ja va portar **25 acusats** i la revocació de llicències en diversos estats, i va deixar pacients exposats a professionals no qualificats. La fase II, iniciada el 2025, va afegir dotze acusats més i va confirmar que la falsificació continua sent una amenaça creixent [3]. Mentre les autoritats combaten aquest mercat subterrani, les **deepfakes** —imatges generades per IA que superposen cara i veu d'una persona sobre el cos d'una altra— s'estenen al món dels exàmens i entrevistes remotes. Un estudiant pot ara fer passar la seva identitat davant una càmera d'examen amb una versemblança que enganya tant els algoritmes com els supervisors humans, i aquestes manipulacions poden ser emmagatzemades i reutilitzades per a futures oportunitats d'avaluació, destruint la confiança construïda al llarg de dècades [4].

El patró comú entre ambdues amenaces és clar: **la credencial i la identitat es poden falsificar**. El títol ja no és un segell fiable de competència; la cara que apareix a la pantalla no garanteix la presència real del candidat, exposant una vulnerabilitat fonamental en el model educatiu actual, basat en documents impresos o signatures digitals replicables i manipulables amb facilitat.

La solució no passa només per reforçar els mecanismes de detecció — s'ha d'establir una **infraestructura de verificació que no depengui de mirar-les**. Les credencials verificables basades en blockchain codifiquen cada títol i registre d'identitat amb un hash únic i les segellen en una cadena immutable, fent impossible la modificació sense deixar empremta. Aquest model garanteix l'autenticitat del document i permet a qualsevol part interessada (universitats, entitats reguladores o hospitals) comprovar instantàniament la seva validesa sense intermediaris.

En aquest context, el frau de credencials i la suplantació digital són una crida urgent a l'acció: cal adoptar sistemes descentralitzats que restableixin la confiança en l'educació i la salut, perquè els títols siguin realment **títols que valen**.

La resposta: credencials verificables

El primer pas cap a una educació que recuperi la confiança ja es va provar al laboratori del MIT, on el projecte Blockcerts va posar en marxa un pilot de **111 diplomes emesos en blockchain** l'any 2017. En aquest esquema les dades sensitives del títol —nom, data d'obtenció i programa d'estudi— es mantenen fora de la cadena; només s'incrusta a la xarxa un **hash unidireccional** que representa el contingut complet del document i una transacció segellada que certifica que el MIT ha creat aquell registre. Aquesta arquitectura és idèntica al model hash-àncora emprat per la prova d'autoria/existència, on el mateix mecanisme demostra que algú posseïa un arxiu en un moment determinat i que no ha estat alterat posteriorment [5].

A Europa, l'enfocament s'ha escalat a escala continental gràcies a **EBSI (European Blockchain Services Infrastructure)** i al marc de les **European Digital Credentials for Learning**. Aquestes plataformes emeten credencials amb **segells electrònics eIDAS**, assegurant la validesa legal i la interoperabilitat transfronterera. Fins ara s'han generat més de **76.000 credencials verificables**, que poden ser consultades instantàniament per qualsevol empresa o organisme regulador sense necessitat d'intermediaris ni processos manuals. L'estandardització ha arribat amb la **Recomanació W3C Verifiable Credentials Data Model 2.0** (maig-2025), que defineix com empaquetar, signar i validar aquestes credencials de forma segura i compatible amb qualsevol infraestructura blockchain pública [6].

El valor afegit d'aquest model és doble: elimina el risc de **diplomes falsos**, com els detectats a l'operació Nightingale, on més de **7.600 certificats d'infermeria falsificats** van posar en perill la seguretat dels pacients als EUA (DOJ 2023; fase II amb 12 acusats addicionals el 2025) [3]; i contraresta la **suplantació via deepfakes** i altres formes de proctoring digital que han compromès exàmens remots, ja que cada resposta d'un estudiant pot ser vinculada a una credencial verificable que garanteix l'origen i la integritat del treball [4].

En pràctica, un ocupador o una autoritat reguladora només ha d'introduir el **hash** del títol a la interfície de verificació corresponent; la cadena blockchain retorna l'empremta de temps i la signatura digital del proveïdor (MIT, universitat europea, etc.), confirmant que aquell document no s'ha modificat des de la seva emissió. No cal trucar a la institució, enviar correus electrònics o esperar setmanes per una resposta oficial: la verificació es completa en segons i és **immutable**. Això crea un ecosistema on el valor del títol deixa d'estar lligat a la reputació de l'entitat emissora —que pot ser objecte de fraus o falles administratives— i passa directament al **registre criptogràfic**, que és transparent, auditable i resistent a manipulacions.

Segons l'informe HEPI el 2025, com hem vist, l'ús de la IA en avaluacions ha experimentat un augment dràstic; amb credencials verificables basades en blockchain, les universitats poden establir una barrera tècnica que impedeixi que la IA produeixi documents falsificats sense deixar rastre, reforçant la confiança tant en l'emissor com en el receptor.

En definitiva, la combinació de **diplomes en blockchain**, **segells eIDAS** i l'estàndard **W3C Verifiable Credentials 2.0** constitueix una resposta concreta i provada que restableix les dues formes bàsiques de confiança en l'educació: el reconeixement del títol i la prova d'autoria. És ara, més que mai, el moment d'adoptar aquestes tecnologies descentralitzades per garantir que els nostres títols siguin **realment títols que valen** [1].

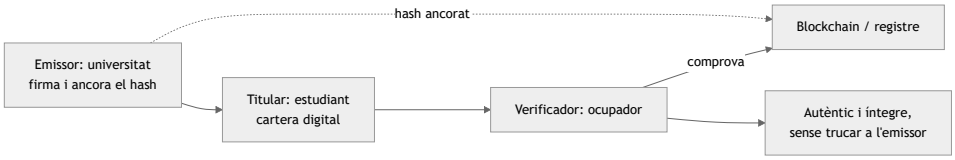


Figura 19.1 — L'emissor firma i ancora el hash de la credencial; el titular la presenta; qualsevol verificador en comprova l'autenticitat i la integritat sense intermediaris.

Provar l'autoria

En un món on la IA generativa pot reproduir text amb una fidelitat que desdibuixa les línies entre el que és original i el que és copiat, la veritable prova d'autoria esdevé la pedra angular de qualsevol sistema educatiu fiable. La solució no resideix en intentar demostrar l'absència d'intervenció —una tasca pràcticament impossible quan els algoritmes són cada vegada més opacs— sinó en certificar **QUAN** i

QUÈ s'ha creat. Aquesta és la premissa de la prova d'existència: un hash únic, combinat amb un segell de temps immutable, demostra que el creador posseïa el document en un moment determinat, establint així la prioritat d'autoria abans que el contingut arribi a qualsevol revisió o publicació.

El mecanisme és senzill però potent. En generar el hash —un resum criptogràfic de longitud fixa— es captura l'estat complet del fitxer en aquell instant i es registra a una cadena de blocs pública, on cada bloc conté un segell de temps verificable per la xarxa descentralitzada. El resultat és una prova irrefutable que el document existia i no havia estat alterat des d'aquell moment [7]. Això ofereix dos avantatges crucials: primer, enfront del plagi, el creador pot demostrar «jo ho tenia abans», i segon, contra les acusacions de falsos positius produïts per detectors poc fiables, es disposa d'una evidència objectiva que rebutja qualsevol dubte sobre la legitimitat de l'obra.

Com hem vist, el projecte MIT/Blockcerts va certificar 111 estudis el 2017 i la Unió Europea ha emmagatzemat més de 76.000 credencials fins al maig del 2025, amb el model W3C Verifiable Credentials 2.0, demostrant que la infraestructura per a la prova d'autoria ja està operativa i escalable [5][6].

El mateix principi s'aplica al treball intel·lectual dels investigadors i estudiants. Cada article, cada projecte de tesi o fins i tot cada codi font pot ser «segellat» abans de ser compartit amb supervisors o revisors. Això no només protegeix l'autor contra acusacions injustes, sinó que també reforça la confiança en els processos d'avaluació acadèmica; com hem vist, l'ús d'IA en avaluacions s'ha disparat recentment [1]. En aquest context, les institucions no poden seguir depenent únicament de detectors d'autoria que són «poc fiables» i que sovint permeten negar la responsabilitat [2].

Una prova tangible d'aquesta pràctica es troba a l'obra que llegeixes ara. Abans de publicar **time2act**, el manuscrit va ser hashat i segellat en una cadena de blocs, garantint que ningú —ni tan sols l'autor— pogués modificar-lo sense deixar empremta. Aquest gest no és un simple exercici tècnic; és la manifestació concreta del principi que defensa aquest capítol: **la confiança es reconstrueix amb proves verificables, no amb suposicions**.

La crida a l'acció és clara. Educadors, administradors i investigadors han d'adoptar immediatament les eines de prova d'existència basades en blockchain per a tots els seus productes intel·lectuals. Això implica integrar solucions com Blockcerts o EBSI als fluxos de treball acadèmics, establir polítiques que obliguin al segellat pre-publicació i formar el personal en la gestió d'aquestes credencials digitals. Només així podrem garantir que els títols i les produccions intel·lectuals siguin realment **títols que valen**, i que la nostra educació recuperi les dues confiances fonamentals: el reconeixement del títol i la prova d'autoria.

La promesa i el perill

Imagina una aula digital d'una universitat europea on una professora acaba de publicar els resultats finals d'un curs de bioenginyeria. Un cop carregat el fitxer al repositori institucional, un algoritme genera automàticament un *Verifiable Credential* basat en el model W3C 2.0 (recomanat per la W3C el maig del 2025) i l'anomena «Diploma de Bioenginyeria». L'estudiant que ha superat el curs rep instantàniament una credencial blockchain amb un hash únic i un segell de temps verificable. Sense cap paper, sense trucades telefòniques al registre central, qualsevol empresa o autoritat pot comprovar la validesa del títol en segons: només cal consultar l'explorador públic d'EBSI o el node nacional corresponent.

Aquesta fluïdesa és la promesa que sustenta tot el paradigma de les credencials digitals. Un títol es converteix en un actiu portable, interoperable i immutable; la prova d'autoria, a través del mateix mecanisme de hash + segell de temps, garanteix que l'estudiant era el propietari del treball en el moment exacte de la seva creació (com demostra el projecte MIT/Blockcerts amb 111 estudiants pilotats el 2017) [5]. La verificació és instantània i descentralitzada: les empreses poden validar milers de sol·licituds d'ocupació sense dependre d'una oficina de certificació central, reduint costos administratius i eliminant fraus com els 7.600 diplomes falsos detectats en l'Operation Nightingale als EUA (2023-2025) [3].

No obstant això, la mateixa infraestructura que ofereix confiança pot generar nous perills. El *proctoring* invasiu, impulsat per plataformes de supervisió basades en IA i reconeixement facial, recull dades biomètriques d'estudiants menors de 18 anys sense un marc clar de consentiment ni control sobre l'ús posterior d'aquests registres. La privacitat es veu amenaçada quan les institucions emmagatzemen imatges, àudios i patrons de comportament en servidors centralitzats o, pitjor encara, en cadenes públiques sense anonimització adequada.

A més, l'equitat acadèmica corre el risc d'esdevenir una nova bretxa digital. Segons l'estudi HEPI 2025, el 92 % dels estudiants del Regne Unit ja fan servir IA, i la proporció que la utilitza en avaluacions ha pujat del 53 % al 88 % en només un any [1]. Qui no disposi d'accés a dispositius capaços de generar o verificar credencials blockchain quedarà relegat a processos manuals més lents i menys reconeguts, augmentant la desigualtat entre institucions ben finançades i les que operen amb recursos limitats.

La dependència d'un proveïdor únic de serveis de segellat també és una vulnerabilitat estructural. Si una empresa que controla la infraestructura clau pateix un atac o decideix modificar les condicions del servei, tota la cadena educativa pot veure compromesa la integritat dels títols i les proves d'autoria. Els riscos de falsos positius —i la base d'engany contractual del 15,7 % detectada en l'estudi de Newton— demostren que cap sistema no és infal·lible [2].

Per tal d'aprofitar la promesa sense caure en els perills, cal dissenyar una arquitectura centrada en la privacitat i l'equitat. La divulgació selectiva ha de permetre a l'estudiant decidir quines dades comparteix amb tercers; el control sobre les seves credencials ha d'estar integrat en interfícies amigables que no requereixin coneixements tècnics avançats. A més, les polítiques institucionals han d'incloure mecanismes de verificació descentralitzada i auditories independents per garantir que els proveïdors mantinguin uns estàndards de seguretat robustos.

En resum, la blockchain pot convertir l'educació en un ecosistema on títols fiables i autoria justa siguin la norma; però només si es protegeixen les dades personals, s'assoleix equitat d'accés i es diversifica la infraestructura de confiança. Adoptar aquestes tecnologies ara decidirà si els nostres sistemes educatius avancen cap a una veritable *trust-by-design* o esdevenen punts febles per a l'abús i la discriminació.

És hora d'actuar

Les universitats i els centres d'ensenyament superior són el primer front on la crisi de confiança es tradueix en pèrdues concretes: diplomes falsos que arriben a les sales d'operació ([3]), exàmens suplantats per deepfakes que amenacen la integritat dels processos de selecció ([4]) i una generació d'estudiants que, com hem vist, ja el 92 % fa servir IA en les seves tasques acadèmiques, amb un augment de 35 punts percentuals en l'ús per avaluacions en només un any ([1]). La solució no passa per dependre de detectors cada vegada més sofisticats —que, com avisa TEQSA, són «poc fiables» i sovint deixen l'acusat amb la possibilitat de negar-ne l'ús ([2])– sinó per reconstruir el model de credencialització des del seu nucli.

1. Universitats i centres: emetre credencials verificables

Adoptar els estàndards oberts com el W3C Verifiable Credentials Data Model 2.0 (maig-2025) ([6]) permet que cada títol acadèmic es converteixi en un «hash + transacció segellada» a la cadena de blocs, tal com demostra el projecte Blockcerts del MIT amb 111 estudiants pilotats el 2017 ([5]). Aquestes credencials són immutables, verificables instantàniament i compatibles amb els sistemes d'identitat digital europea (EBSI) que ja gestionen més de 76.000 certificats ([6]). Les universitats han de crear infraestructures pròpies o unir-se a xarxes federades per emetre i registrar aquests segells, garantint alhora la privacitat dels estudiants mitjançant la divulgació selectiva de dades.

2. Estudiants i investigadors: segellar la prova d'existència del propi treball

Cada article, projecte o tesi ha de ser «timestamped» a una blockchain pública o permissionada abans de la seva difusió. El mateix mecanisme que protegeix aquesta obra (hash + segell de temps) assegura la prioritat d'autoria i impedeix la suplantació ([7]). Les plataformes de gestió de recerca han d'integrar API que automatitzin aquest procés, oferint a l'autor una prova verificable que pot ser consultada per qualsevol lector o revisor.

3. Ocupadors i col·legis professionals: verificar credencials a l'instant

Els processos de contractació i acreditació han d'incorporar consultes en temps real al registre blockchain dels títols, eliminant la necessitat de trucades telefòniques o documents escanejats que es poden falsificar. Això redueix el risc de contractar professionals amb diplomes fraudulents —un problema ja evidenciat per l'Operation Nightingale ([3])– i augmenta la confiança en les competències declarades.

4. Reguladors i agències d'acreditació: reconèixer estàndards interoperables

Els organismes reguladors han de formalitzar el reconeixement oficial de les credencials verificables, establint marcs de compliment que siguin compatibles amb eIDAS i altres normatives internacionals. Això crea una capa de «trust-by-design» a escala macro, evitant la fragmentació del mercat educatiu i assegurant que les noves tecnologies no es converteixin en punts febles per a l'abús o discriminació.

5. Plataformes educatives: integrar procedència amb privacitat

Els proveïdors d'aprenentatge en línia han de dissenyar sistemes on la propietat intel·lectual del contingut i les credencials dels usuaris es gestionin amb divulgació selectiva, tal com recomana el model de dades verificables. Això permet que els estudiants demostrin competències sense revelar informació personal innecessària, alineant la privacitat amb la transparència.

Protegir l'autenticitat del títol i de l'autoria és, en última instància, defensar el mèrit mateix de l'educació. Cada institució que adopti credencials verificables i proves d'existència no només reforça la confiança dels seus graduats, sinó que contribueix a un ecosistema global on la veritat acadèmica es manté intacta davant les amenaces de la IA generativa. És **time2act**: el futur de l'aprenentatge depèn de la nostra capacitat per construir-lo avui.

---

[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 veritat com a arma: defensa i drets humans

«Vaig jurar no callar mai, onsevulla i quan sigui que éssers humans pateixin sofriment i humiliació.»

— Elie Wiesel, discurs del Premi Nobel de la Pau (1986)

Era el 16 de març de 2022, tres setmanes després que les forces russes trenquessin la frontera ucraïnesa i iniciessin una ofensiva que sacsejava tot Europa. A l'alba, els telèfons mòbils d'oficines diplomàtiques, les tauletes dels periodistes de guerra i les pantalles de mig país mostraven el mateix missatge: un vídeo en què el president Volodímir Zelenski apareixia demanant als seus soldats que «deposin les armes». La imatge, difosa per la cadena Ucraïna 24 –que havia estat piratejada aquell matí– es projectava sobre el rètol informatiu de l'estació de televisió i, simultàniament, s'incrustava a la seva pàgina web.

El clip era evidentment una falsificació: resolució baixa, contorns facials difuminats i un to de pell que no coincidia amb el color natural del president. No obstant això, en la frenètica cursa informativa d'una guerra activa, el vídeo es va propagar per les xarxes socials com una onada de desinformació, alimentant rumors i va generar un primer senyal d'alarma: cap líder del país cridava a la rendició, i potser hi havia una ruptura interna que calia explotar.

En poques hores, però, la resposta oficial va ser tan ràpida com contundent. Zelenski va publicar un vídeo —un instant àgil i autèntic on es veia el seu rostre sense filtres— i, amb veu clara, va rebutjar rotundament la demanda: «No pensem deposar cap arma». El missatge, difós a través dels canals verificats de la Presidència i retransmès per les agències internacionals, va desactivar la falsificació en una jornada.

Aquell episodi es converteix avui en el primer cas documentat d'una «deepfake armada» —una falsificació audiovisual emprada directament com a arma psicològica dins un conflicte bèl·lic en curs. El seu impacte no es limità a la confusió momentània; va demostrar que qui controla la percepció de la veritat pot guanyar un avantatge estratègic decisiu, alterant les decisions militars i la confiança del poble. La guerra d'informació, com un front invisible però vital, demostra que la veritat mateixa es converteix en un recurs escàs i disputat.

En aquest context, el desafiament no és només detectar els deepfakes una vegada ja han circulat; la defensa duradora requereix autenticar les comunicacions des del moment de la seva creació i segellar-les amb tecnologies com l'hashing criptogràfic i la blockchain, assegurant que cada declaració oficial, cada imatge d'un testimoni ocular, porti una prova inalterable d'origen. Aquesta necessitat es converteix en el nucli de la nostra proposta: transformar la veritat en una arma defensiva per a la defensa dels drets humans i la justícia internacional. [1]

L'arma de la desinformació

En l'últim decenni, les operacions d'influència han transcendit el simple enviament de propaganda per convertir-se en una arquitectura digital que manipula realitats i modela decisions polítiques a escala global. La campanya russa coneguda com a «Doppelganger», per exemple, ha desplegat una xarxa de bots i sistemes d'intel·ligència artificial capaços de clonar webs de mitjans i governs occidentals, desvirtuant notícies i amplificant narratives hostils a Ucraïna. Aquestes plataformes falsificades apareixen en motors de cerca com a resultats legítims, enganyant tant lectors casuals com analistes professionals. La Unió Europea, reconeixent la gravetat del fenomen, ha imposat sancions contra les entitats vinculades al projecte, destacant que el seu objectiu no és només desinformar sinó erosionar la confiança en institucions democràtiques [2].

El 2024 ha marcat un punt d'inflexió: una temporada electoral global que ha coincidit amb l'explosió de deepfakes a múltiples continents. A Eslovàquia, dies abans del vot, es va difondre un àudio fals atribuït a un líder polític, alterant el discurs oficial i incitant al descontentament social. Als Estats Units, una trucada automatitzada —un «robocall»— reproduïa la veu clonada del president Joe Biden demanant explícitament que els ciutadans no emetessin el seu vot. La Federal Communications Commission (FCC) ha proposat una multa de 6 milions de dòlars a l'operador polític responsable, Steve Kramer, per aquest intent de coacció electoral, un precedent que evidencia com les tecnologies de síntesi vocal es converteixen en armes d'intimidació política [3]. A Moldàvia i Taiwan, vídeos manipulats mostraven la presidenta Maia Sandu i el candidat Lai Ching-te pronunciant declaracions inexistents, generant protestes i crides a la revocació que van requerir una resposta institucional ràpida.

Aquests casos il·lustren més que un simple «error de fact-check». El veritable perill és el que els experts anomenen el **«dividend del mentider»**: quan la capacitat de falsificar es converteix en omnipresent, el públic comença a dubtar fins i tot de les proves verificades. Aquesta corrosió de la fe en l'evidència crea un buit on qualsevol afirmació —falsa o veritable— pot ser descartada com a manipulació potencial. En aquest context, la defensa dels drets humans es veu amenaçada per una crisi de credibilitat: jutges internacionals, tribunals penals i organismes d'investigació es troben incapaços d'establir l'autenticitat d'evidències crucials sense recursos tecnològics avançats.

La solució no resideix únicament en detectar deepfakes posteriors, sinó en **autenticar les comunicacions des del seu origen**. La tecnologia d'hashing criptogràfic i la inserció immutable a blockchain ofereixen una pista verificable que pot ser consultada per qualsevol part interessada. Quan un missatge militar o una declaració oficial es registra amb un hash únic en el moment de la seva creació, qualsevol alteració posterior és evident i rebutjada automàticament pel sistema. Així, els actors malintencionats es veuen desincentivats a crear falsificacions, ja que la veritat documental queda «segellada» amb una prova d'existència incapaç de ser suprimida o manipulada.

En definitiva, el cinquè front —la defensa i els drets humans— es converteix en una batalla per preservar la confiança en la informació. Només adoptant protocols que garanteixin l'origen i la integritat de les dades podrem contrarestar el dividend del mentider i transformar la veritat en una arma real contra la desinformació.

Ordres falses, comandaments suplantats

El març del 2024 va circular un vídeo que semblava provenir directament del cap de la intel·ligència militar ucraïnesa, Kirilo Budanov. Compost a partir d'entrevistes prèvies amb Budanov i amb el secretari del Consell de Seguretat i Defensa Nacional, el clip fabricava una falsa «admissió» que atribuïa a Ucraïna l'atac contra la sala de concerts Crocus City Hall. El material combinava fragments de veu i d'imatge reals amb manipulacions generades per IA, fins a fer que el resultat fos gairebé indistingible de la realitat. L'episodi il·lustra el perill imminent que suposa la tecnologia del deepfake quan una veu o una cara clonada es col·loca damunt d'una ordre o d'una confessió fabricada [4].

Aquesta vulnerabilitat no és només un problema de confusió momentània; té implicacions estratègiques que poden alterar l'equilibri d'un conflicte. Una ordre falsificada pot conduir a moviments innecessaris, exposar forces a emboscades i, en el pitjor dels escenaris, desencadenar una escalada accidental de violència. Per això, la guia conjunta emesa per la NSA, el FBI i la CISA el 2023 identifica el Departament de Defensa i la base industrial de defensa com a objectius prioritaris d'atacs de suplantació, i recomana dos eixos complementaris: (1) detectar deepfakes amb eines avançades d'anàlisi forense i (2) establir la procedència verificable dels mitjans utilitzats per transmetre ordres i informes [4].

L'establiment de la procedència es basa en l'ús d'identificadors criptogràfics que asseguren que cada missatge o document ha estat signat digitalment pel seu emissor legítim i que el hash resultant queda ancorat a una cadena de blocs immutable. Aquest model ja s'ha posat en pràctica en projectes com **eyeWitness to Atrocities**, on una aplicació genera un hash criptogràfic en temps real al moment de la captura d'evidència, garantint-ne la integritat i la data d'origen; més de 20.000 ítems verificables ja s'han usat com a prova en casos judicials [6]. De manera similar, el **Starling Lab** juntament amb Hala Systems ha enviat proves de crims de guerra a la Fiscalia de la CPI utilitzant hash, blockchain, C2PA i Filecoin, creant un registre auditable que impedeix qualsevol manipulació posterior [7].

El risc s'estén més enllà del camp de batalla terrestre. La recerca sobre «deepfake geography» del 2021 va demostrar com es poden crear imatges satel·litals sintètiques d'aspecte realista, capaces de falsificar la presència o l'absència d'activitats militars a zones crítiques [5]. El director de la National Geospatial-Intelligence Agency (NGA) ja havia alertat el 2019 que aquests enganys podrien ser utilitzats per amagar moviments de tropes, manipular negociacions diplomàtiques o justificar intervencions armades basades en proves falses. Si un govern es basa en una imatge satel·lital manipulada per planificar una operació, el resultat pot ser una resposta militar equivocada i la pèrdua de vides innocents.

La solució, tal com proposen les autoritats nord-americanes, consisteix a integrar sistemes d'autenticació d'extrem a extrem que combinin signatures digitals, ancoratge en blockchain i protocols d'avaluació per part d'agències certificades independentment. Només amb una cadena de confiança verificable des del moment de la generació fins al consum final es pot garantir que les ordres militars no siguin instruments d'engany, sinó instruments fiables d'una defensa responsable. En aquest escenari, la veritat deixa d'ésser un luxe i es converteix en l'arma més poderosa contra la desinformació ben armada.

La veritat com a prova: drets humans

En una tarda d'octubre del 2023, al centre de comandament avançat prop de Kharkiv, un equip del Starling Lab i Hala Systems va rebre una càrrega digital aparentment ordinària. El fitxer incloïa milers de metadades — marques de temps, coordenades GPS precises, hash criptogràfic generat al moment i un enllaç a la xarxa descentralitzada Filecoin on es guardaria el contingut. No era només un document; era la materialització del model **t2p**, un registre immutable des del primer instant, capaç d'impedir qualsevol intent de manipulació.

El protocol es va basar en el precedent establert per l'aplicació *eyeWitness to Atrocities*, creada el 2015 per l'International Bar Association juntament amb LexisNexis. Cada imatge o vídeo capturat es transforma immediatament en un hash criptogràfic, acompanyat de metadades de temps i coordenades GPS; aquest hash puja a una cadena de confiança verificable i qualsevol alteració trenca l'associació hash-fitxer, revelant la falsificació amb una claredat que els tribunals tradicionals no poden oferir [6]. Fins ara s'han enviat més de 20.000 ítems a la Comissió d'Investigació de les Nacions Unides, convertint-se en proves verificables en processos judicials relacionats amb el conflicte ucraïnès.

Quan aquests elements es van combinar amb la infraestructura blockchain del Starling Lab, l'impacte va ser exponencial. El dossier presentat a la Fiscalia de la Cort Penal Internacional (CPI) el 2022 incloïa evidències de presumptes crims de guerra a Kharkiv: publicacions i vídeos d'atacs indiscriminats, amb les metadades registrades i un hash per a cada ítem. Cada peça estava ancorada en una cadena immutable, preservada a Filecoin segons els estàndards de procedència **C2PA** i alineada amb el **Protocol de Berkeley**, adoptat l'any 2020 com a referent global per a proves digitals d'organismes com l'OHCHR [7].

Aquesta arquitectura no només garanteix autenticitat, sinó que crea un escut legal que impedeix la manipulació informativa. En la CPI, una ordre d'arrest del 2017 ja havia mostrat que les proves recollides a les xarxes socials podien ser la base d'una acusació formal; ara, amb hash i blockchain, la prova arriba a un nivell de certitud que supera qualsevol dubte sobre la seva integritat. La veritat deixa d'ésser una narració subjectiva i es converteix en **una arma legal**: cada fragment de realitat queda segellat des del moment de la captura, inalterable fins al tribunal.

El missatge és clar: el model *t2p* no és només una solució tècnica, sinó un mecanisme de defensa per a drets humans en l'era de les deepfakes i la guerra d'informació. Codificar la veritat amb hash i ancorar-la a una cadena immutable constitueix una barrera infranquejable contra la falsificació que podria desencadenar pànic o justificar atrocitats, i ja ha demostrat ser capaç de salvaguardar la justícia i garantir una veu autèntica i inalterable per a les víctimes.



Figura 20.1 — Captura amb hash a l'origen → metadades i geolocalització → ancoratge immutable → prova admissible: la cadena que converteix un testimoni digital en evidència.

La defensa respon

Les agències d'intel·ligència i els aliats de l'OTAN van adonar-se aviat que la simple detecció de deepfakes només constitueix una primera línia de defensa. El programa MediFor, impulsat pel DARPA, va establir un marc per validar la integritat d'imatges i vídeos mitjançant anàlisis forenses avançades; però el seu èxit es va veure limitat quan les xarxes neuronals generatives van començar a produir contingut indistingible de l'original en qüestió de dies. En paral·lel, SemaFor —el complement de forènsica semàntica— va culminar el 2024 amb un catàleg obert d'eines per a la detecció, atribució i caracterització de material manipulat [8], i la NATO StratCom COE manté una vigilància contínua sobre les noves tècniques d'engany digital [8].

El que aquestes iniciatives demostren és un principi fonamental: **la detecció posterior no pot revertir els danys causats per una informació falsificada que ja ha circulat**. Com hem vist amb el deepfake de la «rendició» de Zelenski del 16 de març de 2022, un vídeo fals va generar pànic i va influir en les operacions militars abans que qualsevol eina forense pogués confirmar-la [1]; de manera similar, la campanya russa «Doppelganger», que clona webs de mitjans occidentals amb bots i IA per difondre notícies manipulades, ha estat sancionada per la UE però segueix demostrant que **la propagació prèvia a la identificació** és el veritable motor del dany [2].

Per això cal **autenticar les comunicacions i les proves des del moment de la seva creació**, una pràctica ja provada en el camp dels drets humans. L'aplicació de l'hash criptogràfic a l'origen, tal com ho fa l'app eyeWitness to Atrocities —que genera un resum únic i immutable en temps real durant la captura d'evidència visual— ha permès que més de 20.000 ítems siguin verificables en casos judicials, establint un precedent directe per al concepte de «t2p» [6]. Aquest model s'ha escalat a iniciatives com Starling Lab i Hala Systems, que van presentar a la Fiscalia de la CPI documents d'atrocitats amb hash, blockchain i el marc C2PA, convertint les proves en un registre inalterable i legalment reconeixible [7].

La resposta institucional ha d'evolucionar cap a una **estratègia de segellatge preemptiu**: cada transmissió militar, cada informe d'intel·ligència i cada testimoni ocular es codifica amb una signatura digital que es registra immediatament en una cadena immutable. Això impedeix la manipulació posterior i ofereix a jutges i investigadors un rastre verificable de procedència —una prova que no pot ser desmentida per l'últim model generatiu.

En aquest context, el repte públic establert per SemaFor el 2024 es converteix en una crida a l'acció: **desenvolupar i desplegar estàndards oberts de segellatge d'origen** compatibles amb les infraestructures blockchain globals. Cal integrar aquests protocols en la cadena de comandament i control (C2), assegurant que cada ordre i cada informe operatiu porti una capa d'autenticitat criptogràfica des del primer byte.

Així, el front més impactant —la defensa contra la falsificació en temps de guerra— no es basa únicament en detectar mentides, sinó en impedir que les mentides **prosperin**. La veritat, codificada i ancorada a una cadena immutable, es converteix en l'arma més poderosa per preservar els drets humans i garantir la responsabilitat en un món on la informació pot ser fabricada amb una sola pulsació de botó.

La promesa i el perill

En les zones de conflicte la veritat esdevé un bé escàs, però la tecnologia pot convertir-la en una arma imparable: l'autenticació criptogràfica garanteix que les ordres al front siguin genuïnes i que les proves d'atrocitats es puguin presentar als tribunals sense dubte sobre la seva integritat. El projecte *eyeWitness to Atrocities* (IBA + LexisNexis) ja genera un hash criptogràfic en el moment de la captura i enllaça les metadades a una cadena immutable; més de 20.000 ítems verificats s'han usat com a evidència a Ucraïna, establint un precedent per al marc *t2p* [6]. De manera similar, Starling Lab i Hala Systems han enviat proves de presumptes crims de guerra a la Fiscalia de la CPI amb hash i blockchain, emprant estàndards com C2PA i Filecoin; el Protocol de Berkeley adoptat per l'OHCHR (2020) ja preveia aquesta cadena de confiança [7].

Aquesta infraestructura no només reforça els tribunals, sinó que impedeix que les potències militars construeixin pretextos falsificats per iniciar o prolongar conflictes. El deepfake de la «rendició» de Zelenski, difós el 16 de març de 2022 i desmentit en hores, mostra com una manipulació audiovisual pot generar pànic abans que les autoritats reaccionin [1]; si cada transmissió fos signada digitalment, l'impacte d'aquestes falsificacions es reduiria dràsticament. El mateix val per la suplantació de comandaments, com el deepfake del cap d'intel·ligència ucraïnès Budanov (2024); les recomanacions de NSA/FBI/CISA (2023) per establir la procedència i l'autenticitat en les comunicacions defensives són ara més rellevants que mai [4].

Tanmateix, l'amenaça vinculada a aquesta capacitat d'autenticació és profunda: la codificació i l'ancoratge de metadades a una cadena immutable poden desanonimitzar testimonis, víctimes i periodistes en zones de guerra si no es disposen les salvaguardes adequades. Un registre que reveli la ubicació geogràfica o l'hora exacta d'una gravació pot costar vides, especialment quan els règims autoritaris tenen recursos per rastrejar i perseguir dissidents. A més, aquests governs podrien instrumentalitzar la tecnologia per conferir un «segell oficial» a propaganda fabricada, com demostra la campanya russa «Doppelganger», que clona webs de mitjans occidentals amb bots i IA, sancionada per la UE però encara capaç d'usar tecnologies de verificació per legitimar falsedats [2].

Per equilibrar aquesta dualitat cal un disseny centrat en la seguretat i la privacitat. La divulgació selectiva hauria de permetre que només les parts autoritzades accedeixin a metadades sensibles, mantenint la transparència necessària per a la verificació judicial. Els protocols han d'incloure mecanismes de control del testimoni, com claus temporals o credencials descentralitzades revocables en cas de compromís. Només amb aquest marc èticament conscient i madur podrem aprofitar la promesa d'una veritat immutable sense caure en el perill d'un control totalitari de la informació.

És hora d'actuar

Les forces armades i les agències de seguretat ja no poden confiar únicament en la veu del comandament; han d'**autenticar cada transmissió** abans que arribi al camp de batalla. El cas del deepfake del cap d'intel·ligència ucraïnès Budanov, que el 2024 intentava fabricar una falsa atribució d'un atac, ha demostrat que la manca d'un mecanisme de verificació pot desencadenar decisions estratègiques errònies i augmentar el risc d'escalada [4]. Per això, les forces han d'incorporar signatures digitals basades en claus temporals i credencials descentralitzades, tal com recomanen la NSA, el FBI i la CISA per a la procedència de les comunicacions militars (2023). Cada ordre i cada informe d'intel·ligència ha d'arribar amb un **hash criptogràfic verificable** que garanteixi l'origen i la integritat del missatge abans de ser executat.

Les organitzacions de drets humans i els periodistes són el front més vulnerable a les manipulacions. L'aplicació *eyeWitness to Atrocities*, desenvolupada per l'IBA i LexisNexis, ha demostrat que un **hash generat al moment de la captura** pot proporcionar una prova d'existència immutable; més de 20.000 ítems ja s'han usat com a evidència fiable en tribunals ucraïnesos [6]. Aquest model ha de ser adoptat globalment: cada foto, vídeo o testimoni gravat en zones de conflicte ha d'estar immediatament segellat amb una cadena de blocs pública i verificable. Les organitzacions han d'invertir en equips mòbils que integrin la tecnologia C2PA i Filecoin, tal com ho van fer Starling Lab i Hala Systems per a la CPI el 2022 [7], assegurant que la font sigui protegida però la prova no es pugui falsificar.

Els tribunals i les fiscalies han d'anar més enllà de l'acceptació passiva. Han d'establir **protocols obligatoris** basats en el Protocol de Berkeley (OHCHR, 2020) que exigeixin proves amb hash i blockchain per a qualsevol documentació relacionada amb crims de guerra. Això implica crear guies operatives per a jutges i fiscals, capacitacions especialitzades i una infraestructura judicial digital capaç de validar les proves en temps real. La primera ordre d'arrest basada principalment en xarxes socials (al-Werfalli, 2017) ja ha mostrat com les evidències digitals poden ser decisives; ara cal un marc formalitzat per garantir-ne l'admissibilitat i autenticitat.

Les plataformes de difusió –des de X fins a TikTok– han d'assumir una responsabilitat proactiva en la preservació de la procedència del contingut relacionat amb conflictes; cal integrar sistemes que registrin metadades, marques de temps i hashes en pujar un vídeo o una imatge i oferir eines per a verificadors independents. La normativa europea ja ha sancionat campanyes de suplantació com la «Doppelganger» russa [2]; les plataformes han d'anar més enllà del simple bloqueig i garantir transparència total sobre l'origen del material.

Cada usuari, com a primer filtre, ha d'aprendre a verificar abans de compartir imatges o àudios de guerra, emprant aplicacions que mostrin els hashes i la cadena de blocs associada. El deepfake de rendició de Zelenski el 2022 –desmentit en hores però capaç d'alimentar rumors massius– demostra com l'absència de verificació pot crear pànic i legitimar accions violentes [1].

Els responsables polítics han de legislar estàndards clars per a la seguretat i la salvaguarda d'aquestes tecnologies, establint marcs ètics que impedeixin un control totalitari de la informació mentre fomenten una veritat immutable. **Time2act** no és només un lema: és una crida urgent perquè la prova d'existència sigui el fonament de la justícia i la pau.

---

[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* (campanya de desinformació russa). https://www.disinfo.eu/doppelganger-hub/ ↩

[3] FCC — *Proposed $6M fine for AI-deepfake Biden robocall* (2024); IPI (Eslovàquia). 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 a la captura; casos a Ucraïna). 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); Protocol 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)* i *Deepfake Defense* (2024); NATO StratCom COE. https://www.darpa.mil/research/programs/semantic-forensics ↩

Crèdits de carboni: el mercat del compliment

«Un objectiu central de la política pública hauria de ser facilitar el desenvolupament d'institucions que treguin el millor dels humans.»

— Elinor Ostrom, lliçó Nobel (2009)

El matí del 19 de gener de 2011, els operadors de mig continent van trobar la mateixa resposta a les seves pantalles: *transferència no disponible*. No era una avaria informàtica. Era una decisió deliberada de la Comissió Europea, que aquell dia va prémer el botó d'apagada del mercat de carboni més gran del món. Durant les setmanes anteriors, uns atacants havien buidat comptes de diversos registres nacionals —Àustria, la República Txeca, Grècia, Estònia i Polònia— mitjançant correus de *phishing* i troians que robaven contrasenyes. En pocs dies van desaparèixer més de dos milions de drets d'emissió, valorats en uns 28-30 milions d'euros; el registre txec va ser el més castigat, amb pèrdues d'uns 7 milions [11]. Aquells drets representaven tones reals de CO_2 que algú tenia l'obligació legal de compensar, i havien volat amb un sol clic cap a comptes d'Alemanya, Estònia i el Regne Unit.

La Comissió no va tenir més remei que suspendre les transferències a **tots** els registres nacionals alhora i reobrir-los de manera esglaonada, només quan cadascun complís uns mínims de seguretat [11]. Durant dies, el principal instrument climàtic d'Europa —un mercat que mou desenes de milers de milions d'euros— va quedar congelat perquè la seva veritat vivia en bases de dades que es podien buidar de matinada. La paradoxa era cruel: un sistema dissenyat per salvar el clima havia estat segrestat per un robatori d'allò més corrent.

Aquell apagat és la millor porta d'entrada a una pregunta incòmoda. Si el carboni té preu —i en té—, qui garanteix que la tona que es compra, es ven o es compensa va existir de debò, una sola vegada, i que ningú no l'ha alterada després? Aquest capítol tracta del **mercat del compliment**: els sistemes obligatoris que posen preu a les emissions. Funcionen, mouen el capital i ja han fet baixar emissions. Però la seva integritat no depèn del preu, sinó d'una cosa més humil i més fràgil: la confiança en les dades.

Posar preu a l'aire

El cor del mercat europeu és el règim de comerç de drets d'emissió (EU ETS), un esquema de cap-and-trade o «límit i comerç». La idea és senzilla i elegant: l'estat fixa un sostre decreixent sobre el total de gasos que es poden emetre i reparteix o subhasta drets —les anomenades EUA, European Union Allowances— en què cada dret equival a una tona de CO_2 equivalent. Qui contamina menys del que li correspon pot vendre els drets sobrants; qui contamina més, ha d'adquirir-ne. El preu recompensa qui es descarbonitza i penalitza qui s'endarrereix.

Vint anys després que Paul Roberts, periodista i analista d'energia, descrigués a *The End of Oil* (2004) els mercats energètics com una gran borsa on els preus arbitraven entre l'oferta i la demanda, l'ETS és potser el mercat més ambiciós mai construït damunt d'una abstracció: el dret a no emetre. Com hem vist, cobreix aproximadament el 40 % de les emissions de gasos d'efecte hivernacle de la UE i ha recaptat més de 175.000 milions d'euros des del 2013. El sistema —electricitat, calor, indústria pesada, aviació i, des del gener de 2024, el transport marítim— ha contribuït a reduir les emissions dels sectors coberts al voltant d'un 47 % respecte al 2005. El sostre revisat apunta a una reducció del 62 % el 2030 en comparació amb aquell any [1].

El preu de la tona, que durant anys va ser massa baix per moure res, avui ja mossega; a mitjan 2026 cotitzava al voltant dels **80 euros**, després d'haver arribat a gairebé **106 euros el febrer de 2023** [2]. Per tal que aquest senyal no s'esfondri quan sobren drets, la UE manté una **Reserva d'Estabilitat del Mercat** que retira l'excedent de circulació [5]; i per evitar la fuga de carboni cap a països sense preu del carboni, el 2026 ha entrat en escena la peça més nova i discutida: el **Mecanisme d'Ajust en Frontera per Carboni** (CBAM).

El CBAM va estrenar la seva **fase definitiva l'1 de gener de 2026** [3] i fa pagar a les importacions de productes intensius en carboni —ferro i acer, alumini, ciment, fertilitzants, electricitat i hidrogen— el mateix preu de CO_2 que ja paga la indústria europea. El primer preu trimestral del certificat CBAM, publicat el 7 d'abril de 2026, es va fixar en **75,36 euros per tona**, calculat a partir de la mitjana de les subhastes d'EUA del primer trimestre [4]. Les vendes i lliuraments de certificats no comencen fins al febrer de 2027 i la primera declaració venç el 30 de setembre d'aquell any; un llindar mínim de 50 tones a

l'any allibera el 90 % dels importadors petits, però manté cobert el 99 % de les emissions incorporades [4]. Paral·lelament, l'assignació gratuïta de drets a la indústria s'anirà retirant a mesura que el CBAM agafi força, i a l'aviació ja desapareix el 2026 [5].

L'**ETS2**, el nou mercat pensat per posar preu al carboni dels edificis i del transport per carretera, s'ha **ajornat fins al 2028**: l'acord polític es va segellar el novembre de 2025, en el marc de l'objectiu climàtic europeu per al 2040, i la formalització va arribar a principis de 2026 [6]. Més enllà d'Europa, l'aviació internacional té el seu propi esquema, el **CORSIA** de l'Organització d'Aviació Civil Internacional: només el 2024, els vols internacionals van emetre prop de **597 milions de tones** de CO_2 i el sector va quedar obligat a compensar-ne unes **58 milions** [7]. Tres mercats, tres dissenys diferents; un mateix taló d'Aquil·les.

El crim que va segrestar el clima

Perquè un mercat com aquest existeixi, una tona de CO_2 ha de poder canviar de mans tan ràpidament com una acció en borsa. Aquí rau la vulnerabilitat: un dret d'emissió és un actiu purament digital, sense pes ni textura, que es transfereix en segons entre comptes de tot Europa. Aquesta liquiditat, virtuosa per al mercat, va resultar ser una temptació irresistible per al crim organitzat.

Entre el 2008 i el 2010, una onada de **fraude carrusel de l'IVA** —el que els investigadors anomenen *missing trader fraud*— va infectar el mercat. L'esquema era tan vell com el comerç mateix: un defraudador compra drets en un país sense IVA, els ven en un altre cobrant l'impost i desapareix sense ingressar-lo a Hisenda, repetint l'operació en cercle. L'agència policial europea **Europol** va calcular que aquest frau va causar **més de 5.000 milions d'euros** de pèrdues als contribuents europeus i, com hem vist, en alguns països el frau podia arribar a gairebé tot el volum del mercat [9]. L'epicentre va ser la borsa francesa BlueNext, que oferia reemborsament immediat de l'IVA i va veure com l'activitat s'hi disparava a final del 2008. A Alemanya, la fiscalia va xifrar el forat en uns **850 milions d'euros** i, al desembre de 2011, un tribunal va condemnar sis persones a penes d'entre tres i set anys i deu mesos de presó [11].

Qui millor ha reconstruït aquell episodi és **Marius-Christian Frunza**, doctor en matemàtiques per la Sorbona i antic responsable d'estructuració al braç de matèries primeres de la Caisse des Dépôts francesa, avui investigador del frau financer. En el seu llibre *Fraud and Carbon Markets: The Carbon Connection* (Routledge, 2013) i en l'article acadèmic *An Assessment of Carousel VAT Fraud in the European Carbon Market* (2014), Frunza demostra amb estadística forense que la **velocitat de transferència d'un actiu intangible i sense traçabilitat** el va convertir en el vehicle perfecte per al carrusel [10]. La lliçó és incòmoda: un mercat construït sobre simples apunts comptables, sense una capa que segelli l'evidència, és vulnerable des de l'origen. El robatori de 2011 amb què s'obria aquest capítol no va ser una anomalia; va ser el segon acte d'una mateixa obra.

El regulador i la cadena de la veritat

Davant d'aquests forats, la resposta reguladora ha estat construir una arquitectura de control cada cop més exigent. Tota la credibilitat de l'ETS descansa en un acrònim: **MRV**, de *Monitoring, Reporting and Verification* —seguiment, notificació i verificació. Dos reglaments el sustenten, el de Seguiment i Notificació (MRR) i el d'Acreditació i Verificació (AVR), que obliguen cada instal·lació a mesurar les seves emissions, a redactar-ne un informe i a fer-lo validar per un **verificador acreditat** independent abans del 31 de març de cada any [8].

Vista de prop, tota aquesta maquinària és, en el fons, una llarga **cadena d'afirmacions de dades**. Quantes tones va emetre aquella central? Quant CO_2 porta incorporat l'acer que travessa la frontera amb un certificat CBAM? Quant carboni va cremar aquell vol? Cada baula de la cadena és un document —una lectura de sensor, un full de càlcul, un informe en PDF, un certificat— que viatja de mà en mà fins a arribar al regulador. I cada document és, alhora, un punt on la veritat es pot trencar: per error, per negligència o, com hem vist, per dol.

El problema és que les eines tradicionals per protegir aquesta cadena —metadades, segells corporatius, l'auditoria anual, la fe en el registre central— són exactament les que la digitalització ha afeblit. Un PDF es pot editar; un full de càlcul, retocar; un registre central es pot piratejar i, llavors, s'ha d'apagar sencer. La integritat del mercat del carboni s'enfronta al mateix dilema que recorre tot aquest llibre: en un món on les proves es poden fabricar, **demostrar que una dada va existir, intacta, en una data certa** ja no és un tràmit, sinó la base de tot.

Proves que es poden editar

Imaginem una instal·lació industrial que prepara el seu informe anual d'emissions. El tècnic descarrega les lectures dels sensors, les bolca en un full de càlcul, hi aplica els factors de conversió i genera un PDF que el verificador signarà. Entre la lectura del sensor i la signatura del verificador hi ha una dotzena de passos en què el número es pot «ajustar»: un decimal aquí, una hora de funcionament que s'oblida allà. No cal imaginar una conspiració; n'hi ha prou amb la pressió de tancar l'exercici amb menys tones de les reals, perquè cada tona estalviada és un dret que es pot vendre.

El verificador fa la seva feina amb rigor, però treballa amb el que li donen: documents que ja han passat per mans interessades i que res no impedeix retocar a posteriori. Si demà sorgeix una disputa —una inspecció, un litigi, una sospita de doble comptabilització entre dos registres nacionals—, com es demostra quina era la lectura **original** del sensor, abans de cap ajust? La resposta honesta, avui, sovint és que no es pot. La cadena de custòdia de la dada climàtica és tan feble com la de qualsevol fitxer digital. I un mercat que mou milers de milions sobre dades que no es poden auditar fins a l'origen és un mercat que convida al frau.

La prova d'existència com a capa de confiança del carboni

Aquí és on la **prova d'existència** —la tecnologia que vertebra *time2act* a través de **t2p**— entra en escena, no com a bala de plata, sinó com una baula que faltava. La idea és atacar el problema allà on neix: en lloc de confiar que ningú no tocarà la dada després, se segella la dada en el moment exacte en què es genera.

El mecanisme és el mateix que ja coneixem d'altres capítols, aplicat ara al carboni. L'informe MRV verificat, la lectura bruta d'un sensor d'emissions, el càlcul de les emissions incorporades d'un producte CBAM o el certificat d'una unitat CORSIA reben, en origen, una **empremta criptogràfica SHA-512** calculada al mateix dispositiu. Aquesta empremta s'ancora a la cadena pública; complementàriament, un **segell de temps RFC 3161** conforme a la normativa europea eIDAS, independent de la cadena, hi afegeix la certificació d'una autoritat; a partir d'aquell instant qualsevol alteració posterior del PDF, del full de càlcul o del registre del sensor es detecta immediatament. Per a les auditories de camp —la inspecció d'una instal·lació o la comprovació d'un projecte de compensació—, el **GPS forense** i la **prova de vida** afegeixen una capa més: segellen *on* i *quan* es va prendre la mostra o la fotografia i lliguen l'evidència a una persona real present, fent molt més difícil el clàssic «informe d'escriptori» fabricat des d'un despatx.

I encara hi ha un detall decisiu, que connecta directament amb el gener de 2011 —com hem vist—. L'evidència es pot empaquetar en un **contenidor .asice**, un format verificable *fora de línia*: un regulador o un comprador d'acer subjecte al CBAM pot comprovar la integritat de tota la cadena **sense dependre del registre central**. És a dir, sense el punt únic de fallada que aquell dia s'havia hagut d'apagar. La confiança deixa de viure en una sola base de dades vulnerable i passa a ser comprovable per qualsevol.

No és una idea marginal. El **Banc Mundial**, a través del seu programa Climate Warehouse i de la plataforma **Climate Action Data Trust** —desenvolupada amb el govern de Singapur i l'associació internacional del comerç d'emissions—, ja construeix exactament això: una capa de dades comuna i a prova de manipulació, recolzada en tecnologia de registre distribuït, que harmonitza la informació entre registres nacionals per impedir el **doble comptatge** d'un mateix crèdit [12]. La tesi del Banc Mundial és nítida: la integritat dels mercats de carboni de l'era post-París depèn d'una infraestructura de dades compartida que la simple comptabilitat en fulls de càlcul mai no podrà oferir [12].

Convé, però, ser honest amb els límits, fidels a la dualitat de **«la promesa i el perill»** que Don Tapscott, coautor de *Blockchain Revolution* (2016), fa servir per pensar la tecnologia. La prova d'existència garanteix que una dada no s'ha tocat *després* de segellar-la i, combinada amb un registre distribuït, ajuda a impedir el doble comptatge. Però **no** valida que el sensor estigués ben calibrat ni que la mesura inicial fos certa: «escombraries a l'entrada, escombraries a la cadena». Tampoc hauria aturat el frau carrusel de l'IVA, que era un problema fiscal, no d'integritat de la dada. El segell no substitueix l'auditoria ni el seny; només fa que, quan calgui, la veritat de l'origen es pugui demostrar.

La promesa i el perill

La promesa és tangible. Un mercat del carboni amb evidència segellada a l'origen seria molt més resistent al frau, faria les auditories més ràpides i barates, i permetria que un comprador, un inversor o un ciutadà comprovés per ell mateix que una tona compensada va existir de debò. En un sistema que ja mou més de 175.000 milions d'euros, com hem vist, recuperar aquesta confiança no és un luxe: és la condició perquè el preu del carboni faci la feina per a la qual va ser inventat.

El perill, com sempre, demana matís. Una capa tècnica mal dissenyada pot generar una falsa sensació de seguretat —el segell certifica el *quan* i el *què*, no la veritat física de la mesura—. La concentració de la verificació en poques mans, o en una sola plataforma, recrearia el mateix punt únic de fallada que volem evitar. I la traçabilitat total, mal governada, pot xocar amb la confidencialitat comercial legítima de les empreses. La prova d'existència és una capa **necessària** dins d'una arquitectura de confiança més àmplia, no una drecera que ens estalviï la governança.

És hora d'actuar

Per als operadors d'instal·lacions subjectes a l'ETS: segellar les lectures dels sensors i els informes MRV en origen, abans de cap tractament, perquè la dada original sigui sempre demostrable. Per als importadors subjectes al CBAM: ancorar el càlcul de les emissions incorporades dels seus productes, de manera que la xifra declarada a la frontera sigui auditable fins a la fàbrica. Per als verificadors acreditats: exigir proves d'existència com a part de la cadena de custòdia i no acceptar documents que s'hagin pogut editar després de generar-se. Per als gestors dels registres i els reguladors: avançar cap a una capa de dades distribuïda i interoperable —en la línia del Climate Action Data Trust— que faci impossible apagar tot el mercat amb un sol clic, i reconèixer legalment el valor probatori del segell.

Com vam veure el 19/01/2011, Europa va haver d'apagar el seu mercat de carboni perquè la veritat es trobava en llocs que es podien buidar de matinada. Quinze anys després disposem de les eines per evitar-ho; el preu del carboni només funcionarà si podem confiar en cada tona que hi entra, i demostrar aquesta confiança és time2act.

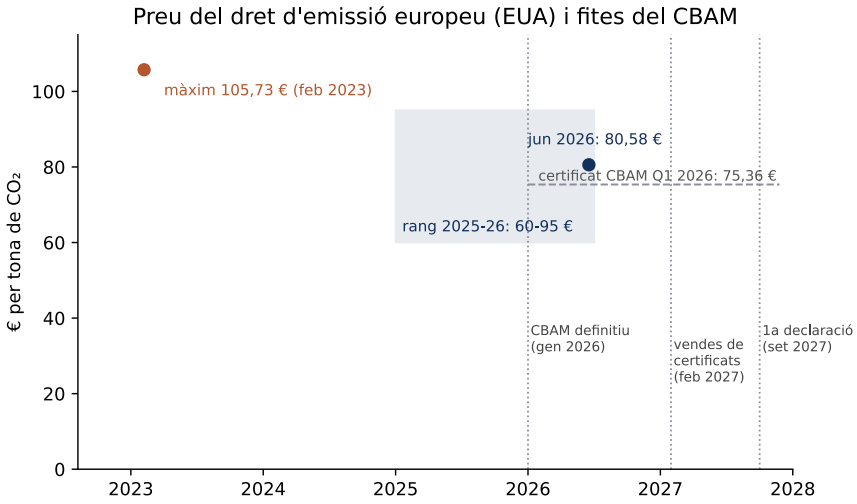


Figura 21.1 — El preu del dret d'emissió europeu (EUA) va escalar fins a un màxim de 105,73 € el febrer de 2023 i es movia al voltant dels 80 € a mitjan 2026; en paral·lel, el CBAM va entrar en fase definitiva l'1 de gener de 2026, amb un primer certificat fixat en 75,36 €/t. Fonts: Trading Economics; Comissió Europea; S&P Global.

[1] Comissió Europea — *About the EU Emissions Trading System* (cobertura ~40 %, 175.000 M€ recaptats, −47 % vs 2005, −62 % el 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; màxim històric 105,73 € el feb-2023). https://tradingeconomics.com/commodity/carbon ↩

[3] Comissió Europea (Taxation and Customs Union) — *Carbon Border Adjustment Mechanism (CBAM)* (fase definitiva des de l'1-gen-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, assignació gratuïta). https://icapcarbonaction.com/en/ets/eu-emissions-trading-system-eu-ets ↩

[6] Comissió Europea — *ETS2: buildings, road transport and additional sectors* (inici ajornat al 2028; acord nov-2025). https://climate.ec.europa.eu/eu-action/carbon-markets/ets2-buildings-road-transport-and-additional-sectors_en ↩

[7] EASA — *ICAO CORSIA* (emissions internacionals 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] Comissió Europea — *Monitoring, reporting and verification of EU ETS emissions* (MRR i AVR; informe verificat abans del 31 de març). 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* (fins al 90 % del volum fraudulent en alguns països). 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) i *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] Comissió Europea — *Announcement: transitional measure for the EU ETS registry system* (19-gen-2011) i OCCRP — *Germany: Six Executives Stand Trial for Emissions Fraud* (~850 M€; sis condemnats). 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] Banc Mundial — *Why data infrastructure is key for a transparent carbon market* i plataforma *Climate Action Data Trust*. https://blogs.worldbank.org/en/climatechange/why-data-infrastructure-key-transparent-carbon-market · https://climateactiondata.org/ ↩

El mercat voluntari del carboni: promesa, frau i la cursa per la integritat

«Si, com la veritat, la mentida només tingués un rostre, ens n'aniria millor… Però el revers de la veritat té cent mil figures i un camp indefinit.»

— Michel de Montaigne, Assaigs, I, 9 («Dels mentiders», 1580)

El 18 de gener de 2023, tres redaccions —*The Guardian* a Londres, *Die Zeit* a Hamburg i el col·lectiu d'investigació *SourceMaterial*— van publicar alhora el resultat de nou mesos de feina. Havien creuat estudis satel·litals amb treball de camp i amb la ciència acadèmica per respondre una pregunta aparentment tècnica: els crèdits de carboni que les grans marques compren per declarar-se «neutres», funcionen de debò? La conclusió va sacsejar tot un sector. Més del **90 % dels crèdits de selva tropical** certificats per Verra —el major estàndard del món— eren probablement **«crèdits fantasma»**: no representaven cap reducció real d'emissions [1].

El detall que feia mal era la llista de compradors. Empreses com Disney, Shell, Gucci o easyJet havien comunicat productes i vols «carbon neutral» recolzant-se en aquells crèdits. Segons l'anàlisi, l'amenaça de desforestació que els projectes deien evitar estava sobreestimada de mitjana al voltant d'un **400 %**, i només una petita fracció dels crèdits examinats corresponia a reduccions reals [1]. Verra va rebatre la investigació amb duresa, titllant-la de «manifestament poc fiable» i acusant els estudis d'usar «controls sintètics» que comparaven pomes amb taronges [2]. Però el dany ja estava fet: quatre mesos després, el 22 de maig de 2023, David Antonioli, conseller delegat fundador de Verra, anunciava la seva sortida després de gairebé quinze anys al capdavant [3].

Aquell terratrèmol resumeix la paradoxa del mercat voluntari del carboni. És, sobre el paper, una de les idees més boniques de la lluita climàtica: permetre que qui no pot reduir les seves emissions pagui perquè algú altre les redueixi o les absorbeixi —plantant boscs, conservant selves, capturant metà. Però quan la prova que això ha passat de debò es redueix a uns informes que es poden inflar, el somni es transforma en una fàbrica de coartades. Aquest capítol tracta de com recuperar la confiança en un mercat que la necessita desesperadament.

Com funciona —i com es trenca— el mercat voluntari

A diferència del mercat del compliment del capítol anterior, aquí ningú no obliga a res: les empreses compren crèdits **voluntàriament**, per complir promeses de «zero net» o per millorar la seva imatge. Un crèdit equival, nominalment, a una tona de CO_2 evitada o eliminada. Cinc programes de certificació —ACR, ART, Climate Action Reserve, Gold Standard i, sobretot, **Verra**— concentren prop del **98 %** del mercat [8]. Verra, en solitari, n'ha arribat a controlar al voltant de dos terços.

És un mercat petit i volàtil. Després de tocar sostre cap als **2.000 milions de dòlars el 2021**, es va contreure dos anys seguits fins als **723 milions el 2023**, amb una caiguda del **56 % en el volum de transaccions** respecte al 2022 i un preu mitjà de tot just **6,53 dòlars per tona** [8]. Aquesta fragilitat de preus té una causa de fons: ningú no sap del cert què val un crèdit perquè ningú no pot verificar fàcilment què hi ha al darrere.

I al darrere hi ha d'haver quatre coses, totes difícils de demostrar. **Addicionalitat**: que la reducció no hagués passat igualment sense els diners del crèdit. **Línia base**: quanta desforestació o emissió s'ha evitat *de debò* respecte a un escenari hipotètic. **Permanència**: que el bosc segueixi dret d'aquí a deu o trenta anys, i no cremat o talat. I **no doble comptatge**: que la mateixa tona no es vengui dues vegades ni la comptin alhora el comprador i el país on es genera. Cadascuna d'aquestes propietats es «certifica», avui, amb documents, fotografies i informes que es poden manipular. És exactament aquí on s'ha colat el frau.

L'escàndol dels crèdits fantasma

La investigació de 2023 no va sortir del no-res; confirmava una sospita que la ciència ja apuntava. **Patrick Greenfield**, periodista ambiental de *The Guardian* i un dels autors del treball, va resumir-ne la tesi: la majoria dels crèdits de selva tropical de Verra usats per les grans marques no representaven reduccions reals, i el risc de tala que deien evitar estava sistemàticament inflat [1]. No era una opinió aïllada. Un estudi revisat per parells dirigit per **Alejandro Guizar-Coutiño**, investigador de la

Universitat de Cambridge, havia avaluat el 2022 quaranta projectes REDD+ en nou països i havia trobat que sí reduïen la desforestació, però només un **47 %** de mitjana: reduccions reals, sí, però molt per sota del que prometien els crèdits venuts [6]. Un altre estudi, publicat a *Science* el 2023 sobre vint-i-sis emplaçaments en sis països —amb anàlisi detallada de la línia base en divuit—, anava encara més enllà i sostenia que la majoria de projectes no havien reduït significativament la desforestació, tot i que aquest treball va rebre una rèplica formal i encara es discuteix la tria dels seus escenaris contrafactuals [7].

El cas que millor il·lustra el problema és **Kariba**, al nord de Zimbàbue: un dels majors projectes REDD+ del món, de prop de 785.000 hectàrees, que havia venut crèdits a gegants com Volkswagen, Gucci, Nestlé o McKinsey. Quan Verra el va investigar a fons —arran, en part, d'un reportatge de *The New Yorker*—, la pròpia auditoria del certificador va concloure que s'havien emès **15.220.520 crèdits en excés d'un total de 26.822.953**, és a dir, un **57 % de sobreemissió** [4]. El desenvolupador del projecte, l'empresa suïssa South Pole, va trencar el contracte amb el soci local el 27 d'octubre de 2023 [5]. Milions de crèdits «escombraria» ja circulaven pel mercat, convertits en certificats de neutralitat que mai no van existir físicament.

El mecanisme del frau, en el fons, és sempre el mateix: no cal falsificar el bosc, n'hi ha prou amb inflar la *història* sobre el bosc. Un escenari base exagerat, una fotografia reaprofitada, una mesura presa des d'un despatx, un informe datat després d'un incendi. Tot plegat, paper i píxels que ningú no pot contrastar fins a l'origen.

La cursa per la integritat

Davant del descrèdit, el sector ha engegat una cursa per recuperar la confiança. La peça central és l'**Integrity Council for the Voluntary Carbon Market** (ICVCM), un organisme independent presidit per **Annette Nazareth**, antiga comissària de la SEC nord-americana. Al març es van publicar els **Core Carbon Principles** (CCP), una mena de segell de qualitat que un crèdit ha de complir en permanència, mesura robusta, verificació i addicionalitat. Com va explicar Nazareth, l'etiqueta CCP existeix perquè els compradors puguin distingir els crèdits que sí compleixen requisits rigorosos [9]. El juny de 2024, l'ICVCM va aprovar les primeres set metodologies amb segell CCP, habilitant uns 27 milions de crèdits d'alta integritat [9]. En paral·lel, la iniciativa **VCMI** va llançar un codi de bones pràctiques per al costat de la demanda —què pot dir i què no una empresa que compra crèdits [10].

A escala d'estats, l'**article 6 de l'Acord de París** intenta posar ordre al comerç internacional. A la cimera COP29 de Bakú, el novembre de 2024, es van adoptar els estàndards que fan operatiu el mecanisme de les Nacions Unides [13]. La clau és l'**ajust correspondent**: cada crèdit autoritzat per a ús internacional obliga el país venedor a restar aquella reducció del seu propi inventari, de manera que la tona es comptabilitza una sola vegada. És, en llenguatge climàtic, la solució contra el doble comptatge —el mateix problema que, en el món digital, resol ancorar una empremta única en un registre que ningú no pot reescriure.

La temptació de la blockchain mal feta

Aquí convé una advertència que aquest llibre no pot estalviar-se. Quan algú diu «blockchain», sovint imagina una vareta màgica que ho fa tot transparent; la història del carboni tokenitzat demostra el contrari: **la tecnologia mal aplicada va empitjorar el problema**.

Com hem vist, l'octubre del 2021 els projectes Toucan i KlimaDAO van llançar a la xarxa Polygon la *Base Carbon Tonne*, un token que prometia equivaler a una tona de CO_2. En pocs mesos, més de 21,6 milions de crèdits van migrar a la cadena. El centre d'anàlisi **CarbonPlan** va destapar el problema: els seus investigadors **Danny Cullenward i Grayson Badgley**, en l'estudi *Zombies on the blockchain* (abril del 2022), van demostrar que gairebé un 28 % d'aquells crèdits provenien de projectes «zombi» —crèdits vells i de baixa qualitat que els compradors curosos ja havien descartat, i que la tokenització havia ressuscitat [11]. La blockchain s'havia convertit, deien, en un abocador on els pitjors crèdits trobaven una segona vida. El token estrella va arribar a valer gairebé 3.900 dòlars i va acabar enfonsat a uns 20. El maig del 2022, la mateixa Verra va prohibir tokenitzar crèdits ja retirats [12].

La lliçó és exactament la dualitat de **«la promesa i el perill»** amb què Don Tapscott, coautor de *Blockchain Revolution* (2016), insisteix a pensar tota tecnologia. Posar una cosa «a la cadena» no la fa veritable; només la fa *immutable*. Si el que ancores és escombraria, tindràs escombraria immutable. La pregunta correcta no és *si* fem servir la blockchain, sinó **què hi ancorem i en quin moment**.

La prova d'existència ben feta: segellar l'evidència, no inventar-la

És en aquesta pregunta on la **prova d'existència** de **t2p** marca la diferència respecte als experiments fallits. La idea no és tokenitzar el crèdit final —el producte ja contaminat per una metodologia dubtosa—, sinó **segellar l'evidència primària** en el mateix instant i lloc en què es genera, abans que ningú la pugui retocar.

A la pràctica: cada fotografia d'una repoblació, cada mesura d'una parcel·la d'inventari, cada lectura d'un sensor de camp rep en origen una **empremta SHA-512** calculada al dispositiu, ancorada a la **blockchain pública** amb un **segell de temps RFC 3161** i acompanyada de **GPS forense** i **prova de vida** del tècnic. Així queda demostrat que *aquesta* fotografia es va prendre *en aquella coordenada*, *en aquella data*, per *una persona real present*: no recuperada de Google Earth, ni generada per IA, ni datada amb trampa després d'un incendi. Tot el paquet d'evidència d'un monitoratge —fotos, mesures, coordenades, signatura— es pot tancar en un **contenidor .asice verificable fora de línia**, que un auditor, una agència de qualificació com Sylvera o BeZero, o el mateix registre poden comprovar **sense dependre de qui ven el projecte**, fins i tot anys després. Aquestes empremtes es poden encadenar amb sistemes de **MRV digital** oberts, com Open Forest Protocol, i amb la traçabilitat que exigeix l'ajust correspondent de l'article 6 [14].

Cal ser, però, escrupolosament honest amb el límit, i és un límit important. La prova d'existència **no resol l'addicionalitat ni corregeix una línia base inflada** —que és el cor de l'escàndol Verra i Kariba. Si la metodologia és dolenta, el segell només certificarà, amb gran fidelitat criptogràfica, que algú va mesurar alguna cosa en un lloc i un moment. «Escombraries a l'entrada, escombraries a la cadena.» El que aporta t2p no és validar la suposició contrafactual, sinó **elevar la confiança en l'evidència de camp**: fa impossible la foto reaprofitada, la mesura de despatx i l'informe postdatat. La integritat climàtica segueix depenent de la bona ciència de la línia base i de l'auditoria independent. La tecnologia és condició necessària, no suficient.

La promesa i el perill

La promesa és poderosa. Un mercat voluntari on cada peça d'evidència estigui segellada a l'origen seria molt més difícil d'enganyar, permetria a un comprador comprovar pel seu compte que el bosc que finança existeix i es manté, i tornaria a fer creïbles uns crèdits que avui es venen amb descompte per culpa de la desconfiança. En un sector que ha perdut més de la meitat del seu volum en un sol any, recuperar la credibilitat és, literalment, una qüestió de supervivència.

El perill té tres cares. La primera, la temptació de creure que la tecnologia substitueix la ciència: cap segell no compensa una metodologia dolenta. La segona, l'efecte placebo invers — que una empresa compri crèdits «verificats criptogràficament» per no fer la feina dura de reduir les seves pròpies emissions; el segell certifica l'evidència, però no l'exime de descarbonitzar. I la tercera, la concentració: si la verificació i la qualificació queden en molt poques mans, recreem el punt únic de confiança que volíem dissoldre. La prova d'existència és una eina al servei de la integritat, no un substitut de la integritat.

És hora d'actuar

Per als desenvolupadors de projectes: segellar l'evidència de camp en origen —fotos, mesures, coordenades— perquè la qualitat del projecte sigui demostrable i no s'hagi de creure sobre la paraula. Per a les empreses compradores: exigir crèdits amb evidència ancorada i etiqueta d'integritat (CCP), sense adreçar-los per ajornar la reducció de les emissions pròpies. Per als registres i estàndards (Verra, Gold Standard, ICVCM): integrar la prova d'existència i el MRV digital en les seves metodologies, tancant la porta a la tokenització de crèdits zombi. Per a les agències de qualificació: usar l'evidència verificable fora de línia com a base de les seves notes. Per als reguladors: fer operatiu l'ajust corresponent de l'article 6 amb infraestructura de dades a prova de manipulació.

El mercat voluntari, nascut d'una idea generosa, s'ha estavellat contra la seva pròpia opacitat; té els anys comptats si no demostra el que promet. Com hem vist, la diferència entre un crèdit fantasma i un crèdit real no és el discurs, sinó la prova, i generar aquesta prova abans que ningú la pugui inflar és **time2act**.

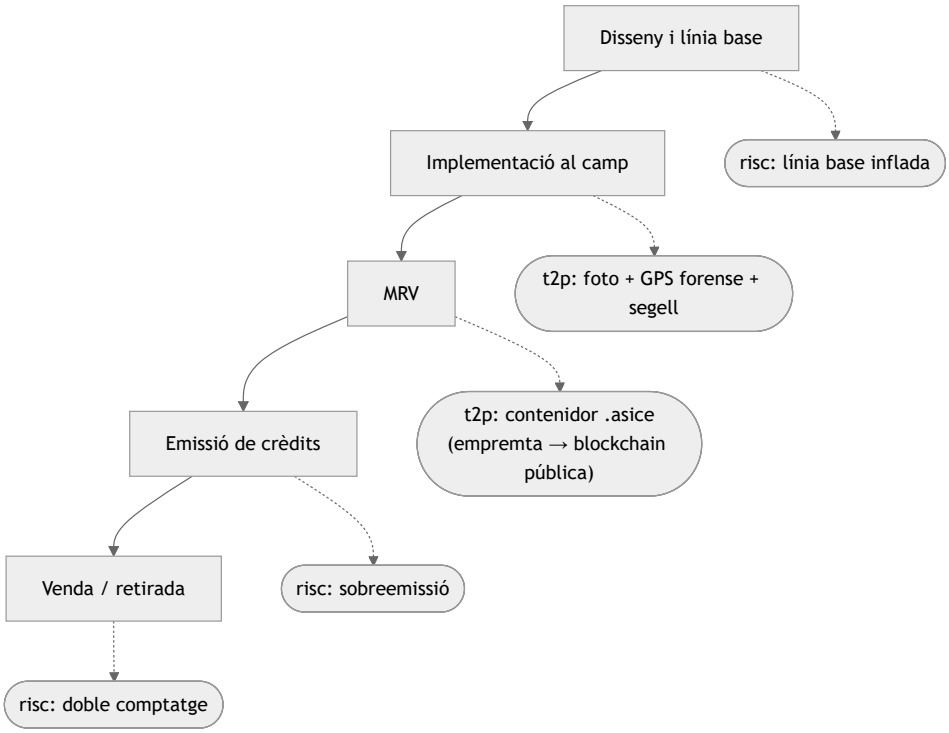


Figura 22.1 — Al llarg de la vida d'un crèdit —disseny i línia base, implementació al camp, MRV, emissió, venda i tokenització opcional— el frau s'infiltra sobretot en la línia base inflada i en l'evidència de camp manipulable. La prova d'existència ancora les baules d'evidència (foto, mesura, informe) però no corregeix una metodologia defectuosa. Fonts: 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-gen-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* (rèplica). https://verra.org/verra-response-guardian-rainforest-carbon-offsets/ ↩

[3] Mongabay — *Head of Verra, top carbon credit certifier, to leave in June* (dimissió de David Antonioli, 22-maig-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 crèdits en excés 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; desforestació −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 emplaçaments en 6 països; resultat disputat, rèplica arXiv 2312.06793). https://www.science.org/doi/10.1126/science.ade3535 ↩

[8] Ecosystem Marketplace / Forest Trends — *State of the Voluntary Carbon Market 2024* (mercat ~2.000 M$ el 2021 → 723 M$ el 2023; volum −56 %; preu mitjà 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* i *First high-integrity CCP-labelled carbon credits* (juny 2024; ~27 M de crèdits). 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-juny-2023). https://vcmintegrity.org/launch-claims-code/ ↩

[11] CarbonPlan — Danny Cullenward i Grayson Badgley, *Zombies on the blockchain* (7-abr-2022; ~28 % de crèdits zombi). https://carbonplan.org/research/toucan-crypto-offsets ↩

[12] Verra — *Verra Addresses Crypto Instruments and Tokens* (prohibició de tokenitzar crèdits retirats, 25-maig-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 obert). https://forestsnews.cifor.org/76905/blockchain-platform-offers-reforestation-efforts-access-to-carbon-finance ↩

CAE: certificar l'estalvi sense fer trampa

«Si no és correcte, no ho facis; si no és veritat, no ho diguis.»

— Marc Aureli, Meditacions, XII, 17

A Pordenone, al nord-est d'Itàlia, hi havia una empresa de serveis energètics que sobre el paper era un model d'eficiència. Des de 2013 havia presentat al gestor públic italià, el GSE, gairebé tres-cents projectes d'estalvi d'energia: calderes substituïdes, aïllaments instal·lats, equips renovats a casa de centenars de clients. El GSE els va validar i l'empresa va cobrar **50.322 certificats blancs**, els títols que premien cada quilowatt-hora estalviat, amb un benefici de més de deu milions d'euros.

Hi havia un sol problema. L'empresa no tenia oficines, ni logística, ni empleats. I les obres no existien. Els «clients» eren noms trets de llistes d'una distribuïdora de material termohidràulic i d'una de plaques solars, persones que mai no havien encarregat res. La Guàrdia di Finanza ho va destapar i el Tribunal de Comptes regional va xifrar el dany a l'erari públic en uns **10,4 milions d'euros** [10]. Era el frau perfecte en la seva senzillesa: certificats d'un estalvi mesurat amb precisió mil·limètrica... sobre instal·lacions que només existien en un PDF.

El cas de Pordenone condensa la fragilitat d'un dels instruments més intel·ligents de la política energètica europea: els **certificats d'estalvi**. La idea és brillant —pagar per l'energia que *no* es consumeix, perquè el quilowatt-hora més net és el que no cal generar. Però tot l'edifici descansa sobre una prova humil: que l'actuació d'estalvi es va fer de debò, allà on es diu i quan es diu. I aquesta prova, fins ara, era un grapat de papers i fotografies que qualsevol podia inventar.

Pagar per l'energia que no es gasta

Tot arrenca d'una obligació europea. La **Directiva d'Eficiència Energètica** (la 2023/1791, en el seu article 8) obliga cada estat a aconseguir nous estalvis d'energia final any rere any: un 0,8 % anual entre 2021 i 2023, un 1,3 % el 2024-2025, un 1,5 % el 2026-2027 i fins a un **1,9 % anual el 2028-2030**. La Comissió mateixa reconeix que la directiva refosa «més que duplica» l'obligació d'estalvi cap al 2028 [1]. Per a Espanya, l'objectiu acumulat d'estalvi d'energia final de la dècada arriba als **53.593 ktep** [5]. És una muntanya d'estalvi que algú ha de generar i, sobretot, demostrar.

L'instrument que ho fa possible són els **certificats blancs**, coneguts amb noms diferents a cada país. A Espanya són els **CAE**, els Certificats d'Estalvi Energètic, creats pel **Reial decret 36/2023** del 24 de gener. La regla d'or és tan neta com un quilòmetre marcat: **un CAE equival a un quilowatt-hora d'energia final estalviat i acreditat** [2]. El sistema reparteix l'esforç entre uns actors ben definits: els **subjectes obligats** —les comercialitzadores de gas i electricitat i els operadors de productes petrolífers— han de generar uns estalvis proporcionals a les seves vendes; poden fer-ho directament, a través d'un **subjecte delegat**, o aportar diners al Fons Nacional d'Eficiència Energètica. Cada actuació l'ha de validar un **verificador acreditat** per ENAC, i tot el sistema el coordina el Ministeri per a la Transició Ecològica a través d'un catàleg de mesures estandarditzades [2][3].

El model funciona. En el seu primer any complet, el 2024, el sistema CAE espanyol va mobilitzar més de **1.200 actuacions**, va certificar prop de **2 TWh** d'estalvi anual, va evitar unes **500.000 tones de CO_2** i va generar uns **230 milions d'euros** en venda de certificats, amb la indústria com a gran protagonista (un 68 % de l'estalvi) [4]. França fa servir el mateix principi des de 2006 amb els seus **CEE**, comptabilitzats en una unitat pròpia, el «kWh cumac» —energia estalviada al llarg de tota la vida útil de l'equip—, amb una obligació que per al període 2026-2030 arriba als **1.050 TWh cumac l'any** [6]. Itàlia té els seus certificati bianchi. Tres països, tres noms, un mateix taló d'Aquil·les.

Qui millor ha estudiat aquests esquemes és **Louis-Gaëtan Giraudet**, economista del CIRED i de l'École des Ponts i una de les autoritats europees en certificats blancs. En treballs com *Selling and Saving Energy: Energy Efficiency Obligations in Liberalized Energy Markets* (2020), Giraudet conclou que aquests sistemes solen tenir un balanç cost-benefici positiu, però que la seva integritat **depèn críticament de com es mesuren i es verifiquen els estalvis** davant la línia base [12]. És a dir: l'instrument val exactament el que valgui la seva prova.

El frau ataca la prova, no la fórmula

Aquí rau la qüestió. El defraudador d'estalvi energètic gairebé mai discuteix la fórmula del quilowatt-hora; el que falsifica és **la prova que l'actuació física existeix**. Instal·lacions fantasma, estalvis inflats respecte a la línia base, factures falses, doble comptabilització i mesures no addicionals que s'haurien fet igualment. Cada atac convergeix en el mateix punt feble: l'evidència.

França n'és el cas d'estudi més madur i dolorós. L'esquema dels CEE va donar lloc al fenomen de la «isolation à 1 euro»: empreses que captaven particulars per telèfon prometent aïllar-los la casa «per un euro», sovint dient-se mandatades per organismes oficials. El resultat eren materials dolents, obres barroeres o directament inexistents i sol·licituds de certificats inflades. L'estiu de 2018 l'autoritat francesa de consum i repressió del frau, la DGCCRF, va controlar 469 establiments del sector i va trobar que el 56 % no respectava plenament les normes [8]. El degoteig ha continuat: com hem vist, el govern francès ha bloquejat 480 milions d'euros de frau a la transició energètica, dels quals 236 milions corresponen als CEE [9]; i al febrer del 2025 les duanes judicials van desarticular una xarxa que havia desviat tretze milions mitjançant obres fictícies i transferències a paradisos fiscals.

Itàlia ha respost amb una doctrina jurídica reveladora. El seu màxim tribunal administratiu, el Consiglio di Stato, ha confirmat que l'assignació d'un certificat blanc és un «procés de formació progressiva»: encara que el GSE l'hagi validat inicialment, conserva el poder-deure de comprovar després que l'estalvi va existir de debò i, si el beneficiari no pot provar-ho amb documentació, revocar el certificat i exigir-ne la devolució [11]. En altres paraules: un certificat emès **no és un dret intocable**. La càrrega de la prova recau, per sempre, sobre qui l'ha cobrat; i si la prova és un arxiu de fotos que ningú no pot autenticar, aquella càrrega és fum.

El regulador ja demana la prova forense

El més interessant és que els reguladors ja han arribat, per la via dels fets, a la conclusió que vertebra aquest llibre: que la confiança s'ha de poder demostrar. La resposta francesa al frau ho il·lustra gairebé literalment. La **Llei 2025-594, del 30 de juny de 2025**, no només va augmentar el sostre de les sancions —del 4 % al **10 %** de la facturació, i fins al 12 % en cas de reincidència—; també va obligar que determinades operacions d'estalvi es justifiquin amb **fotografies datades i geolocalitzades** —*horodatées et géolocalisées*— o amb vídeo a distància, proves que cal **conservar sis anys** i posar a disposició dels agents de control [7].

L'Estat francès, després d'anys de certificats falsos, ha deixat de creure en la paraula de l'instal·lador i exigeix per llei una **fotografia amb data i coordenada verificables** de cada actuació. Això és, exactament, una prova d'existència. Els controls de tercers sobre el terreny han pujat del 10 % al 15 % entre el 2023 i el 2025 [9]; el regulador ha descrit el remei, però encara manca la garantia que aquella fotografia, un cop presa, no es pugui manipular ni datar amb trampa.

De requisit legal a rastre inalterable

I aquí és on la **prova d'existència** de **t2p** transforma una bona intenció reguladora en una garantia tècnica. La llei francesa demana una foto datada i geolocalitzada; el problema és que una data i unes coordenades, en un fitxer corrent, també es poden falsejar. La prova d'existència tanca aquella escletxa segellant l'evidència en el moment i el lloc exactes en què es genera.

El mecanisme, aplicat a una actuació d'estalvi —el canvi d'una caldera, un aïllament, un motor industrial eficient, un enllumenat LED—, és el següent. Es captura l'evidència completa: foto de l'*abans* i del *després*, lectura del comptador inicial i final, factura de l'instal·lador, número de sèrie de l'equip i signatura del verificador. Cada fitxer rep al dispositiu una **empremta SHA-512**, que s'ancora a la **blockchain pública** amb un **segell de temps RFC 3161** conforme a eIDAS i amb **GPS forense** que fixa la coordenada de l'obra. La foto del «després» incorpora, a més, **prova de vida** per impedir reaprofitar imatges antigues o de catàleg. Tot plegat s'empaqueta en un contenidor **.asice verificable fora de línia**.

El resultat ataca cadascun dels vectors de frau. La geolocalització i la prova de vida obliguen a ser físicament a l'adreça declarada: adéu a les instal·lacions fantasma de Pordenone. El segell de temps i l'empremta delaten qualsevol foto reaprofitada d'una altra obra o d'un catàleg. Qualsevol retoc posterior d'una factura o d'un certificat trenca l'empremta ancorada, i la mateixa empremta no es pot acreditar dues vegades, cosa que tanca la porta al doble comptatge. El que la llei francesa ja exigeix —foto datada, geolocalitzada, conservada sis anys— t2p ho converteix en un **rastre d'auditoria inalterable**, verificable pel Coordinador espanyol, pel control francès o pel GSE italià **sense haver de confiar en**

l'arxiu del mateix obligat, i amb un cost de verificació molt més baix que els mostrejos sobre el terreny.

Convé, com sempre, ser honest amb el límit. Ancorar una prova **no certifica que l'estalvi sigui real**: si el verificador acreditat avala una mesura inflada, o si la línia base està mal calculada, la cadena només garantirà que aquell document existia en aquella data i en aquell lloc, no la seva veracitat tècnica. «Escombraries a l'entrada, escombraries a la cadena.» La prova d'existència blindarà la **integritat de l'evidència i la identitat de qui la signa**, desplaçant el frau del «document falsificable» al «pèrit que menteix conscientment», una conducta molt més difícil, més rastrejable i amb responsabilitat nominal. No substitueix el verificador ni la mesura física; els fa de fonament fiable.

La promesa i el perill

La promesa és directa i quantificable. Un sistema de certificats d'estalvi amb evidència segellada a l'origen seria molt més resistent al frau, abaratiria les verificacions, acceleraria el pagament dels certificats legítims i protegiria els milers de milions d'euros públics i privats que mouen aquests esquemes. En un instrument on cada euro mal gastat és un euro que no compra estalvi real, la integritat de la prova no és burocràcia: és eficàcia climàtica.

El perill demana matís, en la línia de la dualitat de «la promesa i el perill» que recorre tota aquesta obra. Una capa tècnica pot generar una falsa sensació de seguretat: el segell certifica el *quan* i el *on*, no la qualitat de la mesura. La geolocalització i la biometria de la prova de vida toquen dades sensibles d'instal·ladors i veïns, i exigeixen un disseny respectuós amb la privacitat. I si la verificació es concentra en poques plataformes, recreem el punt únic de confiança que volíem dissoldre. La prova d'existència és una eina al servei de la integritat dels certificats, no un substitut del verificador ni del bon disseny de la línia base.

És hora d'actuar

Per als **subjectes obligats i delegats** (comercialitzadores, empreses de serveis energètics): segellar l'evidència de cada actuació en origen, perquè la qualitat de la feina sigui demostrable i els certificats siguin inatacables. Per als **verificadors acreditats**: exigir proves d'existència com a base de la validació, i no acceptar fotografies o factures que s'hagin pogut editar posteriorment. Per als **coordinadors i organismes de control** (MITECO, PNCEE francès, GSE italià): reconèixer el valor probatori del segell, integrar-lo en els requisits del catàleg de mesures i reduir així el cost dels mostrejos. Per als **reguladors europeus**: harmonitzar el requisit de prova forense que França ja ha establert per llei, abans que cada estat reinventi la roda.

A Pordenone, una empresa sense oficines va cobrar mig centenar de milers de certificats per unes obres que no existien. La tecnologia per fer impossible aquell frau ja existeix, i un país sencer comença a exigir-la per llei. Certificar l'estalvi sense fer trampa —demostrar que cada quilowatt-hora estalviat va existir de debò— és, també aquí, **time2act**.

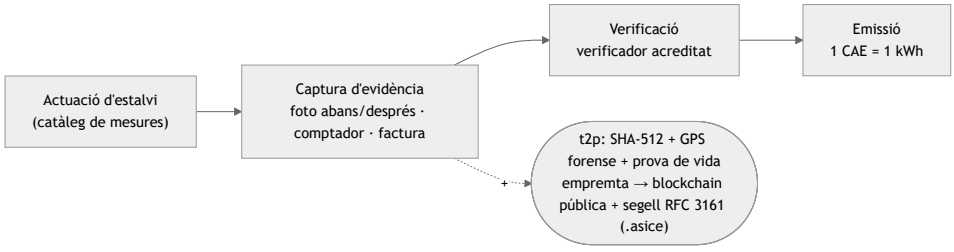


Figura 23.1 — Del catàleg de mesures a l'emissió del certificat: l'actuació es captura com a evidència (foto abans/després, comptador, factura), es verifica i es converteix en CAE (1 CAE = 1 kWh). La prova d'existència s'insereix en el moment de capturar l'evidència —SHA-512, GPS forense, segell RFC 3161, prova de vida i contenidor .asice—, just on la llei francesa ja exigeix fotografies datades i geolocalitzades. Fonts: BOE (RD 36/2023); Légifrance (Llei 2025-594); Funcas.

[1] Comissió Europea — *Energy Efficiency Directive* (Directiva 2023/1791, art. 8; nous estalvis fins a l'1,9 % anual el 2028-2030; «more than doubles» cap al 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 d'energia final acreditat; subjectes obligats/delegats, verificador, coordinador). https://www.boe.es/buscar/doc.php?id=BOE-A-2023-2027 ↩

[3] BOE — *Orden TED/845/2023, de 18 de julio* (catàleg de mesures estandarditzades d'eficiència energètica). 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* (resultats 2024: ~1.200 actuacions, ~2 TWh, ~500.000 t CO_2, ~230 M€; indústria 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* (objectiu acumulat d'estalvi 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 n° 2025-1048 du 30 octobre 2025* (CEE, 6è període 2026-2030; 1.050 TWh cumac/any). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000052486193 ↩

[7] Légifrance — *Loi n° 2025-594 du 30 juin 2025* (sancions fins al 10-12 %; fotografies *horodatées et géolocalisées* o vídeo a distància, conservades 6 anys). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000051824277 ↩

[8] DGCCRF (economie.gouv.fr) — *Rénovation énergétique : focus sur l'isolation à 1 euro* (469 establiments controlats; 56 % d'incompliment). https://www.economie.gouv.fr/dgccrf/laction-de-la-dgccrf/les-enquetes/renovation-energetique-focus-sur-lisolation-1-euro ↩

[9] Hellio / Govern francès — *Fraude aux CEE* (480 M€ de frau bloquejat el 2024, 236 M€ en CEE; taxa de control 10 %→15 %). https://www.hellio.com/actualites/reglementation/fraude-cee ↩

[10] ANSA / PordenoneToday — *Contributi per 10 milioni su certificati bianchi inesistenti* (292 projectes ficticis; 50.322 TEE; dany ~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 i l'anul·lació de títols d'eficiència energètica* (doctrina de la «formació progressiva»; cas 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 i 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 ↩

Autoconsum i comunitats energètiques: la lectura verificable

«El sol també brilla avui.»

— Ralph Waldo Emerson, Nature (1836)

El vespre que arriba la factura, la casella diu: «compensació d'excedents — 0 €». A l'altra pantalla, l'aplicació de l'inversor mostra un mes sencer de sol comptabilitzat: una xifra que no s'assembla de res a la de la comercialitzadora. El prosumidor mira les dues finestres, l'una al costat de l'altra — dues realitats que no quadren, i cap manera de saber quina mana.

No és una anècdota de nínxol [1]: l'autoconsum fotovoltaic espanyol ha arribat als 9,3 gigawatts de potència instal·lada — la cinquena font de generació elèctrica del país per potència, per davant de la nuclear. Només el 2025 s'hi van sumar 36.330 llars, dins d'un total de 1.139 megawatts nous comptant també els sectors comercial i industrial; i l'objectiu del pla nacional d'energia i clima és arribar als 19 gigawatts [1]. Milions de famílies i pimes han posat estalvis a la teulada — i han esdevingut, sense acabar d'adonar-se'n, generadors amb comptabilitat energètica pròpia.

Aquest capítol tanca un cercle que el llibre va obrir a la Part II: vam començar amb la màquina energètica, i la retrobem ara a les teulades — perquè la transició energètica també és una transició de confiança. Els certificats d'estalvi energètic — les actuacions que es paguen — són al capítol 23; l'acta de la comunitat de veïns, al capítol 37; els sensors ciutadans ambientals, al capítol 97; els mercats de carboni, als capítols 21 i 22. Pregunta clau: qui té el comptador quan la factura no quadra amb el sol que has generat? Resposta: l'altra part — llevat que la lectura pròpia tingui data certa: les sèries de l'inversor i del comptador segellades per lots encadenats amb **t2p** — l'empremta SHA-512 calculada al dispositiu, l'ancoratge de l'empremta a la blockchain pública i el segell de temps RFC 3161/eIDAS complementari, dins d'un contenidor .asice [3]. I amb la simetria de sempre: la mateixa traça desarma la reclamació infundada contra la comercialitzadora que liquida bé.

El comptador de l'altra part

El marc és clar i, en general, ben pensat [2]: el Reial decret 244/2019 regula l'autoconsum i crea la compensació simplificada d'excedents — voluntària, per a instal·lacions renovables de fins a 100 kW: l'energia abocada a la xarxa es compensa econòmicament a la factura de cada mes (facturació neta mensual, no balanç net anual). L'autoconsum pot ser individual o col·lectiu — diversos consumidors associats a una mateixa instal·lació, amb coeficients de repartiment —, i les regles recents n'han ampliat el radi fins a 5 quilòmetres per a plantes de fins a 5 megawatts [2]. Sobre aquesta base creixen les comunitats energètiques: veïns, ajuntaments i pimes agrupats per compartir generació.

El problema no és el marc: és la prova. La liquidació dels excedents es fa sobre les lectures del comptador fiscal i els sistemes de la comercialitzadora. El prosumidor té l'inversor — que mesura la seva producció en temps real — i la seva aplicació; però quan les dues xifres divergeixen, o la compensació triga mesos a aparèixer, o un canvi de comercialitzadora perd el fil, la reclamació es fa contra dades alienes: les de l'altra part.

En el model col·lectiu, la incertesa es multiplica: els coeficients pactats entre veïns, les altes i baixes de participants, els acords d'assemblea — sovint consignats en un full de càlcul de bona voluntat. I als contractes de compra d'energia a llarg termini, els preus i volums pactats han de contrastar-se amb els liquidats, una capa documental més.

La conclusió és la d'aquest llibre: la transició energètica ha descentralitzat la generació, però no la prova. Qui genera a casa mereix una comptabilitat energètica amb data certa pròpia — no per desconfiar de ningú per sistema, sinó perquè quan els números no quadrin, la conversa sigui de fets.

La prova d'existència aplicada

Quatre gestos — la majoria, automàtics — converteixen la teulada en un generador amb comptabilitat verificable [3].

1. La lectura pròpia, per lots encadenats

Les exportacions periòdiques de l'inversor i del comptador propi — producció, autoconsum instantani, excedents — se certifiquen amb t2p per lots: cada tancament, setmanal o mensual, rep la seva empremta SHA-512, encadenada amb la de l'anterior [3]. És la mateixa lògica que l'Estat ja imposa a les factures — el capítol 34 ho explica — aplicada a la teulada pròpia. El resultat: una sèrie datada que ningú no pot reescriure — ni tan sols el prosumidor mateix, i per això val davant de tercers.

2. La factura contrastada

Cada factura, capturada amb data certa en arribar; la casella de compensació, contrastada contra la sèrie pròpia del mateix període [3]. Quan no quadren, la reclamació porta números datats: aquests excedents va comptar el meu inversor, això em vau compensar, aquesta és la diferència. I la simetria: la comercialitzadora que liquida bé té, en els seus registres i en la sèrie del client, la prova que la seva factura era correcta — la reclamació infundada mor de dates.

3. L'acta de la comunitat energètica

Els coeficients de repartiment, l'alta i la baixa de cada participant, els acords de l'assemblea — segellats amb data certa, com les actes de la comunitat de veïns del capítol 37 [3]. Quan un participant discuteixi el seu percentatge, o algú entri a mig any, la història dels acords serà una cadena de versions ancorades, no una discussió de records. Les comunitats energètiques només escalaran si la confiança entre desconeguts no depèn de la bona voluntat d'un full de càlcul.

4. El contracte congelat

El contracte de compensació, l'oferta de la comercialitzadora el dia de signar, el PPA — el contracte de compra d'energia a llarg termini — amb els seus preus i volums: capturats i segellats en el moment [3]. Quan les condicions «canviïn» o la lletra petita es reinterpreti, el document d'aquell dia existeix, exacte i datat. El mateix gest que el capítol 33 aplica a la tarifa del telèfon, aplicat al contracte més llarg que signa una família.

Els límits, dits clarament: el segell acredita sèries i documents — no liquida, no tarifa i no substitueix la metrologia legal: el comptador fiscal és el que és, i la lectura pròpia contrasta, no reemplaça. Un inversor mal calibrat segella la seva pròpia desviació — manteniment i calibratge primer. I les discrepàncies petites són normals — pèrdues, moments de mesura —: la traça serveix per a les grans i les persistents.

La promesa i el perill

La promesa: prosumidors que reclamen amb sèries pròpies datades [1][3]; comunitats energètiques que creixen perquè els acords tenen data certa; comercialitzadores diligents que resolen reclamacions en dies perquè les dues parts porten números verificables; i la cinquena font de generació del país [1] amb la comptabilitat de confiança que li pertoca.

Els perills, mirats de cara.

El primer és **la guerra de comptadors**. Si cada part branda la seva sèrie, no hem guanyat res. La resposta és metodològica: equips calibrats, metodologia declarada, i la lectura pròpia com a contrast documentat que obliga a revisar el comptador fiscal — no com a substitut.

El segon és **la sobrecàrrega del prosumidor**. La família que va posar plaques per estalviar no vol una comptabilitat criptogràfica. El segellat ha de ser automàtic — l'exportació periòdica que s'ancora sola [3] — o no serà; el gest manual és per al dia de la discrepància, no per a cada dia.

El tercer és **el perfil energètic com a intimitat**. La corba de consum d'una llar explica quan dorms, quan cuines, quan ets fora. Les sèries queden al dispositiu o als sistemes del prosumidor; a la cadena, només empremtes [3]; la revelació, selectiva i davant de qui toqui.

I el quart és **el tecnosolucionisme solar**. Cap hash no accelera un permís d'accés, no amplia una xarxa saturada ni arregla una regulació lenta. La prova d'existència fa justes les liquidacions; que l'autoconsum arribi als 19 gigawatts [1] és feina de política energètica.

És hora d'actuar

Que cada quilowatt generat a casa tingui la seva data certa.

Per als prosumidors: activeu l'exportació periòdica segellada de l'inversor [3]; el dia que la factura no quadri, tindreu la vostra sèrie — i no només la vostra paraula.

Per a les comunitats energètiques: coeficients, altes i acords amb data certa [3] — la confiança entre veïns mereix la mateixa traça que qualsevol contracte.

Per a comercialitzadores i distribuïdores: ancoreu les vostres liquidacions i publiqueu-les per empremta — la reclamació infundada mor de dates, i la vostra diligència es torna argument comercial.

Per al regulador i les autoritats de consum: reconegueu la sèrie pròpia ancorada com a contrast qualificat en les disputes de compensació [2]; el prosumidor no pot litigar a cegues contra el comptador de l'altra part.

Per als legisladors: la transició energètica descentralitzada — que ja frega els 9,3 gigawatts i aspira als 19 [1][2] — necessita la seva capa de confiança: que el desplegament de les comunitats energètiques neixi amb actes i liquidacions verificables de sèrie.

Aquest llibre va començar amb el final del petroli fàcil; retroba l'energia ara a les teulades. Que la transició energètica sigui també una transició de confiança. Pel sol de cada teulada, **time2act**.

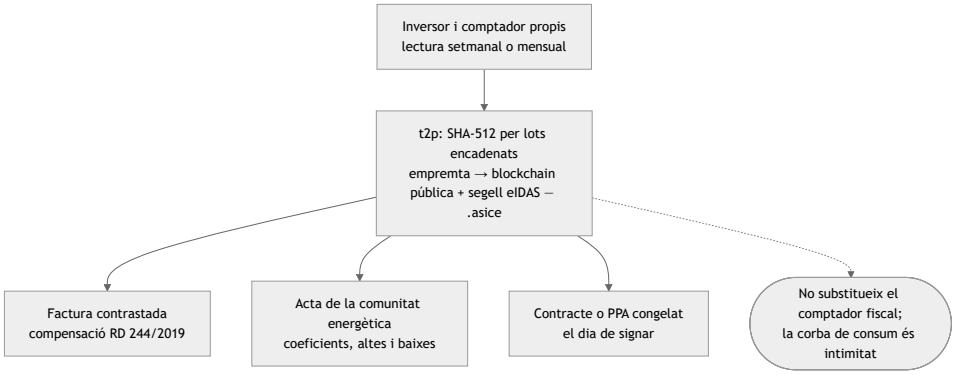


Figura 24.1 — L'autoconsum amb prova d'existència (t2p: empremta SHA-512 al dispositiu, RFC 3161/eIDAS, blockchain pública, .asice): la lectura pròpia de l'inversor i el comptador segellada per lots encadenats, la factura amb compensació contrastada, l'acta de la comunitat energètica (coeficients, altes i baixes amb data certa) i el contracte/PPA congelat el dia de signar. Context: 9,3 GW d'autoconsum a Espanya (UNEF) — cinquena font per potència; RD 244/2019 (compensació simplificada mensual ≤100 kW; col·lectiu fins a 5 km). Límits: la lectura pròpia contrasta el comptador fiscal, no el substitueix; calibratge primer; només empremtes a la cadena (la corba de consum és intimitat). Fonts: UNEF; BOE (RD 244/2019).

---

[1] UNEF — *El autoconsumo fotovoltaico en España alcanza los 9,3 GW instalados* (informe sobre 2025: +1.139 MW l'any, −3,7 % vs 2024; 36.330 llars noves +229 MW; comercial +176 MW; industrial +679 MW; cinquena font de generació per potència instal·lada, per davant de la nuclear; objectiu PNIEC 19 GW); UNEF — *El autoconsumo sigue avanzando, superando ya el umbral de los 8 GW* (2024: +1.182 MW, acumulat 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 — *Reial decret 244/2019, de 5 d'abril* (condicions administratives, tècniques i econòmiques de l'autoconsum; compensació simplificada d'excedents ≤100 kW, voluntària, a la factura mensual — facturació neta; autoconsum individual i col·lectiu; registre administratiu); MITECO — *Preguntas frecuentes sobre autoconsumo*; UNEF — *Real Decreto 244/2019*; Puentes de Muras — *RD 244/2019: novedades* (ampliació del radi de l'autoconsum col·lectiu fins a 5 km, plantes fins a 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 producte (certificar qualsevol fitxer per lots — només l'empremta viatja; captura de pantalla i de pàgina web amb imatge completa + codi font; escàner de documents fins a 50 pàgines; foto amb GPS forense; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; els CAE, al capítol 23; l'acta de la comunitat, al capítol 37; la factura, al capítol 34. ↩

Mobilitat I: flotes i empreses, evidència sòlida

«És un error capital teoritzar abans de tenir dades.»

— Arthur Conan Doyle, «Un escàndol a Bohèmia» (1891)

Una furgoneta de segona mà travessa una frontera europea. Al país d'origen, el comptaquilòmetres marcava 230.000 quilòmetres; quan arriba al concessionari de destí, en marca 150.000. En el trajecte, algú ha connectat un petit aparell al connector de diagnòstic del vehicle i, en menys d'un minut, ha esborrat **vuitanta mil quilòmetres**. El cotxe sembla més jove, val més, i el comprador pagarà de mitjana un 26 % de més per un vehicle que en realitat està molt més gastat [3]. El més inquietant és que aquesta manipulació, segons un estudi del servei d'estudis del **Parlament Europeu** redactat per Enrico Pastori i Raffaele Vergnani, *Odometer manipulation in motor vehicles in the EU* (2018), «no deixa cap rastre»: l'electrònica reescriu el número i la prova del frau s'esvaeix [1].

No és un cas aïllat. Aquell mateix estudi xifra el cost del frau de comptaquilòmetres a la Unió Europea entre **5.600 i 9.600 milions d'euros l'any**, i estima que entre el **30 % i el 50 % dels cotxes venuts a través de fronteres** tenen el quilometratge manipulat [1]. El Consell Europeu de Seguretat en el Transport ho confirma: fins a la meitat dels vehicles de segona mà transfronterers porten el comptaquilòmetres trucat [2].

Fins aquí, una vella estafa del mercat de l'automòbil. Però aturem-nos un moment, perquè la història fa un gir que canvia tot el panorama. Aquells mateixos sensors —el comptaquilòmetres, el GPS, el consum, el registre de càrrega— han deixat de ser només la fitxa tècnica d'un cotxe. Avui són la **matèria primera de nous actius econòmics**: crèdits de carboni, certificats d'estalvi energètic (CAE) i informes d'emissions corporatives. I si la dada que els alimenta es pot esborrar en un minut sense deixar rastre, tots aquests instruments hereten la mateixa fragilitat. Aquest capítol tracta de com les flotes d'empresa poden generar evidència climàtica que ningú no pugui falsejar.

La flota com a fàbrica d'estalvi —i d'evidència

Una flota d'empresa és, des del punt de vista climàtic, una mina d'estalvi. Electrificar-la, formar els conductors en conducció eficient, optimitzar rutes o canviar a pneumàtics de baixa resistència genera reduccions reals d'emissions que es poden convertir en valor. A Espanya, el catàleg del sistema CAE inclou cinc fitxes específiques de transport: la substitució de pneumàtics per altres de més eficients (TRA010), els sistemes de **telemetria i geoposicionament** en flota (TRA020), el vehicle compartit de llarg recorregut (TRA030), la mobilitat col·laborativa urbana (TRA040) i la substitució d'un vehicle de combustió per un d'elèctric pur (TRA050) [5]. Cada actuació, recordem-ho, val un quilowatt-hora estalviat i acreditat.

I el potencial és enorme, perquè la tecnologia ja funciona. L'**International Council on Clean Transportation** (ICCT), una organització independent de recerca sobre transport net, va mesurar l'agost de 2025 noranta-un camions pesants elèctrics en ús real a Europa i va trobar que consumeixen de mitjana un **65 % menys d'energia** que un dièsel equivalent, amb una autonomia real fins i tot superior a l'anunciada pels fabricants [6]. Com resumeix l'ICCT, el problema ja no és la tecnologia, sinó **mesurar i certificar l'estalvi de manera fiable**. A aquesta pressió s'hi afegeix la normativa: sota la directiva europea d'informació de sostenibilitat (CSRD), les emissions de la cadena de transport —l'anomenat Abast 3— són d'obligada divulgació quan són materials, i estan subjectes a verificació externa. I per comptar-les hi ha fins i tot un idioma comú auditat, el **GLEC Framework** del Smart Freight Centre, alineat amb la norma ISO 14083 [11].

El resultat és una paradoxa: tenim els vehicles, tenim les fitxes, tenim els marcs comptables i l'obligació legal de reportar. El que falta és la baula més humil de totes —la garantia que la **dada de partida** és certa.

Sensors que menteixen

Perquè la superfície d'atac d'una flota connectada és enorme, cada porta oberta pot inflar un estalvi o crear un crèdit fals. El comptaquilòmetres es pot recular —com hem vist— i el **GPS es pot suplantar**: en lloc de bloquejar el senyal, l'atacant n'injecta un de fals, de manera que un vehicle «apareix» per rutes eficients que mai no ha recorregut, alimentant crèdits de carboni o CAE de transport. El **bus CAN**, la xarxa interna

que connecta els sensors del vehicle, no autentica qui envia cada missatge; una injecció pel connector de diagnòstic o per la telemàtica pot fer dir al cotxe el que convingui. Les **targetes de combustible** són un clàssic del frau: el 2022 una investigació coordinada per Eurojust va desarticular una xarxa entre Romania, Bèlgica i Àustria que havia estafat 420.000 € amb targetes clonades i repostatges fantasma que viatjaven per mitja Europa [8].

No és teoria. L'empresa de ciberseguretat Upstream va comptabilitzar **494 ciberatacs** a vehicles i flotes durant el 2025, el 92 % en remot i dos de cada tres dirigits a la telemàtica i el núvol [7]. Fins i tot la recàrrega elèctrica té el seu flanc: el protocol OCPP que governa els punts de càrrega autentica cada sessió, però les versions febles permeten manipular els missatges entre el vehicle i l'estació, falsificant els quilowatts-hora facturats o acreditats.

És el cas del problema recurrent en aquest llibre: *escombraries a l'entrada, escombraries a la cadena*. Per molt sofisticat que sigui el registre on s'anoti finalment el crèdit, si la lectura entra ja falsejada queda immutablement falsa. Cap blockchain no salva un odòmetre trucat.

La lliçó de Bèlgica: segellar funciona

Per sort, ja sabem què passa quan se sella la dada en origen, perquè hi ha un experiment a escala real que ho demostra. Es diu **Car-Pass** i és belga. Abans de la seva implantació, Bèlgica patia entre **seixanta mil i cent mil manipulacions de comptaquilòmetres l'any**. El sistema és senzill: cada vegada que un cotxe canvia de mans, se n'enregistra oficialment el quilometratge, i aquest historial segueix el vehicle per sempre. El resultat va ser fulminant. El 2022, en tot Bèlgica, només es van detectar **1.344 casos** de frau —menys del 0,2 % dels cotxes de segona mà—, i el frau en les importacions va caure del 2,4 % el 2020 al 0,87 % el 2022 [4].

La lliçó és lluminosa: quan la veritat d'una dada queda fixada en el moment en què es genera, i aquesta empremta acompanya l'actiu per sempre, el frau s'esfondra. Però Car-Pass té dues limitacions que el fan insuficient per al món de les flotes i els crèdits de carboni. És **nacional** —un cotxe que entra des d'un altre país arriba amb un historial buit o sospitós— i és **centralitzat**, una base de dades sota una sola autoritat. Per a una flota que opera a tot Europa, i per a uns crèdits que es venen a escala global, fa falta el mateix principi de Car-Pass però **descentralitzat, transfronterer i verificable per qualsevol**. I això és, precisament, el que aporta la prova d'existència.

La prova d'existència per a flotes

Apliquem la mecànica de **t2p** a la dada d'una flota. La lectura en brut —els quilòmetres de l'odòmetre, els quilowatts-hora d'una sessió de càrrega, la traça GPS d'un trajecte, el paquet del bus CAN— rep una **empremta SHA-512** calculada al mateix dispositiu de telemàtica, com més a prop possible de la font, abans que cap servidor la pugui tocar. Aquella empremta s'acompanya de **GPS forense** i **prova de vida**, que lliguen la posició i el moment a la dada i delaten una ruta fantasma o un GPS suplantat en creuar el segell amb la geometria real. S'hi afegeix un **segell de temps RFC 3161** qualificat: i aquí hi ha un detall jurídic poderós, perquè sota els articles 41 i 42 del reglament europeu eIDAS, aquest segell té **presumpció legal d'exactitud** de la data i l'hora. En cas de disputa, no és qui presenta la prova qui ha de demostrar que la data és bona; és qui la impugna qui ha de demostrar que és falsa [12]. Finalment, l'empremta s'ancora a la **blockchain pública** i tot el paquet es tanca en un contenidor **.asice verificable fora de línia**, que un auditor de CSRD, un verificador de CAE o un organisme de crèdits de carboni pot comprovar sense dependre de l'emissor.

És, en essència, **Car-Pass elevat a la potència de la blockchain**: un historial de quilometratge i de consum incontrovertible, però descentralitzat i transfronterer. Segellant la lectura a cada repostatge, a cada sessió de càrrega, a cada inspecció tècnica, es crea un registre que fa impossible el retrocés del comptaquilòmetres, els trajectes fantasma per inflar estalvis, la manipulació de les sessions de càrrega o l'inflament de la línia base d'un CAE. I encaixa de manera natural amb dues infraestructures que ja arriben. La primera és l'estàndard d'**Identitat de Vehicle** (VID) de **MOBI**, la *Mobility Open Blockchain Initiative*, un consorci fundat el 2017 per fabricants com BMW, Ford, General Motors, Honda i Renault, que el 2019 va publicar la primera «partida de naixement» digital d'un vehicle en blockchain i el 2024 va demostrar un passaport global de bateria [9]. La segona és el **Passaport de Bateria** europeu, que serà obligatori des del 18 de febrer de 2027 per a totes les bateries de vehicle elèctric de més de dos quilowatts-hora i que registrarà l'estat de salut de cada bateria accessible amb un codi QR [10].

Cal ser honest, també aquí, amb el límit. La prova d'existència garanteix que **la dada no ha canviat des que es va segellar**, no que el sensor digués la veritat en aquell instant. Un odòmetre trucat físicament *abans* de la lectura, o un sensor compromès en el maquinari, seguiria segellant un valor fals. La mitigació és doble: segellar al dispositiu de confiança més proper a la font i fer-ho tan sovint com es pugui, i creuar senyals redundants —GPS contra consum contra quilòmetres— perquè qualsevol incoherència salti a la vista. La tecnologia no elimina la mentida d'arrel; la fa molt més difícil, més cara i més rastrejable.

La promesa i el perill

La promesa, per a una empresa amb flota, és tangible. Una evidència segellada en origen converteix els crèdits de carboni i els CAE de transport en actius sòlids, defensables davant d'un auditor i d'un comprador; protegeix l'empresa de comprar, sense saber-ho, vehicles trucats; i fa que els informes d'Abast 3 que exigeix la CSRD deixin de ser un exercici de fe per convertir-se en dades comprovables. En un mercat on cada tona i cada quilowatt-hora s'han de demostrar, l'evidència fiable és un avantatge competitiu.

El perill demana el matís de sempre, la dualitat de «la promesa i el perill». La telemàtica i la prova de vida recullen dades sensibles — on cada vehicle va, qui el condueix — i exigeixen un disseny escrupolós amb la privacitat dels treballadors. La concentració de la verificació en poques plataformes recrearia el punt únic de confiança que volem dissoldre. I cap segell no eximeix de la feina física: mesurar bé, calibrar els sensors, auditar la línia base. La prova d'existència és el fonament de la confiança, no un substitut de la diligència.

És hora d'actuar

Per als **gestors de flota**: segellar en origen les lectures clau —quilometratge, consum, sessions de càrrega i rutes— perquè els crèdits, els CAE i els informes d'emissions siguin demostrables i inatacables. Per als **proveïdors de telemàtica**: incorporar el segell criptogràfic al dispositiu, tan a prop del sensor com sigui possible, i no en un servidor on la dada ja s'hagi pogut alterar. Per als **verificadors de CAE i els registres de crèdits de carboni**: exigir evidència ancorada com a base de la certificació i aprofitar-la per abaratir els controls. Per als **auditors de sostenibilitat** (CSRD): reclamar proves d'existència per a les dades d'Abast 3. Per als **reguladors**: estendre la lògica del Car-Pass —historial de quilometratge inalterable— a escala europea i descentralitzada, i reconèixer el valor probatori del segell, que el seu propi reglament eIDAS ja empara.

Una furgoneta pot rejovenir vuitanta mil quilòmetres en un minut; però si la lectura del comptaquilòmetres queda segellada a cada canvi de mans, aquell minut deixa d'existir. La diferència entre una flota que afirma estalviar i una flota que **demostra** que estalvia és, cada cop més, la distinció entre un actiu i una sospita. Generar aquesta prova en origen i a prova de manipulacions és time2act.

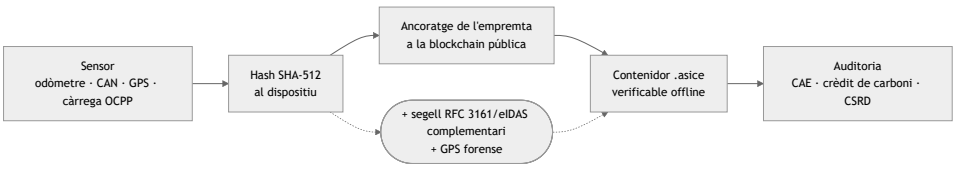


Figura 25.1 — La lectura d'un sensor (odòmetre, bus CAN, GPS, sessió de càrrega OCPP) es resumeix en una empremta SHA-512 al dispositiu, s'hi lliguen el GPS forense i un segell de temps RFC 3161/eIDAS amb presumpció legal, s'ancora a la blockchain pública i s'empaqueta en un contenidor .asice verificable fora de línia, llest per emetre un CAE (fitxes TRA010-TRA050), un crèdit de carboni o un informe CSRD. Caixa comparativa: sense segell, fins al 30-50 % dels odòmetres transfronterers estan manipulats; amb un registre segellat (model Car-Pass), menys del 0,2 %. Fonts: Parlament Europeu (EPRS); Car-Pass; MITECO.

[1] Parlament Europeu (EPRS) — Enrico Pastori i Raffaele Vergnani, *Odometer manipulation in motor vehicles in the EU* (2018; dany de 5.600-9.600 M€/any; 30-50 % en vendes transfrontereres). 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* (fins al 50 % dels cotxes transfronterers). 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€/any; sobrepreu mitjà del 26,3 %). https://www.carvertical.com/en/blog/cost-of-odometer-fraud-in-europe ↩

[4] Car-Pass (Bèlgica) — *Annual report 2022* (1.344 casos el 2022, <0,2 %; importacions 2,4 %→0,87 %). https://www.car-pass.be/en/blog/car-pass-annual-report-2022 ↩

[5] MITECO — *Catálogo de fichas CAE: sector transporte* (fitxes 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* (agost 2025; 65 % menys energia; autonomia 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 ciberatacs el 2025; 92 % remots; 67 % a telemàtica/núvol). 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) i *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] Reglament (UE) 2023/1542 — *Passaport de Bateria digital* (obligatori des del 18-feb-2027 per a bateries de VE i industrials de més de 2 kWh; accés per QR). https://www.circularise.com/blogs/eu-battery-passport-regulation-requirements ↩

[11] Smart Freight Centre — *GLEC Framework v3.0 / ISO 14083:2023* (comptabilitat d'emissions del transport de mercaderies). 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] Reglament (UE) 910/2014 (eIDAS), articles 41-42 — presumpció legal d'exactitud del segell de temps qualificat. https://eur-lex.europa.eu/eli/reg/2014/910/oj ↩

Mobilitat II: cotxe compartit i particulars, repartir la confiança

«Sigui qui sigui vostè... sempre he depès de la bondat dels desconeguts.»

— Tennessee Williams, Un tramvia anomenat Desig (1947)

A Brooklyn, l'agost de 2024, la fiscalia federal del Districte Est de Nova York va presentar càrrecs contra dos homes per una estafa d'una elegància pertorbadora. Eliahou Paldiel i Carlos Arturo Suárez Palacios havien programat una aplicació de **suplantació de GPS** i l'havien repartida a més de vuit-cents conductors d'una plataforma de transport. Amb aquella eina, un conductor podia «aparèixer» en una zona de tarifes altes —les anomenades *surge*— sense ser-hi realment. Multiplicat per centenars de conductors i milers de viatges, l'engany va arribar a defraudar uns **quaranta milions de dòlars** des del novembre de 2018 [5]. Una segona app, anomenada «Screwber», els avançava la destinació i la tarifa de cada petició perquè només acceptessin els trajectes més rendibles.

El cas és gairebé una paràbola. Si la prova que un viatge ha existit és un **punt blau en un mapa**, aquell punt es pot falsificar. I tota l'economia de la mobilitat compartida —del cotxe que comparteixen dos veïns al sistema de bicicletes d'una ciutat— descansa, en última instància, sobre aquesta prova fràgil. En el capítol anterior vam veure com una empresa amb flota pot segellar l'evidència dels seus vehicles. Ara baixem a l'escala més difícil de totes: la del **particular** que comparteix cotxe i que, sense cap operador central que l'avali, vol demostrar que un trajecte va passar de debò per reclamar la seva part justa d'un estalvi, d'un crèdit o d'un cost. Aquí, repartir la confiança és el problema central.

La revolució silenciosa de compartir

Compartir vehicle és una de les palanques climàtiques més potents i menys glamuroses que existeixen. La raó és tan simple com demolidora: un cotxe privat passa aturat al voltant del 95 % del temps. Ho subratlla **Susan Shaheen**, professora d'enginyeria a la Universitat de Califòrnia a Berkeley i codirectora del seu Transportation Sustainability Research Center, probablement la investigadora de referència mundial en mobilitat compartida. En un estudi de tres anys sobre el servei car2go, Shaheen i Elliot Martin van trobar que **cada vehicle compartit retirava entre set i onze cotxes privats** dels carrers de cinc ciutats nord-americanes, i reduïa els quilòmetres conduïts i les emissions dels seus usuaris [1].

Aquella xifra, però, exigeix una cautela honesta que travessa tota la literatura: **el nombre de cotxes privats que substitueix un de compartit és sempre un rang, no una constant**. Un estudi europeu sobre el servei SHARE NOW, amb més de 278.000 usuaris en onze ciutats, va trobar una mitjana de **3,3 cotxes substituïts** —de 2,1 a Madrid i Lisboa fins a 5,3 a Brussel·les—, mentre que altres ciutats arriben a xifres molt més altes segons la metodologia [2]. Qualsevol que us vengui un número únic i rodó (el clàssic «un cotxe compartit en reemplaça deu») us ven màrqueting, no ciència.

La plataforma BlaBlaCar va evitar **2,5 milions de tones de CO_2** el 2024, omplint més de setanta milions de seients buits i transportant noranta-dos milions de passatgers, com hem vist [3]. A Amèrica del Nord, el 2023 es van registrar **157 millions de viatges** en bicicletes i patinets compartits, un rècord històric [4]. És un univers en plena expansió i carregat de potencial climàtic —tant que plataformes de cotxe compartit entre particulars com Turo s'han arribat a certificar «neutres en carboni» [11]— i genera estalvis certificables: crèdits de carboni, CAE de mobilitat col·laborativa —recordeu la fitxa TRA040 del capítol anterior— o simples repartiments justos de cost, sempre que es pugui demostrar que el viatge va existir.

El problema de la prova entre iguals

I aquí topem amb una dificultat que les flotes d'empresa no tenen. Quan una companyia segella les dades dels seus camions, hi ha una organització responsable al darrere. Però quan dos desconeguts comparteixen un trajecte, **qui dona fe que ha passat?** Avui, la resposta és l'aplicació: BlaBlaCar, Turo o qui sigui actua alhora de jutge i de part, i la seva «prova» és un registre dins la seva base de dades, perfectament editable. Per repartir un crèdit entre dos particulars que no es coneixen ni es fien l'un de l'altre, depenem cegament d'un intermediari central —exactament la dependència que aquest llibre, des del primer capítol, qüestiona.

Aquesta fragilitat obre la porta a un frau específic i barat. Es poden inventar **viatges fantasma** per «cultivar» crèdits que mai no s'han generat. Dues comptes poden **confabular-se** per intercanviar-se trajectes falsos. I, com il·lustra el cas de Brooklyn, un **GPS suplantat** pot fabricar rutes senceres que no han existit. En tots els casos, l'atac no és contra la fórmula de l'estalvi, sinó contra la prova que l'activitat física va passar. Mentre aquesta prova sigui un punt blau editable, qualsevol esquema d'incentius a la mobilitat compartida neix amb un forat al cor.

Una moneda nova: els crèdits de mobilitat

Aquest forat és, precisament, el que ha frenat una de les idees més fascinants de l'economia del transport: els **crèdits de mobilitat negociables**. El concepte el van formalitzar els enginyers **Hai Yang i Xiaolei Wang** en l'article *Managing network mobility with tradable credits* (2011). La proposta és tan elegant com equitativa: en lloc de cobrar peatges, una autoritat repartiria a cada ciutadà una quota de crèdits de mobilitat, cobraria l'ús de la xarxa en crèdits i deixaria que es comerciessin lliurement. Qui es desplaça poc —sovint, qui menys té— podria **vendre** el seu excedent a qui es desplaça molt, assolint els mateixos objectius que un peatge però amb neutralitat d'ingressos i molta més justícia social [6].

La idea ha generat una línia de recerca puixant. **Oded Cats**, catedràtic de transport a la Universitat Tècnica de Delft, ha estudiat el disseny i la classificació d'aquests esquemes i ha modelat fins i tot la seva aplicació als viatges de llarga distància a Europa [7]. I tanmateix, hi ha un fet revelador: **fins al 2025 no s'ha implementat cap esquema de crèdits de mobilitat negociables a escala real**. Una revisió acadèmica recent de l'estat de l'art ho confirma sense embuts: només existeixen experiments de laboratori, jocs de simulació i modelitzacions [8]. Els incentius que sí funcionen avui són més modestos: a Bèlgica, el «pressupost de mobilitat» corporatiu ja arriba a uns 18.000 treballadors que bescanvien el cotxe d'empresa per alternatives sostenibles [9]; a la Universitat de Delft, els ciutadans «gasten» crèdits simulats en una sala de joc; i a Brussel·les, la Regió ofereix entre 505 i 1.010 euros l'any a qui dona de baixa la matrícula del cotxe a canvi de transport públic, bici o cotxe compartit [10] —però tot això són incentius, no encara mercats de crèdits.

Per què la idea no acaba d'arrencar? Hi pesen la privacitat, el marc legal i l'acceptació pública. Però hi ha una peça tècnica que sovint s'oblida i que és justament la d'aquest llibre: **sense una manera fiable que cada ciutadà demostri els seus desplaçaments sense lliurar tota la seva vida a una autoritat central, el sistema no és ni verificable ni acceptable**. Un mercat de crèdits de mobilitat necessita, abans que res, una capa de prova de confiança.

Repartir la confiança sense operador central

És aquí on la **prova d'existència** de **t2p** aporta exactament la peça que falta, i ho fa amb una propietat que la distingeix de tota la resta del llibre. Apliquem-la a un trajecte compartit. En tancar el viatge, l'aplicació del particular genera **al seu propi dispositiu** un registre estructurat —ruta GPS forense, ocupants, distància, mode— i en calcula una empremta **SHA-512**, de manera que la dada en brut no surt del telèfon: només ho fa la seva petjada. Aquesta empremta rep un **segell de temps RFC 3161** conforme a eIDAS i s'ancora a la **blockchain pública**, de manera que ningú no pot «crear» després un viatge passat per inflar crèdits.

I llavors arriba la clau de volta, la peça que el sector de la mobilitat compartida necessita més que cap altre: la **prova de vida**. La biometria de *liveness* lliga el segell a la **persona real i present** en aquell viatge, no a un compte ni a un emulador. Això ataca de soca-rel l'estafa de Brooklyn: un emulador pot falsejar coordenades, però no pot superar un repte de prova de vida ancorat a la captura de l'empremta en aquell instant i aquell lloc. Finalment, tot el conjunt es tanca en un contenidor **.asice verificable fora de línia**, i aquí hi ha el gir decisiu: **dos desconeguts poden liquidar el seu trajecte compartit sense confiar en cap operador**, perquè tots dos poden verificar la mateixa prova de manera independent. La confiança ja no la presta una app central; la presten les matemàtiques.

Aquesta capa és, en realitat, la infraestructura que faltava perquè els crèdits de mobilitat de Yang i Cats deixin de ser un experiment de laboratori. Permet repartir crèdits «sense operador de confiança», impedeix els viatges fantasma i la confabulació entre comptes, i fa detectable qualsevol reescriptura retroactiva del registre. Encaixa, a més, amb estàndards oberts d'identitat de vehicle com el VID de MOBI, la *Mobility Open Blockchain Initiative* [12].

Cal ser, una vegada més, honest amb el límit. La prova d'existència certifica que *aquest registre existia, intacte, en aquell moment i lligat a aquesta persona*; **no** garanteix que la lectura de GPS subjacent sigui físicament certa si el maquinari o el firmware del telèfon es van comprometre abans del segellat. Un GPS suplantat a escala de maquinari encara podria passar coordenades falses. La defensa real és la combinació de capes —prova de vida, coherència entre altitud, velocitat i ruta, i segell de temps—, no la cadena de blocs tota sola. I tampoc no demostra l'**addicionalitat**: que aquell viatge compartit realment substituís un cotxe que de debò s'hauria fet servir. Això continua sent un supòsit metodològic. La tecnologia eleva la confiança en l'evidència; no inventa la veritat del món físic.

La promesa i el perill

La promesa és gran i concreta d'aquest sector: una capa de prova entre iguals podria desbloquejar per fi els mercats de crèdits de mobilitat, fer justos i verificables els repartiments de cost entre particulars, i convertir milions de petits gestos quotidians —compartir un cotxe, agafar la bici— en estalvi climàtic comptabilitzat i recompensat sense necessitat d'un gran intermediari que se'n quedi una part.

Però aquí el perill és tan agut, i té un nom: **privacitat**. Es tracta de segellar els desplaçaments de persones concretes. Una infraestructura que demostri on ha anat cada ciutadà pot ser, mal dissenyada, l'eina de vigilància més perfecta mai construïda. Per això la propietat que el hash es calculi al dispositiu i que la dada en brut no en surti no és un detall tècnic: és la línia que separa una eina d'apoderament d'una de control. La prova de vida implica dades biomètriques sensibles. I un mercat de crèdits mal pensat podria castigar qui no té alternativa al cotxe —el veí d'un poble sense tren— en lloc d'ajudar-lo. La prova d'existència ha de ser, en aquest terreny, escrupolosament respectuosa amb la privacitat i el disseny equitatiu, o no serà res de bo.

És hora d'actuar

Per a les **plataformes de mobilitat compartida** (BlaBlaCar, Turo, operadors de bici i patinet): oferir als usuaris proves d'existència dels seus viatges que siguin seves i portàtils, no presoneres de la base de dades de l'empresa. Per als **particulars**: exigir poder demostrar els propis desplaçaments sense haver de cedir tota la seva localització a un tercer. Per als **dissenyadors d'esquemes de crèdits de mobilitat** (autoritats de transport, investigadors com Cats): incorporar la capa de prova entre iguals com a fonament, perquè els seus models surtin per fi del laboratori. Per a les **ciutats i reguladors**: construir aquests sistemes amb la privacitat com a primer requisit, no com a pegat final.

Dos homes a Brooklyn van demostrar que un punt blau en un mapa no és cap prova. Reconstruir la confiança a l'escala més íntima de la mobilitat —la del ciutadà que comparteix un trajecte i vol que compti — exigeix una prova que ni un emulador ni un intermediari interessat puguin fabricar. Repartir aquesta confiança, persona a persona, és la frontera més difícil i més humana de tot aquest llibre. I assolir-la és, també, time2act.

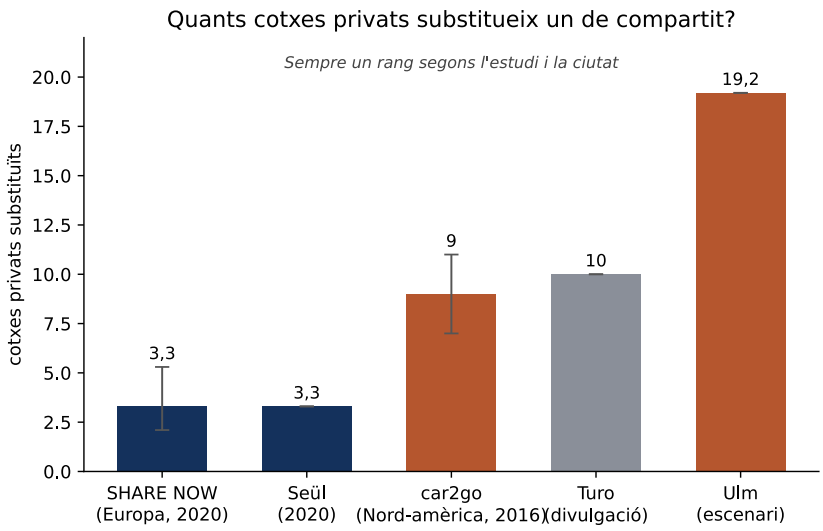


Figura 26.1 — El nombre de cotxes privats que retira del carrer un sol vehicle compartit varia enormement segons la ciutat i la metodologia: de 3,3 de mitjana a l'estudi europeu de SHARE NOW fins als 7-11 de l'estudi de car2go a Nord-amèrica, amb escenaris encara més alts en algunes ciutats. La xifra de divulgació «un per deu» és comercial, no consensuada. La lliçó: cap número únic; sempre un rang amb la seva font. Fonts: UC Berkeley TSRC (Shaheen i Martin, 2016); Transportation Research Part A (2020).

---

[1] Susan Shaheen i Elliot Martin (UC Berkeley, Transportation Sustainability Research Center) — *Impacts of car2go: One-Way Carsharing in North America* (2016; cada vehicle compartit retira 7-11 cotxes privats; VMT i GEI a la baixa). 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; mitjana de 3,3 cotxes substituïts; rang 2,1-5,3). https://pmc.ncbi.nlm.nih.gov/articles/PMC7544607/ ↩

[3] BlaBlaCar — *Sustainability Report 2024* (2,5 Mt CO_2 evitades el 2024; 92 milions de passatgers). 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 (fiscalia EDNY) — *Two charged in $40M ride-hail surge-pricing GPS spoofing scheme* (cas «Fake GPS», agost 2024). https://www.insurancejournal.com/news/east/2024/08/30/790683.htm ↩

[6] Hai Yang i 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) i *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; cap implementació a escala real fins ara). https://www.sciencedirect.com/science/article/pii/S2590198225002908 ↩

[9] Next Mobility / ONSS — *Mobility budget in Belgium: ONSS figures 2024* (18.386 treballadors amb pressupost de mobilitat; 17.030 sense cotxe d'empresa). https://www.nextmobility.be/en/post/mobility-budget-belgium-onss-figures-2024/ ↩

[10] Bruxelles Environnement — *Prime Bruxell'Air* (ajut de 505-1.010 €/any per donar de baixa la matrícula, vigent el 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 ↩

Retards de transport: provar l'hora d'arribada

«No és que tinguem poc temps: és que en perdem molt.»

— Sèneca, De brevitate vitae, I (c. 49 dC)

Una andana qualsevol, una porta d'embarcament qualsevol. El panell salta de «+10» a «+45» sense explicacions; la connexió es perd; l'ambient es tensa. Mesos després, la resposta de la reclamació arriba amb la seva prosa impecable: «denegada per circumstàncies operatives alienes a la companyia». I el viatger descobreix el fons de l'assumpte: ell té el record de l'espera; la companyia té el registre — i el registre el fa qui hauria de pagar.

El context és d'actualitat [1]: l'1 de juliol de 2024, Renfe va retallar el seu compromís voluntari de puntualitat per a AVE, Avlo, Alvia, Euromed i Intercity. Van desaparèixer les indemnitzacions per retards de 15 i 30 minuts, i el nou règim paga el 50 % del bitllet a partir de 60 minuts i el 100 % a partir de 90 — incentivant, a més, el cobrament en punts (el 200 %) o en vals (el 150 %) en lloc d'euros. La justificació oficial: adaptar-se a la liberalització i a la normativa europea. El debat sobre si cal indemnitzar des dels 15 minuts continua obert [1]. I la lliçó probatòria és immediata: quan els llindars pugen, la frontera entre 58 i 61 minuts val mitja tarifa — i la mesura oficial d'aquesta frontera la fa una de les parts.

Aquest capítol tracta el dret de consum més clar i pitjor proveït de prova. La reclamació al servei d'atenció de la companyia és al capítol 33; el rellotge del proveïdor de núvol — el mateix patró en una altra indústria —, al capítol 59; les flotes i la mobilitat compartida, als capítols 25 i 26. Pregunta clau: de qui és el rellotge que decideix si cobres? Resposta: de qui ha de pagar — llevat que l'arribada real tingui data certa al dispositiu del viatger, amb **t2p**: empremta, hora certa i àncora pública — la maquinària del capítol 13 [3]. I amb la simetria de sempre: el registre ancorat del transportista el protegeix de la reclamació inflada.

El dret existeix; la prova, no tant

El marc dels vols és dels més generosos del dret de consum europeu [2]: el Reglament (CE) 261/2004 fixa compensacions de 250 euros per a vols de fins a 1.500 quilòmetres, 400 per als intraeuropeus més llargs i els de 1.500 a 3.500, i 600 per als de més de 3.500; la jurisprudència europea — la doctrina Sturgeon — va equiparar el retard de tres hores o més a l'arribada amb la cancel·lació; i el Tribunal de Justícia ha deixat una precisió preciosa per a aquest llibre: l'«hora d'arribada» és el moment en què s'obren les portes — un instant que el passatger presencia amb el mòbil a la butxaca. L'excepció que ho tensa tot: les «circumstàncies extraordinàries», que eximeixen la companyia i que el viatger difícilment pot contrastar.

El mecanisme de prova, en canvi, és de l'altra època. L'hora d'arribada real la registren els sistemes del transportista; els panells s'actualitzen i s'esborren; el motiu del retard l'anuncia qui l'ha de justificar; i la reclamació es presenta setmanes després, amb una targeta d'embarcament i records difusos. Al tren, el mateix amb el matís espanyol [1]: el compromís és de la casa, i la mesura també.

La conclusió no demana desconfiar de ningú: demana que el minut 61 sigui un fet i no una versió. El dret ja existeix; el que falta és que la seva única variable — quant de tard vas arribar — es pugui acreditar des dels dos costats.

La prova d'existència aplicada

L'arribada, convertida en fet [3].

1. L'arribada amb lloc i hora

El gest decisiu dura deu segons: en obrir-se les portes — la definició del Tribunal de Justícia [2] —, una foto amb el GPS forense de t2p: fix genuí, precisió d'uns 50 metres, antiguitat màxima d'uns 30 segons; una ubicació simulada bloqueja la certificació [3]. Lloc i hora certs de l'arribada real, al dispositiu del passatger. I si el vol anava en mode avió, cap problema: la certificació en segon pla es reprèn sola en recuperar cobertura, i el segell acredita el moment de la captura [3]. El minut 61 deixa de ser una discussió.

2. El panell congelat

El panell amb el retard anunciat — o el motiu al·legat —, la pantalla de l'app amb l'estat del vol o del tren, el correu de la cancel·lació: capturats i certificats amb data [3]. Quan la versió oficial canviï — el retard «per causes tècniques» que després esdevé «circumstància extraordinària» —, el que es va dir a cada moment existeix, exacte i datat, i ningú no el pot reescriure a posteriori.

3. L'expedient del viatge

El bitllet i la targeta d'embarcament, escanejats; les despeses que la companyia havia d'atendre i no va atendre — l'àpat, l'hotel, el taxi — amb tiquets fotografiats amb GPS forense [3]; tot agrupat en un projecte i exportable com a paquet .asice verificable sense connexió [3]. La reclamació a la companyia, a l'agència estatal de seguretat aèria o al jutjat de consum arriba amb fets datats, no amb una història.

4. La simetria del transportista

El mateix mecanisme protegeix qui opera bé: el registre de sortides i arribades ancorat per lots — la lògica de la sonda del capítol 59 — i l'evidència de la circumstància extraordinària de debò — el tancament d'espai aeri, la tempesta, l'incident aliè — segellada quan passa [3]. Contra la reclamació inflada o la del passatger que mai no va volar, el transportista amb registres verificables respon amb dates; i el seu compromís de puntualitat, ancorat i públic per empremta, esdevé un argument comercial que cap competidor no pot imitar sense complir [1].

Els límits, sense embuts: el segell acredita hores, llocs i documents — no decideix si una circumstància era extraordinària: això ho diuen el Reglament i el jutge [2]. No substitueix la reclamació formal dins de termini ni el procediment de cada autoritat. I la proporcionalitat mana: es documenta el viatge propi — mai tripulacions, empleats ni altres passatgers.

La promesa i el perill

La promesa: reclamacions que es resolen sobre hores certes [2][3]; passatgers que cobren el que el dret europeu els reconeix sense batalles de versions; transportistes diligents que acrediten les seves circumstàncies i liquiden les reclamacions legítimes en dies; i un mercat — ara liberalitzat [1] — on la puntualitat verificable competeix.

Ara, els perills.

El primer és **la reclamació industrialitzada**. El frau té dues cares: també hi ha passatgers que reclamen el que no toca. Precisament per això l'expedient datat beneficia tothom: qui va volar i va arribar tard ho pot provar; qui no, no pot fabricar un GPS forense que es nega a certificar ubicacions simulades [3].

El segon és **la guerra de rellotges**. El passatger amb la seva foto contra la companyia amb els seus sistemes. La sortida és la del capítol 59: registres oficials d'operació ancorats i públics per empremta com a estàndard del sector — quan el rellotge oficial és verificable, el particular només cal per excepció.

El tercer és **el viatge com a perfil**. On ets i quan hi ets és intimitat pura. L'expedient del viatge queda al dispositiu; a la cadena, només empremtes [3]; es revela el tram reclamat, mai l'historial de moviments.

El quart perill no és tècnic, sinó de mirada: confondre la prova amb el servei. Cap segell no fa arribar el tren puntual ni evita la tempesta. La prova fa exigible la compensació i honesta l'estadística de puntualitat; el servei el milloren la inversió i la gestió.

És hora d'actuar

Que el rellotge del retard tingui dos propietaris.

Per a tu, viatger: la foto de l'obertura de portes [2][3] — deu segons que valen fins a 600 euros [2]; i guarda el panell i les despeses al mateix projecte.

Per a les companyies aèries i ferroviàries: ancoreu els registres d'operació i publiqueu la puntualitat per empremta [1][3] — la reclamació infundada morirà de dates, i la vostra fiabilitat serà verificable, no publicitària.

Per a les plataformes de reclamació: incorporeu l'expedient segellat del passatger com a estàndard d'entrada [3]; guanyareu els casos amb fets, no amb volum.

Per a les autoritats — aviació i ferrocarril: exigiu als operadors registres d'arribades verificables [1] [2]; la protecció del viatger no pot dependre del rellotge de qui ha de pagar.

Per als legisladors: el debat sobre els llindars — els 15, els 60, els 90 minuts [1] — és legítim; el que no ho és és que la mesura del retard sigui unilateral. Que tot llindar nou neixi amb hora d'arribada verificable.

El pròxim cop que el panell salti de «+10» a «+45», que el teu rellotge també compti — amb data certa. Per cada minut que és teu, **time2act**.

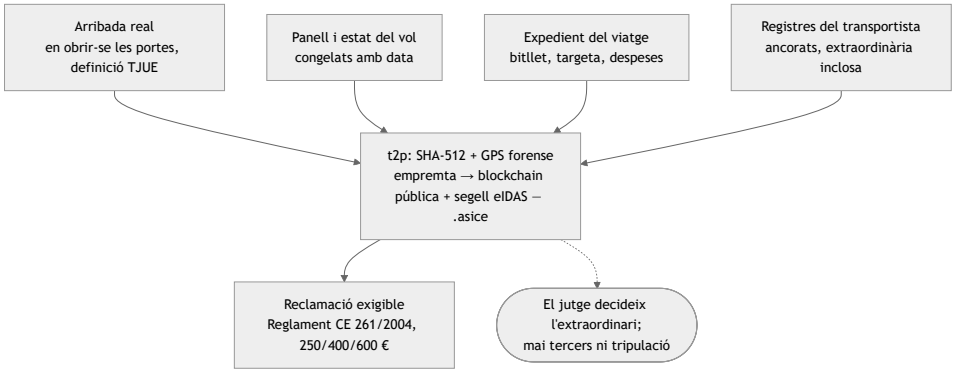


Figura 27.1 — El retard amb prova d'existència (segellat amb t2p — capítol 13): l'arribada amb GPS forense en obrir-se les portes (la definició del TJUE), el panell i l'estat del vol congelats, l'expedient del viatge (bitllet, embarcament, despeses d'atenció) i la simetria del transportista (registres d'operació ancorats; la circumstància extraordinària segellada quan passa). Context: Reglament (CE) 261/2004 (250/400/600 €; Sturgeon ≥3 h); Renfe 1-7-2024: dels 15/30 min als 60/90 (50 %/100 %). Límits: el jutge decideix l'extraordinari; documentar el viatge propi, mai tercers. Fonts: EUR-Lex; Renfe/Newtral.

---

[1] Newtral — *Cómo cambió Renfe las indemnizaciones por retraso del AVE* (1-7-2024: eliminades les indemnitzacions de 15 i 30 minuts per a AVE, Avlo, Alvia, Euromed i Intercity; nou règim 50 % a partir de 60 min i 100 % a partir de 90; devolució del 200 % en punts o 150 % en vals; justificació: liberalització i ajust a la legislació); Renfe — *Compromiso de puntualidad* i nota de premsa de l'actualització; Xataka — *el debat sobre indemnitzar des dels 15 minuts* (situació normativa oberta). 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 — *Reglament (CE) 261/2004* (compensacions de 250/400/600 € per cancel·lació i, per la doctrina Sturgeon del TJUE, gran retard ≥3 hores a l'arribada; excepció de circumstàncies extraordinàries; dret d'atenció; jurisprudència del TJUE: l'«hora d'arribada» és l'obertura de portes). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32004R0261 ↩

[3] t2p — manual de producte (foto amb GPS forense — fix genuí ~50 m / ≤30 s, la ubicació simulada bloqueja la certificació; certificació en segon pla que es reprèn en recuperar cobertura — mode avió; captura de pantalla certificada; escàner de documents; projectes per agrupar l'expedient d'un viatge; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; la reclamació de serveis, al capítol 33; el rellotge del proveïdor, al capítol 59. ↩

Assegurances: la prova del sinistre

«Algú devia haver calumniat Josef K., perquè, sense que hagués fet res de dolent, un matí el van detenir.»

— Franz Kafka, El procés (1925), frase inicial

Un autònom britànic tenia, com tothom, fotos de la seva furgoneta a les xarxes socials: l'eina del seu ofici, aparcada davant d'una obra, lluent i sense una ratllada. El 2024, algú va agafar una d'aquelles imatges públiques, la va editar digitalment per pintar-hi una esquerda al para-xocs i la va fer servir per presentar una reclamació d'assegurança fraudulenta, amb una factura de reparació falsa de més de mil lliures, per un accident que mai no havia passat. L'equip de frau de l'asseguradora LV= ho va destapar perquè la imatge era idèntica a la de les xarxes, però amb danys afegits. Matt Crabtree, responsable d'intel·ligència de delictes financers de LV=, va advertir que els defraudadors fan servir la tecnologia «per als seus fins il·legals i per atacar ciutadans innocents amb ànim de lucre» [6].

El cas és petit en l'import, però immens en el que anuncia. Durant dècades, falsificar un sinistre exigia un taller còmplice, un metge complaent o un cotxe de debò abonyegat. Avui n'hi ha prou amb una app al mòbil. I la prova en què es basa tot el sistema assegurador —la fotografia del dany— ha esdevingut, de cop, la baula més fàcil de fabricar. Aquest capítol tracta de com tornar a fer creïble aquella fotografia: segellant-la en el moment i el lloc en què es pren, abans que la mentida hi entri.

Un robatori que paguem tots

El frau a l'assegurança no és un delicte sense víctimes; el paguem tots a través de primes més altes. La seva magnitud és vertiginosa. Als Estats Units, la **Coalition Against Insurance Fraud** (CAIF), una coalició d'asseguradores, reguladors i consumidors, va publicar el 2022 —amb la Colorado State University Global — el primer càlcul actualitzat en vint-i-set anys: el frau costa al país **308.600 milions de dòlars l'any**, l'equivalent a uns 933 dòlars per cada nord-americà [1]. La salut s'emporta la part més grossa (uns 105.000 milions), seguida de la vida i dels danys materials i de responsabilitat.

A Europa, la federació d'asseguradores **Insurance Europe** estima que el frau —detectat i no detectat— equival a al voltant del **10 % de la despesa total en sinistres**, una xifra que arrossega des d'un informe de 2013 i que segueix repetint perquè és tan robusta com difícil de millorar [2]. Els registres nacionals ho confirmen any rere any. Al Regne Unit, les asseguradores van detectar el 2024 **1.160 milions de lliures** en reclamacions fraudulentes —un 2 % més que l'any anterior— repartides en 98.400 reclamacions, de les quals més de la meitat eren de l'automòbil [3]. A Espanya, el sector va detectar el 2024 **285.407 casos sospitosos** i en va evitar el 63,7 %; l'automòbil concentrava el 61,2 % del frau, amb un import mitjà per reclamació fraudulenta evitada de 2.924 euros i un cost d'investigació de tot just 43 euros per cas —un retorn d'uns 68 euros per cada euro invertit a investigar [4]. Segons el baròmetre de l'asseguradora Línea Directa, el 8,8 % dels comunicats d'accident d'auto a Espanya en els dos anys previs eren intents d'estafa, gairebé cinc vegades més que el 2009 [10].

La nova frontera: el sinistre que mai va passar

Aquestes xifres ja eren altes abans de la intel·ligència artificial. Ara, la IA generativa ha posat una fàbrica de proves falses a la butxaca de tothom i el sector ho viu com un terratrèmol. L'analista de dades de risc **Verisk**, juntament amb el National Insurance Crime Bureau, va publicar al març del 2026 un estudi —enquesta a mil consumidors i tres-cents professionals de sinistres— amb dades que glacen la sang: el **36 % dels consumidors** nord-americans consideraria alterar digitalment una imatge o un document d'un sinistre encara que infringís les normes de l'asseguradora, i la xifra es dispara entre els joves —un **55 % de la generació Z**, un 49 % dels millennials, davant del 12 % dels més grans [5]. El 13 % veu fins i tot acceptable «crear fotos de danys que no van passar mai». I des de l'altra banda, el **99 % de les asseguradores** ja ha topat amb documentació manipulada o alterada amb IA, i el 98 % afirma que aquestes eines estan augmentant el frau digital [5].

No és teoria. Les asseguradores Allianz i Zurich van documentar un **augment del 300 %** en les reclamacions amb fotos manipulades comparant 2021-22 amb 2022-23, i Allianz UK va advertir que el fenomen tenia «tots els senyals de convertir-se en la pròxima gran estafa del sector» [6]; només al primer semestre del 2025, Allianz va destapar al Regne Unit més de **15.800 casos** de frau per **92,6 milions de**

lliures [7]. Els defraudadors compren fotos de cotxes sinistrats en subhastes en línia, hi insereixen amb IA una matrícula real i fabriquen danys de col·lisió. L'equip de Zurich n'ha enxampat molts «observant anomalies als metadades de la imatge i amb l'anàlisi de nivell d'error», una tècnica forense que delata l'edició; en un cas, la foto del vehicle portava marques de temps anteriors a la data del suposat accident [8]. La reasseguradora **Swiss Re**, al seu informe *SONAR 2025*, xifra un **augment del 700 %** d'incidents amb deepfakes al sector fintech el 2023 i recomana, explícitament, combinar biometria, **detecció de prova de vida** i **marques inalterables ancorades en blockchain** [9].

Detectar a posteriori no n'hi ha prou

La resposta immediata del sector és la detecció: analitzar cada imatge rebuda a la recerca d'empremtes d'edició —anomalies de píxel, metadades incoherents, nivell d'error. És una feina valuosa i necessària, però té un defecte estructural que aquest llibre ja ha argumentat per a les deepfakes: és una **cursa armamentística** que el defensor sempre corre per darrere. Cada millora del detector empeny el defraudador cap a una IA millor, i el dia que la imatge generada no deixi cap rastre de píxel, la detecció quedarà cega. A més, analitzar a posteriori vol dir confiar en uns metadades que el mateix telèfon escriu i que qualsevol pot reescriure.

El problema de fons és que la prova —la foto del dany— es genera **fora** del control de l'asseguradora i **després** del fet. El reclamant envia un JPEG per una app o un correu, i aquell JPEG pot ser una foto d'estoc, una imatge d'un desguàs, un dany preexistent o una creació de IA. Mentre la prova neixi així, sense ancoratge, tota l'arquitectura del sinistre descansa sobre sorra. La solució duradora no és analitzar millor la foto que arriba, sinó **garantir l'origen de la foto en el moment en què es pren**.

La prova d'existència: segellar el sinistre a l'escena

És aquí on la **prova d'existència** de **t2p** ataca el problema des de l'arrel. En lloc d'examinar la imatge un cop rebuda, la segella en l'instant de la captura, a l'escena del dany. La foto o el vídeo es **resumeix en una empremta SHA-512 al mateix dispositiu** en el moment de prendre's; qualsevol reedició posterior —afegir una esquerda, alterar una matrícula— canviaria l'empremta i trencaria la cadena. A l'empremta s'hi afegeix un **segell de temps RFC 3161** conforme a eIDAS i un ancoratge a la **blockchain pública** que fixen *quan* es va capturar. I aquí hi ha la clau: això neutralitza exactament el truc que delatava els defraudadors de Zurich —metadades amb dates anteriors en anys—, perquè el segell prové d'una autoritat de confiança, no de l'EXIF manipulable del telèfon.

S'hi sumen dues peces que el sector necessita especialment. El **GPS forense** acredita *on* es va prendre la foto, cosa que ajuda a descartar imatges de subhastes o danys reciclats d'un altre lloc. I la **prova de vida** lliga la captura a *una persona real present a l'escena*, fent molt difícil que algú pugi imatges generades «des de darrere de l'ordinador», el patró que descriuen Allianz i LV=. Tot plegat —imatge original intacta, empremta, segell, GPS, prova de vida— s'empaqueta en un **contenidor .asice verificable fora de línia**, que el pèrit o l'auditor pot validar sense dependre de l'app ni d'un servidor, i que és admissible com a evidència. Val la pena subratllar-ho: és precisament la recepta que Swiss Re recomana —biometria, prova de vida, ancoratge inalterable—, convertida en producte.

Cal ser, com sempre, honest amb el límit. La prova d'existència demostra que *aquesta* imatge existia íntegra, en *aquest* lloc, en *aquest* moment, capturada per *aquesta* persona viva. **No demostra la causa ni la legitimitat del dany.** Algú pot fotografiar amb t2p després d'haver provocat ell mateix un accident escenificat: el segell serà impecable i el sinistre continuarà sent frau. Per això la prova d'existència **complementa, no substitueix, el pèrit**: elimina la capa de frau documental i d'imatge —la de creixement més ràpid— perquè la investigació humana es concentri en la causalitat i la simulació. I només aporta valor si la captura es fa amb l'app en el moment, no per a sinistres ja ocorreguts i documentats amb fotos velles.

La promesa i el perill

La promesa és tangible i quantificable. En un sector on el frau costa centenars de milers de milions, eliminar d'arrel el frau de la foto-prova alliberaria recursos enormes, acceleraria el pagament dels sinistres honestos —la immensa majoria— i abaixaria la pressió sobre les primes de tothom. Una foto segellada a l'escena converteix la part més vulnerable del procés en la més sòlida.

El perill demana el matís de sempre, la dualitat de «la promesa i el perill». Recollir fotos geolocalitzades i biometria de prova de vida toca dades sensibles del client en un moment d'estrès; el disseny ha de ser escrupolós amb la privacitat i no convertir cada comunicat en una cessió excessiva de dades. Cap segell no eximeix el pèrit de jutjar la causa, ni l'asseguradora de tractar el client amb confiança per defecte. I la concentració de la verificació en poques plataformes recrearia el punt únic de confiança que volem dissoldre. La prova d'existència és una capa necessària dins d'una arquitectura de confiança més àmplia.

És hora d'actuar

Per a les asseguradores: oferir la captura segellada a l'origen com a canal preferent del comunicat de sinistre i premiar-la amb una tramitació més ràpida —qui no té res a amagar, en surt beneficiat. Per als assegurats honestos (la immensa majoria): exigir poder demostrar el seu sinistre amb una prova que cap algorisme pugui posar en dubte. Per als pèrits i investigadors: reservar l'esforç humà per a la causalitat i el frau dur, deixant que la tecnologia tanqui la porta al frau d'imatge. Per als reguladors: reconèixer el valor probatori del segell i fixar estàndards que protegeixin simultàniament la integritat de la prova i la privacitat del client.

Un autònom va veure com la foto de la seva furgoneta es convertia en l'arma d'una estafa. La diferència entre una imatge que qualsevol pot fabricar i una prova segellada a l'escena és, cada cop més, la clau per a un sistema que s'autodefensa. Tornar a fer creïble la foto del sinistre —demostrar que el dany va existir, allà i llavors— és, també aquí, time2act.

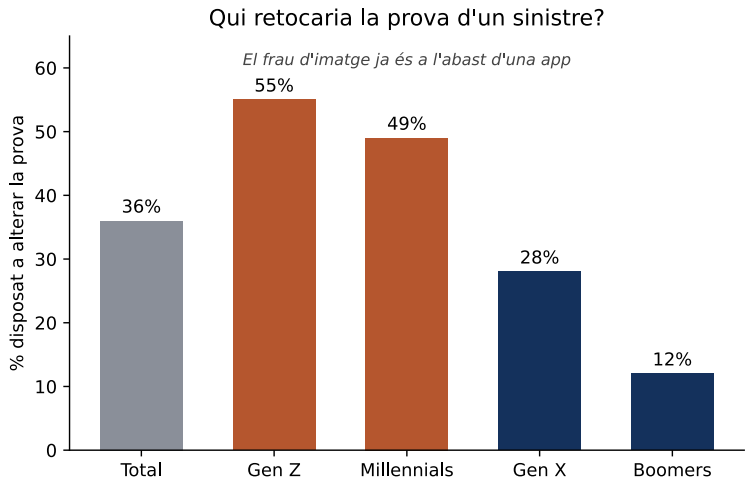


Figura 28.1 — Percentatge de consumidors disposats a alterar digitalment la imatge o el document d'un sinistre, encara que infringeixi les normes de l'asseguradora: un 36 % de mitjana, però fins al 55 % entre la generació Z. La predisposició cau amb l'edat. És el rostre del frau d'imatge per IA que el 99 % de les asseguradores ja ha vist. Font: Verisk amb 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$/any, ~933 $ per 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* (capítol Fraud) i *The impact of insurance fraud* (~10 % de la despesa en sinistres; estimació de 2013, ~13.000 M€ referits 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 reclamacions). 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 %* (Espanya, 2024). https://segurosnews.com/news/el-sector-detecto-285-407-casos-sospechosos-de-fraude-de-los-que-evito-un-637 ↩

[5] Verisk (amb el National Insurance Crime Bureau) — *AI editing tools are fueling a new era of insurance fraud* (març 2026; 36 % de consumidors, Gen Z 55 %; 99 % de les asseguradores). 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 (via PetaPixel) — *Fraudsters are editing photos of damaged vehicles to claim insurance* (cas LV=; +300 % de fotos manipulades, 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* (metadades + anàlisi de nivell d'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 %; recomana prova de vida i ancoratge 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 % dels comunicats d'auto a Espanya). https://www.lineadirectaaseguradora.com/-/vii-barometro-de-fraude-al-seguro ↩

Cadena de subministrament: l'origen verificable contra la falsificació

«No és de la benevolència del carnisser, del cerveser o del forner que esperem el sopar, sinó de l'atenció que presten al seu propi interès.»

— Adam Smith, La riquesa de les nacions, I, 2 (1776)

A la tardor de 2022, als hospitals de Banjul, la capital de Gàmbia, els metges van començar a veure arribar nadons amb una insuficiència renal aguda que no sabien explicar. El rastre va portar a quatre xarops pediàtrics per a la tos i el refredat, fabricats per una empresa índia, Maiden Pharmaceuticals, i contaminats amb dietilenglicol i etilenglicol —dos dissolvents industrials tòxics. Van morir prop de **setanta nens**. El 5 d'octubre de 2022, l'Organització Mundial de la Salut va emetre l'Alerta de Producte Mèdic N°6/2022 [3]. Tres anys després, l'octubre de 2025, la història es va repetir a l'Índia: el xarop «Coldrif», amb gairebé un 48 % de dietilenglicol, va matar almenys vint-i-quatre nens més, i l'OMS va haver d'emetre una nova alerta [4].

El detall que ho canvia tot és aquest: en aquells casos, **l'etiqueta era autèntica i la cadena documental era «legítima»**. Els papers estaven en ordre. El que va fallar no va ser el segell ni el codi de barres, sinó la veritat física del contingut. És la lliçó més dura i més honesta d'aquest capítol, i convé posar-la al davant: cap prova d'origen, per perfecta que sigui, analitza la molècula. Però, com veurem, això no fa la prova d'origen inútil —la fa imprescindible per a tota la resta del problema.

El frau que entra a les cadenes legítimes

La falsificació de productes ja no es limita a bosses de marca venudes a la manta; és un riu que s'infiltra en les cadenes de subministrament legítimes i amenaça la salut. L'**OCDE** i l'**Oficina de Propietat Intel·lectual de la Unió Europea** (EUIPO), en el seu informe *Mapping Global Trade in Fakes 2025*, xifren el comerç mundial de productes falsificats i piratejats en **467.000 milions de dòlars** el 2021 — un **2,3 % de totes les importacions del món** [1]. A la Unió Europea la proporció puja al **4,7 % de les importacions**, uns 117.000 milions [1]; com hem vist, el que més alarma és el gir cap a la **falsificació perillosa**: recanvis d'automòbil, cosmètics, joguines, aliments i medicaments falsos que entren al mercat com si fossin autèntics.

Els medicaments són el cas més letal. L'**Organització Mundial de la Salut** estima que **almenys un de cada deu productes mèdics** als països de renda baixa i mitjana és subestàndard o falsificat, basant-se en més de cent estudis i 48.000 mostres de 88 països [2]. El malbaratament econòmic ronda els **30.500 milions de dòlars** l'any, però el cost real es compta en vides com les de Gàmbia. L'OMS distingeix el producte **subestàndard** —el que no compleix les normes de qualitat per mala fabricació— del **falsificat** —el que tergiversa deliberadament la seva identitat, composició o origen. En ambdós casos, el problema fonamental és que **no hi ha manera fàcil de provar d'on ve realment el que tenim a les mans**.

El regulador exigeix coordenades

Davant d'això, Europa ha fet un gir històric: ara exigeix que l'origen sigui *verificable*, no només declarat. La peça més ambiciosa és el **Reglament contra la desforestació**, el EUDR (Reglament UE 2023/1115). Per primera vegada, la llei obliga a aportar les **coordenades de geolocalització de la parcel·la exacta** d'on prové cada partida de set matèries primeres —bestiar boví, cacau, cafè, oli de palma, cautxú, soja i fusta— per garantir que no surtin de terres desforestades després del 31 de desembre de 2020 [5]. La mecànica és reveladorament concreta: per a parcel·les de més de quatre hectàrees cal un **polígon** de coordenades que en dibuixi el perímetre; per a les més petites n'hi ha prou amb un punt amb sis decimals; tot s'envia en format GeoJSON al sistema d'informació de la Unió. Les dates d'aplicació queden fixades el **30 de desembre de 2026** per als grans i mitjans operadors i el **30 de juny de 2027** per als més petits [6]. És, en una frase, el desplaçament de la prova «del paper a la terra».

No és l'únic exemple. La **Directiva de Medicaments Falsificats**, en vigor des del febrer de 2019, obliga que la majoria de medicaments de recepta portin un **identificador únic** —un codi 2D amb producte, número de sèrie, lot i caducitat— i un dispositiu antimanipulació, verificats contra un repositori

central europeu abans de dispensar-los [7]. I al món del luxe, el **Aura Blockchain Consortium**, com hem vist, ja ha registrat més de **cinquanta milions de productes** en una cadena de blocs que dona al comprador accés directe a la història i la prova d'autenticitat de la seva peça [8][9]. Tres respostes diferents, una mateixa intuïció: la confiança ha de poder demostrar-se.

Per què el segell sol no salva (i per què igualment cal)

Arribats aquí, cal ser implacablement honest, perquè aquest capítol toca vides. La serialització d'un medicament demostra que **la caps** és autèntica, no que **la molècula** de dins ho sigui. A Gàmbia, una foto segellada de la fàbrica no hauria detectat el dissolvent tòxic. És el principi que recorre tot el llibre, aquí en la seva forma més literal: «escombraries a l'entrada, escombraries a la cadena». Una prova d'existència d'una parcel·la **equivocada**, o d'un lot correcte amb un contingut adulterat, continua sent una mentida ben segellada.

Per què, doncs, val la pena? Perquè la immensa majoria del frau de la cadena de subministrament **no** és l'enverinament deliberat, sinó la **retrodatació** de certificats, la **substitució de documents**, la falsificació de l'origen i la reutilització de fotos d'una altra parcel·la o d'un altre any. Contra tot això, segellar l'acte d'origen és demolidor: eleva el cost de mentir, fixa responsabilitats amb nom i data, i deixa un rastre que un auditor pot resseguir fins a la font. La prova d'existència no substitueix el control de qualitat físic —el que hauria salvat els nens de Gàmbia—; el **complementa**, tancant la porta al frau documental perquè la inspecció es concentri en el que de debò importa: el contingut.

La prova d'existència a l'origen

Apliquem la mecànica de **t2p**. En el punt d'origen —la parcel·la, la collita, la fàbrica, el lot— es pren una fotografia georeferenciada i se segella en l'instant: una **empremta SHA-512** calculada al dispositiu, un **GPS forense** que fixa les coordenades, un **segell de temps RFC 3161** conforme a eIDAS i un ancoratge a la **blockchain pública**. Per al EUDR, això vol dir fotografiar la parcel·la amb el seu polígon o el seu punt de sis decimals i convertir la captura en **evidència inalterable** del moment i del lloc exactes. La **prova de vida** pot lligar l'evidència a la persona que fa la inspecció o la collita —l'inspector, el pagès—, reduint el frau de «ningú no pot segellar això sense ser-hi». I tot el conjunt s'empaqueta en un **contenidor .asice verificable fora de línia**, que un agent de duanes, un auditor o un comprador pot comprovar sense connexió i sense confiar en la paraula del proveïdor.

El més important és que la prova d'existència **no competeix** amb la serialització ni amb els passaports digitals; els complementa. El codi 2D del medicament i el passaport d'Aura diuen *quin* producte és; el segell d'origen de t2p afegeix la capa que falta: *aquest lot es va fotografiar aquí, en aquesta data, amb aquesta persona present*. És la diferència entre tenir una etiqueta de confiança i tenir la **prova de l'acte** que aquella etiqueta resumeix. Per al consumidor de luxe que escaneja el seu bolso i en veu la història, i per a l'agent de duanes que verifica un contenidor de cafè, la promesa és la mateixa: poder comprovar l'origen sense haver de creure ningú.

La promesa i el perill

La promesa és enorme i transversal. Una cadena de subministrament amb l'origen segellat seria molt més resistent a la falsificació documental, compliria el EUDR amb evidència real en lloc de declaracions, protegiria les marques honestes i, sobretot, donaria al ciutadà el dret de comprovar què compra. En un comerç on les falsificacions mouen prop de mig bilió de dòlars, recuperar la confiança en l'origen és un avantatge competitiu i una qüestió de salut pública.

El perill demana el matís de sempre, en la dualitat de «la promesa i el perill». El primer, ja explicat: el segell certifica l'acte, no la qualitat física; presentar-lo com a garantia de seguretat seria perillós i fals. El segon, la càrrega que pot recaure sobre els petits productors del Sud global, per a qui geolocalitzar cada parcel·la pot ser una barrera; el disseny ha de ser inclusiu, no un nou mur. I el tercer, la privacitat i la concentració: qui controla la capa de verificació no pot convertir-se en un nou intermediari únic. La prova d'existència és una eina necessària dins d'una arquitectura més àmplia que inclou, sempre, el control físic.

És hora d'actuar

Per als **productors i agricultors**: segellar l'acte d'origen —parcel·la, collita, lot— perquè la traçabilitat sigui demostrable i defensable davant del EUDR i dels compradors. Per als **importadors i marques**: exigir evidència ancorada com a base de la diligència deguda, no acceptar certificats retrodatats. Per als **reguladors i duanes**: reconèixer el valor probatori del segell i integrar-lo en els sistemes d'informació, sense oblidar mai el control físic del producte. Per als **consumidors**: poder escanejar i comprovar l'origen del que mengen, prenen o vesteixen. I per a tothom, recordar la lliçó de Gàmbia: l'origen verificable és necessari, però la seguretat del producte exigeix també analitzar-ne el contingut.

Setanta nens van morir amb una etiqueta autèntica a la mà. Cap tecnologia hauria d'arrogar-se el poder d'evitar tota tragèdia, però sí que podem fer que mentir sobre l'origen sigui molt més difícil i rastrejable. Demostrar d'on ve de debò una cosa —i qui se'n fa responsable— és, també aquí, time2act.

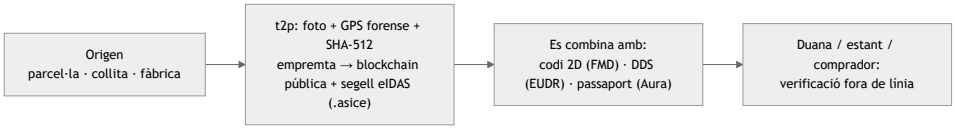


Figura 29.1 — En el punt d'origen (parcel·la, collita, fàbrica) es captura una foto georeferenciada que se segella amb GPS forense, segell de temps eIDAS i empremta SHA-512, i s'empaqueta en un contenidor .asice verificable fora de línia. Aquesta capa de prova de l'acte d'origen es combina amb la serialització (codi 2D del FMD), la declaració de diligència deguda del EUDR o el passaport digital d'Aura, fins a la verificació final a la duana o a l'estant. Fonts: EUDR (UE 2023/1115); EMA; Aura Blockchain Consortium.

---

[1] OCDE / EUIPO — *Mapping Global Trade in Fakes 2025* (falsificacions: 467.000 M$ el 2021, 2,3 % de les importacions mundials; UE 4,7 %). https://www.oecd.org/en/publications/mapping-global-trade-in-fakes-2025_94d3b29f-en.html ↩

[2] Organització Mundial de la Salut — *Substandard and falsified medical products* (≥1 de cada 10 als països de renda baixa/mitjana; ~30.500 M$/any). https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products ↩

[3] OMS — *Medical Product Alert Nº6/2022* (Gàmbia; xarops de Maiden Pharmaceuticals contaminats amb 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* (Índia; xarop «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 — *Reglament (UE) 2023/1115* (EUDR; coordenades de geolocalització de parcel·les; 7 matèries primeres; data de tall 31-des-2020). https://eur-lex.europa.eu/eli/reg/2023/1115/oj/eng ↩

[6] Comissió Europea (Access2Markets) — *Delay until December 2026 — implementation of the EUDR* (segona pròrroga, Reg. UE 2025/2650; aplicació 30-des-2026 / 30-juny-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 únic 2D obligatori des del 9-feb-2019). https://www.ema.europa.eu/en/human-regulatory-overview/public-health-threats/falsified-medicines-overview ↩

[8] Aura Blockchain Consortium — *About* (fundat el 2021 per LVMH, Prada i Cartier; >50 M de productes registrats). https://auraconsortium.com/about ↩

[9] WWD — *Aura Blockchain crosses 50 million products* (LVMH, Prada, OTB; setembre 2024). https://wwd.com/business-news/technology/aura-blockchain-crosses-50-million-products-lvmh-prada-otb-1236606994/ ↩

Consum: ressenyes falses, preus inflats i garanties amb rellotge

«La publicitat tracta de relacions socials, no d'objectes. La seva promesa no és de plaer, sinó de felicitat: la felicitat jutjada des de fora pels altres.»

— John Berger, Ways of Seeing (1972)

Abans de comprar res, fas el que fa tothom: llegeixes les ressenyes. Cinc estrelles, «m'ha canviat la vida», milers de valoracions que semblen la veu col·lectiva d'una multitud satisfeta. El que potser no saps és que darrere d'aquella unanimitat hi pot haver una indústria. El juliol de 2022, Amazon va demandar els administradors de més de 10.000 grups de Facebook dedicats a orquestrar ressenyes falses a canvi de productes gratuïts o diners: un sol grup, «Amazon Product Review», tenia més de 43.000 membres; en un altre es pagaven 10 dòlars per ressenya; la trama operava a les botigues dels Estats Units, el Regne Unit, Alemanya, França, Itàlia, Espanya i el Japó, i esquivava la detecció de Meta canviant lletres de les paraules sensibles [2]. Des del 2020, Amazon havia reportat més de 10.000 grups a Meta; només la meitat havien estat eliminats [2].

Aquest capítol tracta la capa d'informació sobre la qual el consumidor decideix. D'on ve físicament el producte s'explica al capítol 29; qui paga els anuncis que ningú no veu, al capítol 56; què hi ha de debò dins del menjar, al capítol 101. Aquí les preguntes són les del carret de la compra: puc creure aquestes estrelles? aquest descompte és real? i si es trenca, podré demostrar quan i com? La resposta del llibre: tornar la data certa als tres senyals — la ressenya amb compra acreditada, la sèrie de preus segellada i la cronologia de garantia — amb **t2p**: l'empremta SHA-512 al dispositiu, l'ancoratge de l'empremta a la blockchain pública i el segell de temps RFC 3161/eIDAS complementari, dins d'un contenidor .asice [5]. Ni el mercat ni el consumidor no haurien de discutir mai més sobre records.

L'opinió fabricada

La demanda d'Amazon va posar xifres a un secret conegut: les opinions es fabriquen en massa i es venen com un producte més. Grups organitzats amb desenes de milers de membres, tarifes per ressenya, tècniques d'evasió per burlar els filtres de les plataformes [2] — la professionalització completa d'un frau que decideix compres cada segon.

La resposta regulatòria ha arribat. Als Estats Units, la norma final de la FTC — anunciada el 14 d'agost de 2024, en vigor des del 21 d'octubre de 2024 — prohibeix comprar o vendre ressenyes falses, les ressenyes d'«insiders» sense revelar la relació, les webs de ressenyes «independents» controlades per la mateixa empresa, la supressió selectiva de ressenyes negatives i la compravenda d'indicadors falsos d'influència social, amb sancions de fins a 51.744 dòlars per infracció [1].

Però la llei, tota sola, no resol el problema epistemològic: el lector continua sense poder distingir, estrella a estrella, qui ha tocat el producte i qui cobra per opinar. I amb la IA generativa, el cost de fabricar mil opinions versemblants — amb tocs humans, detalls d'ús inventats i to de veí sincer — tendeix a zero.

La sortida no és creure menys: és poder verificar més. Si cada ressenya pot anar lligada a una prova de compra segellada — el justificant empremtat al dispositiu del comprador, sense revelar-ne la identitat [5] —, la plataforma pot distingir, i el lector filtrar, l'opinió de qui va comprar de debò. Pots comprar mil opinions; no pots fabricar mil compres segellades abans d'escriure-les. L'estrella deixa de ser un acte de fe.

El descompte que no ho era

El segon senyal fabricat és el preu «d'abans». L'OCU ho ha mesurat en les seves anàlisis del Black Friday, i el panorama és desolador: només un de cada tres productes s'abarateix de debò; en categories com rellotges intel·ligents, càmeres i auriculars, els preus pugen de mitjana un 13 % les setmanes prèvies a la campanya; el 43 % dels productes dispara el preu durant la campanya mateixa; l'estalvi mitjà anunciat és del 23 %, però els preus reals surten de mitjana un 3 % més cars [3]. I la dada reglamentària: en el 99 % dels casos, el «preu anterior» indicat no és el menor dels últims 30 dies, com exigeix la normativa de rebaixes — molts comerços usen com a referència un «preu recomanat pel fabricant» que sovint mai no ha estat el preu real de venda [3].

L'OCU pot detectar-ho perquè fa el que cap consumidor no pot fer sol: monitorar els preus des de principis de setembre [3]. I aquí és exactament on la prova d'existència canvia el joc: la norma existeix, però la seva verificació és inaccessible per al ciutadà — caldria haver vigilat el preu cada dia.

La sèrie de preus ancorada ho fa per tothom: si els preus es registren amb captures segellades — cada preu, cada dia, amb data certa [5] —, per la plataforma mateixa, per observatoris de consum o per la ciutadania organitzada, el «preu anterior» esdevé un fet verificable en un clic, i el descompte fals, una infracció demostrable. El cartell del «−70 %» deixa de ser una declaració de fe: o resisteix la sèrie, o retrata qui el penja. I per al comerç honest, el mateix segell és màrqueting — el descompte verificable val més que l'inflat del costat.

La garantia amb rellotge

El tercer senyal és la promesa que, si falla, respondran. El marc espanyol vigent és dels més protectors d'Europa: des de l'1 de gener de 2022 — transposant les directives europees —, la garantia legal mínima és de tres anys per als béns (dos per a continguts i serveis digitals); durant els dos primers anys es presumeix que el defecte és d'origen (un any per a productes de segona mà); els fabricants han de garantir recanvis durant deu anys des que el producte deixa de fabricar-se; i el termini per reclamar és de cinc anys [4].

A la pràctica, però, la garantia és una cursa de proves contra el rellotge. Quan vas comprar? — el tiquet ha desaparegut entre factures. Com va arribar? — la ratllada «ja hi era» o «l'has feta tu». Quan vas avisar del defecte? — dins de la presumpció dels dos anys, o fora. Quantes vegades s'ha reparat? Cada pregunta sense prova és una reclamació que mor davant del servei postvenda.

L'aplicació de la prova d'existència és directa. El tiquet i la factura, segellats el dia de la compra, fixen amb data certa l'inici dels tres anys [4][5]: el paper perdut deixa de ser fatal. L'estat del producte en el lliurament — quatre fotos o trenta segons de vídeo empremtats al moment — és l'equivalent consumidor de l'inventari de lloguer: ni el transportista ni el comprador no poden reescriure com va arribar la caixa. I cada avís al venedor, ancorat, fixa si el defecte va aparèixer dins de la presumpció [4]. La garantia deixa de ser una batalla de memòria: no més lluites contra el rellotge — ara el rellotge treballa per a tu.

La prova d'existència aplicada

Una compra qualsevol, tres segells de deu segons — el tiquet, la caixa oberta, el primer avís — i cap discussió possible mesos després.

1. La ressenya amb compra acreditada

El comprador real segella el justificant de compra al seu dispositiu i publica la ressenya acompanyada de la prova: l'empremta que acredita que la compra existeix, sense revelar ni el nom ni les dades del comprador [5]. La plataforma marca aquestes opinions amb un distintiu verificable; el lector filtra per «compra acreditada»; i el mercat negre de ressenyes [2] perd la seva matèria primera. La norma de la FTC posa les multes [1]; la prova d'existència posa el mecanisme que les fa gairebé innecessàries.

2. La sèrie de preus que no menteix

Observatoris de consum, plataformes honestes o la ciutadania organitzada registren els preus amb captures segellades — cada preu, cada dia, amb data certa [5]. Quan arriba la campanya de descomptes, el «preu anterior» es contrasta contra la sèrie ancorada: si el 99 % dels cartells no resisteix la regla dels 30 dies [3], que ho hagi de demostrar la sèrie, no la paciència del comprador. La transparència de preus deixa de dependre de la bona fe del cartell.

3. La caixa oberta amb data certa

El dia que arriba el paquet, trenta segons de vídeo o quatre fotos segellades al moment: l'estat del producte, el número de sèrie, el contingut de la caixa [5]. Si el producte va arribar danyat, la prova existeix des del minut u i el reemborsament no admet dilacions; si el comprador reclama un dany que ell mateix va causar, l'absència de prova coetània el retrata. La guerra diària del comerç electrònic — els danys de transport, el frau de devolucions — es resol sobre imatges amb integritat acreditada, en les dues direccions: el consumidor honest cobra abans, i el tramposo topa amb la criptografia.

4. El rellotge de la garantia

La compra segellada activa els tres anys amb data certa [4][5]; el primer avís de defecte, ancorat, fixa si el problema va aparèixer dins de la presumpció dels dos anys [4]; i cada reparació successiva queda datada, de manera que el producte que encadena avaries dins de garantia — el candidat a substitució o reemborsament — porta la seva pròpia cronologia. Per al venedor diligent, el mateix registre és la defensa contra la reclamació extemporània. La garantia més llarga d'Europa [4] val el que valgui la seva prova — i ara la prova és automàtica.

Els límits, dits amb claredat: el segell acredita que la compra, la foto o l'avís existien en una data — no acredita que la ressenya sigui sincera (un comprador real també pot cobrar per opinar), ni que el producte sigui bo, ni resol qui té raó en un defecte tècnic: això ho fan pèrits, plataformes i tribunals de consum. I la ressenya amb compra acreditada ha de preservar sempre l'anonimat del comprador: acreditar la compra, mai identificar la persona [5].

La promesa i el perill

La promesa: un mercat on les estrelles tenen compra al darrere [1][2], els descomptes resisteixen la regla dels 30 dies [3] i la garantia de tres anys s'exerceix sense guardar tiquets en una capsa de sabates [4]. Confiança de consum amb base verificable: més barata per a l'honest, més cara per al tramposo.

Els perills, amb la mateixa claredat.

El primer és **l'anonimat del comprador**. Acreditar la compra no pot significar identificar la persona. Si el distintiu de «compra acreditada» exigís nom i perfil, hauríem canviat ressenyes falses per vigilància de consumidors. El disseny correcte: la prova criptogràfica de la compra viatja; la identitat, mai [5].

El segon és **la censura per verificació**. Si les plataformes només publiquessin ressenyes amb compra acreditada, silenciarien veus legítimes — el regal rebut, la compra en una altra botiga, l'experiència de servei. El distintiu ha de filtrar i ponderar, no censurar: opinió lliure per a tothom, pes verificable per a qui l'acrediti.

El tercer és **el segell comprat**. El frau s'adapta: venedors que «venen» productes a preu simbòlic per collir compres acreditades, sèries de preus segellades per botigues fantasma. El segell acredita fets, no bona fe — la vigilància de patrons (compres massives, preus impossibles) continua sent feina de plataformes i reguladors [1][3].

I el quart és **el tecnosolucionisme de consum**. Cap empremta no farà els productes millors ni els preus més justos; això ho fan la competència, la inspecció de consum i les normes que ja existeixen [1][3][4]. El segell només garanteix que les regles del joc es puguin verificar. Un mercat pot ser perfectament transparent i perfectament car.

És hora d'actuar

El consumidor decideix amb senyals; que els senyals tornin a ser de fiar.

Per a tu, consumidor: segella el tiquet el dia de la compra, la caixa el dia del lliurament i el primer avís de defecte [4][5]; davant d'un descompte espectacular, recorda la dada — només un de cada tres és real [3]; i davant de mil estrelles unànimes, busca la compra acreditada [2].

Per a les plataformes de comerç i ressenyes: implanteu la ressenya amb compra acreditada i anònima [1][2][5] i publiqueu sèries de preus ancorades — la credibilitat és el vostre producte.

Per als comerços honestos: el descompte verificable contra la sèrie segellada [3][5] és el vostre millor argument contra el cartell inflat del costat.

Per a les autoritats de consum: exigiu la regla dels 30 dies contra sèries de preus ancorades [3] i accepteu la cronologia segellada — compra, desembalatge, avisos — com a prova preferent en les reclamacions de garantia [4].

Per als reguladors: la norma de la FTC marca el camí [1]; completeu-la amb el mecanisme — presumpció de validesa per a la compra acreditada anònima i sancions per als indicadors socials fabricats.

Deu dòlars per ressenya, 43.000 membres en un sol grup [2]: la confiança del consumidor s'havia convertit en mercaderia. Que torni a ser el que era — un senyal honest entre desconeguts. Pel carret de la compra de cada dia, **time2act**.

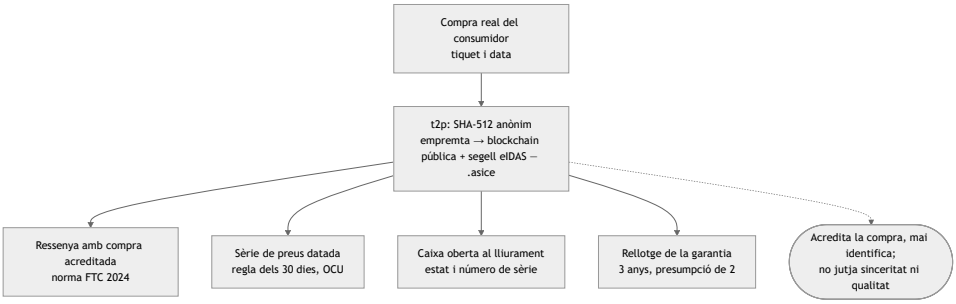


Figura 30.1 — La capa d'informació del consumidor amb prova d'existència: la ressenya amb compra acreditada i anònima (el justificant segellat al dispositiu; el mercat negre de ressenyes es queda sense matèria primera), la sèrie de preus amb data certa (la regla del menor preu dels 30 dies esdevé verificable) i el rellotge de la garantia (compra, unboxing i avisos segellats activen i acrediten els 3 anys legals). Límits: el segell no jutja la sinceritat ni la qualitat; l'acreditació de compra mai no pot identificar el comprador. Fonts: FTC (norma 2024); Amazon vs. grups de Facebook; OCU (Black Friday); CEC/Consum (garantia de 3 anys).

---

[1] Federal Trade Commission — *FTC Announces Final Rule Banning Fake Reviews and Testimonials* (14 d'agost de 2024; en vigor el 21 d'octubre de 2024; fins a 51.744 $ per infracció; prohibeix la compravenda de ressenyes, les ressenyes d'insiders sense revelació, les webs de ressenyes controlades, la supressió selectiva i els indicadors falsos d'influència 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 juliol de 2022; més de 10.000 grups; EUA, Regne Unit, Alemanya, França, Itàlia, Espanya i Japó); Marketing4eCommerce — *Amazon denuncia a los administradores de más de 10.000 grupos de Facebook* («Amazon Product Review», més de 43.000 membres; 10 $ per ressenya; més de 10.000 grups reportats a Meta des de 2020, la meitat eliminats); 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* (només 1 de cada 3 productes s'abarateix; pujades mitjanes del 13 % en les setmanes prèvies en categories com rellotges intel·ligents, càmeres i auriculars; el 43 % dels productes dispara el preu; estalvi anunciat del 23 % vs preus reals un 3 % més cars; en el 99 % dels casos el «preu anterior» no és el menor dels últims 30 dies; monitoratge des de setembre); 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] Centre Europeu del Consumidor a Espanya (Ministeri de Consum) — *España amplía la garantía legal mínima de dos a tres años* (des de l'1 de gener de 2022; transposició de les Directives (UE) 2019/770 i 2019/771; presumpció d'origen del defecte ampliada de 6 mesos a 2 anys — 1 any per a segona mà —; recanvis durant 10 anys; prescripció de 3 a 5 anys); 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 producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; acreditació sense identificació — la prova de compra viatja, la identitat mai; contingut al dispositiu i revelació voluntària). Vegeu els capítols 13 i 15; l'origen del producte, al capítol 29. ↩

La segona mà entre particulars: l'estat de l'article, amb data certa

«La màxima és: doveriai, no proveriai — confia, però verifica.»

— Ronald Reagan (amb Gorbatxov), signatura del Tractat INF (1987)

El comprador obre la caixa que acaba d'arribar. Dins, on hi havia d'haver una consola, hi ha una rajola embolicada amb paper de diari. A l'altra punta del país, un venedor rep una devolució «per defectes» i descobreix que el mòbil retornat no és el que va enviar: una altra carcassa, una pantalla amb marques d'anys. Dues víctimes del mateix buit: entre desconeguts, l'estat d'un objecte en un moment donat no el pot provar ningú.

I el buit és de país sencer [1]: només Wallapop té més de 19 milions d'usuaris actius a Espanya, i el mercat de segona mà entre particulars mou més de 13.000 milions d'euros anuals. La cara fosca: les estafes en aquestes plataformes són el gruix dels més de 412.000 fraus informàtics registrats el 2024, les denúncies van créixer un 60 % el 2025, i la Guàrdia Civil alerta periòdicament de les campanyes [1].

Aquest capítol tracta el contracte més informal de l'economia: la compravenda entre desconeguts. Les ressenyes falses i la garantia del comerç són al capítol 30; el client davant la gran companyia, al capítol 33; l'anunci fals de lloguer, al capítol 36; i el pagament fora de plataforma enganyat — recuperar una transferència — es tracta al capítol 69. Pregunta clau: com es prova en quin estat era un objecte quan va canviar de mans? Resposta: documentant-lo amb data certa als dos extrems del viatge — el vídeo abans d'enviar i el vídeo en obrir — amb **t2p**: la tríada del capítol 13 — empremta al dispositiu, hora certa i àncora a la cadena [3]. La simetria és total: el mateix gest desarma el paquet que no és el promès i el «cambiazo» de la devolució.

Les estafes simètriques

El repertori està documentat [1], i val la pena mirar-lo de cara.

El **pagament fora de plataforma**: l'anunci amb fotos impecables i un preu massa bo, i la insistència a cobrar per Bizum o transferència «per estalviar comissions». Pagat el diner, no arriba res — o arriba qualsevol cosa — i el comprador ha perdut la protecció de la plataforma pel camí: el pagament ja viu fora del seu marc de garanties. (El component bancari — recuperar la transferència enganyada — és matèria del capítol 69.)

El **frau per triangulació i el «cambiazo»**: l'estafador compra amb enviament, rep l'article en bon estat i presenta immediatament una queixa al·legant defectes — aprofitant la protecció que reté el pagament fins que el comprador valida. Demana la devolució, es queda l'article bo i en retorna un altre de tronat. El venedor honest es queda sense diners i sense el seu producte — i davant de la plataforma, només té la seva paraula.

El **phishing del «confirma el pagament»**: l'enllaç que imita la interfície de la plataforma i pesca credencials; i les **etiquetes d'enviament fraudulentes** i suplantacions que vesteixen l'engany de legitimitat [1].

El diagnòstic probatori: la compravenda entre particulars no té factura ni garantia comercial — el vici ocult civil és l'únic recurs de fons — i tota l'evidència viu en fotos d'anunci sense data fiable, xats i seguiments ambigus. Quan la plataforma arbitra, decideix amb això: paraules i imatges que qualsevol pot fabricar o reutilitzar. El desconegut honest no té manera de distingir-se del desconegut estafador — i aquesta és exactament la classe de problema que la data certa resol.

La prova d'existència aplicada

Deu segons a cada extrem del viatge [3].

1. L'article documentat abans d'enviar

El venedor filma l'article amb t2p abans d'empaquetar: l'estat general, el número de sèrie, comprovant-ne el funcionament si escau — amb la data i l'hora sobreimpreses al vídeo i el GPS forense del lloc [3]. Trenta

segons que fixen un fet: aquest objecte, en aquest estat, existia així en aquest moment. La foto de l'anunci pot ser vella o d'un altre; el vídeo certificat, no.

2. El precintat en pla seqüència

L'article entrant a la caixa, el tancament, l'etiqueta d'enviament enganxada — un sol pla, sense talls, certificat [3]. És el gest que desarma el «dins no hi havia res»: el contingut i el paquet queden lligats en un mateix vídeo datat. Per als articles de valor, és la diferència entre una disputa perduda i una tancada en cinc minuts.

3. L'obertura simètrica

El comprador fa el mateix gest a l'altre extrem: el paquet tancat amb l'etiqueta visible, l'obertura, el contingut — en pla seqüència certificat [3]. Si dins hi ha la rajola, el vídeo ho acredita amb data i lloc; si l'article és el promès, també. I contra el «cambiazo» [1], la parella de vídeos — el precintat del venedor i l'obertura del comprador, i els de la devolució en sentit contrari — converteix l'arbitratge en una comparació: què va sortir, què va arribar, què es va retornar.

4. L'expedient de la disputa

L'anunci capturat amb data — les fotos i la descripció que es van prometre —, el xat amb l'acord, el justificant de pagament, el seguiment de l'enviament: agrupats en un projecte [3] i exportables com a paquet .asice verificable sense connexió. Per a l'arbitratge de la plataforma, per a la denúncia a la Guàrdia Civil [1], per a la reclamació civil: fets datats en lloc de captures discutibles.

I un cosí germà d'aquesta economia entre particulars que mereix el seu paràgraf: el préstec entre família i amics. El «t'ho vaig deixar» que anys després esdevé «era un regal» ha trencat més amistats que cap estafa. L'acord breu segellat en el moment de deixar els diners — l'import, el pacte de retorn, dues línies amb data certa [3] — protegeix el prestador i, sobretot, protegeix la relació: quan els termes són un fet, la memòria no ha de fer d'àrbitre.

Els límits, abans que ningú es faci il·lusions: el segell acredita estats i moments — no decideix si el preu era just ni si el defecte era vici ocult: això ho valoren la plataforma, el pèrit o el jutge. La proporcionalitat mana: la venda de 10 euros no necessita expedient; la de 500, potser sí — que cada u calibri. I mai no es grava el repartidor ni cap tercer: es documenta l'objecte, no les persones.

La promesa i el perill

La promesa: disputes que es resolen per comparació de vídeos datats i no per la intuïció d'un moderador [1][3]; el «cambiazo» que deixa de ser rendible perquè l'article retornat es contrasta amb el precintat; venedors i compradors honests que es distingeixen dels estafadors amb un gest de deu segons; i un mercat de 13.000 milions [1] que guanya la confiança que li faltava per créixer.

Els perills, sense embuts.

El primer és **el teatre probatori**. L'estafador també pot filmar: un vídeo amb l'article bo i l'enviament d'un altre. Per això el mètode importa: el pla seqüència sense talls fins a l'etiqueta, el GPS forense que no admet ubicacions simulades [3], i la parella simètrica de vídeos — un teatre ha d'enganyar les dues càmeres i les dues dates alhora, i això ja no és un timo barat.

El segon és **la fricció que mata la venda**. Si vendre un llibre de segona mà exigeix un rodatge, ningú no ho farà. La resposta és la proporcionalitat: el gest curt per a les vendes normals, l'expedient complet per a les valuoses — i les plataformes integrant-ho perquè costi un clic.

El tercer és **la plataforma com a jutge opac**. Els arbitratges interns decideixen amb regles pròpies i sense apel·lació real. La traça verificable els posa fàcil decidir bé; el pas de fons és que valorin evidència ancorada per sobre de captures — i que ho diguin a les seves normes.

I un últim parany: refiar-se que l'eina vigili per tu. Cap segell no substitueix la prudència elemental: pagar dins de la plataforma, desconfiar del Bizum a desconeguts i dels enllaços de «confirmació» [1]. La data certa protegeix la transacció legítima; l'estafa del pagament per fora es combat no picant.

És hora d'actuar

Que el desconegut honest guanyi sempre.

Per a venedors i compradors: el gest de deu segons a cada extrem — l'article, el precintat, l'obertura [3]; i per a les vendes que valen, l'expedient sencer.

Per a les plataformes: integreu l'evidència amb data certa als vostres arbitratges [1][3] — resoldreu més ràpid, expulsareu els professionals del «cambiazo» i el vostre segell de confiança serà alguna cosa més que màrqueting.

Per als transportistes: el pes i l'estat del paquet a l'admissió, ancorats — la vostra part de la cadena també compta.

Per a la Guàrdia Civil i les autoritats de consum: les denúncies creixen un 60 % l'any [1]; l'expedient .asice del ciutadà és la diferència entre arxivar i investigar.

Per als legisladors: la compravenda entre particulars és l'economia real de milions de persones [1]; que la protecció del consumidor digital reconegui l'evidència ancorada — de les dues parts — com a prova qualificada.

El pròxim paquet que enviïs o rebis, que porti el seu moment de veritat gravat. Per un mercat de veïns on el desconegut honest guanyi sempre, **time2act**.

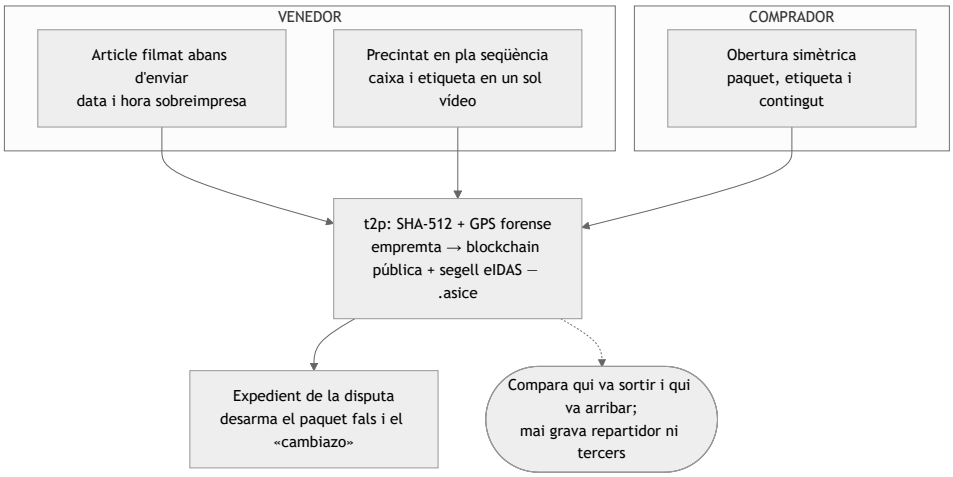


Figura 31.1 — La segona mà entre particulars amb prova d'existència (segellat amb t2p — capítol 13): l'article filmat abans d'enviar (data/hora sobreimpresa + GPS forense), el precintat en pla seqüència, l'obertura simètrica del comprador i l'expedient de la disputa (anunci capturat, xat, pagament, seguiment). Simetria total: desarma el paquet fals I el «cambiazo». Context: >19 M d'usuaris a Wallapop; >13.000 M€/any; les estafes de segona mà, gruix dels >412.000 fraus informàtics del 2024 (+60 % de denúncies el 2025). Límits: proporcionalitat segons valor; el vici ocult el valora el pèrit; mai gravar tercers. Fonts: Guàrdia Civil/premsa especialitzada.

---

[1] Digital Perito — *Estafas en Wallapop y Vinted: cómo denunciar con pruebas* (>19 milions d'usuaris actius a Wallapop a Espanya; mercat de segona mà >13.000 M€ anuals; les estafes de plataformes de segona mà com a gruix dels >412.000 fraus informàtics de 2024; +60 % de denúncies el 2025); Público — *Así operan los estafadores en plataformas de segunda mano* (tipologies: pagament fora de plataforma, triangulació/«cambiazo» aprofitant la protecció al comprador, phishing, etiquetes fraudulentes, suplantació); OKDiario / Genbeta — alertes de la Guàrdia Civil i trucs de detecció. 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] Marc civil de la compravenda entre particulars (vici ocult; absència de garantia comercial de consum). Vegeu el capítol 30 per a la garantia B2C i el capítol 36 per a l'estafa de l'anunci fals.

[3] t2p — manual de producte (vídeo amb data/hora sobreimpresa; foto amb GPS forense — fix genuí ~50 m / ≤30 s, la ubicació simulada bloqueja la certificació; captura de pantalla certificada; certificar qualsevol fitxer; projectes per agrupar l'expedient d'una venda; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; el pagament enganyat, al capítol 69. ↩

El lloguer de coses: l'estat en agafar i en tornar

«No siguis ni manllevador ni prestador, / que el préstec sovint es perd ell mateix i perd l'amic.»

— William Shakespeare, Hamlet, I, 3 (c. 1600)

L'aeroport, la cua del mostrador de lloguer, la volta ràpida al cotxe amb el full de danys a la mà — «aquesta ratllada ja hi és?» — i la tornada amb pressa: la bústia de claus, l'avió. Tres setmanes després, el correu: «càrrec per danys: 460 €», amb dues fotos fetes qui sap quan.

No és mala sort: és un patró documentat [1]. L'informe oficial sobre pràctiques irregulars de companyies espanyoles de lloguer descriu indemnitzacions desproporcionades — de 300 a 1.000 euros per ratllades o desperfectes petits — carregades directament a la targeta del dipòsit, amb el caràcter i la quantia fixats unilateralment per l'empresa; i el Centre Europeu del Consumidor documenta els càrrecs posteriors per neteja o danys menors decidits en revisions fetes sense la presència del consumidor, que queda obligat a assumir-los sense coneixement exprés [1]. Hi ha hagut condemnes: un líder europeu del sector va ser condemnat a retornar danys cobrats indegudament [1].

I la ironia que fa el capítol: el mateix CEC recomana tornar el cotxe amb l'oficina oberta, revisar-lo amb el personal i «fer fotografies de l'interior i l'exterior... podran servir com a prova» [1]. El regulador ja ha entès que això va de proves; el que falta és que les fotos del consumidor valguin tant com la inspecció de l'empresa.

Aquest capítol tracta el contracte sobre l'estat d'una cosa. L'inventari bilateral del pis llogat és al capítol 36; l'estat de la cosa venuda entre particulars, al capítol 31; el cotxe compartit entre iguals, al capítol 26; el càrrec que torna i la reclamació a la companyia, al capítol 33; la devolució del rebut a la targeta, al capítol 69. Pregunta clau: com es discuteix l'estat d'una cosa en dos moments si cap dels dos moments no té registre oposable? Resposta: amb el vídeo d'estat als dos extrems del lloguer — en agafar i en tornar — segellat amb **t2p** — la mecànica de sempre, la del capítol 13 [2]. I amb la simetria de sempre: la mateixa traça protegeix l'empresa honesta del client que nega el cop.

L'asimetria del mostrador

El problema, peça a peça. El **full de danys inicial**: un dibuix amb creuetes que el client signa amb pressa, sovint sense llum ni temps per repassar-lo. La **franquícia i el dipòsit**: la targeta retinguda que permet cobrar primer i discutir després. La **inspecció de tornada**: quan l'oficina és tancada o el client ja vola, l'estat el determina l'empresa sola, sense contrapès [1]. El **preu del desperfecte**: barems interns, no pressupostos — la ratllada valorada en centenars d'euros segons una taula que el client no ha vist mai [1]. I la **distància**: el turista estranger que no tornarà per reclamar.

L'extensió B2B reprodueix el mateix esquema amb imports més grossos: el lloguer de maquinària d'obra i d'equips professionals — l'estat inicial de la retroexcavadora, les hores d'ús, el dany «descobert» al retorn — sovint entre empreses que es necessitaran l'una a l'altra la temporada següent.

El diagnòstic probatori: el lloguer és un contracte sobre l'estat d'una cosa en dos moments — i cap dels dos moments no té, avui, un registre que valgui per a les dues parts. Les fotos del client no tenen data oposable; la inspecció de l'empresa no té el client davant. Quan el càrrec arriba, la discussió és la de sempre: la teva paraula contra la seva targeta.

La prova d'existència aplicada

Dos minuts a cada extrem del lloguer [2].

1. La volta d'agafada

Abans de sortir del pàrquing, la volta completa filmada amb t2p: la carrosseria sencera, les llantes, l'interior, el quadre amb els quilòmetres i el nivell de combustible — amb la data i l'hora sobreimpreses i el GPS forense del pàrquing (fix genuí, precisió d'uns 50 metres; una ubicació simulada bloqueja la certificació) [2]. Cada ratllada preexistent, documentada; el full de creuetes, escanejat i segellat. Dos minuts que valen exactament el que l'empresa vulgui reclamar després.

2. La volta de tornada

El mateix gest en tornar — i aquí és on es guanya o es perd tot: en la devolució fora d'hores, amb la bústia de claus i ningú de l'empresa davant [1], el vídeo certificat de l'estat final és l'única inspecció amb data certa que existirà. El càrrec de tres setmanes després [1] topa amb un fet: així estava el cotxe el dia que el vaig tornar, a aquesta hora, en aquest pàrquing.

3. El contracte i el càrrec

El contracte, l'inventari d'estat i les condicions de la franquícia, escanejats i segellats en signar [2]; i quan el càrrec tardà arriba, la reclamació datada — a l'empresa, al mediador de consum, i si cal la devolució del rebut al banc, el camí que el capítol 69 explica. L'expedient .asice — voltes, contracte, càrrec, reclamació — verificable sense connexió per qualsevol [2].

4. La simetria del llogador honest

L'empresa — o el particular que lloga la seva màquina — que documenta amb el client davant té la mateixa protecció: la inspecció d'entrega i la de retorn, filmades i segellades, amb el client present o notificat [2]. Contra el client que nega el cop nou, la parella de vídeos respon; i el barem del desperfecte, publicat i ancorat per endavant, converteix el preu de la ratllada en una condició coneguda, no en una sorpresa. Al B2B de la maquinària, aquest expedient bilateral és senzillament la diferència entre conservar un client i perdre'l en un plet.

Els límits, negre sobre blanc: el segell acredita estats i moments — no valora si el desperfecte és ús normal o dany, ni si el preu és proporcionat: això ho diuen el contracte, el mediador i el jutge [1]. La volta filmada ha de ser completa i amb llum — un vídeo fosc segella la seva pròpia inutilitat. I la proporcionalitat de sempre: el patinet de deu euros no necessita expedient; el cotxe amb franquícia de 1.200, sí.

La promesa i el perill

La promesa: consumidors que tornen el cotxe fora d'hores amb la tranquil·litat d'un fet datat [1][2]; càrrecs tardans que moren en veure l'expedient; empreses honestes que liquiden danys reals amb evidència bilateral i es desmarquen de les males pràctiques que embruten el sector [1]; i el lloguer de coses — del cotxe de vacances a la retroexcavadora — funcionant sobre estats verificables.

I els perills, un per un.

El primer és **el vídeo de mala fe**: filmar esquivant el cop que ja has fet. El mètode ho combat: la volta completa en pla seqüència, la data sobreimpresa, el GPS del pàrquing [2] — i la parella de vídeos: el que amaga un cop a la seva volta, l'ensenya a la de l'altre extrem.

El segon és **la fricció del mostrador**. Si agafar un cotxe exigeix un ritual, el client no ho farà. Dos minuts, un gest guiat — i les empreses que ho integrin al seu propi procés (la volta conjunta filmada) ho convertiran en argument de venda.

El tercer és **el barem unilateral que sobreviu**. La prova de l'estat no arregla el preu abusiu de la ratllada [1]: això és feina del regulador de consum i dels jutges. La data certa fa la disputa neta; la justícia del barem és una altra batalla.

Queda el quart: la temptació de delegar-ho tot al segell. Cap segell no substitueix tornar el cotxe amb l'oficina oberta quan es pot [1], ni llegir la franquícia abans de signar. La prova és per quan la prudència no basta.

És hora d'actuar

Que l'estat de la cosa tingui dos testimonis: un a cada extrem.

Per a tu, que llogues: la volta de dos minuts als dos extrems [2] — i si tornes fora d'hores, no te la saltis mai: és l'única inspecció que tindràs.

Per a les empreses de lloguer: inspeccions bilaterals filmades i barems publicats per empremta [1][2] — el càrrec documentat es cobra sense discussió, i el sector es neteja de la fama que l'acompanya.

Per al lloguer professional i de maquinària: l'expedient d'entrega i retorn com a annex estàndard del contracte [2]; els plets d'estat són els més evitables del vostre negoci.

Per a les autoritats de consum i el CEC: ja recomaneu les fotos [1]; el pas següent és reconèixer l'evidència amb data certa del consumidor com a contrapès formal de la inspecció unilateral.

Per als legisladors: la revisió sense el client present i el càrrec unilateral a la targeta [1] són el forat; que tot càrrec per danys exigeixi evidència d'estat verificable dels dos moments.

La pròxima bústia de claus d'aeroport, que no sigui un acte de fe. Dos minuts de vídeo, i el cotxe tornat queda tornat — per a tots dos. Pel lloguer sense sorpreses, **time2act**.

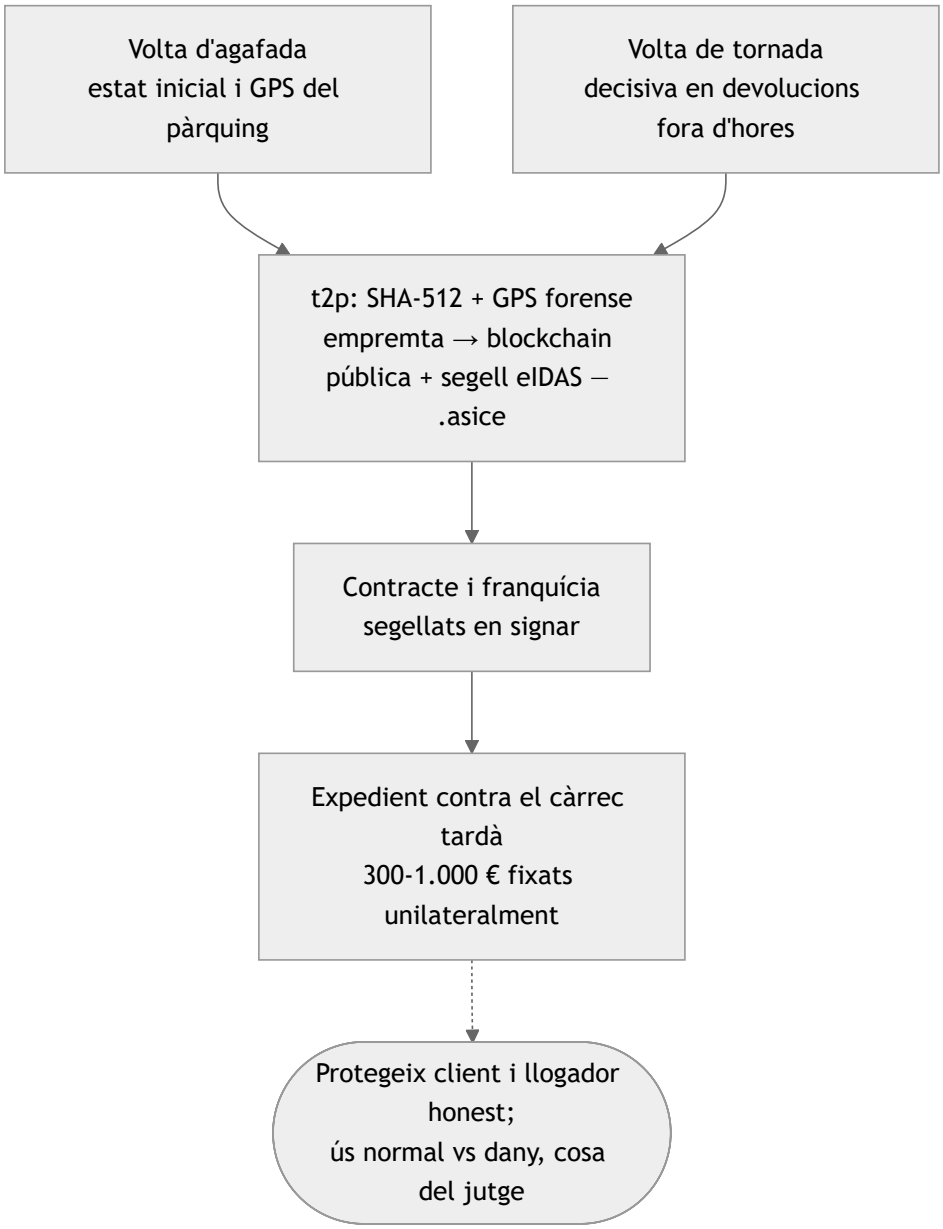


Figura 32.1 — El lloguer de coses amb prova d'existència (segellat amb t2p — capítol 13): la volta d'agafada filmada (data/hora sobreimpresa + GPS forense del pàrquing), la volta de tornada — decisiva en devolucions fora d'hores —, el contracte i la franquícia segellats, i l'expedient contra el càrrec tardà. Simetria: la inspecció bilateral protegeix l'empresa honesta del client que nega el cop; extensible al lloguer de maquinària B2B. Context: pràctiques irregulars documentades (càrrecs de 300-1.000 € fixats unilateralment; revisions sense el client); el CEC ja recomana fotos — hi faltava la data certa. Límits: ús normal vs dany i preus, cosa del contracte i el jutge. Fonts: Consumo/DSCA; CEC-España.

---

[1] Direcció General de Consum (DSCA) — *Prácticas irregulares de compañías españolas de alquiler de coches* (indemnitzacions desproporcionades de 300 a 1.000 € per ratllades o desperfectes petits, carregades a la targeta del dipòsit amb quantia fixada unilateralment); CEC-España (Centre Europeu del Consumidor) — *Alquiler de vehículos: derechos y*

recomendaciones (càrrecs posteriors per neteja o danys menors; revisions sense la presència del consumidor; recomanacions: tornar amb l'oficina oberta, revisar amb el personal, demanar justificant i «fer fotografies de l'interior i l'exterior com a prova»); 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 producte (vídeo amb data/hora sobreimpresa; foto amb GPS forense — fix genuí ~50 m / ≤30 s, la ubicació simulada bloqueja la certificació; escàner de documents; projectes per agrupar l'expedient d'un lloguer; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; l'inventari del pis, al capítol 36; l'estat de la cosa venuda, al capítol 31; el càrrec a la targeta, al capítol 69. ↩

El client contra la companyia: la baixa, la permanència i el call center

«Si el pilar principal del sistema és viure en la mentida, no és estrany que l'amenaça fonamental contra ell sigui viure en la veritat.»

— Václav Havel, El poder dels sense poder (1978)

La música d'espera, un quart d'hora llarg, i per fi una veu: «truqui demà, que ara el sistema no em funciona». L'endemà, una altra veu: «li passo amb el departament de retencions». Una oferta, una promesa — «li mantenim el preu i la baixa queda anotada» — i la sensació d'haver acabat. Tres mesos després, el càrrec continua arribant, i el servei d'atenció al client respon amb tota la tranquil·litat del món: «no consta cap sol·licitud de baixa». Ningú no recorda exactament què es va dir; només queda un acord verbal que mai no s'ha materialitzat.

És la queixa de consum més quotidiana del país, i el desequilibri que l'alimenta és estructural: la companyia grava cada trucada «per garantir la qualitat del servei» — però la gravació la té ella; el codi de la reclamació el genera el seu sistema; el registre de la baixa viu als seus servidors. Quan la disputa arriba, el client aporta la seva memòria; la companyia, la seva base de dades. La Llei 10/2025 acaba de donar drets nous al consumidor [1] — però un dret sense prova pròpia és un dret que depèn de la bona fe de l'altre.

Aquest capítol tracta la relació probatòria del client amb la gran companyia de serveis: la baixa, la permanència, el càrrec que torna, la promesa del call center. Les ressenyes, els preus i la garantia del producte són al capítol 30; la relació amb l'Administració pública, al capítol 44; la licitud i la tècnica de gravar les converses pròpies — la STC 114/1984 —, al capítol 75; la veu clonada que truca fent-se passar per tu, al capítol 68. Pregunta clau: com s'exerceix un dret quan tota l'evidència viu a casa de l'adversari? Resposta: documentant cada gestió al moment amb **t2p** — el paquet probatori que el capítol 13 desgrana peça a peça [3] — de manera que la data certa quedi, per fi, també al costat del client. I amb la neutralitat de sempre: la mateixa traça acredita la companyia diligent que atén bé i tramita a temps.

Drets nous, prova vella: la Llei 10/2025

La novetat legislativa és de primer ordre [1]: la Llei 10/2025, de 26 de desembre, de serveis d'atenció a la clientela — publicada al BOE el 27 de desembre de 2025, amb dotze mesos perquè les empreses s'hi adaptin — imposa obligacions concretes i mesurables. Atendre el 95 % de les trucades en menys de tres minuts de mitjana. Assignar a cada consulta, queixa, reclamació o incidència un codi identificatiu que permeti seguir-ne l'estat. Respondre les reclamacions en quinze dies com a màxim — i en només cinc els càrrecs no autoritzats. Avisar amb quinze dies d'antelació de cada renovació automàtica, facilitant la cancel·lació. Fer la baixa senzilla, sense laberints: n'hi ha prou amb el DNI i el número de contracte. I prohibir l'atenció exclusivament automatitzada: el client té dret a un operador humà.

Sobre el paper, és un abans i un després. Però mira-ho amb els ulls d'aquest llibre i hi veuràs el forat: la llei dona drets; no dona proves. Qui acredita que la trucada va durar quaranta-set minuts? Que la baixa es va demanar el dia 3 i no el 28? Que el càrrec era no autoritzat i es va comunicar dins de termini? Que la renovació va arribar sense avís? El codi de seguiment el genera i el custodia la companyia; l'expedient sencer viu a les seves bases de dades. Un dret sense prova pròpia s'exerceix per cortesia de l'adversari — i la cortesia, en un call center amb objectius trimestrals, no és una garantia processal.

Quan el càrrec torna: els casos

Les sancions existeixen, i dibuixen el mapa del problema [2].

Vodafone va ser multada amb 20.000 euros per cobrar a una consumidora serveis de tercers que ella havia desconnectat: va vulnerar fins a tres vegades el seu dret de desconnexió i va obstruir la inspecció de consum; va acabar assumint la responsabilitat i pagant 20.100 euros amb la reducció legal. Movistar va rebre una multa de 20.000 euros després que una gestora de cobraments assetgés una consumidora per un deute fals de 1.741 euros — tres línies que mai no havia contractat. I Telefónica arrossega una multa de 765.000 euros, confirmada pel Tribunal Suprem, per limitar el dret dels seus clients a rebre la factura en

paper. A la mateixa llista de greuges, les associacions de consumidors mantenen denunciades les penalitzacions per baixa anticipada que consideren clàusules abusives [2].

La lliçó comuna és la d'aquest llibre: totes aquestes sancions van arribar perquè algú va poder documentar el que passava — i sovint després d'anys de lluita. Per cada cas que acaba en multa, quants moren a la primera trucada, quan el client no pot provar ni tan sols que va trucar? La normativa de consum reconeix el dret a la baixa en la mateixa forma en què es va contractar; el que hi falta és que el fet de demanar-la deixi un rastre verificable a les mans de qui la demana.

La prova d'existència aplicada

El mateix telèfon que fa la gestió pot segellar-la [3].

1. La baixa segellada

El client fa la gestió i la documenta al moment: la gravació de la seva pròpia trucada — conversa pròpia, lícita, com explica el capítol 75 —, la captura de pantalla certificada del formulari de baixa enviat o del xat amb el bot, el correu de confirmació escanejat [3]. Cada peça rep la seva empremta SHA-512 al dispositiu i la seva data certa. La sol·licitud de baixa del dia 3 esdevé un fet, digui el que digui el sistema de la companyia el dia 28 — i el certificat PDF amb codi QR s'adjunta a la reclamació de consum tal qual.

2. El contracte i les seves versions

Les condicions publicades el dia que vas contractar, capturades amb el navegador integrat de t2p — la imatge completa de la pàgina i el seu codi font, empaquetats i certificats [3]; el contracte escanejat, fins a 50 pàgines en un únic PDF; i cada modificació unilateral, capturada amb la seva data. Quan la tarifa «per sempre» puja al vuitè mes, la comparació és aritmètica: això deies, això dius.

3. La trucada i la promesa

La promesa verbal — «li mantenim el preu un any més si es queda» — gravada per qui la rep, amb el mode d'àudio que continua en segon pla [3], i segellada en penjar. L'oferta de retenció que després «no consta» deixa de ser indemostrable. I els projectes de l'app agrupen l'expedient sencer del cas — trucades, captures, correus — ordenat i datat [3].

4. L'expedient del client — i la simetria

Quan la reclamació arriba a consum o al jutjat, el client exporta el paquet .asice: cada peça amb la seva empremta, el seu segell de temps i les instruccions de verificació, comprovable per qualsevol sense confiar en ningú [3]. I la simetria de sempre: la companyia diligent — la que atén en dos minuts, tramita la baixa el dia 3 i respon en cinc dies — té en els seus propis registres ancorats la millor defensa contra la reclamació infundada i la millor evidència de compliment de la Llei 10/2025 [1].

I els límits, que també n'hi ha: el segell acredita gestions — què vas demanar, quan, què et van respondre —, no dona la raó de fons: si la penalització era procedent o la tarifa correcta, ho diran la llei i el jutge. La gravació és sempre de converses pròpies, mai de tercers, i la protecció de dades del teleoperador exigeix proporcionalitat: es documenta la gestió, no es persegueix la persona que atén. I cap empremta no substitueix la reclamació formal dins de termini.

La promesa i el perill

La promesa: el client que exerceix els drets de la Llei 10/2025 amb l'expedient a la mà [1][3]; reclamacions de consum que es resolen sobre fets datats i no sobre versions; males pràctiques — el càrrec que torna, la baixa que «no consta» [2] — que deixen de ser rendibles perquè deixen rastre; i la companyia honesta que es distingeix amb proves, no amb eslògans.

Els perills, amb la mateixa franquesa.

El primer és **la guerra de gravacions**. Si cada trucada esdevé un camp de mines probatori, la relació es degrada per a tothom. La resposta és la proporcionalitat: es documenta la gestió que importa — la baixa, el càrrec, la promesa contractual —, no cada interacció humana; i la gravació pròpia és un escut per a la disputa, mai un instrument d'assetjament contra el treballador que atén.

El segon és **l'asimetria que persisteix**. El client amb eines continua sent més feble que la companyia amb departament jurídic. La prova anivella la disputa concreta; la protecció real és col·lectiva — associacions de consumidors, autoritats amb règim sancionador, i la Llei 10/2025 aplicada de debò [1][2].

El tercer és **el tecnosolucionisme del tiquet**. Cap segell no fa que t'agafin el telèfon en tres minuts ni que la baixa sigui senzilla: això ho ha de fer complir el regulador. La prova fa l'incompliment visible i reclamable; que tingui conseqüències és feina de qui sanciona.

I el quart és **la privadesa de l'expedient**. L'expedient del client conté la seva vida de consum: ha de quedar al seu dispositiu — només empremtes a la cadena [3] —, revelar-se selectivament davant l'òrgan que toqui, i no esdevenir mai un perfil comercialitzable.

És hora d'actuar

Que la paraula del client pesi tant com la base de dades de la companyia.

Per a tu, client: documenta les gestions que importen — la baixa, el càrrec no autoritzat, la promesa de tarifa — al moment i amb data certa [3]; i reclama dins de termini: la Llei 10/2025 et dona quinze dies de resposta màxima, i cinc per als càrrecs no autoritzats [1].

Per a les associacions de consumidors: recomaneu l'expedient segellat com a pràctica estàndard de reclamació [2][3]; cada cas documentat és jurisprudència en potència.

Per a les companyies: ancoreu els vostres registres d'atenció — el codi de seguiment de la Llei 10/2025 [1] amb data certa verificable és la vostra prova de compliment i la fi de la reclamació infundada.

Per a les autoritats de consum: valoreu l'evidència ancorada del consumidor com el que és — data certa neutral — i exigiu a les companyies registres igualment verificables [1][2].

Per als legisladors: el desplegament de la Llei 10/2025 [1] és l'ocasió: que el codi identificatiu de cada reclamació porti segell de temps qualificat, i que el registre de la baixa sigui verificable per les dues parts.

La pròxima vegada que una veu digui «truqui demà», que el demà tingui data certa. Pel client que compleix i per la companyia que atén, **time2act**.

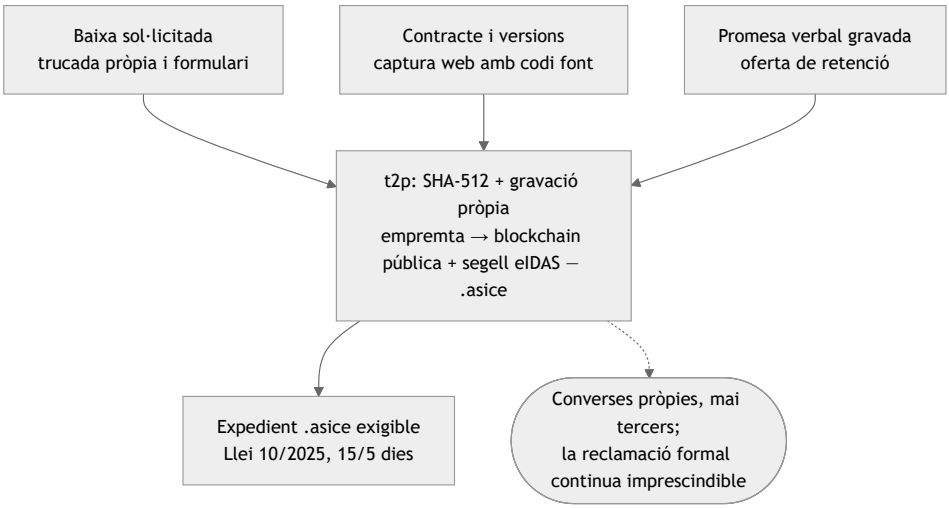


Figura 33.1 — El client davant la companyia amb prova d'existència (segellat amb t2p — capítol 13): la baixa segellada (gravació de la trucada pròpia, captura certificada del formulari), el contracte i les seves versions (captura web amb codi font), la promesa verbal gravada i l'expedient .asice exportable a consum. La Llei 10/2025 dona els drets (3 minuts, codi de seguiment, 15/5 dies, baixa simple); la data certa els fa exigibles — i acredita la companyia diligent. Límits: converses pròpies, proporcionalitat amb el teleoperador, la reclamació formal continua sent imprescindible. Fonts: BOE (Llei 10/2025); FACUA (multes Vodafone/Movistar/Telefónica).

---

[1] BOE — *Llei 10/2025, de 26 de desembre, per la qual es regulen els serveis d'atenció a la clientela* (BOE 27-12-2025; 12 mesos d'adaptació; 95 % de trucades en <3 minuts; codi identificatiu de seguiment; resposta en 15 dies — 5 per a càrrecs no autoritzats; avís 15 dies abans de renovacions automàtiques; baixa senzilla amb DNI i número de contracte; prohibició d'atenció exclusivament automatitzada); 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* (vulneració del dret de desconnexió fins a tres vegades; obstrucció a la inspecció; 20.100 € amb reducció); FACUA — *Multa a Movistar por acosar a través de una gestora de cobros a una socia por una deuda falsa* (1.741 € per línies mai contractades); 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 producte (gravació d'àudio en segon pla; captura i gravació de pantalla certificades amb verificació de l'app en primer pla; captura de pàgina web amb imatge completa + codi font; escàner de documents fins a 50 pàgines; projectes per agrupar captures per cas; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió; només empremtes a la cadena). Vegeu els capítols 13 i 15; la licitud de gravar converses pròpies, al capítol 75; la veu clonada, al capítol 68. ↩

La factura i la morositat: el rellotge del cobrament

«Recorda que el temps és diner.»

— Benjamin Franklin, «Advice to a Young Tradesman» (1748)

Un taller de fusteria en un polígon qualsevol. La comanda — mobles a mida per a una cadena de restaurants — surt pel moll a la tarda, amb l'albarà signat de qualsevol manera sobre el capó de la furgoneta. La factura s'envia per correu electrònic l'endemà. I comença l'espera: «la setmana que ve», «està pendent de validació», «no ens consta». Mentrestant, les nòmines del taller no esperen: la caixa avança el que el client gran no paga.

L'escena té llei des de fa vint anys — i la llei té dades que fan vergonya [2]. La Llei 3/2004 fixa terminis màxims de pagament entre empreses: 60 dies naturals com a màxim pactat, 30 per defecte des de la recepció de la mercaderia o del servei; estableix un interès de demora automàtic — sense necessitat d'avís, i que el primer semestre de 2025 era de l'11,15 % — i 40 euros fixos de costos de cobrament per factura. La realitat, segons l'informe de 2025 de la Plataforma Multisectorial contra la Morositat: el 85 % de les grans companyies incompleix els terminis legals, finançant-se en part a costa de les seves proveïdores; les Administracions Públiques paguen de mitjana a 70 dies — més del doble del seu límit de 30 —, i el sector privat, a 67 [2].

Per què una llei amb interessos automàtics s'incompleix massivament i gairebé ningú no els reclama? Perquè reclamar exigeix provar: la data del lliurament, la data de recepció de la factura, l'inici exacte del còmput. I aquestes dates viuen en papers de part, correus discutits i albarans que es perden. Aquest capítol tracta el desert probatori entre l'emissió i el cobrament — i com la data certa el travessa. El finançament del comerç internacional — cartes de crèdit, coneixements d'embarcament — és al capítol 54; l'evidència comptable per a l'auditor, al capítol 55; el pedigrí de la mercaderia mateixa, al capítol 29; el client particular davant la companyia, al capítol anterior. Pregunta clau: quan comença, exactament, el rellotge del cobrament? Resposta: quan el lliurament i la factura tenen data certa oposable entre privats — l'empremta SHA-512 al dispositiu, l'ancoratge de l'empremta a la blockchain pública i el segell de temps RFC 3161/eIDAS complementari de **t2p**, dins d'un contenidor .asice [3]. I l'Estat, sense dir-ho amb aquestes paraules, acaba de donar la raó a aquesta tesi: es diu VeriFactu.

VeriFactu: l'Estat construeix mitja prova

El Reial decret 1007/2023 — desplegament de la llei antifrau — imposa una arquitectura nova a tots els programes de facturació, els anomenats SIF [1]. Cada factura ha de generar un registre normalitzat amb una **empremta encadenada**: el hash de cada registre incorpora el hash de l'anterior, formant una cadena on qualsevol alteració retrospectiva canta. Cada registre se signa electrònicament, i la factura porta un **codi QR** que permet contrastar-la amb l'Agència Tributària. Hi ha dues maneres de complir: la modalitat «Verifactu» — enviament immediat i voluntari dels registres a l'AEAT — o la conservació inalterable de la cadena a disposició de la Inspecció [1].

El calendari, després de l'ajornament d'un any aprovat pel Reial decret llei 15/2025, de 2 de desembre: obligatori l'1 de gener de 2027 per a les societats i l'1 de juliol de 2027 per a la resta d'obligats. Les sancions no són simbòliques: fins a 50.000 euros per exercici per a qui faci servir programari no conforme, i fins a 150.000 per als fabricants que el venguin [1].

Atura't un moment en el que això significa per a la tesi d'aquest llibre: l'Estat espanyol imposa per llei hashos encadenats, registres inalterables i verificació per codi QR. És, peça per peça, l'arquitectura de la prova d'existència — aplicada a l'antifrau fiscal. Ja no és una proposta teòrica: és BOE.

I ara, la precisió sobre el que VeriFactu no fa — perquè aquí comença aquest capítol. Primer: protegeix Hisenda, no el creditor — el registre acredita que la factura es va emetre i no s'ha alterat, no que el client la va rebre ni que et deu diners. Segon: no acredita el lliurament — l'albarà, la recepció de la mercaderia, el moment en què arrenca legalment el termini de pagament queden fora de la cadena. I tercer: no és una data certa pensada per ser oposable entre privats en un jutjat — és una prova dirigida a l'Administració tributària. La capa que falta — la que mira el creditor i el deutor, no el contribuent — és exactament la que la prova d'existència neutral hi afegeix [3].

La prova d'existència aplicada

La mateixa pime que emet la factura pot segellar tot el trajecte del cobrament [3].

1. L'albarà amb lloc i hora

Al moll de descàrrega, el transportista o el tècnic fotografia l'albarà signat amb t2p: el GPS forense exigeix un fix genuí — precisió d'uns 50 metres, antiguitat màxima d'uns 30 segons; una ubicació simulada bloqueja la certificació del tot [3] — i l'empremta SHA-512 amb segell de temps fa del lliurament un fet: què es va lliurar, on i quan. Si el polígon no té cobertura, la certificació en segon pla es reprèn sola en recuperar-la, i el segell acredita el moment de la captura [3]. El «no ens va arribar la mercaderia» topa amb una acta que cap de les dues parts no pot reescriure.

2. La factura amb doble data certa

La factura, escanejada i segellada en emetre's — fins a 50 pàgines en un únic PDF certificat [3] — i, sobretot, el seu enviament capturat: el correu amb la factura adjunta, certificat amb pantalla i data [3]. Emissió i lliurament, totes dues amb data certa. El clàssic «no m'ha arribat la factura» — el comodí que atura rellotges — deixa de funcionar: la factura existia tal dia i es va enviar tal altre, i el certificat amb codi QR ho diu a qui ho vulgui comprovar.

3. El rellotge que arrenca sol

Amb el lliurament datat i la factura lliurada, el còmput de la Llei 3/2004 [2] ja no es discuteix: 30 o 60 dies des d'un fet cert, l'interès de demora automàtic — l'11,15 % — i els 40 euros per factura, calculables al cèntim des del dia exacte. La reclamació d'interessos, que avui gairebé cap pime no fa perquè no pot fixar el dia u, esdevé aritmètica. I la posició negociadora canvia: qui deu sap que el comptador corre — i que està acreditat.

4. El requeriment i el monitori

Quan cal reclamar, cada pas queda datat: el requeriment de pagament enviat i capturat, la promesa de pagament del client desada amb data, i l'expedient sencer — albarà, factura, enviament, requeriments — exportat com a paquet .asice verificable sense connexió [3], a punt per al procediment monitori o per al fons que compra la cartera. I la simetria de sempre: el client que va pagar a temps té en el seu propi registre ancorat la prova contra la reclamació duplicada o l'interès mal calculat.

Els límits, dits clarament: el segell acredita dates i documents, no la qualitat de la feina ni la raó de fons d'una disputa comercial — si la mercaderia era defectuosa, ho dirà el pèrit. VeriFactu [1] i t2p [3] es complementen però no es confonen: l'un mira Hisenda, l'altre mira les parts. I cap empremta no cobra una factura: converteix el crèdit en exigible — que no és poc —, però el cobrament final depèn del jutjat i de la solvència del deutor.

La promesa i el perill

La promesa: pimes que reclamen els interessos que la llei els reconeix des de fa vint anys, perquè per fi poden fixar el dia u [2][3]; morosos que paguen abans perquè el comptador acreditat corre; monitoris que es resolen sobre expedients verificables; i un país on VeriFactu [1] haurà normalitzat una idea més gran que l'antifrau: que els registres econòmics porten hash encadenat i data certa — el pas cultural cap a la prova d'existència universal.

Els perills, amb la mateixa franquesa.

El primer és que **el poder de mercat no es cura amb hashos**. La pime sovint no reclama interessos per por de perdre el client gran, no per manca de prova. La data certa treu l'excusa probatòria, però el desequilibri és econòmic: calen règims sancionadors de morositat i observatoris públics que facin la reclamació innecessària — que pagar tard surti car per defecte.

El segon és **el VeriFactu-solucionisme**. Complir amb Hisenda no és pagar a temps: una empresa pot tenir tots els registres encadenats del món i pagar a 120 dies. Confondre l'antifrau fiscal amb la protecció del creditor seria llegir malament la reforma [1].

El tercer és **la càrrega sobre la micropime**. Si documentar el cobrament esdevé burocràcia afegida, l'autònom no ho farà. L'eina ha de ser el gest de deu segons al moll [3], no un departament administratiu — i el gruix de l'esforç, la cadena fiscal, ja el fa el programari de facturació per obligació legal [1].

I el quart és **la traça com a arma de pressió**. El mateix expedient que protegeix el creditor pot servir per assetjar el deutor de bona fe amb reclamacions industrialitzades. El contrapès és doble: la neutralitat de la prova — també acredita qui va pagar — i el control judicial del monitori.

És hora d'actuar

Que cada factura porti el seu rellotge, i cada rellotge el seu dia u.

Per a pimes i autònoms: segelleu el trajecte sencer — l'albarà amb GPS forense, la factura enviada, els requeriments [3]; el dia que reclameu, el rellotge de la Llei 3/2004 [2] tindrà dia u acreditat.

Per a gestories i assessors: incorporeu l'expedient de cobrament ancorat al servei estàndard; VeriFactu [1] ja us porta a la cadena de hashos fiscal — oferiu al client la capa entre parts.

Per a les grans empreses pagadores: ancoreu les vostres recepcions i pagaments — la prova que pagueu a temps és el vostre millor argument davant l'informe anual de morositat [2].

Per a les Administracions: pagar a 70 dies amb un límit de 30 [2] és insostenible; amb registres de recepció i pagament ancorats i publicats per empremta, el període mitjà deixarà de ser una xifra discutida.

Per als legisladors: el règim sancionador de la morositat, pendent des de fa anys, té ara la infraestructura probatòria a punt [1][2][3]; i que la factura electrònica B2B en desplegament incorpori la data certa de recepció, no només d'emissió.

Perquè cobrar a temps deixi de ser un privilegi, **time2act**.

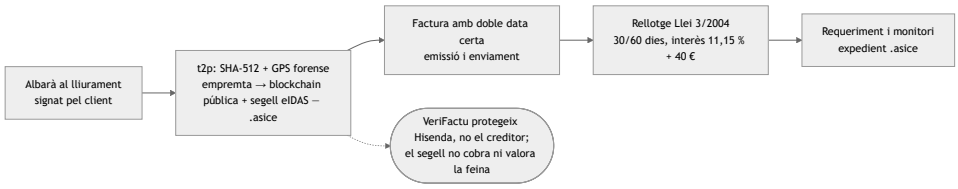


Figura 34.1 — El rellotge del cobrament amb prova d'existència (segellat amb t2p — capítol 13): l'albarà fotografiat amb GPS forense al lliurament, la factura amb doble data certa (emissió i enviament), el còmput automàtic de la Llei 3/2004 (30/60 dies; interès de demora 11,15 % + 40 €) i l'expedient .asice per al monitori. Context: VeriFactu (RD 1007/2023, ajornat a 2027 pel RD-llei 15/2025) ja imposa registres de facturació amb hash encadenat i QR — l'Estat construeix mitja prova d'existència; t2p hi afegeix la capa oposable entre privats. Límits: el segell no cobra factures ni valora la feina; VeriFactu protegeix Hisenda, no el creditor. Fonts: AEAT; BOE; PMcM 2025 (85 % de grans incomplidores; AAPP a 70 dies).

---

[1] AEAT — *Sistemas Informáticos de Facturación (SIF) y VERI*FACTU *(RD 1007/2023: registre de facturació normalitzat amb empremta encadenada — cada registre conté el hash de l'anterior —, signatura electrònica i QR de verificació; modalitats «Verifactu» d'enviament immediat voluntari i conservació inalterable; FAQ oficial); Guía Fiscal* — Verifactu 2026-2027 *i Davisa* — Guía Verifactu 2026* (calendari ajornat pel RD-llei 15/2025, de 2 de desembre: 1-1-2027 societats, 1-7-2027 resta; sancions de fins a 50.000 €/exercici per a usuaris i 150.000 € per a fabricants). 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 — *Llei 3/2004, de 29 de desembre, de mesures de lluita contra la morositat en les operacions comercials* (60 dies naturals de màxim pactat entre empreses, 30 per defecte des de la recepció; interès de demora automàtic; 40 € de costos de cobrament per factura; AAPP 30 dies — Llei 15/2010); Togas — *Los intereses de demora en el primer semestre de 2025: 11,15 %* (Resolució del Tresor de 30-12-2024); PMcM / Revista Limpiezas — *Informe sobre morosidad 2025* (el 85 % de les grans companyies incompleix els terminis; AAPP a 70 dies de mitjana, +3 el 2025; sector privat 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 producte (foto amb GPS forense — fix genuí ~50 m / ≤30 s, la ubicació simulada bloqueja la certificació; certificació en segon pla que es reprèn en recuperar cobertura; escàner de documents fins a 50 pàgines en un PDF; captura de pantalla i de correu certificades; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de

temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió; només empremtes a la cadena). Vegeu els capítols 13 i 15; el comerç internacional, al capítol 54; l'auditoria, al capítol 55. ↩

Immobiliari: l'estat de la propietat i el registre de la terra

«El primer que, havent tancat un terreny, gosà dir "això és meu" i trobà gent prou senzilla per creure-se'l, fou el veritable fundador de la societat civil.»

— Jean-Jacques Rousseau, Discurs sobre l'origen de la desigualtat (1755)

Un dia qualsevol, un propietari descobreix que la seva casa s'ha posat a la venda. Ell no l'ha venuda; algú ha falsificat una escriptura —sovint una *quitclaim deed*, l'escriptura de renúncia nord-americana— i l'ha presentat al registre per transferir-se una propietat que no és seva. L'oficina de Boston de l'FBI va alertar l'abril de 2025 de l'augment d'aquest frau, i l'associació del sector assegurador de títols, l'**American Land Title Association** (ALTA), va documentar que el 28 % de les seves empreses havien patit intents de **suplantació de venedor** el 2023, amb un objectiu predilecte: el **sòl sense edificar** (un 85 % dels casos), perquè no hi viu ningú que se n'adoni [5][6]. En molts d'aquells intents, els defraudadors fan servir credencials de notari falses —un 43 %— o n'usurpen de reals.

El frau immobiliari modern, fixem-nos-hi, no ataca tant la cadena de títols com **la identitat del firmant** i **l'estat de la cosa**. I aquí, el sistema té un forat que aquest capítol vol omplir. Però convé començar amb una distinció que el lector tendeix a confondre i que travessa tot el capítol: una cosa és el **títol legal** —el que crea o transfereix la propietat, competència exclusiva del registre i del notari— i una altra, ben diferent, és l'**evidència**: la prova que un document o un estat físic existien, íntegres, en un moment, un lloc i a càrrec d'una persona. La prova d'existència no substitueix el registre. Aporta la capa d'evidència amb data certa que avui falta o és discutible.

La propietat insegura

El problema de fons és sorprenentment massiu. El Banc Mundial, en un treball dels seus experts Laura Tuck i Wael Zakout, calcula que només al voltant del 30 % de la població mundial té els seus drets sobre la terra i l'habitatge legalment registrats; és a dir, prop del 70 % no disposa d'un títol documentat [1]. I la inseguretat no afecta únicament els països pobres. La iniciativa Prindex, la major enquesta global sobre percepció de seguretat de la tinença, va trobar el 2024 que uns 1.100 milions d'adults —el 23 %, davant del 19 % de 2020— temen perdre la seva terra o casa; als Estats Units aquesta inseguretat percebuda ha pujat del 13 % al 25 % en quatre anys, i colpeja sobretot joves i llogaters [2]. Un informe de la FAO de 2026 ho confirma: només un 35 % de la terra del món està formalment documentada [3].

On hi ha opacitat, hi ha frau. L'FBI va registrar el 2025 més de 12.000 víctimes de frau immobiliari als Estats Units, amb pèrdues d'uns 275 milions de dòlars, un 59 % més que l'any anterior [4]. Entre el 2019 i el 2023 el frau immobiliari va deixar 58.141 víctimes i 1.300 milions de dòlars en pèrdues [6]. I a l'altre extrem de l'escala —el dels milions sense títol—, la inseguretat no es mesura en dòlars robats sinó en famílies que poden ser desallotjades de la terra que treballen perquè no poden provar-ne la propietat.

Pioners i fracassos: Geòrgia, Suècia, Hondures

Davant d'això, alguns estats han fet de la necessitat una virtut. El cas pioner és la **República de Geòrgia**, un país postsoviètic marcat per la corrupció registral. El 2016, la seva Agència Nacional de Registre Públic, amb l'empresa Bitfury i amb l'economista **Hernando de Soto** —el gran teòric del capital mort dels pobres sense títol— com a padrí del projecte, va iniciar l'ancoratge a la cadena de blocs de Bitcoin de l'empremta de cada certificat de propietat. Al 2018, prop d'1,5 milions de títols estaven segellats de manera que, en paraules de la pròpia agència, «ningú, ni tan sols l'Estat, NO pot alterar-ne la marca de temps» [7]. El 2017 el pilot es va ampliar a compravendes, hipoteques i lloguers [8]. La paradoxa és bella: un Estat que dona als seus ciutadans una prova que ell mateix ja no pot falsificar.

Suècia va anar per un camí semblant: el seu registre, el Lantmäteriet, amb l'empresa ChromaWay, va calcular que segellar les transaccions immobiliàries podia estalviar més de **100 milions d'euros l'any** al contribuent i reduir el temps entre la signatura i la transferència de tres a sis mesos a uns pocs dies [9]. Però no totes les històries acaben bé, i aquí hi ha una lliçó. Hondures va anunciar el 2015, amb l'empresa Factom, el primer registre nacional de terres «a prova de manipulació» —motivat, precisament, perquè alguns funcionaris piratejaven la base de dades estatal per robar-se finques. A finals d'aquell any, el

projecte es va encallar per «qüestions polítiques» i no es va desplegar mai [10]. La tecnologia prometia blindar la propietat; la manca de voluntat política la va deixar en una carta d'intencions. És la prova que el segell és condició necessària, però no suficient: cal que el registre, el notari o el tribunal l'acceptin.

La prova d'existència aplicada

Vegem com **t2p** omple el buit de l'evidència en tres escenaris molt diferents.

El primer, quotidià i universal: les **disputes per la fiança del lloguer**. El clàssic «ja estava trencat / no, ho vas trencar tu» és una de les causes més freqüents de litigi entre propietari i llogater, fins al punt que disset estats nord-americans exigeixen per llei un informe de l'estat de l'habitatge a l'entrada per poder retenir legalment la fiança. Amb **t2p**, l'inquilí o el gestor fotografia l'estat del pis i el segella a l'instant: **empremta SHA-512** al dispositiu, **GPS forense** que prova quin pis i quan, **segell de temps** eIDAS, **prova de vida** que lliga la captura a una persona real present —adéu a les fotos velles reciclades— i tot empaquetat en un **contenidor .asice** que l'altra part o un jutge poden verificar fora de línia.

El segon: **escriptures, contractes i due diligence**. Segellar l'empremta d'un esborrany d'escriptura, d'un contracte d'arres o d'un informe de taxació els dona **data certa**, fent impossible la retrodatació. En el vector de suplantació del venedor, capturar amb prova de vida i GPS el moment de la identificació afegeix una traça que les credencials de notari falsificades no poden fabricar després.

El tercer, el més transformador: els **contextos de registre feble**, com hem vist. On no hi ha un registre fiable, segellar fotografies georeferenciades de l'ocupació, les millores i les llindes crea un **historial verificable de possessió**. No és un títol —això només ho pot crear l'Estat—, però sí una evidència amb data certa, oposable, en l'esperit del que va fer Geòrgia. És, per a milions de famílies, la diferència entre una possessió muda i una possessió que es pot demostrar.

Cal dir els límits amb claredat, fidels a la dualitat de «la promesa i el perill». «Escombraries a l'entrada, escombraries a la cadena»: si la foto menteix o el document d'origen és fals, la cadena només certifica que *aquella mentida* existia íntegra en aquell instant. La prova d'existència demostra existència, integritat, temps, lloc i persona; **no** demostra la veritat física prèvia —que el mur estigués bé abans, o que el venedor sigui l'amo real—. I, com a Hondures, el seu valor ple només apareix quan el registre, el notari o el tribunal accepten aquesta evidència.

La promesa i el perill

La promesa és doble. Per als països rics, tancar la porta al frau d'escriptures i a les disputes de fiança, i donar data certa a cada document immobiliari. Per als països amb registres febles, oferir a centenars de milions de persones una manera de fer la seva possessió sense esperar que l'Estat construeixi un cadastre perfecte. En tots dos casos, més seguretat jurídica amb menys cost i menys intermediaris.

El perill demana matís. El primer, la confusió perillosa entre evidència i títol: vendre la prova d'existència com si transferís la propietat seria un frau en si mateix. El segon, la privacitat: les fotos geolocalitzades de l'interior d'un habitatge i la biometria de prova de vida són dades sensibles que exigeixen un disseny escrupolós. I el tercer, la lliçó d'Hondures: sense voluntat política i reconeixement institucional, la millor tecnologia es queda en una promesa. La prova d'existència és una capa necessària dins d'una arquitectura que inclou, sempre, el registre i la llei.

És hora d'actuar

Per als **arrendataris i propietaris**: segellar l'estat de l'habitatge a l'entrada i a la sortida, evitant que una disputa de fiança es resolgui per la veu més forta. Per als **compradors i les asseguradores de títol**: exigir evidència amb data certa i prova de vida del venedor, tallant la suplantació. Per als **registres i notaris**: reconèixer el valor probatori del segell i integrar-lo, com va fer Geòrgia. Per als **governs amb registres febles**: oferir una capa d'evidència de possessió mentre es construeix el cadastre, sense obligar la població a esperar. Per als **reguladors**: protegir simultàniament la integritat de la prova i la privacitat de les llars.

Un propietari pot descobrir un dia que la seva casa s'ha «venut» sense ell. Milions de famílies viuen tota la vida sense poder demostrar que la terra que treballen és seva. Entre la propietat verificable i la basada en

la confiança d'un document manipulable es dibuixa cada cop més la frontera de la seguretat. Donar a cadascú la prova del que és seu —o de l'estat en què ho va rebre— és, també aquí, **time2act**.

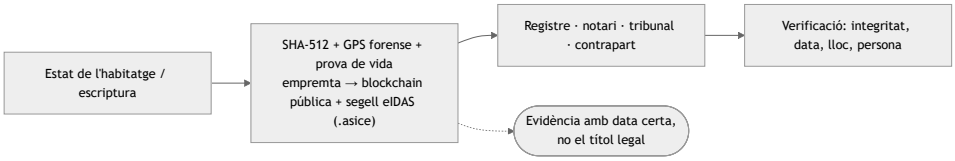


Figura 35.1 — L'estat de l'habitatge (lloguer) o un document (escriptura, contracte) es captura i se segella al dispositiu amb SHA-512, GPS forense, segell de temps eIDAS i prova de vida, s'ancora a la blockchain pública i s'empaqueta en un contenidor .asice verificable fora de línia, llest per al registre, el notari, el tribunal o l'altra part. La prova d'existència aporta evidència amb data certa, no el títol legal (que crea el registre). Barra de context: ~70 % de la població mundial sense títol registrat; ~1.100 M de persones insegures sobre la seva propietat; Geòrgia, ~1,5 M de títols ancorats. Fonts: Banc Mundial; Prindex; Exonum/Bitfury.

---

[1] Banc Mundial — Laura Tuck i Wael Zakout, *7 reasons for land and property rights to be at the top of the global agenda* (~30 % de la població amb títol registrat). 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 d'adults, 23 %, inseguros sobre la seva terra/habitatge). https://www.prindex.net/news-and-stories/tenure-insecurity-on-the-rise/ ↩

[3] FAO (informe SOFA, via UN News) — *Global report highlights slow progress in expanding secure land tenure* (~35 % de la terra documentada; >1.100 M temen perdre-la). https://news.un.org/en/story/2026/02/1167037 ↩

[4] FBI IC3 (via National Association of Realtors) — *Online real estate fraud climbed to $275M in 2025* (12.368 víctimes). 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* (juliol 2024; 28 %; sòl sense edificar 85 %; credencials de notari falses 43 %). https://www.alta.org/news-and-publications/news/20240730-Seller-Impersonation-Fraud-Attempts-Increase-Study-Shows ↩

[6] FBI Boston (via ALTA) — *FBI Boston Issues Quit Claim Deed Fraud Warning* (abril 2025; frau immobiliari 2019-2023: 58.141 víctimes / 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 títols ancorats a Bitcoin; «ningú pot alterar la marca de temps»). https://exonum.com/story-georgia ↩

[8] Eurasianet — *Georgia authorities use blockchain technology for developing land registry* (ampliació feb-2017; Hernando de Soto, assessor). 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€/any d'estalvi). https://www.computerweekly.com/news/450421958/Sweden-trials-blockchain-for-land-registry-management ↩

[10] CoinDesk — *Blockchain land title project stalls in Honduras* (Factom; encallat per qüestions polítiques, 2015). https://www.coindesk.com/markets/2015/12/26/blockchain-land-title-project-stalls-in-honduras ↩

Lloguer i habitatge: l'estat de les coses, amb data certa

«La casa és el nostre racó del món. És —s'ha dit sovint— el nostre primer univers.»

— Gaston Bachelard, La poètica de l'espai (1957)

Ets davant d'un portal immobiliari conegut i el cursor s'atura sobre un anunci que sembla un regal: pis bonic, ben situat, clarament per sota del preu del barri. El «propietari» escriu amb urgència — hi ha més interessats, cal una paga i senyal per reservar-lo — i no hi ha manera de visitar-lo abans: és fora, per feina. Només un número de compte on transferir els diners. Així va començar, per a una víctima que buscava pis al centre de Valladolid, la història que la Guàrdia Civil va acabar batejant com a Operació ISLEDA (2026): una trama d'«estafa immobiliària a escala nacional», amb anuncis falsos repartits pel país i víctimes per tot Espanya; tres detinguts d'entre 19 i 34 anys a San Fernando (Cadis); i un detall que retrata l'època — els comptes bancaris receptors s'havien obert amb documentació personal robada en estafes prèvies d'ofertes de feina falses. Delictes: estafa, blanqueig i organització criminal [1]. El patró és sempre el mateix: preu-ganxo, propietari que no dona la cara i pressa perquè paguis abans de poder comprovar res [2].

El capítol 35 va tractar la propietat: el títol, el registre, la terra. Aquest capítol tracta el que passa a dins: la vida del contracte de lloguer, on gairebé tot es discuteix a posteriori. Si el pis existia. Com estava el dia que vas rebre les claus. Quan vas avisar de la humitat. Quan hi va entrar l'ocupant. La pregunta clau: com es prova l'estat de les coses quan cada part en recorda una versió diferent? La resposta no pot ser la memòria: és la data certa en el moment — **t2p**: l'empremta SHA-512 de cada foto, acta i missatge, calculada al dispositiu, amb segell de temps RFC 3161/eIDAS i ancoratge a la blockchain pública dins d'un contenidor .asice [5]. I amb neutralitat total: la mateixa eina empara el llogater, el propietari i qualsevol que actuï de bona fe.

El pis que no existeix

La mecànica de l'estafa dels anuncis falsos està ben documentada: pisos inexistents — o que no són de qui els anuncia — publicats amb fotos atractives i preus per sota de mercat per generar cua de víctimes; un «propietari» que sovint diu ser a l'estranger; i comunicació ràpida amb pressió per pagar una reserva o la primera mensualitat abans de cap visita [1][2]. L'Operació ISLEDA, coneguda la primavera de 2026, en va mostrar la maduresa industrial: víctimes per tot el territori, anuncis distribuïts pel país, identitats robades per obrir els comptes receptors i una estructura d'organització criminal [1].

L'asimetria de fons explica per què funciona. Per muntar l'estafa només calen fotos boniques, un text persuasiu i una adreça de correu; el cost és negligible al costat de la recaptació. En canvi, per demostrar que ets el propietari de debò, avui no hi ha cap gest senzill: el llogater no pot distingir l'anunciant legítim de l'impostor fins que és massa tard, i el propietari honest competeix contra pisos fantasma més barats que el seu.

La sortida estructural és l'anunci verificable. El propietari real pot segellar l'oferta — vinculada a la seva acreditació de titularitat, la cadena registral del capítol 35 — amb data certa [5]; el portal pot mostrar el distintiu de l'anunci acreditat; i el llogater aprèn la regla inversa: oferta sense segell i amb pressa, sospita per defecte [2]. L'estafador pot copiar les fotos, però no pot acreditar ni la titularitat ni la continuïtat en el temps. Sense el distintiu, el seu anunci deixa de competir; amb la regla apresa, deixa de cobrar.

La guerra de la fiança

Quan el contracte s'acaba, comença l'altra batalla. El marc és clar sobre el paper: la fiança s'ha de retornar en el termini d'un mes des del final del contracte, i passat el termini meriten interessos legals [3]; els motius vàlids de retenció són taxats — deutes de renda o subministraments, i danys que excedeixin el deteriorament normal per l'ús [3]. Una pintura desgastada pel temps no justifica retenir res; una rajola trencada o una porta forçada, sí.

La clau, però, és processal: els tribunals solen fallar a favor del llogater quan l'arrendador no aporta proves suficients — factures, informes de desperfectes — que justifiquin la retenció; i a favor del propietari quan acredita despeses reals per mal ús [3]. Traduït: la fiança no la guanya qui té raó, sinó qui té proves.

I aquí apareix el ritual que falta. Els experts recomanen formalitzar un acord de liquidació signat, amb comprovació detallada de l'inventari en el lliurament de claus [3]; a la pràctica es fa poc, tard i sense data fiable — fotos soltes al mòbil de cadascú, missatges dispersos, records enfrontats.

La versió segellada del ritual ho arregla d'arrel: el dia de les claus, les dues parts fotografien l'habitatge — cada estança, cada desperfecte preexistent — i segellen les imatges i l'acta al moment, des dels dos dispositius: empremta SHA-512, data certa, ancoratge [5]. El dia de la sortida, el mateix recorregut. La discussió sobre «com estava el pis» desapareix: queda la comparació entre dues sèries d'imatges amb integritat acreditada. Ni el llogater pot negar el forat que hi va fer, ni el propietari pot atribuir-li l'esquerda que ja hi era.

Les 48 hores i els 15 dies

L'okupació és el conflicte més enverinat del mercat, i el seu nou marc legal ha convertit el temps en l'element central. La Llei Orgànica 1/2025, d'eficiència del servei públic de justícia, en vigor des del 3 d'abril de 2025, fa que l'allanament de morada (article 202 del Codi Penal: ocupar el domicili habitual d'algú) i la usurpació d'immoble (article 245: ocupar una propietat que no és domicili habitual) es tramitin per judici ràpid, amb terminis de resolució de l'ordre de quinze dies; si l'ocupació es detecta dins de les primeres 48 hores, les forces de seguretat poden desallotjar sense esperar ordre judicial, com a delicte flagrant; i en aquesta via se suprimeix l'informe previ de vulnerabilitat [4].

Fixem-nos en què penja tota la via ràpida: de dates. Quan va entrar l'ocupant? Quan ho va descobrir el propietari? L'immoble era domicili habitual o segona residència? Quan es va denunciar? Cada resposta mou el cas d'un article a l'altre, d'una via a l'altra, del desallotjament immediat al procediment llarg. I avui aquestes preguntes es responen amb testimonis i indicis — el material probatori més fràgil que existeix.

Amb prova d'existència, es responen amb cronologia. El propietari d'un habitatge buit pot establir la línia de base amb proves d'estat periòdiques — la visita mensual, la foto amb data certa [5] —; si un dia troba la porta forçada, el descobriment queda datat al minut i la denúncia porta hora ancorada: la flagrància de les 48 hores i el judici de quinze dies [4] treballen sobre fets datats, no sobre estimacions.

I la simetria és imprescindible, i cal dir-la amb el mateix èmfasi: la mateixa eina protegeix el llogater legítim de ser tractat com a ocupant. El contracte, els rebuts de renda i els pagaments de subministraments segellats al seu dispositiu són la seva cronologia de possessió legítima [5], l'escut contra el desallotjament abusiu o l'acusació infundada. La data certa no té bàndol: distingeix l'ocupació il·legal de la possessió legal, sigui quin sigui el costat que ho hagi de provar.

Humitats, avaries i el rellotge

La tercera guerra del lloguer no és ni l'entrada ni la sortida: és el mentrestant. La taca d'humitat que creix, la caldera que falla a l'hivern, la reparació que «ja vindrà». Jurídicament, aquestes disputes són cronologies pures: quan es va avisar el propietari, per quin canal, què va respondre, quant va trigar la reparació, com va evolucionar el dany mentrestant. Qui no pot datar l'avís, no pot exigir; qui no pot datar la resposta, no es pot defensar.

Imaginem la seqüència amb prova d'existència. El llogater detecta la humitat al novembre i envia l'avís segellat — empremta i data certa del missatge [5]. La resposta del propietari, també segellada, arriba l'endemà: inspecció la setmana vinent. El tècnic documenta el dany amb fotos datades; la reparació queda registrada; i si la taca torna al gener, la sèrie fotogràfica ancorada mostra la progressió sencera. Cap de les dues parts no depèn ja de la memòria: el llogater que va avisar a temps pot exigir; el propietari que va reparar diligentment pot demostrar-ho; i el que va callar — sigui qui sigui — queda retratat pel seu propi silenci, perquè els buits de la cronologia també tenen data [5].

En un contracte de tracte successiu, la justícia és qüestió de rellotge. I el rellotge, per ser just, ha de poder ser auditat per qualsevol: això és exactament el que aporta el segell.

La prova d'existència aplicada

Un lliurament de claus qualsevol: dos mòbils que fotografien les mateixes estances, deu minuts de ritual — i un any de disputa estalviat.

1. L'inventari segellat

El dia de l'entrada, llogater i propietari recorren el pis junts: fotos de cada estança i dels desperfectes preexistents, una acta breu d'inventari, i tot segellat al moment des dels dispositius de totes dues parts — empremta SHA-512, data certa, ancoratge a la blockchain pública [5]. El dia de la sortida, el mateix recorregut. La fiança es liquida sobre la comparació de dues sèries d'imatges amb integritat acreditada, no sobre records: els tribunals ja premien qui aporta proves [3]; el segell fa que totes dues parts en tinguin, de la mateixa qualitat, des del primer dia.

2. L'anunci verificable

El propietari legítim segella l'oferta amb la seva acreditació de titularitat (capítol 35) i el portal la distingeix amb el distintiu d'anunci verificat [5]. Davant del pis «massa barat» amb propietari a l'estranger i presses [1][2], el llogater aplica una regla de tres paraules: sense segell, sense diners. L'Operació ISLEDA va necessitar una denúncia, una investigació i mesos de feina policial per desmantellar la trama [1]; un mercat d'anuncis acreditats l'hauria deixada sense víctimes des del primer clic.

3. La cronologia de la possessió

Per al propietari d'un habitatge buit: proves d'estat periòdiques i segellades que estableixen la línia de base; si un dia troba la porta forçada, el descobriment queda ancorat al minut, la denúncia també, i la via ràpida de la LO 1/2025 — les 48 hores, el judici en uns quinze dies [4] — treballa sobre una cronologia indiscutible [5]. Per al llogater legítim: el contracte, els rebuts i els subministraments segellats són l'escut que impedeix que ningú el pinti com a ocupant. La mateixa empremta serveix les dues cares del conflicte: aquesta és exactament la seva virtut.

4. El diàleg amb data certa

L'avís d'avaria segellat, la resposta del propietari segellada, la progressió del dany en sèrie fotogràfica ancorada [5]: la disputa d'humitats deixa de ser un «t'ho vaig dir» contra un «no m'ho vas dir». Qui va avisar a temps pot exigir; qui va reparar diligentment pot demostrar-ho; i el silenci de qui no va fer ni una cosa ni l'altra queda datat amb la mateixa precisió que tota la resta.

Cal dir també què no fa el segell: acredita l'estat i el moment, però no reparteix culpes ni interpreta la Llei d'Arrendaments Urbans — això ho fan els jutges; una foto segellada no substitueix la inspecció física quan cal un pèrit; i les imatges de l'interior d'una llar són dades íntimes — només l'empremta s'ancora, el contingut resta als dispositius de les parts i es revela únicament en cas de disputa [5].

La promesa i el perill

La promesa és un mercat de lloguer on l'anunci fals no troba víctimes [1][2], la fiança es liquida en deu minuts de comparació i no en mesos de guerra [3], l'okupació i la possessió legítima es distingeixen per cronologia [4], i les reparacions tenen un rellotge que totes dues parts poden auditar. Menys jutjats, menys por, més confiança entre desconeguts — en el contracte més quotidià que existeix.

Els perills exigeixen la mateixa honestedat.

El primer és **el desequilibri de poder**. Si només una part segella, l'eina esdevé arma. Un mercat on els grans tenidors documenten industrialment i el llogater vulnerable no, agreuja l'asimetria que ja existeix. Per això el ritual ha de ser bilateral per disseny — l'inventari segellat des dels dos dispositius — i l'eina, gratuïta o de cost negligible per a la part feble.

El segon és **la privadesa de la llar**. Les fotos de casa teva són el mapa de la teva intimitat. Cap imatge no ha de sortir del dispositiu: només empremtes a la cadena, revelació només davant de disputa, revocabilitat quan el contracte s'acaba i cap registre central d'interiors [5].

El tercer és **la barrera burocràtica**. Si el segell es converteix en un requisit més per accedir a un pis — una «puntuació de documentació» que expulsa qui menys té —, haurem empitjorat el problema que volíem resoldre. El segell ha de resoldre disputes, no filtrar persones: senzill, gratuït i opcional per a qui lloga.

I el quart, dit sense embuts: **això no és política d'habitatge**. Cap empremta no abaixa el preu del lloguer ni construeix cap pis. La crisi de l'habitatge és de preus, d'oferta i de polítiques públiques; aquest

capítol només neteja la capa de conflictes que la fa encara més cruel. Confondre les dues coses seria vendre fum sobre el sostre de la gent.

És hora d'actuar

En el contracte més important de la vida quotidiana, la memòria no pot ser l'única prova.

Per als llogaters: segella l'inventari d'entrada encara que el propietari no ho faci; guarda amb data certa el contracte, els rebuts i cada avís d'avaria [3][5]; i davant d'un anunci amb pressa i preu-ganxo, sense segell ni visita, ni un euro [1][2].

Per als propietaris: inventari segellat bilateral el dia de les claus [3]; per als pisos buits, la prova d'estat periòdica [4][5]; i acredita el teu anunci — el distintiu et distingeix de l'estafador que copia les teves fotos [1].

Per als portals immobiliaris: implanteu el distintiu d'anunci verificat amb segell de titularitat i data certa [1][2][5]; el cost és mínim i el mercat sencer hi guanya credibilitat.

Per a administradors de finques i cambres de la propietat: estandarditzeu l'acta d'inventari segellada com a servei bàsic del lloguer professionalitzat [3].

Per a jutges i cossos policials: valoreu la cronologia segellada en la via ràpida de la LO 1/2025 [4] — les 48 hores i els quinze dies necessiten dates fiables més que cap altra cosa.

Per als legisladors: doneu presumpció d'autenticitat a l'inventari segellat bilateral, i vetlleu perquè cap eina probatòria no esdevingui mai barrera d'accés a l'habitatge.

La víctima de Valladolid va perdre els diners per un pis que no existia [1]. Que el pròxim anunci fals no trobi ningú a qui enganyar, i que la pròxima fiança es torni sense guerra. Per un mercat on l'estat de les coses tingui data certa, **time2act**.

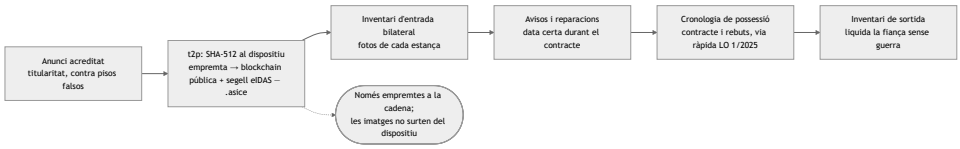


Figura 36.1 — El cicle del lloguer amb prova d'existència: l'anunci acreditat (titularitat + segell, contra l'estafa del pis inexistent), l'inventari d'entrada segellat bilateralment, els avisos i reparacions amb data certa durant el contracte, la cronologia de possessió (contracte i rebuts del llogater; proves d'estat periòdiques del propietari; via ràpida LO 1/2025) i l'inventari de sortida que liquida la fiança sense guerra. Només les empremtes SHA-512 s'ancoren a la blockchain pública (RFC 3161/eIDAS, .asice); les imatges de la llar no surten mai dels dispositius. Fonts: Guàrdia 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 maig de 2026; Operació ISLEDA; 3 detinguts de 19-34 anys a San Fernando; destapada a Valladolid; comptes oberts amb identitats robades en falses ofertes de feina; estafa, blanqueig i organització 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* (preus-ganxo, propietaris «a l'estranger», pagaments abans 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* (termini d'un mes; interessos legals; acord de liquidació amb inventari); Ático Jurídico — *Devolución de la fianza del alquiler* (els tribunals exigeixen proves a qui reté: factures, 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 d'abril de 2025; allanament art. 202 CP i usurpació art. 245 CP per judici ràpid; desallotjament policial dins de les primeres 48 hores; supressió de l'informe de vulnerabilitat en aquesta via); 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 producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; el contingut no surt mai del dispositiu; revelació voluntària; els buits de la sèrie queden datats). Vegeu els capítols 13 i 15; per a la titularitat i el registre, el capítol 35. ↩

La comunitat de propietaris: actes, derrames i acords amb data certa

«Les ciutats tenen la capacitat d'oferir alguna cosa a tothom, només perquè, i només quan, són creades per tothom.»

— Jane Jacobs, The Death and Life of Great American Cities (1961)

La junta anual, al vestíbul o al local de sota l'escala: cadires plegables, el llibre d'actes sota el braç de l'administrador, la discussió eterna sobre la derrama de l'ascensor. S'alcen mans, el recompte es fa de pressa, algú protesta i algú altre ja parla del punt següent. Tres setmanes després arriba l'acta — i més d'un dels presents no reconeix el que s'hi diu que es va votar.

Milions de persones viuen en règim de propietat horitzontal, i tota la seva vida col·lectiva — obres, diners, normes — penja d'una cadena documental fragilíssima: una convocatòria que potser va arribar, una votació que ningú no va registrar, una acta redactada després per una sola persona, un llibre d'actes que viu en un calaix. Quan hi ha confiança, tot rutlla; quan es trenca — i en una comunitat es trenca sovint —, tot esdevé «la teva paraula contra la del president».

Aquest capítol tracta la democràcia més petita del país i la seva memòria. El títol de propietat i el registre són al capítol 35; la vida del contracte de lloguer, al capítol 36; la relació amb l'Administració, al capítol 44; i si mai cal desempatar una plaça d'aparcament per sorteig, el capítol 45 explica com fer-ho de manera irrefutable. Pregunta clau: com es governa un edifici quan l'única memòria oficial la redacta i la custodia una sola mà? Resposta: donant data certa a cada peça — la convocatòria, l'acta, els comptes, la comunicació — amb **t2p**: hash al dispositiu, segell de temps i àncora pública — el trípode del capítol 13 [3]. A l'abast de qualsevol veí — i de l'administrador honest, que n'és el primer beneficiat.

El llibre d'actes en una sola mà

El cas real que ho il·lustra [1]: un administrador de finques de Gijón, condemnat a un any i mig de presó — condemna confirmada — per apropiar-se de 2.984,04 euros del compte de la comunitat. El mètode: maniobres enganyoses al llibre d'actes, fent signar els expresidents documents que suposadament resolien tràmits amb el banc; per encobrir-se, va aportar rebuts d'obra i serralleria que no corresponien a cap despesa comunitària. I el detall que importa a aquest llibre: el frau només es va descobrir quan van canviar el president i el tresorer, i el nou equip va repassar els comptes minuciosament.

El delicte és l'excepció — la immensa majoria d'administradors fan bé una feina ingrata —, però l'arquitectura que el va permetre és la norma: el llibre d'actes com a única memòria oficial, redactada i custodiada per una sola part; els comptes que només es miren quan algú sospita; les signatures que es demanen «per un tràmit». El Codi Penal hi posa nom quan tot ha passat — l'apropiació indeguda de l'article 253 [1] —; el que no hi ha és res que ho faci visible abans.

I el conflicte civil és molt més freqüent que el penal. La Llei de Propietat Horitzontal permet impugnar els acords contraris a la llei, lesius o abusius [2] — però impugnar exigeix provar què es va convocar, què es va dir i què es va votar exactament. Sense registre, la impugnació és un acte de fe; i la defensa de la junta que ho va fer tot bé queda igualment a mercè dels records.

La prova d'existència aplicada

La mateixa junta, el mateix administrador — i cada peça de la vida comunitària amb data certa [3].

1. La convocatòria que consta

La convocatòria amb l'ordre del dia, escanejada i segellada en enviar-se — i l'enviament mateix capturat amb data certa: el correu, el tauler o la bústia fotografiada amb GPS forense [3]. El «a mi no em va arribar» i el «es va convocar fora de termini» deixen de ser discutibles: la convocatòria existia tal dia, deia això i es va comunicar per aquest canal. Protegeix el veí — i protegeix la junta que convoca bé.

2. L'acta del mateix dia

La votació, comptada en veu alta i — si la junta ho acorda — gravada [3]; l'acta, redactada i segellada el mateix dia o l'endemà, no tres setmanes després. Cada acta rep la seva empremta SHA-512 amb segell de temps, i el llibre d'actes esdevé una cadena de versions ancorades que ningú — ni administrador, ni president, ni veí — no pot reescriure retroactivament [3]. La impugnació de la LPH [2] passa a discutir el fons, no els fets; i la maniobra del cas de Gijón [1] — tocar el llibre a posteriori — esdevé impossible de fer en silenci.

3. La derrama traçable

L'expedient de l'obra, agrupat en un projecte de l'app [3]: els pressupostos rebuts — escanejats, fins a 50 pàgines cadascun —, l'acord d'aprovació amb la seva acta segellada, les factures, les certificacions. Cada euro de la derrama, del vot al pagament, amb data certa. Els comptes anuals, contrastables per qualsevol veí sense demanar permís — i l'administrador honest, blindat: els seus registres ancorats són la seva auditoria permanent.

4. La comunicació fefaent de veïnat

Les comunicacions que importen — el requeriment a l'administrador, l'avís del desperfecte que després serà sinistre, la queixa formal — enviades i capturades amb data certa [3], sense burofax ni notari per a cada minúcia. I quan el conflicte escala, l'expedient sencer s'exporta com a paquet .asice verificable sense connexió [3], a punt per a l'advocat o el jutjat.

Els límits, per no vendre fum: el segell acredita convocatòries, actes i comptes — no resol el fons de cap disputa veïnal: si la derrama era justa o l'obra necessària, ho decideixen les majories i, si cal, el jutge [2]. La gravació de juntes exigeix l'acord de la mateixa junta i proporcionalitat: es documenta la decisió col·lectiva, mai la vida dels veïns. I les actes contenen dades personals: la publicació és per empremta; el contingut queda a la comunitat.

La promesa i el perill

La promesa: comunitats on la confiança no depèn de la memòria de ningú [1][3]; impugnacions que discuteixen el fons sobre fets certs [2]; administradors honestos amb la millor credencial de la professió — registres verificables —; i la democràcia més petita del país funcionant, per fi, amb la traçabilitat que exigim a les grans.

Ara toca mirar els perills.

El primer és **la comunitat vigilada**. Si cada escala esdevé un camp de gravacions creuades, s'haurà perdut més que no es guanya. La línia és nítida: es documenten els actes de govern — convocatòria, votació, acta, comptes — per acord col·lectiu; mai la convivència, mai els veïns entre si.

El segon és **la guerra de bloquejos**. El veí processiu amb eines pot inundar la comunitat d'impugnacions documentades. El contrapès és la mateixa simetria: la junta que ho fa bé té l'expedient que ho prova, i la impugnació infundada mor de fets.

El tercer és **la bretxa digital del replà**. La comunitat és de tothom, també de qui no té mòbil intel·ligent. Cap sistema no pot excloure: el paper continua valent — s'escaneja i s'ancora —, i qui certifica és la comunitat com a òrgan, no cada veí pel seu compte.

El quart perill viu al replà mateix: esperar que la tècnica faci de bon veí. Cap empremta no arregla la comunitat enverinada ni paga la derrama de qui no pot. La data certa pacifica la capa dels fets; la convivència i la solidaritat entre veïns són — i seran — feina humana.

És hora d'actuar

Deu minuts d'acord a la primera junta estalvien anys de discussions.

Per a presidents i juntes: acordeu el protocol — convocatòries, actes i comptes segellats [3]; és una votació curta que canvia la vida de la comunitat.

Per als administradors de finques: ancoreu el llibre d'actes i els comptes que gestioneu [1][3] — la vostra feina ben feta mereix ser indiscutible, i la professió sencera guanya quan el frau no té on amagar-se.

Per als veïns: guardeu amb data certa el que us afecta — la convocatòria, l'avís del desperfecte, la comunicació a l'administrador [3]; el dia de la impugnació [2], els fets valdran més que els records.

Per als col·legis d'administradors: feu del registre ancorat un estàndard professional i un segell de qualitat — el cas de Gijón [1] és el contraexemple que la professió no es pot permetre.

Per als legisladors: la Llei de Propietat Horitzontal ja admet juntes telemàtiques [2]; el pas natural és el llibre d'actes electrònic amb data certa verificable — la fe pública de la vida comunitària, a cost de cèntims.

A la pròxima junta, quan s'alcin les mans, que el recompte tingui data certa — i que la discussió de l'any que ve sigui sobre l'ascensor, no sobre què es va votar. Per la democràcia del replà, **time2act**.

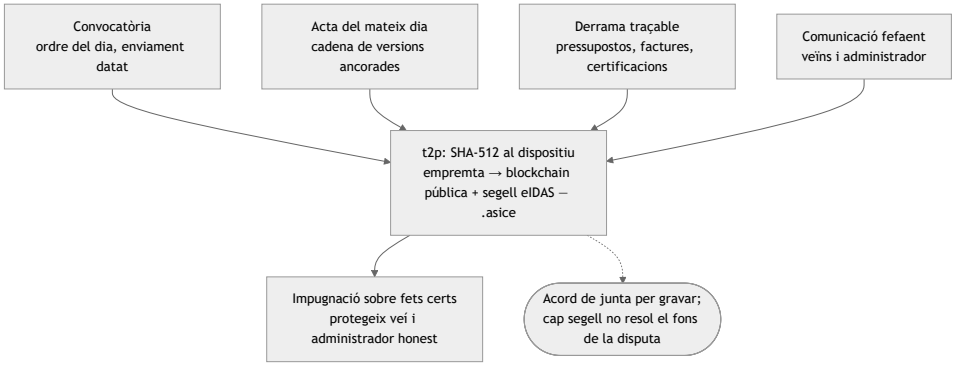


Figura 37.1 — La comunitat de propietaris amb prova d'existència (segellat amb t2p — capítol 13): la convocatòria amb data certa d'enviament, l'acta segellada el mateix dia (llibre d'actes com a cadena de versions ancorades), la derrama traçable (pressupostos, acord, factures, certificacions en un projecte) i la comunicació fefaent entre veïns i administrador. Simetria: protegeix el veí que impugna i l'administrador honest. Límits: acords de junta per gravar, publicació només per empremta (dades personals), i cap segell no resol el fons de les disputes (LPH). Fonts: condemna de Gijón (art. 253 CP); Llei de Propietat Horitzontal.

---

[1] Vecindia — *Condenado administrador de fincas por apropiación indebida* (Gijón: 1 any i mig de presó confirmats; 2.984,04 € del compte comunitari; maniobres enganyoses al llibre d'actes fent signar expresidents; rebuts d'obra i serralleria falsos per encobrir-se; descobert en canviar president i tresorer); 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 (impugnació d'acords contraris a la llei, lesius o abusius; convocatòries i actes; juntes telemàtiques habilitades per reforma recent); 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 producte (escàner de documents fins a 50 pàgines en un PDF certificat; gravació d'àudio; captura de pantalla i correu certificades; foto amb GPS forense; projectes per agrupar l'expedient d'una obra; certificar qualsevol fitxer — només l'empremta viatja; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; la propietat i el registre, al capítol 35; el lloguer, al capítol 36. ↩

Reformes a casa: la bestreta, l'obra i la prova

«Quan construïm, pensem que construïm per sempre.»

— John Ruskin, The Seven Lamps of Architecture (1849)

La cuina, a mig fer: taulells arrencats, tubs a la vista, una capa de pols sobre cada superfície. Al centre del desordre, un telèfon que ja no contesta. L'últim missatge deia: «la bestreta està pagada, els materials encarregats — torno demà». La data de tornada es repeteix des de llavors: sempre demà.

No és una excepció: és un guió documentat [1]. La Guàrdia Civil i la policia investiguen periòdicament el mateix patró: l'anunci atractiu en un portal digital, el pressupost sospitosament barat, el primer pagament per avançat «per a la compra de materials», i la desaparició. A Vigo i la seva comarca, una sola investigació va comptar almenys sis víctimes amb pèrdues de fins a 10.000 euros cadascuna; en altres casos, les pèrdues acumulades han superat els 77.000 euros; i a Guadalajara, un veí va perdre els estalvis davant d'un fals paleta d'internet fins que la Guàrdia Civil va acorralar l'estafador a Madrid [1].

I el matís que fa el capítol sencer: per cada estafador hi ha centenars de professionals honestos que pateixen el mateix buit de prova des de l'altra banda — el client que regateja l'última factura al·legant defectes, els «extres» que sí que es van demanar de paraula, la reputació d'un ofici sencer tacada pels qui fugen. Aquest capítol tracta el contracte més car que una família signa sense signar gairebé res. La derrama i l'obra comuna de l'edifici són al capítol 37; el cobrament del professional, al capítol 34; la construcció industrial, al capítol 94; l'assegurança de la llar, al capítol 28. Pregunta clau: com es discuteix una obra quan tot el que hi ha són WhatsApps, un PDF sense signar i records? Resposta: donant data certa a cada pas — el pressupost, l'estat inicial, les fases, els pagaments, la recepció — amb **t2p**: la cadena empremta–hora–àncora descrita al capítol 13 [3]. Protegeix la família de l'estafador — i el professional honest, del client que no vol pagar.

El contracte que mai no s'escriu

Molt més freqüent que l'estafa penal és el conflicte ordinari, i tothom n'ha sentit una versió: el pressupost verbal que creix — «han sortit coses» —; la qualitat promesa que ningú no pot contrastar; els terminis que s'allarguen sense data; els pagaments que van per davant de la feina feta; els «extres» mai pactats per escrit; l'obra que queda a mitges amb la relació trencada. El marc hi és — el Codi Civil regula el contracte d'obra, i la normativa de consum exigeix pressupost previ i factura quan el client és consumidor [2] — però l'evidència típica d'una reforma domèstica és un PDF sense signar, una cadena de WhatsApps i transferències sense concepte.

La reforma té totes les característiques del conflicte perfecte: import alt, durada llarga, especificacions que evolucionen, dues parts sense hàbit documental — i un objecte, la casa, que canvia cada dia esborrant l'estat anterior. Quan arriba la discussió, ni el client pot provar què es va pactar ni el professional pot provar què va fer. I el pitjor: l'estat inicial de l'habitatge — la paret que «ja estava esquerdada», el parquet que «ja estava ratllat» — desapareix físicament sota l'obra mateixa, per sempre.

Els drets existeixen; els fets, no. Cada missatge es pot esborrar, cada transferència queda sense concepte, cada acord verbal viu en dues memòries que divergeixen. El que falta no és més normativa: és que el que es pacta i el que es fa deixin rastre datat a les mans de tots dos.

La prova d'existència aplicada

Cinc minuts el primer dia, deu segons a cada fita [3].

1. El pressupost i les seves versions

El pressupost acceptat — i cada modificació pactada després — escanejat i segellat amb t2p el dia que es pacta: fins a 50 pàgines en un únic PDF certificat [3]. Els «extres» deixen de ser una discussió: o tenen data i document, o no existeixen. Protegeix el client del pressupost que creix sol — i el professional del client que «no recorda» haver demanat el canvi.

2. L'estat inicial: la foto que protegeix tots dos

Abans de la primera maceta, un recorregut fotogràfic per l'habitatge amb GPS forense [3]: les parets, els terres, les finestres, allò que ja estava fet malbé. És l'evidència que l'obra destruirà físicament — i l'única defensa contra les dues acusacions simètriques: «m'heu fet malbé el parquet» i «això ja estava així». Cinc minuts que valen tot el conflicte.

3. Les fases amb fites: pagar contra fets

Cada fita d'obra — l'enderroc acabat, la instal·lació passada, l'alicatat fet — documentada amb fotos i un vídeo curt amb data i hora sobreimpreses [3], i el pagament corresponent lligat a la fita al mateix projecte de l'app: pressupost, fase, evidència, justificant. La bestreta deixa de ser un acte de fe: es paga contra fets documentats — el patró que desarma l'estafa de la bestreta [1], perquè qui no pensa tornar no vol fites.

4. La recepció signada

L'obra acabada — o cada fase — es rep amb la signatura forta de t2p: el vídeo-selfie amb reptes de vida i verificació biomètrica, de totes dues parts [3]. La recepció datada tanca el perímetre de la responsabilitat: els defectes que apareguin després es discuteixen sobre l'estat rebut i documentat, no sobre memòries. I l'expedient sencer — pressupost, estat inicial, fases, pagaments, recepció — s'exporta com a paquet .asice verificable sense connexió [3]: per a la reclamació de consum, la via civil o la denúncia [1].

Els límits, com sempre, per endavant: el segell acredita documents, estats i moments — no valora la qualitat tècnica de l'obra: això ho fan els pèrits i, si cal, el jutge [2]. No substitueix triar bé — referències, professionals identificables, desconfiança del pressupost impossible [1]. I la proporcionalitat mana: el lampista que ve una hora no necessita expedient; la reforma de 30.000 euros, sí.

La promesa i el perill

La promesa: famílies que paguen contra fets i no contra promeses [1][3]; professionals honestos blindats davant del mal client — i un ofici que recupera la reputació que els estafadors li roben; conflictes d'extres i terminis que es resolen mirant documents datats [2]; i l'estafa de la bestreta, cada cop més difícil: qui no pensa tornar no accepta fites.

Els perills, que no són pocs.

El primer és **el client-expedient**: qui documenta obsessivament per construir excuses de no pagar. La simetria el desarma: si cada fase té evidència i recepció signada, l'impagament final es queda sense relat — la mateixa traça que protegeix el client, l'obliga.

El segon és **la fricció al petit ofici**. L'autònom que fa tres feines al dia no pot administrar expedients. El gest ha de ser el de deu segons — la foto de la fita, l'escaneig del pressupost [3] — i, ben mirat, és el mateix que ja fa per WhatsApp: només que amb data certa i sense dependre d'un xat.

El tercer és **l'estafador que també documenta**: el teatre del professional fals amb fotos boniques. La traça no substitueix la prudència: el patró de l'estafa és previ a l'obra — el preu impossible i la pressa per la bestreta [1] — i cap segell no valida un pressupost; valida que existia.

I encara un quart: creure que documentar bé és construir bé. Cap empremta no fa bona una obra ni honest un ofici. La qualitat la fan les mans i els materials; la prova només garanteix que, si surt malament, la discussió sigui de fets. I la millor regla continua sent antiga: no pagar mai gaire per davant del que hi ha fet.

És hora d'actuar

Que la confiança es guanyi amb fites, no amb promeses.

Per a les famílies: el ritual dels cinc minuts — pressupost segellat, estat inicial fotografiat, pagaments contra fites [3]; i davant del preu impossible amb pressa per la bestreta, la resposta és no [1].

Per als reformistes i els gremis: l'expedient datat és el vostre millor comercial — pressupost, fases i recepció signada [3] us blinden del mal client i us distingeixen de l'estafador que us taca l'ofici [1].

Per als administradors de finques: exigiu l'expedient verificable a les obres que superviseu — la derrama del capítol 37 i la reforma privada comparteixen la mateixa lògica.

Per a les autoritats de consum i la Guàrdia Civil: l'expedient .asice de la víctima [1][3] és la diferència entre una denúncia arxivable i una investigació amb fets.

Per als legisladors: la normativa de consum ja demana pressupost previ i factura [2]; el pas natural és reconèixer el pressupost i la recepció amb data certa com a prova qualificada del que es va pactar.

Que la pròxima cuina a mig fer tingui, almenys, un expedient sencer — i que el professional que acaba la feina pugui cobrar-la sense discutir records. Per les cases que es reformen i els oficis que les aixequen, **time2act**.



Figura 38.1 — La reforma amb prova d'existència (segellat amb t2p — capítol 13): el pressupost i les seves versions segellats el dia de pactar-se, l'estat inicial fotografiat amb GPS forense (la prova que l'obra esborra), les fases amb fites — pagar contra fets documentats — i la recepció signada amb vídeo-selfie de les dues parts. Simetria: protegeix la família de l'estafa de la bestreta i el professional honest del client que no vol pagar. Context: investigacions de la Guàrdia Civil (Vigo: ≥6 víctimes de fins a 10.000 €; pèrdues >77.000 € en algun cas). Límits: la qualitat la valoren els pèrits; proporcionalitat; no pagar per davant dels fets. Fonts: premsa/Guàrdia Civil; normativa de consum.

---

[1] Atlántico — *Investigan varias estafas en reformas de viviendas en Vigo y su comarca* (almenys sis víctimes; fins a 10.000 € cadascuna; constructor que inicia obres i desapareix); Liberal de Castilla — *Un vecino de Guadalajara pierde sus ahorros ante un falso albañil de internet* (Guàrdia Civil; estafador localitzat a Madrid); Telemadrid — *Destapamos al presunto estafador de las reformas*; Allende Abogados — *Estafas en reformas* (patró: oferta digital atractiva, pressupost barat, bestreta «per a materials», desaparició; pèrdues que superen els 77.000 € en alguns 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] Marc del contracte d'obra (Codi Civil) i normativa de consum aplicable a reformes amb consumidors (pressupost previ i factura). Vegeu el capítol 34 per al cobrament del professional i el capítol 37 per a l'obra comuna. ↩

[3] t2p — manual de producte (escàner de documents fins a 50 pàgines en un PDF certificat; foto amb GPS forense — fix genuí ~50 m / ≤30 s; vídeo amb data/hora sobreimpresa; projectes per lligar pressupost, fases, evidències i pagaments; signatura amb vídeo-selfie, reptes de vida i biometria; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; la derrama, al capítol 37; la factura, al capítol 34. ↩

Actius del món real: tokenitzar amb proves, no a cegues

«Cada home té una propietat en la seva pròpia persona... El treball del seu cos i l'obra de les seves mans són pròpiament seus.»

— John Locke, Segon tractat del govern civil, V, §27 (1689)

El 20 de març de 2024, el gestor d'actius més gran del món va fer un gest que va sacsejar Wall Street. BlackRock va llançar el seu primer fons tokenitzat, el BUIDL, sobre la xarxa pública Ethereum: lletres del Tresor nord-americà, efectiu i repos posats dins d'un token que es pot moure en una cadena de blocs. En dotze mesos, el fons va superar els **mil milions de dòlars** [4][5]. El seu conseller delegat, **Larry Fink**, ho havia anunciat a la seva carta anual als inversors com «la propera generació dels mercats»: convertir accions, bons i immobles en tokens digitals negociables, capaços de «democratitzar el rendiment».

Però en aquell gest hi havia un detall que conté tota la tensió d'aquest capítol. El token viu a la cadena; els bons reals que l'avalen, no. Continuen en un custodi, **fora de la cadena**, i el token només *hi apunta*. El mateix Fink ho va admetre amb una franquesa reveladora: perquè això escali, va dir, cal resoldre la verificació d'identitat —saber qui hi ha a l'altra banda i que el token estigui realment avalat [10]. Aquesta és la pregunta del capítol: quan tokenitzem el món real, el token apunta a una **promesa** o a una **prova**?

La gran aposta —i el seu forat

La promesa econòmica és vertiginosa, encara que ningú no es posa d'acord en la xifra. La consultora **BCG**, amb la borsa de mercats privats ADDX, va projectar el 2022 en el seu informe *Relevance of On-chain Asset Tokenization* que el mercat creixeria cinquanta vegades, fins a uns **16,1 bilions de dòlars el 2030** —un 10 % del PIB mundial [1]. **McKinsey**, com hem vist, preveia uns **2 bilions** el 2030, amb un rang d'1 a 4 [2]; la diferència —vuit vegades— no és un detall tècnic: reflecteix quanta escombraria estan disposades a admetre i la velocitat real de l'adopció. Standard Chartered projecta uns **30,1 bilions** el 2034 [9].

La realitat actual és més modesta i reveladora. A mitjan 2025, el mercat de RWA tokenitzats —sense comptar les stablecoins— era d'uns **24.000 milions de dòlars**, un 380 % més que tres anys abans [3]. El segment més gran no eren els bons del Tresor, sinó el **crèdit privat** (uns 14.000 milions), seguit dels Tresors (uns 7.000) i de l'or tokenitzat (uns 4.000). Aquest or il·lustra bé el problema i la solució: el token PAXG està avalat per barres amb número de sèrie guardades a les cambres de Brink's a Londres, i des de febrer de 2025 l'auditoria KPMG n'emet atestacions mensuals que verifiquen l'aval unça per unça [6]. La pregunta és: i si l'atestació es pogués falsejar o retrodatar? Tot l'edifici descansa, una vegada més, sobre una prova.

El problema de l'oracle

Aquí rau la fragilitat estructural de tota la tokenització, i té nom tècnic: el **problema de l'oracle**. El token és a la cadena, però el valor és fora —la barra d'or, l'escriptura, el bo, l'informe de custòdia—, i algú ha de fer de pont entre ambdós mons. El **Consell d'Estabilitat Financera** (FSB), organisme que coordina la regulació financera global, ho va advertir amb claredat en el seu informe *The Financial Stability Implications of Tokenisation* (octubre del 2024): la tokenització «depèn sovint de proveïdors externs, com custodis per guardar els actius de referència i oracles per recollir-ne les dades», cosa que «introdueix nous punts de vulnerabilitat» i pot provocar un «desajust entre el preu del token i el valor de l'actiu de referència» [7]. L'agència de qualificació **Moody's** hi va afegir que molts emissors i proveïdors tecnològics tenen un «historial limitat» i que una fallada d'oracle pot interrompre els pagaments encara que el codi funcioni perfectament [8].

No és una por abstracta. El març de 2022, la stablecoin Cashio, a la xarxa Solana, es va esfondrar quan un atacant va explotar un error que li permetia encunyar tokens «avalats»... sense cap col·lateral real [8]. És la imatge literal del principi que recorre aquest llibre: «escombraries a l'entrada, escombraries a la cadena». Un token perfectament vàlid a la cadena que no estava avalat per res. I aquí convé recordar la lliçó ja explicada amb els crèdits de carboni: quan es tokenitza sobre un subjacent no verificat, la cadena

s'omple de «crèdits zombi». Traslladat als actius del món real, el mateix error es repetiria a escala de bilions.

Tokenitzar a cegues o tokenitzar amb proves

La conclusió és nítida i és la tesi del capítol. La blockchain no fa veritat el que tokenitza; el fa *negociable i immutable*. Si el que hi ha a sota és una promesa sense prova, tindrem una promesa immutable —que és exactament el pitjor: una mentida que es ven amb l'aparença de la certesa criptogràfica. La diferència entre un mercat de 2 bilions sòlids i un de 16 bilions inflats no la marca la tecnologia del token, sinó **la qualitat de la prova del que hi ha a sota**. Tokenitzar a cegues és repetir l'error dels zombis; tokenitzar amb proves és la condició perquè aquesta revolució financera no acabi en una crisi de confiança.

La prova d'existència sota el token

És aquí on **t2p** aporta la peça que falta. No resol la custòdia ni la legalitat —això pertoca al custodi, a l'auditor i al registre—, però **segella l'evidència documental que un token hauria de referenciar**, de manera verificable fora de línia. El mecanisme és el de sempre, aplicat al respatller. El document que constitueix el respatller del token —l'escriptura, l'informe de taxació, el certificat de custòdia o d'auditoria, la pòlissa, la fotografia de la barra amb el seu número de sèrie— rep una **empremta SHA-512** calculada al dispositiu, s'ancora a la **blockchain pública** i s'acompanya d'un **segell de temps RFC 3161** conforme a eIDAS. Per als actius físics, la captura porta **GPS forense** i data segellats: «aquesta foto de l'actiu es va prendre aquí, aquest dia». I la **prova de vida** lliga l'evidència a una persona real —el taxador, el custodi, el firmant—, resolent precisament la verificació d'identitat que Fink assenyalava com a coll d'ampolla.

Tot s'empaqueta en un **contenidor .asice verificable fora de línia**, sense dependre de t2p ni de la cadena del token. I aquí hi ha el gir: el token RWA pot **apuntar a l'empremta d'un .asice** en lloc d'apuntar a una promesa. El comprador deixa de confiar que hi ha un bo al darrere; pot **comprovar per ell mateix** que l'evidència existia íntegra en aquell moment, lloc i persona. Això tanca la porta a la substitució o la postedició del document de respatller, a reutilitzar el mateix informe per a diversos tokens i a l'opacitat sobre *quan* existia la prova. Convertir «confia que hi ha un actiu» en «aquí tens el segell de l'evidència, verifica'l» és, en si mateix, una transformació del risc.

Cal ser, com sempre, escrupolosament honest amb el límit, perquè aquí és especialment perillós oblidar-lo. La prova d'existència demostra que **un registre va existir, íntegre, en un moment, lloc i persona**; **no** demostra que la barra segueixi a la cambra, que no s'hagi pignorat dues vegades, ni que el token confereixi un dret legal sobre ella. La custòdia, l'auditoria independent de l'inventari i l'exigibilitat legal del dret continuen sent imprescindibles. t2p reforça la **capa d'evidència**, no substitueix el custodi ni l'auditor; és complementari, per exemple, a sistemes de prova de reserves que verifiquen el respatller connectant-se als custodis. És, en una frase, la diferència entre tokenitzar a cegues i tokenitzar amb proves.

La promesa i el perill

La promesa és immensa: una tokenització recolzada en evidència verificable podria obrir als petits inversors avui actius il·líquids —immobles, fons privats, infraestructures—, fer els mercats més ràpids i transparents, i fer-ho sense sacrificar la confiança. En un mercat que podria valdre bilions, que cada token apunti a una prova i no a una promesa és la diferència entre una revolució i una bombolla.

El perill demana el matís de sempre, en la dualitat de «la promesa i el perill». El primer, ja dit: confondre el segell de l'evidència amb la garantia del dret legal o de la custòdia seria un frau pitjor que el que es vol evitar. El segon, la falsa sensació de seguretat que pot donar una capa tècnica brillant sobre un actiu dolent. I el tercer, la concentració: si la verificació de l'evidència queda en molt poques mans, recreem l'intermediari únic que la blockchain prometia dissoldre. La prova d'existència és una capa necessària dins d'una arquitectura que inclou, sempre, el custodi, l'auditor i el regulador.

És hora d'actuar

Per als **emissors i tokenitzadors**: ancoratge de l'evidència del respatller —taxacions, certificats de custòdia, fotos serialitzades— perquè cada token apunti a una prova verificable, no a una promesa. Per als **custodis i auditors**: segellar les seves atestacions en origen, impedint que es puguin retrodatar ni reutilitzar. Per als **inversors**: exigir poder comprovar l'evidència del subjacent abans de comprar i desconfiar del token que només ofereix una promesa. Per als **reguladors** (FSB, supervisors nacionals): reconèixer el valor de la capa d'evidència i tancar el buit de l'oracle abans que el mercat arribi als bilions anunciats.

BlackRock va posar bons del Tresor dins d'un token, però els bons continuen fora de la cadena. Tota la tokenització del món real depèn d'aquell fil invisible entre el token i la prova del que el recolza. Fer que aquest fil sigui verificable per qualsevol —tokenitzar amb proves, no a cegues— és, també aquí, time2act.

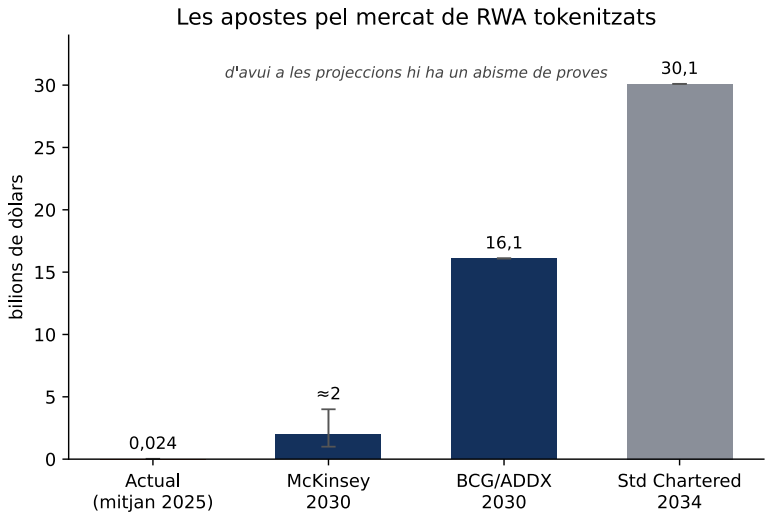


Figura 39.1 — Les dues projeccions de referència per al mercat de RWA tokenitzats el 2030 difereixen unes vuit vegades: l'escenari prudent de McKinsey (~2 bilions de dòlars, rang 1-4) i l'optimista de BCG/ADDX (~16,1 bilions); el punt de partida real era d'uns 24.000 milions a mitjan 2025. La distància depèn, en el fons, de quanta «escombraria» s'admeti: del buit entre el token i la prova del seu respatller —el problema de l'oracle— que la prova d'existència ajuda a tancar. Fonts: McKinsey (2024); BCG/ADDX (2022); CoinDesk/RWA.xyz (2025).

---

[1] BCG i ADDX — *Relevance of On-chain Asset Tokenization in 'Crypto Winter'* (2022; ~16,1 bilions $ el 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; cas base ~2 bilions $, rang 1-4, exclou 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$; crèdit privat ~14.000 M$). 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* (març 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* (barres serialitzades a Brink's Londres; atestacions mensuals de KPMG). https://www.paxos.com/paxg-transparency ↩

[7] Financial Stability Board — *The Financial Stability Implications of Tokenisation* (octubre 2024; custodis i oracles com a nous punts de vulnerabilitat). https://www.fsb.org/2024/10/the-financial-stability-implications-of-tokenisation/ ↩

[8] Moody's (via CoinDesk) — *Tokenized fund adoption grows but brings technology risks* (2024; fallades d'oracle, historial limitat). https://www.coindesk.com/markets/2024/01/15/tokenized-fund-adoption-grows-but-brings-technology-risks-moodys ↩

[9] Standard Chartered i 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 verificació d'identitat com a condició). https://www.investmentnews.com/alternatives/larry-fink-takes-aim-at-investment-inequality/259910 ↩

Autoria creativa: provar qui ho va fer primer en l'era de la IA

«Perquè les obres mestres no són naixements únics i solitaris; són el fruit de molts anys de pensar en comú [...] de manera que darrere la veu única hi ha l'experiència de la multitud.»

— Virginia Woolf, Una cambra pròpia (1929)

El 4 d'abril de 2023, un usuari anònim que es feia dir *ghostwriter977* va penjar una cançó a les plataformes de streaming. Es titulava «Heart on My Sleeve» i sonava com una col·laboració inèdita entre Drake i The Weeknd, dos dels artistes més grans del planeta. No ho era: les seves veus havien estat clonades amb intel·ligència artificial. La cançó es va escampar com la pólvora —només a TikTok va acumular uns **quinze milions de visualitzacions**— fins que, el dilluns següent, plataforma a plataforma, va desaparèixer. A YouTube hi quedava el cartell: «Aquest vídeo ja no està disponible per una reclamació de copyright d'Universal Music Group» [7]. La discogràfica va aconseguir retirar-la al·legant que entrenar i generar IA amb les veus dels seus artistes vulnerava els seus acords i la llei.

L'escena conté tota la inquietud d'aquest capítol. Dos dels músics més poderosos del món van quedar, durant uns dies, a mercè d'un anònim, i la cançó ni tan sols contenia les seves gravacions: només les seves veus sintètiques. Per a un creador sense l'exèrcit jurídic d'una multinacional —una il·lustradora, un fotògraf, un guionista, un músic independent—, la pregunta és encara més angoixant: com demostro que **una obra és meva i que existia abans** que una màquina se l'empassés o que algú la copiés? Aquest capítol tracta d'això: de tornar a fer demostrable l'autoria en l'era de la còpia infinita.

La maquinària que s'empassa l'autoria

El cas de la cançó és la punta d'un iceberg de litigis que estan redefinint la creació. El **New York Times** va demandar OpenAI i Microsoft el desembre de 2023 per haver copiat «milions» dels seus articles sense permís ni pagament per entrenar els seus models; com a prova, va adjuntar un annex de 127 pàgines que alinea, columna contra columna, paràgrafs del diari i sortides gairebé idèntiques de GPT-4 —la demostració visual que el model «memoritzava» el periodisme que suposadament només havia «après» [1]. El cas avança a poc a poc: el gener de 2026, un jutge va obligar OpenAI a lliurar als demandants una mostra de vint milions de registres de converses de ChatGPT [2]. **Getty Images** va portar Stability AI als tribunals de Londres per haver processat milions de les seves imatges sense llicència [3][4]. I un grup d'artistes va demandar Stability, Midjourney i DeviantArt per haver alimentat els generadors amb la seva obra.

Una d'aquelles artistes és **Karla Ortiz**, il·lustradora que ha donat forma a personatges de Marvel. El juliol de 2023 va declarar davant del Comitè Judicial del Senat dels Estats Units una frase que resumeix el greuge de tota una professió: sobre la pràctica totalitat de la seva obra ingerida pels models, «mai m'han preguntat, mai m'han acreditat, mai m'han compensat ni un cèntim» [6]. No és un rebuig a la tecnologia. Com subratlla la mateixa Getty —que sí que llicencia el seu catàleg a desenvolupadors d'IA respectant els drets—, el conflicte no és la IA en si, sinó **el consentiment i la llicència** [3]. I a Hollywood, la vaga d'actors de SAG-AFTRA, la més llarga de la història contra els estudis, es va saldar amb un acord que exigeix consentiment informat i compensació justa abans de crear una «rèplica digital» d'un intèrpret [8].

El creador i la prova de prioritat

Sota tots aquests casos hi ha un mateix problema, i és de **prioritat temporal**: demostrar que un tema, una il·lustració, un guió o una foto existien, signats per tu, *abans* que un model els ingerís o que algú els copiés. I aquí la llei ha donat una pista decisiva. L'Oficina de Copyright dels Estats Units va establir el gener de 2025 que **l'autoria humana és el fonament del copyright**: una obra generada enterament per IA no és registrable, i la simple tria de instruccions, per detallada que sigui, no basta per crear una obra protegible [10]. La conseqüència és profunda: en un món inundat de contingut sintètic, el valor es desplaça cap a **qui va crear què, i quan**. La prova de l'autoria humana i de la seva data esdevé l'actiu central.

Per què l'etiqueta sola s'esborra

La indústria ja ha intentat respondre amb una bona idea: les **Content Credentials** de l'estàndard **C2PA**, una coalició sota la Linux Foundation que inclou Adobe, la BBC, Google, Microsoft, OpenAI o Sony. Funcionen com una «etiqueta nutricional» del contingut digital: un manifest signat criptogràficament i incrustat al fitxer que registra qui el va crear, quan, amb quines eines i amb quin historial d'edició [9]. És una eina valuosa i necessària. Però té un taló d'Aquil·les confirmat, i és demolidor: **la majoria de xarxes socials recomprimeixen les imatges en pujar-les i esborren el manifest**. WhatsApp, iMessage o Facebook reescriuen el fitxer i eliminen les credencials; una captura de pantalla, un canvi de format o un reescalat n'hi ha prou per trencar-les. La pròpia C2PA ho reconeix i ha introduït «credencials duradores» amb marca d'aigua invisible, però admet que el sistema «depèn del compliment de tot l'ecosistema», una cosa poc realista en un entorn obert. L'etiqueta, doncs, viatja dins del fitxer i es perd amb ell. Falta una àncora independent.

La prova d'existència: segellar l'obra en néixer

És aquí on **t2p** aporta exactament aquesta àncora. En lloc d'escriure la prova *dins* del fitxer —d'on es pot esborrar—, la fixa *fora*, en una cadena pública. En el moment de la creació, es calcula l'**empremta SHA-512** de l'obra —el `.wav` de la maqueta, el `.psd` per capes, el `.raw` de la foto, el guió— **al mateix dispositiu, sense que el fitxer surti**: un detall crucial per al creador que encara no ha publicat i no vol pujar la seva obra inèdita a cap servidor. Aquella empremta s'ancora a la **blockchain pública** amb un **segell de temps RFC 3161** conforme a eIDAS, creant una **data certa d'autoria** verificable per qualsevol, que sobreviu encara que el creador canviï de plataforma o desaparegui. El **GPS forense** i la **prova de vida** lliguen el moment de creació a un lloc i a una persona viva —útil contra les disputes de «qui ho va fer primer» i contra les rèpliques sintètiques, perquè vinculen l'obra a un autor humà real. I tot s'empaqueta en un **contenidor .asice verificable fora de línia** que un tribunal o un comprador poden comprovar pel seu compte.

La clau és que t2p **no competeix amb C2PA, la completa**. Les Content Credentials aporten la traçabilitat llegible dins del fitxer; la prova d'existència aporta l'**àncora immutable** que sobreviu encara que el manifest s'esborri o algú faci una captura de pantalla: el hash a la cadena segueix demostrant que aquell fitxer exacte existia en tal data, lloc i persona. La parella natural és aquesta: credencials per a la traçabilitat, prova d'existència per a l'àncora. I el **marketplace NFT** afegeix un historial de procedència i de llicències que no es pot editar a posteriori, útil per llicenciar legítimament a qui sí vulgui entrenar amb consentiment —el model Getty: llicència, no espoli.

Cal dir els límits sense embuts, fidels a la dualitat de «la promesa i el perill». «Escombraries a l'entrada, escombraries a la cadena»: la prova d'existència demostra **quan, què, on i qui** va segellar, no que l'obra sigui **original o no infractora**. Si segelleu un plagi, tindreu un plagi amb data certa. Tampoc no resol la qüestió jurídica de fons —si entrenar amb obra protegida és o no ús legítim—, que decidiran els tribunals i els reguladors. I l'autoria humana que exigeix la llei continua sent un requisit separat: el segell prova precedència, no converteix en registrable el que la llei no protegeix. Finalment, ancorar abans de publicar només ajuda si es fa abans de la filtració; no rebobina el que ja s'ha espoliat.

La promesa i el perill

La promesa és immensa per a milions de creadors. Una capa de prova d'autoria a l'origen els donaria, per primera vegada, una manera barata i universal de demostrar la prioritat de la seva obra, de defensar-se davant d'un tribunal i de llicenciar-la en els seus termes en lloc de veure-la espoliada. En una economia creativa amenaçada per la còpia infinita, poder dir «això és meu, i ho puc provar» és recuperar el poder de negociar.

El perill demana matís. El primer, no confondre precedència amb originalitat: el segell no neteja un plagi ni resol per si sol l'autoria legal. El segon, la càrrega per als creadors menys tecnològics, que el disseny ha de fer trivialment fàcil per no excloure ningú. I el tercer, la privacitat: la prova de vida i la geolocalització de l'acte creatiu són dades sensibles que cal protegir. La prova d'existència és una eina d'apoderament del creador, no una drecera que substitueixi els tribunals ni la llei.

És hora d'actuar

Per als **creadors** (músics, il·lustradors, fotògrafs, guionistes): segellar l'obra en el moment de crear-la, abans de compartir-la, per tenir data certa d'autoria. Per a les **plataformes**: deixar de destruir les credencials de procedència en pujar el contingut i reconèixer l'àncora independent. Per als **desenvolupadors d'IA**: llicenciar l'obra amb consentiment —el model Getty— en lloc d'espoliar-la, fent servir el rastre de procedència per identificar i compensar els autors. Per als **reguladors i tribunals**: tancar el marc legal del consentiment i l'ús just, i reconèixer el valor probatori del segell d'autoria.

Dos dels músics més grans del món van quedar indefensos davant d'una veu sintètica; el creador individual ho està encara més. La diferència entre una obra que qualsevol pot reclamar o copiar i una obra que neix amb una prova d'autoria inalterable és, cada cop més, la diferència entre crear i ser espoliat. Com hem vist, demostrar qui ho va fer primer —i que era humà— és, també aquí, time2act.

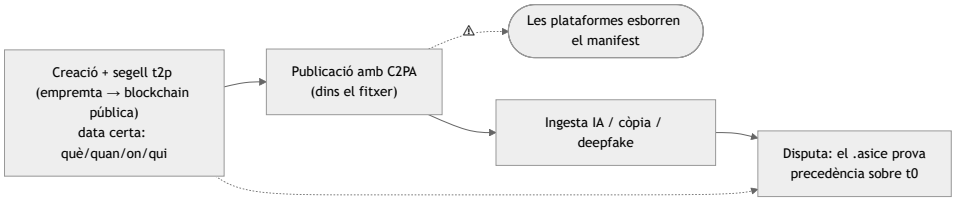


Figura 40.1 — En el moment de crear (t0), l'obra se segella amb empremta SHA-512 al dispositiu, àncora a la blockchain pública, segell de temps eIDAS, GPS i prova de vida: data certa de què, quan, on i qui. En publicar-la (t1), les credencials C2PA poden esborrar-se en pujar-la a les xarxes; quan un model la ingereix o algú la copia (t2), el contenidor .asice encara demostra que el fitxer existia intacte a t0, abans de t2. La prova d'existència demostra precedència, no originalitat. Fonts: C2PA; U.S. Copyright Office; casos NYT, Getty, Andersen.

---

[1] NPR — *The New York Times sues OpenAI and Microsoft for copyright infringement* (27-des-2023; annex de 127 pàgines amb sortides 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* (gener 2026). https://news.bloomberglaw.com/ip-law/openai-must-turn-over-20-million-chatgpt-logs-judge-affirms ↩

[3] Getty Images — *Getty Images statement* (acció contra Stability AI; consentiment i llicència, gener 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 major part de les reclamacions 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 des d'agost 2024). https://copyrightalliance.org/andersen-v-stability-ai-copyright-case/

[6] Karla Ortiz — *Testimony before the U.S. Senate Judiciary Committee* (12-jul-2023; «mai m'han preguntat, acreditat ni compensat»). 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 per 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; consentiment per a la «rèplica digital»). https://en.wikipedia.org/wiki/2023_SAG-AFTRA_strike ↩

[9] C2PA / Content Authenticity Initiative — *Content Credentials* (manifest signat; les plataformes l'esborren en recomprimir). https://c2pa.org/ ↩

[10] U.S. Copyright Office — *Copyright and Artificial Intelligence, Part 2: Copyrightability* (29-gen-2025; l'autoria humana com a fonament). https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf ↩

Patents i prior art: la publicació defensiva amb data certa

«Es pot resistir la invasió dels exèrcits; no es pot resistir la invasió de les idees.»

— Victor Hugo, Histoire d'un crime (1877)

Hi ha una escena que es repeteix als despatxos d'advocats de patents de tot el món. Un inventor independent arriba amb un sobre tancat, groguenc pels anys. A dins hi ha la descripció del seu invent, que ell mateix es va enviar per correu certificat fa temps, convençut que aquell mata-segells era una mena de **«patent del pobre»** que protegiria la seva idea. Ara un competidor ha patentat alguna cosa semblant, i l'inventor vol fer valer el seu sobre. L'advocat ha d'explicar-li, amb tacte, que aquell gest repetit durant dècades **mai no va protegir res**: enviar-se un sobre a un mateix no estableix cap dret de patent ni és una prova reconeguda pels tribunals [5]. I encara hi ha una notícia pitjor: des del 2013, als Estats Units, ni tan sols la data importa davant de qui va presentar primer la sol·licitud.

Aquesta escena conté el nus d'aquest capítol. La propietat industrial és una cursa cara i implacable, i la majoria d'inventors —els autònoms, les petites empreses, els investigadors— no s'hi poden permetre córrer. Però existeix una jugada poderosa i poc coneguda que els canvia les regles: en lloc de patentar, **publicar amb data certa** per impedir que ningú altre ho patenti. I aquí la prova d'existència ofereix una eina gairebé feta a mida.

La cursa de qui presenta primer

Per entendre la jugada, cal conèixer el terreny. El 16 de març del 2013, els Estats Units van abandonar el vell sistema de «primer a inventar» i van adoptar el de **«primer a presentar»** (*first-invention-to-file*), amb l'entrada en vigor de l'America Invents Act. Com resumeix la mateixa oficina de patents nord-americana, l'**USPTO**, a partir d'aquella data «la data de la invenció és irrellevant»: el que compta és qui presenta abans la sol·licitud [1]. El sistema premia la velocitat i el capital, no la paternitat de la idea.

Segons les estimacions del sector, redactar una sol·licitud de patent d'utilitat als Estats Units costa entre 9.000 i 17.000 dòlars, i cal pressupostar **entre 15.000 i 25.000 dòlars** abans que la patent es concedeixi, sense comptar les taxes de manteniment que s'estenen durant tota la seva vida [3]. Per a una gran corporació és calderilla; per a un inventor individual, una barrera sovint infranquejable. Existeix una via oficial més econòmica per fixar la data —la sol·licitud provisional, que per uns centenars de dòlars atorga l'estatus de «patent pending» durant dotze mesos—, però no s'examina i caduca si no es presenta després la sol·licitud completa [4].

Un concepte clau obre una porta. L'**Organització Mundial de la Propietat Intel·lectual** (WIPO) defineix l'**estat de la tècnica** —el *prior art*— com tota informació posada a disposició del públic en qualsevol lloc del món abans de la data de presentació; perquè una invenció sigui patentable, ha d'aportar una característica nova que no hi sigui [2]. I aquí ve el gir decisiu: la WIPO recorda que **divulgar públicament una invenció abans de presentar la sol·licitud pot destruir-ne la novetat** i fer-la impatentable —tret que la llei prevegi un «període de gràcia», present als Estats Units o al Canadà però no a Europa, i a la Xina només de manera molt restringida [2]. Aquesta espasa de doble tall és precisament l'arma defensiva.

Publicar per defensar-se

Si divulgar destrueix la novetat, es pot divulgar a propòsit per impedir que un altre ho patenti. És la **publicació defensiva**: difondre deliberadament una descripció de la invenció perquè entri al domini públic i es converteixi en prior art, derrotant qualsevol sol·licitud de patent posterior d'un tercer sobre la mateixa idea. No dona drets exclusius —un cop publicada, la invenció ja no es pot patentar—, però evita els costos d'una patent i, sobretot, impedeix que un competidor t'ho prengui i t'en cobri l'ús.

No és una idea marginal; és una indústria. **Technical Disclosure Commons**, una plataforma **gratuïta** operada per a Google, permet a qualsevol publicar una divulgació tècnica que el sistema **data automàticament** i que **Google Patents indexa**, de manera que un examinador la trobarà en avaluar una sol·licitud rival [6]. **IP.com** ofereix una base de dades de prior art on cada publicació es tanca amb un **segell de temps criptogràfic** —del servei Surety AbsoluteProof— que en protegeix la integritat i la data.

I **Research Disclosure**, el servei degà del sector, publica divulgacions defensives des de 1960. Tot aquest material es pot cercar en bases gegantines: l'Espacenet de l'Oficina Europea de Patents va superar els **160 milions de documents** l'abril de 2025, i la PATENTSCOPE de la WIPO en ronda els 128 milions [9][10]. Com expliquen els advocats de patents Richard Coller i Alexander Covington en un treball de referència sobre l'estratègia, la publicació defensiva no substitueix mai el valor d'una patent per a una innovació important, però és una manera molt rendible de bloquejar competidors quan cal prendre decisions difícils de pressupost [8].

Fixem-nos en un detall, perquè és la clau de tot: IP.com ja segella les seves publicacions amb una marca de temps criptogràfica i un fitxer validable per qualsevol. És, en essència, un **notari digital** que congela el contingut i la data. I aquí és on entra t2p, generalitzant aquell servei a qualsevol persona.

La prova d'existència per a la invenció

La mecànica de **t2p**, aplicada a la invenció, és senzilla i potent. L'inventor pren el document de divulgació —la memòria tècnica, els plànols, el codi, el quadern de laboratori on consta la concepció— i en calcula l'**empremta SHA-512** al dispositiu, sense que el document surti. Aquella empremta s'ancora a la **blockchain pública** amb un **segell de temps RFC 3161** conforme a eIDAS, i tot s'empaqueta en un **contenidor .asice verificable fora de línia**. El **GPS forense** i la **prova de vida** poden lligar el moment a un lloc i a una persona real.

El resultat demostra, de manera inalterable i verificable globalment, que **aquell contingut exacte existia íntegre en aquella data**, opcionalment en aquell lloc i per aquella persona. És, a la pràctica, dues coses alhora: una **publicació defensiva instantània i barata amb data certa** —si, a més, el contingut es fa públic en aquella data—, i una **prova de la data de concepció** per a disputes entre coinventors, entre empresa i empleat o entre socis. Davant del pressupost de quinze a vint-i-cinc mil dòlars d'una patent, el cost d'un segellat és marginal. I contra la retrodatació, és impenetrable: ningú no pot fabricar després un document «d'aquella data», perquè l'empremta ancorada i el segell són immutables.

Cal dir els límits amb tota la cruesa, fidels a la dualitat de «la promesa i el perill», perquè aquí confondre's surt car. La prova d'existència **no demostra novetat, patentabilitat, utilitat ni que l'invent funcioni**: això ho decideix l'examinador contra tot el prior art mundial. Tampoc no converteix un document privat en prior art per si sola: per bloquejar un tercer, la divulgació ha de ser **accessible al públic** —un hash ancorat sense publicar el contingut prova *possessió en una data*, no *disponibilitat per al públic*. I a Europa, on no hi ha període de gràcia, publicar **també destrueix la teva pròpia novetat**: la data certa no substitueix la decisió estratègica entre patentar i publicar, només la fa més sòlida un cop presa. «Escombraries a l'entrada, escombraries a la cadena»: el segell prova fecha i contingut, no que la idea sigui realment teva ni original.

La promesa i el perill

La promesa és profundament democratitzadora. Una eina de data certa barata posa a l'abast de l'inventor individual una jugada —la publicació defensiva— que fins ara dominaven les grans corporacions amb departaments de patents. Permet protegir la prioritat d'una idea, bloquejar que un gegant la patenti i resoldre disputes d'autoria, tot per una fracció del cost del sistema. En una economia de la innovació on la velocitat i el capital ho decideixen tot, significa tornar una mica de poder a qui crea.

El perill demana matís. El primer, ja dit: confondre el segell amb una patent o amb una prova de novetat seria un error costós; la prova d'existència és precedència, no patentabilitat. El segon, la temptació de segellar sense publicar i creure's protegit contra tercers, quan només la divulgació pública crea prior art oponible. I el tercer, la decisió irreversible: publicar defensivament tanca per sempre la porta a patentar aquella invenció. La prova d'existència és una eina al servei d'una estratègia, no un substitut del consell expert sobre quan patentar i quan publicar.

És hora d'actuar

Per als **inventors individuals i les petites empreses**: segellar la concepció amb data certa i, quan la jugada sigui defensiva, publicar la divulgació per bloquejar patents alienes a una fracció del cost. Per als **departaments de R+D**: integrar el segellat en el flux de treball, per tenir prova de prioritat de cada idea

abans de decidir què es patenta i què es publica. Per a les **plataformes de publicació defensiva**: oferir l'ancoratge independent com a complement al seu segell. Per a les **oficines de patents**: reconèixer i indexar aquestes divulgacions datades com a prior art de ple dret.

L'inventor del sobre groguenc va confiar la seva idea a un gest que no protegia res. Avui, qualsevol persona pot deixar constància inalterable que una idea era seva en una data certa i convertir-la en una muralla contra qui la vulgui patentar. Demostrar qui ho va concebre primer —i fer-ho a l'abast de tothom— és, també aquí, **time2act**.



Figura 41.1 — L'inventor segella el document de divulgació amb empremta SHA-512, àncora a la blockchain pública i segell de temps eIDAS (data certa, integritat i autoria), per un cost marginal davant dels 15.000-25.000 dòlars d'una patent. Si a més el publica (Technical Disclosure Commons, IP.com, web), es converteix en prior art indexat per Espacenet o Google Patents; quan arriba la sol·licitud d'un rival, l'examinador hi troba la divulgació datada i la rebutja per falta de novetat. El segell prova data i contingut, no la patentabilitat —que decideix l'examinador. Fonts: USPTO; WIPO; Technical Disclosure Commons.

---

[1] USPTO — *America Invents Act (AIA): Frequently Asked Questions* (primer a presentar des del 16-mar-2013; «la data de la invenció és irrellevant»). https://www.uspto.gov/patents/laws/america-invents-act-aia/america-invents-act-aia-frequently-asked ↩

[2] WIPO (Organització Mundial de la Propietat Intel·lectual) — *Patents: Frequently Asked Questions* (prior art; la divulgació prèvia destrueix la novetat; el període de gràcia no és universal). https://www.wipo.int/en/web/patents/faq_patents ↩

[3] BitLaw — *What does a patent application cost?* (redacció 9.000-17.000 $; pressupostar 15.000-25.000 $ abans de la concessió). https://www.bitlaw.com/guidance/patent/what-does-a-patent-application-cost.html ↩

[4] USPTO — *Fee Schedule* (sol·licitud provisional: fixa data, 12 mesos; taxes oficials). 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?* (sense valor legal; obsoleta des del first-to-file de 2013). https://www.mclane.com/insights/know-the-law-is-the-poor-mans-patent-real/ ↩

[6] Technical Disclosure Commons — *FAQ* (gratuït; data de publicació automàtica; indexat per Google Patents). https://www.tdcommons.org/faq.html ↩

[7] IP.com — *Publishing Disclosures to the Prior Art Database* (segell de temps mitjançant Surety AbsoluteProof). https://kb.ip.com/pad/knowledge-base/publishing-disclosures-to-the-prior-art-database-pad/

[8] Richard Coller III i 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 Patents (EPO) — *Espacenet reaches 160 million patent documents* (abril 2025). https://agip-news.com/news.aspx?id=76074&lang=en ↩

[10] WIPO — *PATENTSCOPE* (~128 milions de documents de patent; 5,4 M de sol·licituds PCT). https://patentscope2.wipo.int/ ↩

Secrets empresarials: provar sense revelar

«Ningú no pot guardar un secret si no es concedeix un petit marge de dissimulació, que és, per dir-ho així, la cua o el ròssec del secret.»

— Francis Bacon, Assaigs, «De la simulació i la dissimulació» (1625)

Un dels enginyers estrella del projecte de cotxe autònom de Google — el que esdevindria Waymo — es descarrega milers de fitxers confidencials al seu portàtil abans de plegar. Funda una empresa de camions autònoms, Otto. Uber la compra al cap de pocs mesos. I Waymo demanda Uber: anys i fortunes de recerca condueixen ara pel carril del costat. El 2018, Uber tanca l'afer amb un acord que la premsa va valorar en uns 245 milions de dòlars en accions [1]. El març de 2020, Anthony Levandowski es declara culpable de robatori de secrets comercials; a l'agost, el jutge William Alsup el condemna a divuit mesos de presó amb una frase per als annals: «el crim de secrets comercials més gran que he vist mai». I l'epíleg de novel·la: el 20 de gener de 2021, l'últim dia del seu mandat, el president Trump el va indultar [1].

Si això li va passar a Google — amb els millors advocats i sistemes del món —, què no passa cada setmana a escala petita: el comercial que marxa amb la llista de clients, el soci que surt amb el procediment de fàbrica, el proveïdor que «reinventa» el disseny que li vas ensenyar sota acord de confidencialitat. I la víctima descobreix aleshores el nus del secret empresarial: per defensar-lo davant d'un jutge ha de provar què tenia, des de quan i que ho protegia — sense revelar-ho una segona vegada pel camí.

Aquest capítol tracta l'únic actiu que es defensa ocultant-lo — i que per això té el pitjor problema probatori del dret. És el mirall del capítol 41: la patent protegeix publicant; el secret, ocultant. L'autoria creativa és al capítol 40; els registres que un atacant no pot reescriure, al capítol 57; i l'alertador que revela il·lícits — que no és un lladre de secrets — al capítol 62. Pregunta clau: com proves que tens una cosa que no pots ensenyar? Resposta: amb el dipòsit segellat per empremta de **t2p** — la SHA-512 calculada al dispositiu, el segell de temps RFC 3161/eIDAS, l'ancoratge a la blockchain pública [3] —, on només l'empremta viatja i el contingut no surt mai de casa: possessió amb data certa, perímetre exacte, i cap revelació. I amb la simetria que fa el capítol honest: la mateixa eina defensa l'exempleat o el competidor acusat injustament, que pot provar el seu desenvolupament independent previ.

Tres requisits i un nus

El marc és la Llei 1/2019, de secrets empresarials — transposició de la directiva europea — i és exigent [2]: perquè una informació sigui secret protegible ha de complir tres requisits. Ha de ser secreta — no generalment coneguda ni fàcilment accessible en els cercles que treballen amb aquesta mena d'informació. Ha de tenir valor empresarial precisament per ser secreta. I ha d'haver estat objecte de mesures raonables del seu titular per mantenir-la en secret. Fórmules químiques, processos productius, bases de dades, estratègies, llistes de clients, algorismes, know-how: tot hi cap — si compleixes els tres requisits.

El nus probatori viu al tercer. Sense mesures raonables demostrables, no hi ha secret protegible: la informació pot ser valuosíssima i haver-se filtrat igualment, i el jutge et dirà que no la protegies prou. La documentació de les mesures esdevé, doncs, part del secret mateix — i la seva absència, la trampa clàssica de l'empresa descuidada.

Els altres dos fils del nus: per litigar has de delimitar què era exactament el secret — i cada paraula de més que reveles al procés és secret que mor, de manera que la redacció ha de ser quirúrgica; i has de provar la prioritat temporal — que tu ho tenies abans —, com a les patents del capítol 41, però sense cap registre públic on apuntar-la: aquí la data se l'ha de procurar el titular mateix.

I l'equilibri que la mateixa llei imposa — i que aquest llibre subscriu [2]: la protecció no s'estén a l'experiència i les competències que el treballador adquireix honestament durant la seva carrera, ni pot servir per restringir la seva mobilitat. La frontera entre «el nostre know-how» i «el seu ofici» és la línia de combat de gairebé tots aquests litigis — i sense fets datats, cada banda hi dibuixa el que vol.

La prova d'existència aplicada

Aquí la prova d'existència juga el seu partit perfecte, perquè és l'única que prova sense ensenyar [3].

1. El dipòsit segellat

L'empresa certifica amb t2p els fitxers que són el seu secret — la fórmula, el codi, la base de clients, el procediment —: l'empremta SHA-512 es calcula al dispositiu i només l'empremta s'ancora; el contingut no surt mai de casa [3]. El resultat és triple: possessió amb data certa — ho tenies el dia X —; perímetre exacte — byte a byte, què és i què no és el teu secret —; i una mesura raonable en si mateixa: un protocol de custòdia datat és exactament el que el tercer requisit demana [2]. El dia del litigi, la revelació és selectiva i davant del jutge — les mesures de confidencialitat processals de la llei hi ajuden [2] — i el certificat amb codi QR acredita que allò és el que existia aquell dia.

2. La cronologia del know-how

Cada versió del desenvolupament — el quadern de laboratori, les iteracions del codi, els assajos — segellada en el moment [3]. La cadena de dates certes dibuixa el camí propi: quan el competidor aparegui amb «el mateix» producte, la teva cronologia prova anterioritat i desenvolupament independent. Com al capítol 41, la precedència és el cor de la disputa — però aquí sense publicar res.

3. La sortida de l'empleat

El moment de risc màxim, documentat amb neutralitat: l'acta de devolució d'equips i credencials, escanejada i segellada — fins a 50 pàgines en un PDF [3] —; l'inventari d'accessos que tenia, ancorat; el recordatori del NDA, lliurat amb data certa. Sense drames ni sospites: un tràmit de deu minuts que protegeix les dues parts — l'empresa, si després apareixen els seus fitxers on no toca; i l'extreballador, que té acta del que va tornar i de quan.

4. El NDA amb perímetre — i la defensa de l'innocent

El NDA signat amb la signatura forta de t2p — vídeo-selfie amb reptes de vida i verificació biomètrica [3] — i, com a annex, el perímetre del secret definit per empremta: el receptor sap exactament quins fitxers no pot usar, sense que el contingut viatgi. I la simetria que fa aquest capítol honest: l'exempleat que munta la seva empresa, o el competidor que va desenvolupar la seva solució pel seu compte, té en la seva pròpia cadena de segells la millor defensa contra l'acusació infundada [2][3] — el seu coneixement previ, datat abans de qualsevol contacte.

Els límits, dits clarament: el segell no fa secreta una informació que ja és pública, ni decideix si allò era secret protegible o experiència professional — això ho dirà el jutge amb la llei a la mà [2]. No substitueix la seguretat real — controls d'accés, xifratge, prevenció de fugues —: acredita el que tenies, no impedeix que t'ho robin; per als registres de l'atac, capítol 57. I mai no pot servir per segellar-ho tot i reclamar-ho tot: el perímetre inflat es gira en contra al procés.

La promesa i el perill

La promesa: litigis de secrets que es resolen per dates certes i perímetres exactes en lloc de per testimonis i sospites [1][2][3]; el tercer requisit — les mesures raonables — complert per disseny i demostrable amb un certificat; pimes que protegeixen el seu know-how sense pagar el que costa una guerra processal; i treballadors que canvien de feina amb el seu bagatge documentat i la consciència tranquil·la.

Els perills, mirats de cara.

El primer és **la caça de l'exempleat**. El mateix expedient que protegeix el secret pot industrialitzar l'amenaça contra qui marxa: cartes intimidatòries amb annexos segellats per congelar la competència. El contrapès és triple: l'equilibri exprés de la llei — l'experiència honesta i la mobilitat no es toquen [2] —, la simetria de la prova — el desenvolupament independent del demandat també data [3] — i els jutges mercantils castigant l'abús processal.

El segon és **el perímetre inflat**. Segellar-ho tot i dir que tot és secret no prova mesures raonables: prova desordre. El secret protegible és el que es delimita, es custodia i es tracta com a tal — el segell documenta la disciplina, no la substitueix.

El tercer és **el secret contra l'interès públic**. Cap dipòsit segellat no converteix en secret allò que la llei obliga a revelar, ni pot usar-se contra l'alertador que denuncia un il·lícit — aquesta frontera és del capítol 62, i és sagrada.

I el quart és **el tecnosolucionisme del calaix fort**. L'empremta no evita la filtració: la detecta i la data. Qui confongui el dipòsit amb la seguretat acabarà amb un secret perfectament documentat… i

perfectament robat. Xifratge, accessos mínims i cultura interna continuen sent la primera línia.

És hora d'actuar

Que el que no es pot ensenyar es pugui provar.

Per a empreses i fundadors: inventarieu els vostres secrets, delimiteu-los i dipositeu-ne les empremtes amb data certa [2][3]; el dia que us calgui, «mesures raonables» serà un certificat, no un al·legat.

Per als departaments legals i assessors de PI: NDA amb perímetre per empremta i actes de sortida ancorades com a pràctica estàndard [3]; i recordeu al client l'equilibri de la llei: el secret es defensa, l'exempleat no es persegueix [2].

Per als treballadors i emprenedors que marxen: segelleu el vostre bagatge previ i el vostre desenvolupament independent [3] — la vostra llibertat professional val una cadena de dates.

Per als jutges mercantils: el dipòsit per empremta amb revelació selectiva resol la paradoxa del procés de secrets [2]; exigiu-lo — i castigueu tant el robatori com l'acusació estratègica.

Per als legisladors: la llei de 2019 va posar els tres requisits [2]; el pas següent és reconèixer expressament el dipòsit d'empremta amb data certa com a mesura raonable i com a prova qualificada de possessió.

Que el pròxim Levandowski [1] trobi empremtes on esperava boira — i que el pròxim innocent tingui dates on esperava sospites. Pel coneixement que val precisament perquè no es veu, **time2act**.

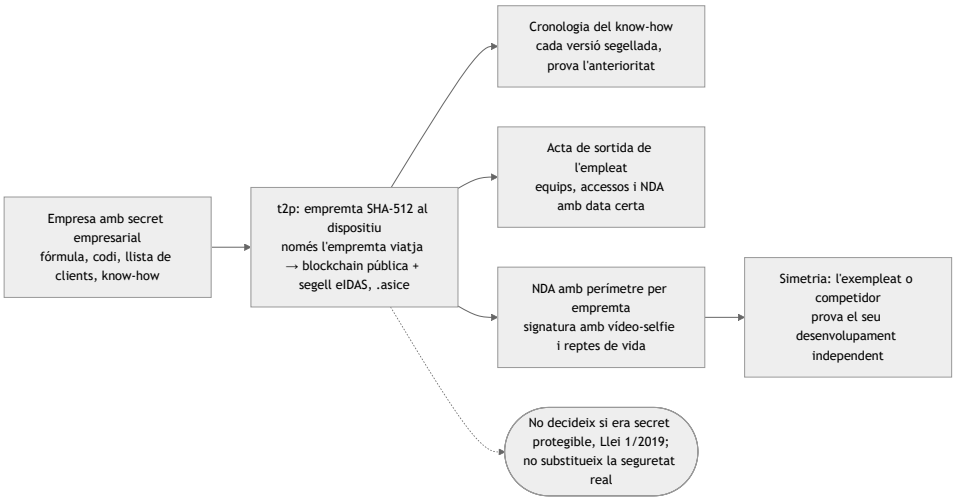


Figura 42.1 — El secret empresarial amb prova d'existència (t2p: empremta SHA-512 al dispositiu — el contingut no surt mai —, RFC 3161/eIDAS, blockchain pública, .asice): el dipòsit segellat (possessió + perímetre + mesura raonable del tercer requisit de la Llei 1/2019), la cronologia del know-how versió a versió, l'acta de sortida de l'empleat i el NDA amb perímetre per empremta i signatura amb vídeo-selfie. Simetria: la cadena de dates de l'acusat innocent prova el desenvolupament independent. Mirall del capítol 41: la patent protegeix publicant; el secret, ocultant — i per això només la prova que no revela el pot defensar. Fonts: cas Waymo/Uber/Levandowski; Llei 1/2019.

---

[1] CNBC — *Trump pardons Anthony Levandowski, the engineer who stole self-driving car secrets from Google* (milers de fitxers descarregats abans de marxar; Otto comprada per Uber; acord Waymo-Uber de 2018 valorat per la premsa en ~245 M$ en accions; culpabilitat el març de 2020; 18 mesos de presó — jutge William Alsup: «the biggest trade secret crime I have ever seen»; indult total el 20-1-2021, últim dia de mandat); TechCrunch — *Former Google engineer Anthony Levandowski among list of last-minute Trump pardons*; Wikipedia — *Anthony Levandowski* (acord 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 — *Llei 1/2019, de 20 de febrer, de Secrets Empresarials* (transposició de la Directiva (UE) 2016/943; tres requisits: secret + valor empresarial + mesures raonables; abast: fórmules, processos, bases de dades, llistes de clients, algorismes, know-how; equilibri: no cobreix l'experiència i competències adquirides honestament pel treballador ni pot restringir la seva mobilitat; mesures de confidencialitat processals); 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 producte (certificar qualsevol fitxer — només l'empremta viatja, el contingut no surt mai del dispositiu; escàner de documents fins a 50 pàgines; signatura amb vídeo-selfie, reptes de vida i biometria; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice amb revelació selectiva verificable sense connexió). Vegeu els capítols 13 i 15; el prior art i la patent, al capítol 41; els registres d'un atac, al capítol 57; els alertadors, al capítol 62. ↩

Govtech: contractació pública i registres a prova de manipulació

«Però qui vigilarà els mateixos vigilants?»

— Juvenal, Sàtires, VI, 347-348 (c. 100 dC)

El juny de 2020, una aliança insòlita —el Fòrum Econòmic Mundial, el Banc Interamericà de Desenvolupament i la Procuradoria General de Colòmbia— va anunciar un experiment que semblava sortir d'una metàfora. Volien posar en una cadena de blocs la fase de licitació del **Programa d'Alimentació Escolar**, que compra els dinars per als nens més vulnerables del país i on, històricament, s'havia filtrat la corrupció. La idea era senzilla i commovedora: fer que ningú no pogués robar, en silenci i a posteriori, els diners del dinar dels nens. El prototip va funcionar sobre la xarxa pública Ethereum i va registrar automàticament cada modificació o intervenció. Però els seus impulsors van ser honestos amb els límits, i la seva conclusió val per a tot aquest capítol: «la tecnologia no pot resoldre del tot allò que és al cor del comportament humà» [8].

Aquell experiment toca el nervi d'aquest darrer front. La contractació pública és, com diu la mateixa OCDE, l'activitat governamental més vulnerable a la corrupció, pel volum de diners i la discrecionalitat que mou. I la confiança que els ciutadans hi dipositen —que els seus impostos comprin escoles, ponts i dinars reals— descansa, una vegada més, sobre proves que es poden manipular. Aquest capítol tracta de com fer que aquella confiança es pugui *demostrar*, i de fer-ho amb la humilitat que l'experiment colombià ja va aprendre.

La despesa més vulnerable

La magnitud del que hi ha en joc costa d'imaginar. La contractació pública mundial supera els **13 bilions de dòlars l'any**, prop del 13-15 % del PIB global; és, de lluny, la major palanca econòmica en mans dels estats [1]. I una part esfereïdora s'evapora. El **Banc Mundial** calcula que els governs malgasten al voltant d'**una quarta part** d'aquesta despesa per ineficiència i corrupció, i que una contractació sòlida podria alliberar un **milió de milions —un bilió— de dòlars l'any**, el que anomena «el bilió ocult» [2]. El mateix Banc Mundial segueix el progrés del govern digital arreu amb el seu GovTech Maturity Index, que cobreix 198 economies [10]. En el sector de la construcció el forat és encara més brutal: la iniciativa de transparència de la infraestructura **CoST** estima que **entre el 10 % i el 30 % del valor d'una obra pública** es perd per mala gestió i corrupció [3].

Bona part d'aquesta pèrdua té un mecanisme amb nom propi. L'OCDE, en les seves directrius contra la **licitació col·lusòria** —el *bid rigging*—, adverteix que quan les empreses es posen d'acord per amanyar un concurs, eliminar aquella col·lusió podria abaratir els preus dels contractes un **20 % o més** [4]. Les formes són conegudes: ofertes de cobertura, supressió o rotació d'ofertes, repartiment del mercat, sovint amb la complicitat d'un infiltrat dins de l'organisme contractant. El resultat global d'aquesta erosió el mesura cada any **Transparency International** amb el seu Índex de Percepció de la Corrupció: el de 2025 va marcar una mitjana mundial de tot just **42 sobre 100, un mínim històric**, amb més de dos terços dels països suspesos [5].

Transparència no és el mateix que prova

Davant d'això, els estats han assajat dues estratègies que convé no confondre, perquè il·lustren la diferència exacta entre *veure* i *demostrar*.

La primera és la **transparència**: obrir les dades perquè tothom les pugui mirar. El millor exemple és **ProZorro**, el sistema de contractació oberta que Ucraïna va construir el 2016 amb el lema «tothom ho veu tot». Segons l'organització Open Contracting Partnership, ha estalviat a l'erari uns **6.000 milions de dòlars**, i la comunitat ciutadana de vigilància Dozorro va arribar a detectar irregularitats en més de 33.000 licitacions [6]. És una eina poderosíssima —un país en guerra va demostrar que l'arma anticorrupció era obrir les dades, no amagar-les—, però té un límit: la transparència deixa veure el que hi ha publicat, però no garanteix per si sola que aquell registre no s'hagi alterat ni datat amb trampa.

La segona estratègia ataca precisament aquest límit: la **integritat a prova de manipulació**. El pioner és Estònia, que després dels ciberatacs estatals de 2007 es va convertir, el 2012, en el primer país del món

a posar la cadena de blocs en producció per blindar els seus registres, amb la tecnologia **KSI** de l'empresa Guardtime. El disseny és elegant i és, ja ho veurem, el mateix de t2p: **a la cadena només s'hi envia l'empremta del document, mai la dada original**, que no surt del servidor de l'Estat [7]. Així, Estònia pot demostrar matemàticament que cap funcionari no ha reescrit a posteriori un historial mèdic, un assentament de propietat o una acta judicial. Transparència és deixar veure; prova d'integritat és poder demostrar que el que es veu no s'ha tocat.

La prova d'existència aplicada al diner públic

És aquí on **t2p** garanteix la integritat d'Estònia sense que cap ajuntament o agència hagi de muntar una cadena de blocs nacional, amb tres punts d'ancoratge.

El primer, el segell de les ofertes i els plecs, contra la retrodatació. En presentar una oferta o publicar un plec, es calcula l'**empremta SHA-512** del document al dispositiu, s'ancora a la **blockchain pública** i s'hi afegeix un **segell de temps RFC 3161** qualificat conforme a eIDAS. Això fixa criptogràficament que *aquell document exacte existia en aquella hora*, de manera que ningú no pugui antedatar una oferta, substituir un plec després de l'obertura ni alterar un sobre sense que l'empremta i la data canviïn. A més, l'**article 41 del reglament eIDAS** atorga al segell de temps qualificat una presumpció legal d'exactitud de la data i de la integritat de les dades [9], cosa que la transparència de ProZorro no garanteix per si sola.

El segon, **el segell dels registres públics**, a l'estil d'Estònia però com a servei: cada assentament o versió d'un expedient —una adjudicació, una modificació contractual, una acta— es resumeix en una empremta i s'ancora; qualsevol reescriptura posterior queda matemàticament detectable per un auditor extern.

I el tercer, el més distintiu, on el diner públic de debò aterra: **el segell de l'obra entregada**. Un funcionari o un ciutadà captura la **fotografia de la infraestructura lliurada** —el pont, l'aula, el dinar escolar— amb **GPS forense, data i prova de vida** de l'operador, tot empaquetat en un **contenidor .asice verificable fora de línia**. Així, un auditor pot comprovar independentment que *el diner va comprar alguna cosa real, en aquell lloc, en aquella data*, atacant directament la pèrdua observada en l'obra pública («com hem vist»). És el pas que tanca el cercle: de l'oferta segellada a la verificació ciutadana del que es va construir.

Cal dir el límit amb la mateixa honestedat que va tenir l'experiment colombià, fidels a la dualitat de «la promesa i el perill». La prova d'existència demostra que **un registre va existir íntegre en un moment, lloc i per una persona determinats**; **no** demostra la veritat física del que hi ha al darrere ni l'honestedat de la decisió. Si l'oferta segellada ja estava amanyada per col·lusió, si la foto amb GPS mostra una obra dolenta presentada com a bona, o si el funcionari que en dona fe és còmplice, t2p segellarà fidelment una dada corrupta. El que fa —i no és poc— és **encarir i fer detectable la manipulació a posteriori i la retrodatació**, creant una cadena de custòdia auditable. No substitueix la investigació de la competència, ni el control de qualitat de l'obra, ni el judici sobre el fons de l'adjudicació. «La tecnologia no pot resoldre del tot el comportament humà», com van reconèixer a Colòmbia; però pot tancar moltes de les portes per on s'escapa el diner.

La promesa i el perill

La promesa es mesura en aquell «bilió ocult». Una contractació on les ofertes, els registres i les obres estiguin segellats i siguin verificables per qualsevol ciutadà faria molt més difícil la retrodatació, la substitució d'expedients i l'obra fantasma, i tornaria a la ciutadania una eina per comprovar que els seus impostos compren el que diuen que compren. Com hem vist, aquest sector mou 13 bilions de dòlars; recuperar aquesta confiança és, literalment, recuperar recursos per a hospitals i escoles.

El perill demana el matís de sempre. Primer, el segell no neteja una decisió corrupta ni una obra dolenta; confondre la integritat del registre amb l'honestedat del fons seria una perillosa falsa seguretat. Segon, la vigilància: una infraestructura que segelli cada acte de l'administració ha de servir per controlar el poder, no els ciutadans, i exigeix un disseny garantista. Tercer, la concentració: qui operi la capa de verificació no pot convertir-se en un nou porter únic del que és públic. La prova d'existència és una eina al servei de la rendició de comptes, no un substitut de la política honesta ni del control democràtic.

És hora d'actuar

Per als **organismes de contractació**: segellar ofertes, plecs i adjudicacions en origen, perquè la integritat temporal del procés sigui demostrable i la retrodatació sigui impossible. Per als **òrgans de control i auditoria**: exigir el segell de l'obra entregada —foto, GPS, data— com a base de la fiscalització, per comprovar que el diner ha adquirit quelcom real. Per a la **ciutadania i el periodisme**: reclamar poder verificar pel seu compte tant les dades obertes com la seva integritat. Per als **governs i reguladors**: combinar la transparència de dades a l'estil ProZorro amb la prova d'integritat a l'estil estonià, i reconèixer el valor probatori del segell que el reglament eIDAS ja empara.

A Colòmbia van intentar impedir que algú robés, en silenci, el dinar dels nens. Van descobrir que la tecnologia no ho cura tot —i tenien raó—, però també que fer cada moviment del diner públic verificable per qualsevol és una de les muralles més efectives contra la corrupció. Que el ciutadà pugui demostrar que els seus impostos van comprar alguna cosa real és, en aquest darrer front i com a tots els altres, **time2act**.

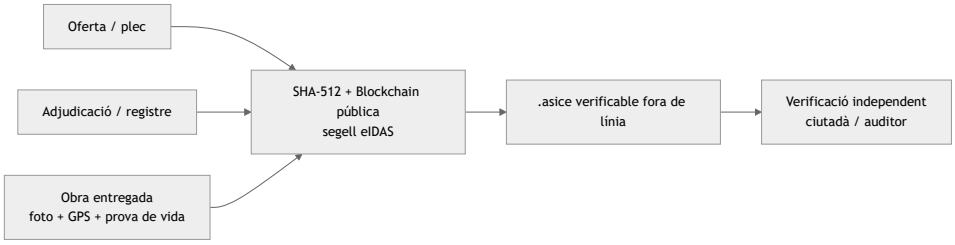


Figura 43.1 — Cada pas del diner públic —l'oferta o el plec, l'adjudicació registrada i l'obra entregada (foto amb GPS i data)— es resumeix en una empremta SHA-512, s'ancora a la blockchain pública i rep un segell de temps RFC 3161/eIDAS, amb prova de vida en l'obra; tot s'empaqueta en un contenidor .asice que un ciutadà o un auditor pot verificar de manera independent i fora de línia. Context: contractació pública mundial ≈13 bilions de dòlars l'any; entre el 10 % i el 30 % de l'obra pública es perd per corrupció i mala gestió. La prova d'existència demostra integritat, moment, lloc i persona —no l'honestedat de la decisió ni la qualitat de l'obra. Fonts: Banc Mundial; CoST; OCDE; eIDAS art. 41.

---

[1] Spend Network / Banc Mundial — *The $13 trillion global value of public procurement* (~13-15 % del PIB; menys del 3 % en dades obertes). https://www.spendnetwork.com/13-trillion-the-global-value-of-public-procurement/ ↩

[2] Banc Mundial — *The hidden $1 trillion: halting waste in public procurement* (~una quarta part malgastada; ~1 bilió $/any). 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 l'obra pública; ~6 bilions $/any cap al 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 col·lusió pot encarir els contractes un 20 % o més). 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* (mitjana mundial 42/100, mínim històric; Dinamarca 89, vuitè any al capdavant). https://www.transparency.org/en/news/cpi-2025-findings-insights-corruption ↩

[6] Open Contracting Partnership — *The impact of ProZorro in Ukraine* (~6.000 M$ estalviats; Dozorro, 33.000+ licitacions). https://www.open-contracting.org/impact-stories/impact-ukraine/ ↩

[7] e-Estonia — *KSI Blockchain* (primer Estat amb blockchain en producció, 2012; Guardtime; només s'ancora l'empremta). https://e-estonia.com/solutions/cyber-security/ksi-blockchain/ ↩

[8] World Economic Forum — *Exploring Blockchain Technology for Government Transparency to Reduce Corruption* (Colòmbia, Programa d'Alimentació Escolar, BID, 2020). https://www.weforum.org/publications/exploring-blockchain-technology-for-government-transparency-to-reduce-corruption/ ↩

[9] EUR-Lex — *Reglament eIDAS (UE 910/2014), article 41* (presumpció legal d'exactitud del segell de temps qualificat). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG ↩

[10] Banc Mundial — *GovTech Maturity Index* (198 economies; quatre àrees de maduresa del govern digital). https://www.worldbank.org/en/programs/govtech/gtmi ↩

El ciutadà davant l'Administració: el rellotge del silenci

«El concepte de "secret d'ofici" és la invenció específica de la burocràcia, i res no és defensat per la burocràcia tan fanàticament com aquesta actitud.»

— Max Weber, Economia i societat (pòst., 1922)

Davant d'una pantalla que repeteix la mateixa frase implacable a qualsevol hora del dia o de la nit — «No hi ha cites disponibles» —, algú actualitza per enèsima vegada la pàgina de cita prèvia d'estrangeria. Demà, igual. La setmana que ve, igual. El que aquella persona no veu és que les cites existeixen: les capturen bots en el mateix instant de publicar-se i es revenen per WhatsApp entre 50 i 350 euros, amb casos de fins a 600 — un mercat negre sencer aixecat sobre un tràmit gratuït. L'advocacia, les ONG i el Defensor del Pueblo ho han denunciat: la institució ha instat el Ministeri de l'Interior a corregir les «demores excessives» i rep queixes constants — prop de 3.000 en un any, amb més de 163.000 sol·licituds d'asil el 2023 desbordant el sistema [2]. El Govern ha anunciat que perseguirà les màfies de la revenda [2]. Però el problema de fons és més profund que les màfies: quan l'accés a l'Administració és una loteria opaca, el ciutadà no pot ni tan sols demostrar que ho ha intentat.

Aquest capítol tracta la relació probatòria del ciutadà amb el procediment administratiu: què vas presentar, quan t'ho van notificar, quan vencia el termini. La contractació pública — l'Administració per dins — és al capítol 43; la identitat digital, al capítol 47. Pregunta clau: com corre el ciutadà una cursa de rellotges si només una part controla el cronòmetre? Resposta: amb data certa pròpia a cada pas — la presentació, la notificació, el venciment, la cita — mitjançant **t2p**: l'empremta SHA-512 al dispositiu, l'ancoratge de l'empremta a la blockchain pública i el segell de temps RFC 3161/eIDAS complementari, dins d'un contenidor .asice [3]. I amb neutralitat: la mateixa traça que protegeix el ciutadà acredita la diligència de l'Administració que fa bé la seva feina i del funcionari honest.

L'arquitectura dels terminis

El procediment administratiu espanyol — la Llei 39/2015, d'1 d'octubre — és una màquina de rellotges. Amb caràcter general, l'Administració té tres mesos per resoldre i notificar (article 21.2), llevat que la norma del procediment estableixi un termini diferent. Si el termini venç sense resolució, apareix el silenci administratiu: la ficció jurídica que converteix el no-res en un «sí» o en un «no» segons el procediment, amb efectes des del venciment; i la seva existència es pot acreditar amb un certificat que l'òrgan competent ha d'expedir d'ofici en quinze dies — i, si no ho fa, a petició de l'interessat [1].

Les notificacions electròniques tenen el seu propi rellotge, i és implacable: des de la posada a disposició a la bústia electrònica, l'interessat té deu dies naturals per accedir-hi; si no ho fa, la notificació s'entén rebutjada i el procediment continua com si l'hagués rebuda [1]. Deu dies de vacances mal triades poden costar un recurs no presentat, una sanció ferma, una subvenció perduda.

El diagnòstic probatori: tot aquest edifici penja de dates — quan vas presentar, quan van posar a disposició, quan venç — i les dates les custodia majoritàriament una de les parts. El ciutadà té resguards que acrediten que va presentar alguna cosa, però no sempre què exactament; té una bústia el registre d'accés de la qual és del sistema, no seu; i té un venciment de silenci que ha de calcular i acreditar ell mateix. En una relació ja prou desequilibrada en poder i en mitjans, l'asimetria probatòria és la tercera càrrega.

La cita que mai no hi és

El cas d'estrangeria mereix mirada pròpia, perquè és el paradigma del punt d'accés opac. El quadre verificat: un sistema crònicament col·lapsat; bots que acaparen les cites en el moment de publicar-se; revenda per WhatsApp entre 50 i 350 euros, fins a 600 [2]; denúncies de l'advocacia, les ONG i el Defensor del Pueblo, amb milers de queixes anuals; més de 163.000 sol·licituds d'asil el 2023, per sobre de la capacitat del sistema; i l'anunci governamental de perseguir les màfies [2].

Però l'anàlisi ha d'anar més enllà de l'escàndol: el mercat negre és el símptoma; la malaltia és l'opacitat del punt d'accés. Ningú — ni el ciutadà, ni el Defensor, ni sovint la mateixa Administració — no pot auditar quantes cites es van publicar, quan, i qui les va capturar en quant de temps. Sense registre verificable de la

disponibilitat, tot són sospites: el ciutadà no pot demostrar que ho va intentar cent vegades; l'Administració no pot demostrar que va publicar les cites que diu; i el bot prospera exactament en aquesta foscor.

La resposta estructural és la disponibilitat auditable. Si cada publicació de cites i cada assignació queden ancorades — quantes, quan, assignades en quant de temps [3] —, l'acaparament automatitzat esdevé visible a simple vista: cap humà no pren dues-centes cites en tres segons. El ciutadà pot acreditar els seus intents datats, la persecució de les màfies [2] treballa sobre dades i no sobre anècdotes, i la reforma es pot exigir amb xifres. La transparència del punt d'accés no resol el col·lapse de fons — calen mitjans [2] —, però converteix un forat negre en un problema mesurable.

La prova d'existència aplicada

Una sol·licitud qualsevol, un registre electrònic qualsevol — i, per primera vegada, un expedient del qual el ciutadà té la seva pròpia cronologia completa.

1. La presentació amb contingut segellat

El ciutadà que presenta una sol·licitud, un recurs o una al·legació segella al seu dispositiu el document complet i el justificant de presentació, junts [3]: l'empremta SHA-512 del què i la data certa del quan. Si mai l'expedient «perd» un annex, si es discuteix quina versió es va presentar, si el resguard oficial només acredita un assentament genèric — la còpia segellada tanca la discussió. I la simetria funciona: l'Administració que ancora els seus propis registres té la mateixa protecció davant del ciutadà que al·lega haver presentat el que mai no va presentar. Ningú no pot negar la presentació; ningú no pot inventar-la.

2. El rellotge del silenci

La presentació segellada activa el cronòmetre amb data certa: tres mesos — o el termini que toqui [1] — comptats des d'un fet indiscutible. Al venciment, el ciutadà té la cronologia completa per exigir el certificat de silenci [1] o per anar al contenciós: la sol·licitud existia, deia això, es va presentar aquell dia, i el silenci va véncer aquest altre. El silenci administratiu deixa de ser una boira processal per esdevenir un fet datat — i l'Administració diligent, que resol dins de termini, té en els seus propis registres ancorats la prova de la seva puntualitat.

3. La notificació amb traça neutral

El rellotge més perillós — els deu dies de la notificació electrònica [1] — mereix una traça que no depengui de cap de les dues parts: la posada a disposició ancorada (quan, exactament, va aparèixer a la bústia) i l'accés ancorat (quan, exactament, s'hi va entrar) [3]. Contra el «rebutjada per no accedir» que arriba en el pitjor moment, el ciutadà pot acreditar què hi havia — o no hi havia — a la seva bústia i quan; contra el «mai no em va arribar» de mala fe, l'Administració pot acreditar la posada a disposició al segon. La indefensió i la picaresca moren de la mateixa medicina.

4. La cita auditable

El registre ancorat de la disponibilitat de cites [2][3]: cada lot publicat, cada assignació, amb hora exacta. El ciutadà que porta setmanes intentant-ho pot acreditar els seus intents datats; l'anàlisi del registre fa visible l'acaparament automatitzat — les captures instantànies i massives que cap mà humana no pot fer —; i el mercat negre perd el seu actiu principal: l'opacitat. Per a l'Administració, el mateix registre és la defensa: si publica el que diu que publica, les dades l'avalen.

Els límits, dits amb claredat: el segell no resol expedients ni posa més funcionaris a la finestreta — el col·lapse d'estrangeria és un problema de recursos i de política [2] que cap empremta no arregla; no substitueix els registres oficials ni la fe pública — els complementa amb una traça verificable per totes dues parts; i la data certa no interpreta el dret: acredita fets perquè advocats, jutges i el mateix procediment treballin sobre segur.

La promesa i el perill

La promesa: un ciutadà que corre la cursa de rellotges amb cronòmetre propi [1][3]; punts d'accés sense forats negres, on la cita que avui es revèn a 350 euros [2] torna a ser un tràmit gratuït i auditable; i una

Administració que pot demostrar la seva diligència amb la mateixa traça que l'obliga. Menys indefensió, menys picaresca, menys contenciosos sobre fets — i més energia per al fons dels expedients.

Els perills, amb la mateixa claredat.

El primer és **la burocràcia del segell**. Si acreditar cada pas esdevé una càrrega més — un tràmit sobre el tràmit —, haurem empitjorat la relació que volíem sanar. El segellat ha de ser automàtic i invisible: el registre que ancora sol, l'aplicació que segella en presentar — mai un requisit afegit que expulsi qui menys mitjans té, perquè la bretxa digital ja expulsa prou gent.

El segon és **la desconfiança institucionalitzada**. Aquest capítol no és una esmena als funcionaris. Si la traça neutral es presenta com a arma contra l'Administració, es viurà com a agressió i morirà en un calaix; la seva virtut és la simetria — protegeix el ciutadà de l'expedient perdut i el funcionari honest de l'acusació injusta. Traça de fets, mai vigilància dels empleats públics.

El tercer és **el miratge de la finestreta perfecta**. Cap ancoratge no crea cites on no n'hi ha [2] ni escurça terminis que la llei permet exhaurir. La transparència fa el problema mesurable i exigible; la solució continua sent política: mitjans, plantilles, simplificació.

I el quart és **la vigilància del ciutadà**. La cronologia administrativa d'una persona — què sol·licita, què recorre, quan — dibuixa la seva vida. Les traces han de ser de cada expedient i per a les seves parts, mai un perfil central consultable; només empremtes a la cadena, contingut als sistemes de cadascú, i accés regulat pel procediment [3].

És hora d'actuar

La relació més desigual del dret mereix, almenys, un rellotge compartit.

Per a tu, ciutadà: segella el que presentes — document i justificant, junts [3]; anota i ancora els venciments [1]; i si el sistema et diu que no hi ha cites, que els teus intents quedin datats [2].

Per a advocats i gestors administratius: incorporeu la cronologia segellada a cada expedient — la presentació, la notificació, el venciment del silenci [1][3]; és la diferència entre al·legar i acreditar.

Per a les administracions: ancoreu els vostres registres i notificacions [3] — la traça neutral és la vostra millor defensa davant la picaresca i la vostra millor credencial davant del ciutadà; i publiqueu la disponibilitat de cites de manera auditable [2].

Per al Defensor del Pueblo i els òrgans de control: exigiu registres ancorats de disponibilitat i assignació de cites [2] — les 3.000 queixes anuals mereixen dades, no respostes tipus.

Per als legisladors: reconeixeu la presentació i la notificació segellades com a prova qualificada [1][3], imposeu l'auditabilitat dels punts d'accés massius [2] i vetlleu perquè cap traça no esdevingui perfil ciutadà centralitzat.

Que la pròxima persona que actualitzi la pàgina de cites a mitjanit sàpiga — i pugui demostrar — si la cita no hi era o si l'hi havien pres; i que el rellotge del procediment, per fi, marqui la mateixa hora per a tothom. Per la finestreta de cada dia, **time2act**.

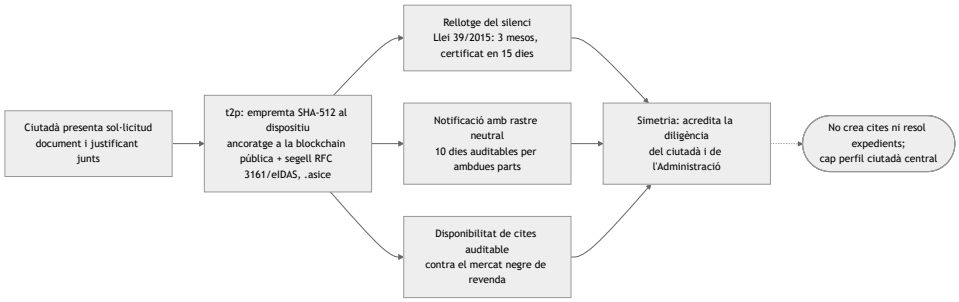


Figura 44.1 — La relació ciutadà-Administració amb prova d'existència (empremta SHA-512 al dispositiu, segell de temps RFC 3161/eIDAS, blockchain pública, .asice): la presentació amb contingut segellat (què i quan), el rellotge del silenci administratiu amb venciments datats (Llei 39/2015: 3 mesos; certificat en 15 dies), la notificació amb traça neutral (els 10 dies auditables per ambdues parts) i la disponibilitat de cites auditable (contra el mercat negre de la cita prèvia). Simetria: la mateixa traça acredita la diligència de l'Administració. Límits: no crea cites ni resol expedients; cap perfil ciutadà central. Fonts: Llei 39/2015; Defensor del Pueblo (cites d'estrangeria).

[1] BOE — *Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques* (art. 21: termini general de tres mesos per resoldre i notificar; silenci administratiu amb efectes des del venciment; certificat acreditatiu del silenci expedit d'ofici en 15 dies; notificacions electròniques: 10 dies naturals des de la posada a disposició, transcorreguts els quals s'entén rebutjada); 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 acaparen cites; revenda; sistema desbordat); OKDiario — *El caos en la web de Extranjería impulsa a las mafias que cobran hasta 350 € por cita* (revenda per WhatsApp de 50 a 350 €, fins a 600 €); Parainmigrantes — *El problema de la cita previa llega al Defensor del Pueblo* (queixes constants, ≈3.000 en un any; >163.000 sol·licituds d'asil el 2023; «demores excessives»); 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 producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; contingut als sistemes de cada part, només empremtes a la cadena; traça verificable per ambdues parts). Vegeu els capítols 13 i 15; la contractació pública, al capítol 43. ↩

L'atzar verificable: sortejos que ningú no pot carregar

«Babilònia no és altra cosa que un infinit joc d'atzars.»

— Jorge Luis Borges, «La loteria a Babilònia», Ficciones (1941)

Una sala municipal plena de gent que no acostuma a coincidir: famílies amb carpetes, un notari amb la seva, un bombo — o un programa informàtic — i una llista. Es reparteixen habitatges protegits, i l'atzar decidirà qui en té un i qui continua esperant. És un dels rituals més antics i més delicats de l'administració pública. A Espanya, l'atzar decideix coses majúscules: l'adjudicació d'habitatges protegits es fa davant notari, segons el procediment de cada administració [2]; l'ordre d'actuació de milers d'opositors i la composició dels seus tribunals surten d'un sorteig públic de lletres amb procediments reglats — fins i tot amb el sistema «mirall» que inverteix l'ordre del DNI perquè l'alfabet no beneficiï sempre els mateixos [1]. I, tanmateix, la sospita sempre troba escletxa: a Los Llanos de Aridane (La Palma), el sorteig de quaranta habitatges va acabar impugnat, amb l'ajuntament demanant que es resolgués «amb prontitud i màxima transparència» [2]. No cal cap frau perquè un sorteig perdi legitimitat: n'hi ha prou amb el dubte raonable de qui no ha tingut sort.

Aquest capítol tracta l'atzar públic: com es reparteix per sorteig de manera que ningú no pugui carregar els daus — ni sospitar-ho. La contractació pública és al capítol 43; les urnes, al capítol 48. Pregunta clau: pot un sorteig ser tan verificable com un recompte? Resposta: sí, amb dues peces. La primera, el compromís previ segellat amb **t2p**: la llista de participants i la regla d'adjudicació, ancorades abans que rodin els daus — empremta SHA-512, segell de temps RFC 3161/eIDAS, blockchain pública [3]. La segona, l'atzar públic verificable: balises com drand, que generen valors aleatoris que ningú no pot predir ni esbiaixar [4]. El resultat: un sorteig recomputable — qualsevol veí amb un ordinador pot comprovar que el resultat és exactament la regla aplicada a la llista. El notari no hi perd la feina; hi guanya el millor instrument de la seva història.

El bombo i la sospita

La loteria tradicional va resoldre el problema de la confiança amb física: bombos transparents, boles visibles, acte públic, càmeres. Qualsevol pot veure girar el bombo, i aquesta exhibició material és tota la garantia — i durant dècades ha estat suficient.

Però el model no escala als sortejos administratius. Les llistes ja no són desenes de boles sinó milers de noms que canvien fins a l'últim dia, gestionats en fulls de càlcul o en programes que només el personal tècnic pot inspeccionar; i l'acte públic sovint es redueix a extreure una lletra o una llavor — tot el que passa abans i després és invisible [1][2]. La transparència cobreix el moment de l'extracció; la sospita viu a tot el que l'envolta.

Els dos punts febles de qualsevol sorteig administratiu tenen nom. El primer és **la llista**: qui hi era, exactament, quan van rodar els daus? Un participant afegit tard, un exclòs indegudament, un duplicat — cap notari no pot detectar-ho si la llista és un fitxer que ningú no ha fixat públicament abans. El segon és **l'atzar**: d'on surt el nombre? Si el genera un ordinador de l'administració convocant, la confiança és cega; si surt d'un bombo, cal ser a la sala per creure-hi.

El cas de Los Llanos il·lustra el cost del dubte — i la precisió importa: una impugnació, no un frau demostrat [2]. Quan un sorteig es discuteix, tot s'atura: les famílies esperen, l'administració es defensa, i la legitimitat del mecanisme sencer queda tocada. El problema de fons no és que els sortejos siguin bruts; és que no poden demostrar que són nets. I en un llibre sobre proves, aquesta distinció ho és tot.

L'atzar que ningú no pot carregar

La solució moderna té dues meitats, i l'ordre entre elles és sagrat.

La primera meitat és **el compromís previ**. Abans que rodin els daus, es fixa tot el que no ha de poder canviar: la llista completa de participants amb els seus números, les bases i la regla exacta d'adjudicació — com es passa del nombre aleatori a l'ordre de la llista. Tot això se segella amb t2p — empremta SHA-512, data certa, ancoratge a la blockchain pública [3] — i l'empremta es publica. Conseqüència: ningú no pot

afegir, treure ni reordenar candidats a posteriori sense que l'empremta canti; i tothom pot guardar-se la llista i comprovar que és la que era.

La segona meitat és **l'atzar públic verificable**. El nombre aleatori no el genera ni l'administració ni cap proveïdor seu, sinó una balisa pública: drand, el far d'aleatorietat de la League of Entropy — una coalició que inclou Cloudflare, l'EPFL, Kudelski Security, Protocol Labs i la Universitat de Xile, amb membres posteriors com la Fundació Ethereum —, que emet a intervals fixos valors aleatoris imparcials, impredictibles i verificables per qualsevol, combinant l'entropia de múltiples operadors independents amb criptografia de llindar: ni un actor ni dos de confabulats no poden esbiaixar el resultat [4]. Les seves aplicacions declarades inclouen, precisament, loteries i eleccions [4].

I la suma és **la recomputabilitat**. S'anuncia per endavant quina ronda futura de la balisa s'usarà — ningú no en coneix encara el valor; arriba el valor; s'aplica la regla compromesa a la llista compromesa; i el resultat el pot refer qualsevol: amb la llista publicada, la regla publicada i el valor públic de drand, cada persona pot reproduir el sorteig sencer al seu ordinador i obtenir exactament el mateix resultat [3][4]. La confiança deixa de ser un acte de fe en una sala: és una comprovació a l'abast de tothom.

La prova d'existència aplicada

El mateix saló d'actes, les mateixes famílies — i un full amb tres empremtes publicades que qualsevol pot comprovar des del mòbil.

1. L'habitatge protegit recomputable

El sorteig d'habitatges [2] amb el protocol complet: la llista de sol·licitants admesos, segellada i publicada per empremta — les dades personals no s'exposen [3]; les bases i la regla d'adjudicació, segellades; la ronda futura de drand, anunciada [4]; i, arribat el dia, una adjudicació recomputable per qualsevol. En un cas com el de Los Llanos [2], la sospita — en el sentit que fos — es podria comprovar en cinc minuts, en una direcció o en l'altra: o els números quadren per a tothom, o no quadren per a ningú. El notari certifica el compromís previ i l'acta final: fe pública sobre fets verificables.

2. Les oposicions amb daus públics

La lletra de l'ordre d'actuació i els sortejos de tribunals [1], extrets d'una ronda de drand anunciada per endavant [4] en lloc d'un bombo en una sala de Madrid: el mateix ritual, però verificable des de qualsevol punt del país per cada opositor. Els procediments correctors — el sistema «mirall» del DNI [1] — es publiquen com a part de la regla compromesa, i el conjunt esdevé recomputable. Cap opositor no haurà de preguntar-se mai més si la lletra va sortir com diuen que va sortir: podrà refer l'extracció ell mateix.

3. L'assignació sensible

La mateixa recepta serveix per a tota assignació aleatòria que reparteixi coses valuoses o càrregues: places escolars quan cal desempatar, torns i destinacions, mostres d'inspecció — quines empreses audita enguany l'administració: un sorteig recomputable impedeix tant el favor com la persecució —, o l'ordre d'una llista d'espera. Regla fixa, llista segellada, atzar públic [3][4]: allà on l'arbitrarietat pot vestir-se d'atzar, la recomputabilitat la despulla. Si algú surt cinquè a la mostra d'auditoria, tothom pot verificar que aquell cinquè és el resultat directe del càlcul — i no d'una trucada.

4. L'acta que sobreviu

Cada sorteig deixa la seva acta ancorada: la llista compromesa, la regla, el valor aleatori usat, el resultat [3]. Anys després — quan arribi el recurs, la revisió o la sospita retrospectiva —, l'expedient sencer es pot reverificar sense dependre de la memòria de cap funcionari ni de la continuïtat de cap sistema informàtic. L'atzar passa; la seva prova, no.

I la versió domèstica del mateix problema, que cada Nadal omple jutjats de pau: el dècim compartit. La participació dita de paraula — «hi vas amb mig» — val el que valgui la memòria quan toca. La foto del dècim amb la llista de participants i les quantitats, segellada abans del sorteig [3], converteix el costum més estimat del país en un pacte amb data certa: deu segons que estalvien la disputa que cap premi no mereix.

Els límits, dits amb claredat: el segell i la balisa fan el sorteig net, no la política justa — qui pot participar, quants habitatges es construeixen o quantes places s'ofereixen són decisions humanes que cap criptografia

no millora; la recomputabilitat exigeix publicar regla i llista, i la protecció de dades s'ha de respectar amb la publicació per empremta i la pseudonimització [3]; i el notari i l'acte públic continuen tenint tot el sentit — la fe pública i el ritual comunitari són part de la legitimitat, ara amb matemàtica a sota.

La promesa i el perill

La promesa: sortejos públics que qualsevol pot recomputar [3][4], impugnacions que es resolen en minuts i no en anys [2], i un patrimoni de legitimitat per a l'administració que reparteix. Quan l'atzar és verificable, la mala sort no deixa ressentiment institucional — només mala sort.

Els perills, amb la mateixa claredat.

El primer és **el ritual buidat**. Si el sorteig recomputable substitueix l'acte públic en lloc de reforçar-lo, es perd la dimensió comunitària que legitima el repartiment — la sala plena, el notari, el moment compartit. La tecnologia ha d'acompanyar el ritual, no escamotejar-lo: l'acte es fa, i a més es pot comprovar des de casa.

El segon és **la complexitat com a nova opacitat**. Per al ciutadà mitjà, «criptografia de llindar» pot ser tan impenetrable com un full de càlcul municipal. Si només quatre experts poden recomputar, haurem canviat una fe per una altra. Calen verificadors públics senzills — la web on qualsevol enganxa el seu número i ho comprova — i pedagogia del mecanisme: la verificabilitat teòrica no basta; cal la practicable.

El tercer és **la llavor capturada**. L'atzar públic ho és si la balisa és realment independent i el compromís és realment previ. Anunciar la ronda després de conèixer-ne el valor, o usar una «balisa» controlada pel convocant, seria el frau vell amb vestit nou [4]. L'ordre dels passos — primer el compromís segellat, després l'atzar — és tot el mecanisme: invertir-lo l'anul·la.

I el quart és **el tecnosolucionisme distributiu**. Cap sorteig net no resol l'escassetat que l'obliga. Si hi ha quaranta pisos per a mil famílies [2], la criptografia garanteix que el repartiment sigui net — no que sigui suficient. La transparència del mecanisme mai no ha de servir per naturalitzar la penúria del que es reparteix.

És hora d'actuar

Si l'atzar decideix vides, que sigui un atzar que tothom pugui comprovar.

Per a les administracions que sortegen: adopteu el protocol complet — llista i regla segellades abans, balisa pública després, acta ancorada sempre [3][4]; i oferiu el verificador senzill, perquè comprovar no exigeixi enginyeria.

Per als notaris: certifiqueu compromisos previs i actes finals [2][3] — la fe pública guanya el seu millor instrument des del paper timbrat.

Per als opositors i sol·licitants: guardeu-vos la llista i l'empremta publicades [3]; el dia del sorteig, recomputeu — o exigiu poder fer-ho [1][4].

Per als jutjats contenciosos: davant d'una impugnació de sorteig [2], demaneu el paquet verificable — compromís, atzar, acta; on n'hi hagi, la resolució és aritmètica; on no, la sospita té base.

Per als desenvolupadors cívics: construïu els verificadors oberts — la web de recomputació d'un clic [4]; la transparència practicable és codi, i és poc.

Per als legisladors: imposeu el compromís previ segellat i l'atzar públic verificable en tot sorteig administratiu que reparteixi béns o càrregues [1][2][3][4] — i que la recomputabilitat sigui un dret de qualsevol participant.

A la pròxima sala plena de famílies amb carpetes, que la mala sort — perquè continuarà existint — no deixi mai més el regust de la sospita: només el nombre que va sortir, comprovable per tothom, fins i tot per qui se'n va sense pis. Per un atzar de tots, **time2act**.

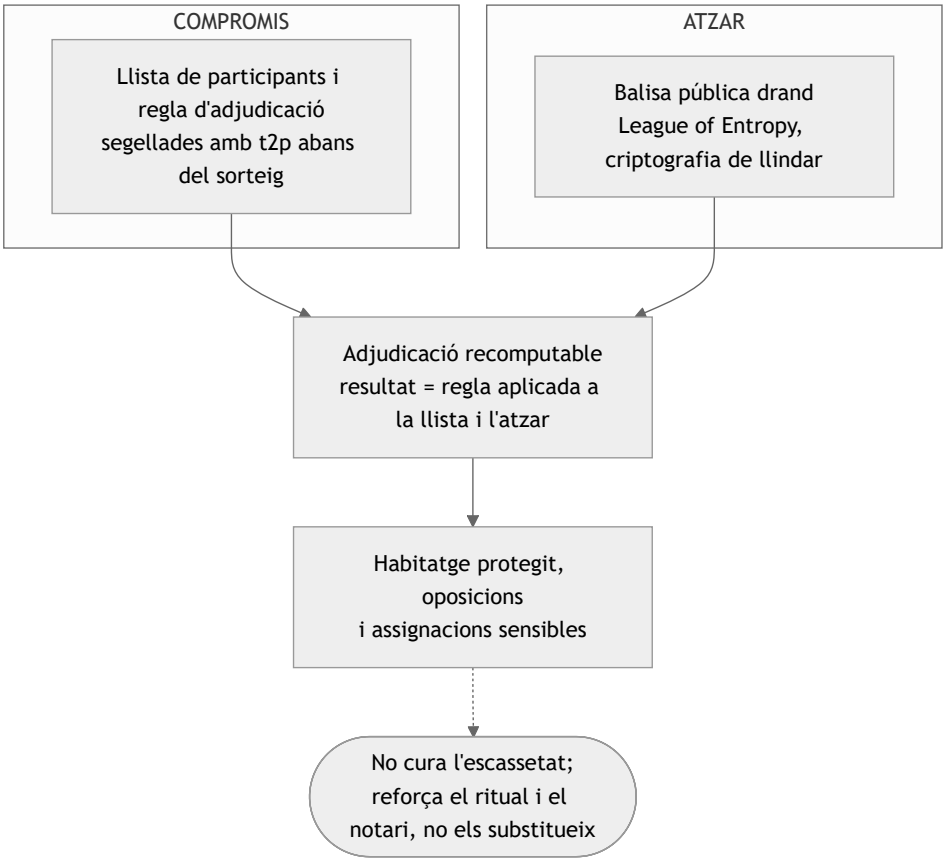


Figura 45.1 — El sorteig que ningú no pot carregar, en dues meitats: el compromís previ (llista de participants i regla d'adjudicació segellades amb t2p — empremta SHA-512, RFC 3161/eIDAS, blockchain pública — i publicades per empremta ABANS del sorteig) i l'atzar públic verificable (balisa drand de la League of Entropy: valors imparcials, impredictibles i verificables, generats per criptografia de llindar entre operadors independents). Resultat: adjudicació recomputable per qualsevol — resultat = regla(llista, atzar). Límits: el sorteig net no cura l'escassetat; el ritual públic i el notari es reforcen, no se substitueixen. Fonts: sortejos d'oposicions i d'habitatge protegit; 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* (sorteig públic de lletres; procediments reglats posteriors; sistema «mirall» d'inversió de l'ordre 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* (sorteig davant notari segons el procediment de cada administració; possibilitat d'impugnació); 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 producte (empremta SHA-512; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; compromís previ per empremta — les dades personals no s'exposen —; actes ancorades i reverificables). Vegeu els capítols 13 i 15; la integritat electoral, al capítol 48. ↩

[4] Cloudflare / League of Entropy — *Distributed Randomness Beacon* (drand: balisa d'aleatorietat distribuïda i públicament verificable; membres fundadors: Cloudflare, EPFL, Kudelski Security, Protocol Labs i Universitat de Xile; valors imparcials, impredictibles i verificables a intervals fixos; criptografia de llindar; aplicacions: loteries i eleccions); PR Newswire — *The League of Entropy launches production drand network* (primera balisa pública verificable en producció); 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 ↩

Oposicions i exàmens: la prova segellada abans

«Convinc amb vós que hi ha una aristocràcia natural entre els homes. Els seus fonaments són la virtut i el talent.»

— Thomas Jefferson, carta a John Adams (28-10-1813)

Un dissabte al matí, en una aula gran de qualsevol ciutat: centenars de persones que fa anys que preparen aquest dia, el sobre que s'obre davant de tothom, el ritual de sempre. I la pregunta que ningú no pot respondre amb proves: aquest examen, l'ha vist algú abans?

El cas que ho fa urgent està documentat [1]. A l'oferta pública d'ocupació d'Osakidetza — el servei basc de salut — de 2016-2017, les denúncies sindicals per filtracions a Anestèsia i Angiologia van destapar un escàndol: un informe va trobar indicis de filtració en 19 exàmens de fins a 12 especialitats mèdiques. Van dimitir el conseller de Salut, Jon Darpón, la directora general d'Osakidetza i dos directius més; la Fiscalia va investigar. I el final, vuit anys després: el desembre de 2024, la jutge va arxivar la causa «al no existir indicios racionales de la comisión del ilícito» — provisional només per a dos investigats d'una especialitat [1]. L'arxivament ni exonerava ni condemnava: vuit anys de sospita, carreres destruïdes, milers d'opositors deixats amb el dubte — i cap manera de provar res, en cap direcció.

La lliçó és la mateixa que la de la disputa de l'ajuda a Somàlia del capítol 50: quan no hi ha registres verificables, ni l'acusació ni la defensa poden provar res — i el dubte s'ho menja tot, culpables i innocents per igual.

Aquest capítol és el germà natural del capítol 45: allà, el sorteig recomputable; aquí, el mateix patró — el compromís previ — aplicat a la prova mateixa. Els títols, les credencials i la IA als exàmens són al capítol 19; el procediment administratiu, al capítol 44; qui denuncia una filtració des de dins, al capítol 62. Pregunta clau: com se sap que les preguntes no han circulat, que la plantilla no s'ha tocat i que el teu full és el que vas entregar? Resposta: segellant-ho tot abans amb **t2p** — l'empremta SHA-512 de l'examen i de la plantilla, ancorades amb data certa ABANS de la convocatòria (només les empremtes: el contingut no surt de la custòdia), i el full de respostes del candidat, datat en sortir [2]. Protegeix l'opositor del tribunal brut — i el tribunal net, de la sospita infinita.

Els tres moments on es trenca la confiança

El primer és **abans de l'examen**. El contingut es redacta, s'imprimeix, es custodia — i passa de mà a mà entre redactors, revisors i tribunal. Cada transferència és una oportunitat perquè una còpia circuli o una versió s'alteri sense deixar rastre. La cadena de custòdia és, en essència, una cadena de confiança personal; i quan la sospita arriba — com al cas basc [1] —, no hi ha manera de reconstruir ni què existia en quin moment ni qui hi va accedir.

El segon és **la plantilla de respostes**. Es publica, arriben les impugnacions, s'anul·len preguntes — rutina legítima del contenciós. Però també és el moment en què una plantilla es pot «ajustar»: si la versió publicada difereix de la que existia el dia de l'examen — encara que només en un parell de preguntes —, les conseqüències mouen places senceres. I sense una prova immutable del contingut original, ningú no pot demostrar si hi ha hagut retoc o no: tot penja de la paraula del tribunal.

El tercer és **el full de respostes**. L'opositor entrega el seu full i se'n va amb les mans buides. Si la correcció s'equivoca, si el full «es perd», si la lectura òptica falla — la seva versió no existeix enlloc, i la veritat queda òrfena.

El sistema demana fe tres vegades. I la fe, com va ensenyar Osakidetza [1], quan es trenca no es repara amb investigacions: només amb registres que existissin des del principi.

La prova d'existència aplicada

El patró del capítol 45 — compromís previ, revelació després — aplicat al contingut de la prova [2].

1. L'examen segellat abans

El tribunal certifica l'examen definitiu amb t2p el dia que el tanca: l'empremta SHA-512 s'ancora amb data certa — i només l'empremta: el contingut no surt de la custòdia [2]. Ningú no veu res; però des d'aquell

moment, l'examen que es reparteixi el dia D es pot contrastar contra l'empremta prèvia: ni substitucions d'última hora, ni «versions» que ningú no sap d'on surten. I cada accés a la custòdia — qui va obrir el sobre digital, quan — deixa el seu registre datat: la cadena de custòdia deixa de ser una cadena de paraules.

2. La plantilla compromesa

La plantilla de correcció, segellada abans de l'examen [2]. Les impugnacions i les preguntes anul·lades continuen sent possibles — són dret dels opositors — però passen a ser transparents: la plantilla original té data; cada revisió posterior, també; i el «canvi silenciós de resposta correcta» esdevé impossible de fer sense deixar rastre. El tribunal que ho fa tot bé té, per primera vegada, la prova positiva que no va tocar res.

3. El full de respostes datat

En sortir de l'aula, l'opositor fotografia la seva còpia autocopiativa — o el resguard que el sistema li doni — amb t2p: la seva versió de les respostes, amb data certa del mateix dia [2]. Contra l'error de correcció, la lectura òptica defectuosa o el full extraviat, ja no està indefens: té el que va entregar, datat abans de conèixer la plantilla. I on el procediment no dona còpia, aquesta és la reforma barata que cal exigir.

4. L'expedient d'impugnació — i la simetria

Quan calgui impugnar, l'expedient .asice ho porta tot: l'empremta prèvia de l'examen i la plantilla, el full de respostes datat, les publicacions oficials capturades amb les seves dates [2] — una cronologia verificable per al tribunal administratiu o el contenciós. I la simetria que el cas basc reclama a crits [1]: el tribunal net pot provar que l'examen no va circular i que la plantilla no es va tocar — la sospita infinita, que també destrueix innocents, mor de dates. Osakidetza en positiu.

Els límits, perquè n'hi ha: el segell acredita integritat i dates — no la qualitat de les preguntes ni la justícia de la puntuació: això és del tribunal i, si cal, del jutge. El compromís previ protegeix el contingut, no impedeix la filtració humana — qui ha vist l'examen el pot explicar: la custòdia física i les persones continuen comptant, i el registre d'accessos les fa responsables. I la implantació ha de ser institucional — l'opositor sol només pot datar el seu full: la resta és feina de qui convoca.

La promesa i el perill

La promesa: oposicions on la integritat de la prova és un fet verificable i no un acte de fe [1][2]; impugnacions que discuteixen el fons — si la pregunta era vàlida — sobre plantilles datades; opositors que conserven la seva versió; tribunals nets blindats contra la sospita; i el proper Osakidetza [1] resolt en dies — en una direcció o en l'altra — en lloc de vuit anys d'ombra.

I ara, els perills, sense edulcorar.

El primer és **el segell com a teatre**: certificar l'examen i deixar la custòdia física com estava. L'empremta prèvia només val si el que es reparteix es contrasta de debò contra ella, i si els accessos queden registrats — el compromís previ és un sistema, no un tràmit.

El segon és **la impugnació industrialitzada**. Si cada opositor té expedient, els contenciosos es poden multiplicar. El contrapès és el mateix mecanisme: contra plantilles datades i exàmens íntegres, la impugnació infundada mor de fets — litigarà menys qui menys raó tingui.

El tercer és **la filtració que cap hash no atura**: qui veu l'examen el pot memoritzar i explicar. La prova d'existència data i delimita responsabilitats — qui hi va accedir, quan —; la confidencialitat humana és una altra capa, i el capítol 62 explica què fer quan algú, des de dins, veu que es trenca.

Hi ha un quart perill, més silenciós: que el joc net faci oblidar el joc just. Cap segell no fa justes les places, ni bones les preguntes, ni curtes les llistes d'espera. La prova d'existència garanteix el joc net; que el joc valgui la pena és feina de qui dissenya les convocatòries.

És hora d'actuar

Que la pregunta «això ho ha vist algú abans?» tingui resposta.

Per als tribunals i òrgans convocants: examen i plantilla segellats abans, accessos registrats, contrast públic el dia D [2] — la vostra integritat mereix ser demostrable, no només certa.

Per als opositors: fotografieu i dateu la vostra còpia de respostes en sortir [2]; i exigiu a les convocatòries el compromís previ — és una línia al plec de bases que ho canvia tot.

Per als sindicats i les acadèmies: la reivindicació barata i transversal: cap examen sense empremta prèvia [1]; qui s'hi negui, que expliqui per què.

Per als tribunals contenciosos: davant d'una impugnació, demaneu el paquet verificable — examen previ, plantilla datada, full de respostes [2]; on n'hi hagi, la resolució és comparació; on no, la sospita té base.

Per als legisladors: després d'Osakidetza [1] — vuit anys per arxivar sense culpables —, que la normativa d'accés a la funció pública incorpori el compromís previ segellat com a requisit de tota convocatòria: costa cèntims i val la confiança de milions.

A la pròxima aula d'examen, quan s'obri el sobre, que la pregunta «això ho ha vist algú abans?» tingui resposta — una empremta amb data, comprovable per tothom que s'hi juga la vida. Per les places que es guanyen estudiant, **time2act**.

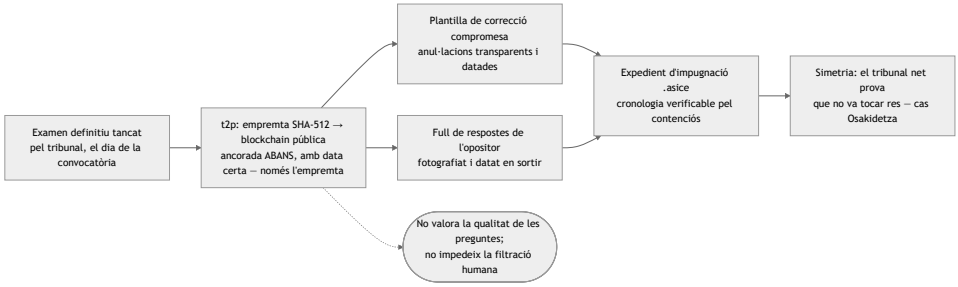


Figura 46.1 — La prova segellada abans (t2p: empremta SHA-512 — només l'empremta s'ancora, el contingut no surt de la custòdia —, RFC 3161/eIDAS, blockchain pública, .asice): l'examen certificat abans de la convocatòria amb accessos registrats, la plantilla de correcció compromesa abans de l'examen (les anul·lacions, transparents i datades), el full de respostes de l'opositor datat en sortir, i l'expedient d'impugnació verificable. Simetria: el tribunal net pot provar que no va tocar res — el cas Osakidetza (19 exàmens amb indicis de filtració, dimissions, vuit anys i arxivament per falta de proves) resolt en dies, en qualsevol direcció. Patró: el compromís previ del capítol 45, aplicat al contingut. Fonts: 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 servei basc de salut; denúncies sindicals a Anestèsia i Angiologia; indicis en 19 exàmens de 12 especialitats; dimissions del conseller de Salut Jon Darpón, la directora general d'Osakidetza i dos directius de RH); Deia — *Archivan la causa por las presuntas filtraciones en la OPE de Osakidetza en 2018 por falta de pruebas* (desembre de 2024: arxivament «al no existir indicios racionales de la comisión del ilícito», provisional per a dos investigats de Cirurgia Plàstica); elDiario.es — *La Justicia cierra sin culpables la investigación* i *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 producte (certificar qualsevol fitxer — només l'empremta viatja, el contingut no surt mai de la custòdia; foto amb data certa; escàner de documents; captura de publicacions oficials amb data; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; el sorteig de tribunals, al capítol 45; les credencials, al capítol 19; els alertadors, al capítol 62. ↩

Identitat digital: la prova que existeixes

«El seu ésser és ser percebut.»

— George Berkeley, Principis del coneixement humà, §3 (1710)

El 28 de setembre de 2017, en un llogaret del districte de Simdega, a l'estat indi de Jharkhand, una nena dalit d'onze anys anomenada Santoshi Kumari va morir demanant arròs a la seva mare. Feia gairebé vuit dies que amb prou feines menjava. La targeta de racionament de la seva família —el dret a la quota d'aliment subvencionat— havia estat cancel·lada perquè no estava vinculada a **Aadhaar**, el sistema d'identitat biomètrica de l'Índia, i durant sis mesos no havien pogut retirar el seu gra [8]. El govern ho va disputar, al·legant malària; la campanya pel dret a l'alimentació va documentar desenes de morts per inanició lligades a fallades del sistema [8].

Comencem per aquesta tragèdia perquè conté l'advertència més important d'aquest capítol, i de tota la Part que ara obrim. La identitat és el dret que precedeix tots els altres: sense una prova que existeixes, no hi ha compte bancari, ni vot, ni escola, ni atenció mèdica, ni ajuda. Però una identitat **mal dissenyada** —centralitzada, obligatòria, sense alternativa— pot matar. Aquest capítol tracta de com donar a centenars de milions de persones la prova que existeixen, i de com fer-ho **sense** convertir aquella prova en una arma contra elles.

Vuit-cents milions d'invisibles

La dimensió del problema és aclaparadora. Segons la iniciativa **Identification for Development** (ID4D) del **Banc Mundial**, prop de **800 milions de persones** —una de cada deu— no tenen cap prova oficial d'identitat; la xifra ha baixat des del 2017, però més de la meitat dels qui no en tenen són **infants el naixement dels quals no es va registrar mai** [1]. **UNICEF** ho confirma des de l'altre extrem: **150 milions de nens menors de cinc anys** són «invisibles» perquè ningú no els ha inscrit al naixement, i la meitat viuen a l'Àfrica subsahariana [3]. A l'altre costat de l'espectre hi ha l'**apatrídia**: l'Alt Comissionat de les Nacions Unides per als Refugiats (**UNHCR**) en comptabilitza oficialment 4,4 milions a finals del 2024, però adverteix que la xifra real arriba probablement als deu milions; el grup més gran són els rohingyes, gairebé 1,8 milions de persones sense cap nacionalitat reconeguda [2].

Aquesta gent no «no existeix»; **existeixen**, treballen, estimen i moren, però cap Estat ho reconeix. L'objectiu 16.9 dels Objectius de Desenvolupament Sostenible es va fixar precisament això: identitat jurídica per a tothom abans del 2030. Però la pregunta clau no és *si* donem identitat, sinó *com*.

Dues maneres de donar identitat

Hi ha dos camins; la diferència entre ambdós és la lliçó de Santoshi.

El primer és el model **centralitzat i biomètric**, exemplificat per Aadhaar. Amb uns **1.340 milions de titulars vius** —més del 99,9 % dels adults indis— i més de 170.000 milions d'autenticacions, és el sistema d'identitat més gran de la història [6]. Ha inclòs molta gent abans exclosa del sistema financer. No obstant això, l'octubre de 2023 les dades personals d'uns **815 milions d'indis** —números d'Aadhaar, passaports, telèfons, adreces— es van posar a la venda a la web fosca, filtrades des d'una base de dades de tests de covid [7]. La dependència d'una sola «font de veritat» biomètrica exclou: les taxes de fallada d'autenticació oscil·len entre el 6 i el 12 %, i al Rajastan, el juliol del 2017, un de cada tres titulars no va poder retirar el seu gra per fallades repetides de l'empremta [9]. L'economista **Reetika Khera**, de l'Institut Indi de Tecnologia de Delhi, resumeix sense pal·liatius que l'Estat no hauria de tractar la identitat biomètrica com l'única font de veritat, perquè el que es ven com a «estalvi» sovint és la denegació de drets per fallades del sistema, no frau eliminat [9]. El Tribunal Suprem de l'Índia, que va avalar Aadhaar el 2018, ho va fer amb un vot discrepant memorable del jutge Chandrachud [9].

El segon camí és una arquitectura nova i descentralitzada, on **la persona controla la seva pròpia identitat**. El consorci d'estàndards **W3C** ha publicat les peces tècniques: els **identificadors descentralitzats** (DID), recomanació oficial del 2022, i les **credencials verificables** (Verifiable Credentials), estàndard des del maig de 2025, que descriuen un ecosistema de tres parts —qui emet, qui posseeix i qui verifica— criptogràficament segur i respectuós amb la privacitat [5]. Europa hi va de bracet: el reglament **eIDAS 2.0** obliga cada Estat membre a oferir una **cartera d'identitat digital** (EUDI

Wallet) abans de finals del 2026, amb **divulgació selectiva** incorporada —per exemple, provar que ets major d'edat sense revelar la teva data de naixement, funció ja pilotada en almenys sis estats [4]. Estònia, amb el seu e-ID per al 99 % de la població, demostra des de fa anys que es pot fer bé. La diferència amb Aadhaar no és la tecnologia; és **qui custodia la prova**.

La prova que existeixes

És en aquest segon camí on **t2p** aporta una peça fonamental: la **prova d'existència d'una persona**. El mecanisme aplica la lògica de tot el llibre al cas més bàsic de tots. L'aplicació captura un gest de **prova de vida** —un vídeo o un repte actiu, resistent a les deepfakes—, opcionalment un tret biomètric, i en calcula l'**empremta SHA-512** al mateix dispositiu. Aquella empremta s'ancora a la **blockchain pública** amb un **segell de temps RFC 3161** conforme a eIDAS i un **GPS forense**, i s'empaqueta en un contenidor **.asice verificable fora de línia**. El resultat, en llenguatge planer: *aquesta persona estava viva, era ella, va ser en aquest lloc, en aquest instant*. Un testimoni signat i datat per a algú que no té papers.

A més, quan una ONG, un metge de camp o una escola emet una **credencial verificable** —«ha completat aquest curs», «ha rebut aquesta vacuna»—, la seva empremta es pot ancorar perquè el titular la dugui **al seu propi dispositiu**, la presenti amb divulgació selectiva i la verifiqui qualsevol sense haver de contactar amb qui la va emetre. És crucial per a qui ho perd tot en un desplaçament: la prova viatja amb la persona, no en un registre que pot cremar o que pot ser piratejat. La diferència amb el model Aadhaar és exactament aquesta: **el titular conserva la prova**, no un repositori central que pot filtrar-se o denegar l'accés.

La promesa i el perill

I aquí, més que en cap altre capítol d'aquest llibre, el perill demana que el diguem abans que la promesa. Una prova d'existència **no és un estatus legal**; només els Estats atorguen nacionalitat, ciutadania i drets jurídics. t2p pot demostrar que una persona existeix, qui és i on es troba, però **no la converteix en ciutadana ni resol l'apatrídia**. Confondre les dues coses seria un engany cruel.

Un perill encara més greu, com hem vist amb els 815 milions de registres filtrats i les morts per fallada d'autenticació, és que centralitzar la biometria pot vigilar i matar poblacions vulnerables. Per això el disseny ha de ser radicalment diferent: **descentralitzat, amb la prova en mans del titular, voluntari i amb una alternativa no biomètrica sempre disponible**. Una prova d'existència mai no pot ser un requisit excloent per accedir a serveis; si algú declara un nom fals, la cadena només certifica que aquella dada es va capturar íntegra, no la seva veritat. La tecnologia és bona només si serveix la persona i no l'Estat contra ella.

La promesa és immensa i profundament humana. Donar a 800 milions d'invisibles una manera de demostrar que existeixen —portàtil, seva, verificable sense demanar permís a ningú— és obrir-los la porta a tots els altres drets, convertint el «no consto enlloc» en «aquí està la prova que sóc».

Una identitat ancorada permanentment a la prova d'existència pot convertir-se en una cadena invisible que impedeixi qualsevol reinvenció personal. Quan el personatge digital es fixa «el més íntimament possible» amb la identitat jurídica offline, s'obre la porta a noves injustícies: decisions de vida —des de crèdits bancaris fins a permisos d'immigració— podrien basar-se en un registre immutable que no deixa espai per a errors o canvis voluntaris [11]. El cas del projecte Worldcoin/World ID il·lustra aquest perill; el seu escaneig d'iris, dissenyat per provar la humanitat, ha estat prohibit o obligat a esborrar dades en més de nou jurisdiccions entre el 2024 i el 2025 —Kenya l'ha declarat inconstitucional i Colòmbia ha ordenat la supressió total de la biometria recollida [12]. Per això el disseny ha d'incloure mecanismes de dissociació temporal controlada, que permetin al titular desconnectar la seva identitat digital del registre legal quan ho necessiti, i garantir una alternativa no biomètrica sempre disponible per evitar que un únic punt de fallada bloquegi tot el seu futur.

És hora d'actuar

Per als **Estats i registres civils**: invertir en un registre de naixements universal i adoptar models descentralitzats que, sense excloure, incorporin la lliçó d'Aadhaar. Per a les **agències humanitàries** (UNHCR, ACNUR, ONG): proporcionar credencials portàtils que siguin controlades per les persones, en lloc de bases de dades biomètriques centrals que les converteixin en subjectes de vigilància. Per als

organismes d'estàndards (W3C, eIDAS): consolidar la identitat autosobirana amb divulgació selectiva com a norma. Per als **dissenyadors**: situar la privacitat i la voluntarietat com a primer requisit, no com a darrer afegit. I per a tothom: recordar que la prova de la teva existència ha de ser un dret a les teves mans, no una cadena al coll.

Una nena va morir perquè un sistema d'identitat li va negar el dret a menjar. La diferència entre una prova d'existència que apodera i una que exclou és tota la diferència del món; garantir a cada persona una prova segura i en les seves mans és, en aquest front fonamental, **time2act**.

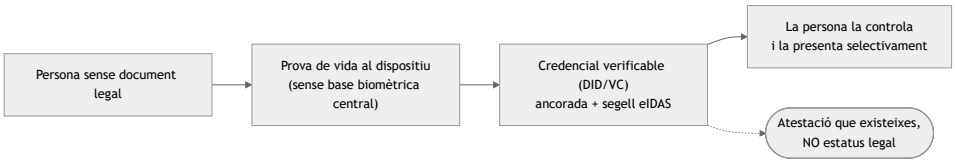


Figura 47.1 — Una persona sense papers genera un gest de prova de vida («sóc jo, estic viu»); al dispositiu se'n calcula l'empremta SHA-512 amb GPS forense i segell de temps eIDAS («aquí, ara»), s'ancora a la blockchain pública i pot acompanyar una credencial verificable W3C; el titular guarda la prova al seu dispositiu i la comparteix amb divulgació selectiva, en un contenidor .asice verificable fora de línia. Escala del repte: ~800 M sense identitat, ~4,4 M (fins a 10 M) apàtrides, 150 M d'infants no registrats. Fonts: Banc Mundial ID4D; UNHCR; UNICEF; W3C.

---

[1] Banc Mundial (ID4D) — *Global progress in identification: 3 findings from the latest data* (2025; ~800 M sense identitat oficial; >50 % són infants no registrats). 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 d'apàtrides oficials, fins a ~10 M reals; rohingyes ~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* (desembre 2024). https://www.unicef.org/press-releases/birth-registration-steadily-increases-worldwide-150-million-children-still-invisible ↩

[4] Comissió Europea — *European Digital Identity (eIDAS 2.0)* (Reg. UE 2024/1183; EUDI Wallet obligatòria a finals de 2026; divulgació selectiva). https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation ↩

[5] W3C — *Verifiable Credentials Data Model v2.0 becomes a W3C Recommendation* (15-maig-2025) i *Decentralized Identifiers (DID) v1.0* (2022). https://www.w3.org/press-releases/2025/verifiable-credentials-2-0/ ↩

[6] Govern de l'Índia (Press Information Bureau) — *Aadhaar* (~1.340 milions de titulars vius; >99,9 % dels adults; >170.000 milions d'autenticacions). 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 milions de registres, 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) — recerca sobre Aadhaar i l'exclusió en programes de benestar (*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; reconeixement d'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: prohibicions i ordres de supressió* (2024-2025). https://www.biometricupdate.com/202510/colombia-orders-world-shut-down-citing-biometrics-compliance-failures ↩

Integritat electoral: provar què va passar a les urnes

«El poble regna sobre el món polític americà com Déu sobre l'univers. És la causa i la fi de totes les coses; tot en surt i tot s'hi absorbeix.»

— Alexis de Tocqueville, La democràcia a Amèrica, I (1835)

L'1 de setembre de 2017, a Nairobi, el president del Tribunal Suprem de Kenya, **David Maraga**, va llegir un veredicte que va fer història. Per quatre vots contra dos, el tribunal declarava «invàlida, nul·la i sense efecte» la reelecció del president en exercici, Uhuru Kenyatta. Era la primera vegada a l'Àfrica que una cort anul·lava la victòria d'un president a instàncies de l'oposició [1]. I el detall que ho va tombar tot no va ser un frau de paperetes, sinó **actes que no quadraven**: de 291 formularis d'escrutini de circumscripció examinats, 56 no tenien trets de seguretat, 31 no portaven número de sèrie i 32 no estaven signats pels agents; molts resultats havien arribat al centre nacional sense les imatges escanejades de les actes de mesa [2]. Va ser la integritat del **procés de transmissió**, no del vot, allò que va decidir qui governava Kenya.

Aquest cas marca la frontera exacta d'aquest capítol. Al capítol 20 vam veure les deepfakes de candidats i la desinformació electoral —l'atac a la *percepció* del votant. Aquí parlem d'una altra cosa: la integritat del **procés** mateix —l'acta, l'escrutini, la transmissió, l'observació—, és a dir, de poder provar **què va passar de debò a les urnes**. I, com veurem, aquí la temptació tecnològica més òbvia és també la més perillosa.

El procés, no la papereta

La fragilitat del procés és global. A la República Democràtica del Congo, el gener de 2019, la comissió electoral va proclamar guanyador Félix Tshisekedi amb un 38,57 %. Però una base de dades filtrada de la pròpia comissió, que cobria el 86 % dels vots, donava la victòria al perdedor oficial, Martin Fayulu, amb gairebé un 60 %; i 39.824 observadors desplegats per l'Església catòlica congolesa arribaven a una xifra encara més alta per a Fayulu. Les dues fonts independents, recollides per separat, coincidien entre elles amb una correlació del 0,98, però divergien del resultat oficial en uns 3,6 milions de vots [3]. L'evidència existia; el que faltava era una cadena de custòdia verificable que la fes incontestable.

És precisament aquesta cadena de custòdia el que vigilen els observadors electorals. Com explica el manual de l'**OSCE/ODIHR**, l'oficina de drets humans de l'Organització per a la Seguretat i la Cooperació a Europa, el valor de l'observació rau en una metodologia sistemàtica que cobreix tot el cicle —marc legal, registre, campanya, votació, escrutini, tabulació— i que permet distingir si les irregularitats són **aïllades o sistemàtiques** [9]. El problema és que el testimoni d'un observador, sense una prova ancorada, sempre es pot qüestionar: «podria ser d'un altre dia, d'un altre lloc, un muntatge».

Per què el vot en blockchain és una mala idea

Arribats aquí, cal fer una advertència que aquest llibre no pot estalviar-se, perquè és contraintuïtiva. La temptació natural és pensar: si la blockchain serveix per a tantes coses, per què no hi votem directament? La resposta de la comunitat de seguretat és unànime i contundent: **votar en blockchain és una mala idea**.

El criptògraf **Ron Rivest**, del MIT i coinventor del sistema RSA, ho va demostrar amb els seus col·legues en un article de referència titulat, sense embuts, *Going from bad to worse: from Internet voting to blockchain voting* (2021). La seva conclusió és que el vot per internet i per blockchain «augmentarien enormement el risc de **fallades electorals indetectables a escala nacional**» [4]. El motiu de fons és profund: una elecció exigeix alhora **secret del vot** i **independència del programari** —que cap error o canvi no detectat al software pugui alterar el resultat sense deixar rastre—, i la transparència de la cadena de blocs trenca el secret, mentre que cap tecnologia coneguda, blockchain inclosa, garanteix la independència del programari en un vot mòbil.

No és teoria. El 2018, Virgínia Occidental va deixar votar 144 persones —molts militars desplegats— amb l'aplicació de blockchain Voatz; el 2020, investigadors del MIT van trobar que un atacant podia «alterar, aturar o exposar el vot» d'un usuari, i l'estat la va abandonar [5]. I a Moscou, l'agost de 2019, l'investigador francès **Pierrick Gaudry**, del CNRS, va descarregar el codi del sistema de vot «blockchain» de la ciutat i, en uns **vint minuts** amb un ordinador corrent i software lliure, en va calcular les claus privades: podria

haver revelat el vot de cada elector [6]. Després del pegat, un altre investigador el va tornar a trencar. L'etiqueta «blockchain» no és cap garantia de seguretat. La prova d'existència, doncs, **no ha de tocar mai l'emissió del vot secret**. El seu lloc és un altre.

La prova d'existència al servei de l'escrutini, no del vot

El lloc correcte de **t2p** són les **parts públiques i observables** del procés. Vegem-ho.

Primer, **el segellat de l'acta a la mesa**. Abans de transmetre cap resultat, el funcionari fotografia l'acta de mesa i la segella: **empremta SHA-512** al dispositiu, **segell de temps RFC 3161** conforme a eIDAS, **GPS forense** de la ubicació de la mesa i **prova de vida** del funcionari que la signa, tot en un contenidor **.asice** ancorat a la blockchain pública. Si algú altera la xifra «en trànsit» entre la mesa i el centre de tabulació —exactament el forat de Kenya—, l'acta original segellada el delata: l'empremta no coincideix. Segon, **l'evidència dels observadors**: una foto o un vídeo d'una irregularitat segellats amb GPS, hora i prova de vida converteixen un testimoni qüestionable en un registre amb lloc, moment i persona provats. Tercer, **la cadena de custòdia**: cada salt de l'acta es pot re-segellar, creant el rastre auditable que distingeix l'aïllat del sistemàtic.

I aquí és clau una complementarietat. L'estadístic **Philip Stark**, de la Universitat de Califòrnia a Berkeley, va inventar les **auditories de risc limitat** (RLA): un mostreig estadístic del paper que limita formalment el risc de proclamar un guanyador equivocat, sempre que existeixi una **papereta verificada pel votant** [7]. La seva màxima és «no confiïs en la màquina, exigeix evidència». La prova d'existència no substitueix la RLA: el paper continua sent la veritat de terreny. t2p assegura que la *foto de l'acta i la seva transmissió* no es manipulin; el recompte autèntic s'audita sobre el paper.

Cal dir el límit amb tota la claredat, perquè és el cor d'aquest capítol. t2p **no és vot per internet ni vot en blockchain**; només segella les parts públiques: actes, fotos, vídeos, transmissió. I «escombraries a l'entrada, escombraries a la cadena»: segellar una acta prova que *aquell paper existia amb aquella xifra, en aquella hora i lloc*, no que la xifra reflecteixi els vots realment dipositats. Si l'acta ja venia falsificada des de la mesa, la cadena la immortalitza igual de falsa. Per això la prova d'existència és **complement** de l'observació i de l'auditoria sobre paper, mai el seu substitut.

La promesa i el perill

La promesa, ben acotada, és valuosa. En països on una xifra alterada en trànsit pot decidir qui governa —i provocar violència—, segellar l'acta a la mesa i donar als observadors una evidència incontestable faria molt més difícil el frau de transmissió i molt més fàcil distingir l'error puntual de la manipulació orquestrada. És tornar credibilitat a un procés del qual depèn la pau.

El perill, aquí, és sobretot l'excés d'ambició. Vendre la prova d'existència com una solució per «votar des del mòbil» seria repetir l'error de Voatz i Moscou, i posar en risc el secret del votant i la confiança en tot el sistema. El segell tampoc no fa veritable una acta falsa. I qualsevol infraestructura que registri l'activitat electoral ha de protegir i garantir l'anonimat del votant. La prova d'existència és una eina per a la transparència del que és públic, no una drecera per digitalitzar el que ha de continuar sent secret i de paper.

A més, el fet de segellar actes a una capa com la que t2p fa servir avui implica confiar en una cadena que es presenta com neutra, però la neutralitat és només formal si el poder de validació i interpretació del protocol queda concentrat en mans d'uns pocs actors. En l'ecosistema L2, el 2026 gairebé la meitat dels blocs (aproximadament un 42 %) es genera a través de relays que apliquen les llistes OFAC, i tots els grans L2 d'Ethereum operen amb un únic seqüenciador corporatiu [12]. Aquesta arquitectura crea una «censura asimètrica»: qui controla el seqüenciador pot decidir quins actius es registren o s'exclouen, sense que la comunitat en sigui conscient. Com recorda Shoshana Zuboff, el nucli del poder és «qui sap, qui decideix, i qui decideix qui decideix» [11]; així, una infraestructura de segellat basada en la blockchain pública podria replicar un domini oligàrquic, on la confiança pública es veu erosionada per la manca de mecanismes anti-concentració. En aquest escenari, la prova d'existència podria acabar servint més com a eina de control que com a garantia de transparència.

És hora d'actuar

Per a les comissions electorals: segellar les actes a la mesa i transmetre-les, evitant l'alteració en trànsit que va tombar Kenya. Per als observadors (OSCE/ODIHR, Carter Center, societat civil): ancorar la seva evidència amb hora, lloc i persona, perquè cap testimoni d'irregularitat es pugui descartar com a «muntatge». Per als auditors: mantenir la papereta de paper verificada pel votant i les auditories de risc limitat com a veritat de terreny. I per a tothom: resistir la temptació del vot en blockchain, que la millor ciència de seguretat ha desaconsellat una vegada i una altra.

Un president va caure a Kenya perquè unes actes no quadraven i ningú no podia provar l'original. Donar a cada acta i a cada observació una prova amb hora, lloc i persona —sense tocar mai el secret del vot— és, en aquest front decisiu per a la democràcia, **time2act**.

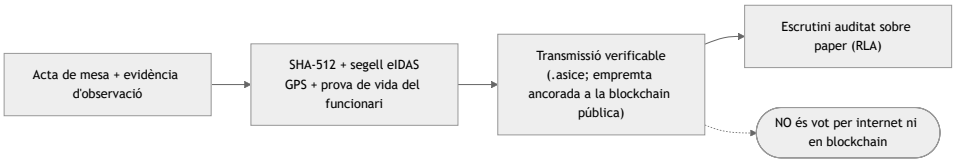


Figura 48.1 — A la mesa, l'acta es fotografia i se segella amb empremta SHA-512, segell de temps eIDAS, GPS forense i prova de vida del funcionari, en un contenidor .asice ancorat a la blockchain pública; si la xifra s'altera en trànsit cap al centre d'escrutini, l'empremta no coincideix i el delata. El que la prova d'existència NO fa: no és vot per internet, no és vot en blockchain, i no demostra que el recompte sigui veritable —això s'audita sobre el paper (RLA). Fonts: Tribunal Suprem de Kenya (2017); Rivest et al. (2021); Philip Stark.

---

[1] Wikipedia (amb BBC / Al Jazeera) — *2017 Kenyan presidential election petition* (anul·lació 4-2; CJ David Maraga; primera a l'Àfrica). https://en.wikipedia.org/wiki/2017_Kenyan_presidential_election_petition ↩

[2] The Standard (Kenya) — *Presidential petition: what scrutiny of key IEBC forms revealed* (291 formularis 34B; 56 sense trets de seguretat, 31 sense número de sèrie, 32 sense signatura). 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 observadors; correlació 0,976-0,991; ~3,6 M de vots). https://cic.nyu.edu/resources/who-really-won-the-congolese-elections/ ↩

[4] Sunoo Park, Michael Specter, Neha Narula i 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; trencat en ~20 minuts). 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 (Universitat de Minnesota) — *Colorado successfully completes the nation's first risk-limiting audit* (2017; límit de risc del 9 %). https://electionacademy.lib.umn.edu/2017/11/27/colorado-successfully-completes-nations-first-risk-limiting-audit/

[9] OSCE/ODIHR — *Election Observation Handbook* (6a edició; observadors de curt i llarg termini; distingir l'aïllat del sistemàtic). https://cdn.osce.org/sites/default/files/f/documents/5/e/68439.pdf ↩

[10] The Carter Center — *Election Standards i 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/ ↩

Ajuda humanitària: provar que l'ajuda arriba

««Tutti fratelli» —tots germans—, repetien elles amb emoció.»

— Henry Dunant, Un record de Solferino (1862)

Al Kivu Sud, a l'est de la República Democràtica del Congo, l'organització GiveDirectly repartia diners en efectiu a famílies en pobresa extrema a través del mòbil. El 2022, part del seu propi personal local va fer una cosa senzilla i devastadora: registrava targetes SIM a nom dels beneficiaris, però se les quedava i posava unes altres als telèfons de la gent. Quan van començar els pagaments, els diners queien en SIM controlades pels mateixos treballadors. El desviament va arribar a uns **1,2 milions de dòlars** i va afectar prop de **1.900 famílies**; l'organització ho va confessar públicament, però només va poder recuperar-ne una part mínima [9]. Darrere d'aquella xifra hi ha una mare que es va endeutar esperant uns diners que no van arribar mai.

Aquest cas planteja la pregunta d'aquest capítol: en l'ajuda humanitària, **com es prova que l'ajuda arriba de debò a la persona que la necessita?** I planteja també, amb una agudesa que no té cap altre capítol del llibre, el seu revers ètic: la temptació de respondre amb biometria pot convertir els més vulnerables en els més vigilats.

Deu mil milions que han d'arribar

L'ajuda en efectiu i vals —donar diners en lloc de béns— ha deixat de ser marginal. Segons l'organització de referència del sector, la **CALP Network**, i les dades de Development Initiatives, va arribar a uns **10.600 milions de dòlars** de despesa de programa el 2022 i representa ja prop d'una quarta part de tota l'ajuda humanitària internacional [5][6]. El Programa Mundial d'Aliments (WFP) n'és el major proveïdor, amb 2.900 milions de dòlars repartits a 51,6 milions de persones en 76 països només el 2023 [5]. Quan es mou tant diner cap a tanta gent en contextos de crisi, **verificar l'entrega no és un detall: és el problema central**.

La resposta tecnològica més coneguda és **Building Blocks**, del WFP, la implementació de blockchain més gran del món humanitari. Va començar el 2017 al camp d'Azraq, a Jordània, i avui dona suport a uns **sis milions de persones**, amb més d'un milió de refugiats que el fan servir cada mes [1][2]. Ha processat uns 555 milions de dòlars en transferències, ha eliminat el 98 % de les comissions bancàries en el pilot i, sobretot, ha demostrat el seu valor en la **desduplicació**: a Ucraïna, el 2022, divuit organitzacions van coordinar 337 milions de dòlars d'ajuda i van evitar uns **35 milions** d'assistència duplicada en detectar solapaments entre agències [1]. Coordinar sense duplicar és, en si mateix, una victòria contra el frau.

El dilema biomètric

Però aquí arriba la part difícil. Per saber que els diners van a la persona correcta, moltes agències han recorregut a la **biometria**. Als supermercats dels camps jordans, el refugiat mira a una càmera i un **escàner d'iris** confirma la seva identitat contra la base de dades de l'Alt Comissariat per als Refugiats, que a finals de 2023 contenia les empremtes i els iris de **15,7 milions de persones** [4]. La promesa és impecable: ningú cobra dues vegades, ningú suplanta. El problema és el poder. Com va observar un periodista al camp de Zaatari, un refugiat anomenat Bassam deia que el nou sistema funcionava millor... però «té poca veu en l'assumpte, perquè ha d'estar al sistema si vol menjar» [3]. Un consentiment que es dona «si vols menjar» no és un consentiment lliure.

I el risc no és abstracte. Al Iemen, el 2019, el WFP va haver de suspendre parcialment l'ajuda a les zones controlades pels houthis després que aquests es neguessin a cedir el control de les dades biomètriques — una eina que el WFP volia, precisament, per aturar un desviament sistemàtic d'aliments que havia documentat; la disputa encara durava el 2023, amb milions de persones necessitades al mig [8]. I el cas més greu el va destapar **Human Rights Watch**: l'organització de drets humans, a través de la seva directora de crisi **Lama Fakih**, va documentar el 2021 que l'Alt Comissariat havia recollit dades biomètriques de refugiats rohingyes a Bangladesh i que se n'havien compartit uns **830.000 noms** amb Myanmar —l'Estat del qual havien fugit— sense un consentiment lliure i informat; 23 de 24 refugiats entrevistats creien que les seves dades només servirien per a la targeta d'ajuda [7]. Com adverteix l'ONG

Privacy International, acumular biometria de poblacions en conflicte és facilitar la vigilància, i quan aquelles dades arriben al país del qual fuges, poden ser una condemna.

Provar l'entrega sense crear un honeypot

És aquí on **t2p** ofereix una alternativa amb una filosofia oposada: provar l'entrega **sense construir una base biomètrica central** que es converteixi en un objectiu.

El mecanisme, al punt de lliurament, és el següent. Es genera un **rebut d'entrega** —beneficiari amb un identificador anònim, import, lloc, hora, agent— del qual es calcula l'**empremta SHA-512** al dispositiu, s'ancora a la **blockchain pública** i s'hi afegeix un **segell de temps RFC 3161** i **GPS forense**. El resultat és un **.asice verificable fora de línia**: la prova que *aquest* beneficiari va rebre *aquesta* ajuda en *aquest* lloc i *aquesta* hora, auditable pel donant sense haver de creure's la paraula de l'executor —exactament el que hauria delatat el frau del Congo. Per confirmar que hi ha una persona viva i consentidora, en lloc d'un escàner d'iris central s'usa la **prova de vida al dispositiu**: la plantilla biomètrica no cal que surti del telèfon ni s'acumuli en cap servidor.

I la peça més elegant resol el dilema de la desduplicació. Un equip de la Escola Politècnica Federal de Lausana, liderat per la criptògrafa **Carmela Troncoso** i en col·laboració amb el Comitè Internacional de la Creu Roja, va dissenyar un sistema anomenat **Janus** que detecta el doble registre **sense crear cap base de dades biomètrica en clar**: revela un sol bit d'informació —«ja registrat» o «nou»— mitjançant càlcul segur [10]. És la demostració que es pot impedir el frau de beneficiaris fantasma sense convertir els refugiats en una població fitxada. La cadena pública guarda *proves d'unicitat*, no identitats.

I aquí, més que enlloc, cal dir el límit sense adorns. La prova d'existència demostra **integritat, hora, lloc i presència de la persona**, però **no la veritat del que passa després**. Si un actor armat obliga el beneficiari a lliurar l'efectiu un cop cobrat —el cas del Iemen—, o si el personal corrupte controla el dispositiu —el cas del Congo—, la cadena registrarà una entrega «vàlida» que va ser desviada: «escombraries a l'entrada, escombraries a la cadena». I encara hi ha un límit més profund: **qualsevol registre biomètric de gent extremadament vulnerable és vigilància**. t2p redueix el risc d'honeypot, però no elimina el dilema del poder i del consentiment. De vegades, l'opció més segura per als més febles no és perfeccionar la biometria, sinó **minimitzar-la**.

La promesa i el perill

La promesa és profundament humana. Una capa de prova d'entrega independent i verificable donaria als donants la certesa que els seus diners arriben, impediria el frau de rebuts inflats i beneficiaris fantasma, i —si es dissenya amb la lògica de Janus— ho faria **sense** crear les bases de dades biomètriques que avui posen en perill els refugiats. En un sector on cada dòlar desviat és un àpat que algú no menja, la integritat de l'entrega és, literalment, una qüestió de vida.

El perill, que en aquest capítol va al davant, és oblidar que la tecnologia toca els més indefensos. Cap sistema no ha de poder ser una eina de vigilància contra qui fuig; cap consentiment arrencat «si vols menjar» és lliure; i cap segell no atura la bala d'un actor armat ni la mà d'un funcionari corrupte que controla l'aparell. La prova d'existència és una eina al servei del principi humanitari de «no fer mal», no una excusa per fitxar el vulnerable.

A més, la traçabilitat permanent d'una població ja vulnerada pot transformar-se en un actiu negociable: cada moviment registrat, cada empremta digital, es converteix en una peça de «matèria primera gratuïta» que empreses i intermediaris poden empaquetar per a mercats d'anàlisi predictiva. Shoshana Zuboff ja advertia aquest fenomen, assenyalant com l'experiència humana és arrebatada i venuda sense cap compensació al subjecte [11]. Si el registre de distribució es converteix en una base de dades persistent, els mateixos patrons que garanteixen transparència podrien ser reutilitzats per a perfils de consum o fins i tot per a predicció d'esdeveniments socials, alimentant un mercat clandestí de «dades de vulnerabilitat». Per evitar aquesta mercantilització, cal establir salvaguardes explícites que prohibeixin la venda o l'alienació de qualsevol registre de tramesa humana, més enllà del simple control de processament al dispositiu. La regulació ha d'estendre-se a la propietat i a l'ús secundari de les dades, tal com la FTC va fer el 2024 prohibint per primera vegada la venda de dades de localització sensibles, i com la DPA neerlandesa va sancionar Clearview AI amb una multa de 30,5 milions d'euros per una base biomètrica massiva [12]. Això assegura que la prova d'existència segueixi servint únicament al principi humanitari de «no fer mal», sense obrir la porta a un nou model de negoci basat en la vulnerabilitat.

És hora d'actuar

Per als donants: exigir una prova d'entrega independent i verificable, perquè cada dòlar arribi a una persona real i no a una SIM robada. Per a les agències (WFP, ACNUR, ONG): aplicar la desduplicació sense honeypot a l'estil de Janus i minimitzar la biometria, amb consentiment realment lliure i alternatives no biomètriques. Per als organismes de privacitat i estàndards: fer del «no fer mal» i de la minimització de dades un requisit, no una recomanació. I per a tothom: recordar que en l'ajuda, més que enlloc, la pregunta no és només «arriba?», sinó «arriba sense convertir qui la rep en un sospitós permanent?».

Una mare congolesa es va endeutar esperant una ajuda que el frau li va robar. Donar a cada entrega una prova independent —i fer-ho sense fitxar els qui ja ho han perdut tot— és, en aquest front que toca la dignitat humana, **time2act**.

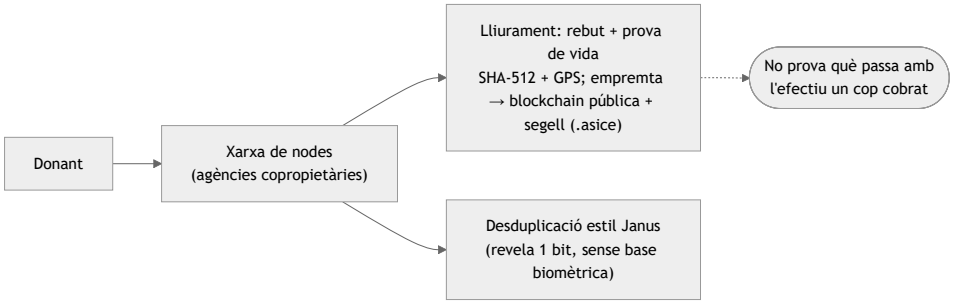


Figura 49.1 — Al punt de lliurament, un rebut d'entrega (beneficiari anònim, import, lloc, hora) se segella amb empremta SHA-512, segell de temps eIDAS i GPS forense, en un contenidor .asice verificable fora de línia; la prova de vida al dispositiu confirma una persona viva sense escàner central; i la desduplicació a l'estil Janus revela només un bit («ja registrat» o «nou»), sense crear cap base biomètrica. Impacte real: a Ucraïna es van evitar ~35 M$ d'ajuda duplicada. Límit: no prova què passa amb l'efectiu un cop cobrat (Iemen, Congo). Fonts: WFP; EPFL/CICR (Janus); Human Rights Watch.

---

[1] WFP — *Building Blocks* (~555 M$ en transferències; ~6 M de persones; Ucraïna: 337 M$ coordinats, ~35 M$ de solapament evitat; 159 organitzacions el 2025). https://www.wfp.org/building-blocks ↩

[2] UN Innovation Network — *How the Building Blocks blockchain network is transforming humanitarian aid* (>1 M de refugiats 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 comissions). 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 persones; PRIMES/BIMS). https://www.unhcr.org/blogs/unhcrs-biometric-tools-in-2023/ ↩

[5] Development Initiatives — *Cash and Voucher Assistance* (~10,6 mil M$ el 2022 → 9,7 mil M$ el 2023; WFP, major proveïdor). 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 noms compartits amb 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 biomètrica amb els houthis, 2019-2023). https://news.un.org/en/story/2023/12/1144417 ↩

[9] GiveDirectly / The New Humanitarian — *DRC mobile-cash fraud* (~1,2 M$ desviats; ~1.900 famílies). https://www.givedirectly.org/drc-case-2023/ ↩

[10] Carmela Troncoso et al. (EPFL SPRING Lab, amb el CICR) — *Janus: Safe Biometric Deduplication for Humanitarian Aid Distribution* (IEEE S&P 2024; revela només un bit, sense base biomètrica). 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 ↩

L'ajuda en espècie: la cadena de custòdia del socors

«Ser home és precisament ser responsable. [...] És sentir, en posar la teva pedra, que contribueixes a bastir el món.»

— Antoine de Saint-Exupéry, Terra dels homes (1939)

El 24 de juny de 2026, a les 18:04 hora local, un sisme de magnitud 7,2 sacseja Veneçuela des de prop de San Felipe, a l'estat de Yaracuy. Trenta-nou segons després en arriba un segon, de magnitud 7,5. Edificis sencers cauen a Caracas, La Guaira i Caraballeda; l'aeroport internacional Simón Bolívar suspèn les operacions; les xarxes mòbils se saturen. Al tancament d'aquest capítol, el balanç és aclaparador: més de 3.300 morts, més de 16.800 ferits, desenes de milers de desapareguts [1]. I el món respon com sap: més de 30 països, més de 3.600 rescatistes, més de 1.000 tones d'ajuda. El Salvador amplia el seu contingent de 150 a 300 rescatistes i de 50 a 150 tones; el Brasil envia 36 bombers i sis gossos de recerca; el xef José Andrés dona un milió de dòlars i viatja al país amb World Central Kitchen; Rosalía en dona dos a UNICEF; Metallica, 100.000 [1][2].

I aleshores comença la segona pregunta, la que aquest llibre no pot esquivar: tot això — les tones, els palets, els contenidors — arribarà a qui ho necessita? Perquè mentre els equips de rescat encara excaven entre la runa, ja hi ha denúncies documentades de subministraments retinguts per funcionaris policials a Altamira, de centres d'acopi civils prohibits per alcaldes que limiten la recollida a la seu del seu partit, de distribucions impedides [1]. La generositat del món ha començat el viatge; el que aquest capítol pregunta és si el viatge es pot auditar.

Aquest capítol tracta l'ajuda en espècie: les coses — aliments, medicines, tendes, generadors — que viatgen del donant a la víctima per mar, per aire i per terra. L'entrega d'ajuda en efectiu i la deduplicació de beneficiaris són al capítol 49; el trajecte del diner del donant — «on va el meu euro» —, al capítol 73; l'origen verificable dels productes comercials, al capítol 29; el frau documental del comerç internacional, al capítol 54; la posició real dels vaixells, al capítol 103; la cronologia de les emergències, al capítol 105. Pregunta clau: com se sap que un palet que surt d'un dipòsit de Panamà arriba sencer a una família de La Guaira? Resposta: fent que cada baula del trajecte — el manifest, el vaixell o l'avió, la duana, el magatzem, el comboi, el punt de repartiment — deixi la seva prova d'existència amb **t2p**: l'empremta SHA-512 calculada al dispositiu, l'ancoratge de l'empremta a la blockchain pública i el segell de temps RFC 3161/eIDAS complementari, dins d'un contenidor .asice [11]. I amb la neutralitat de sempre: la mateixa traça que delata el desviament protegeix l'ONG honesta i l'autoritat diligent de l'acusació falsa. La prova serveix les dues direccions.

Els precedents: quan la confiança es va trencar

Els fraus que han marcat el sector no són llegendes: estan documentats, sovint per les mateixes organitzacions. Convé mirar-los de cara, perquè dibuixen el mapa exacte d'on es trenca la cadena.

El novembre de 2017, la Federació Internacional de la Creu Roja (IFRC) va reconèixer públicament que el frau s'havia endut almenys 6 milions de dòlars dels més de 124 que havia gestionat durant l'epidèmia d'Ebola (2014-2016), la crisi que va matar més d'11.000 persones a l'Àfrica occidental. El desglossament és una lliçó de logística fosca: a Sierra Leone, uns 2,13 milions van desaparèixer per «probable col·lusió» entre personal propi i un banc local que fixava el tipus de canvi al pic de l'epidèmia; a Guinea, uns 1,17 milions es van perdre en la facturació fraudulenta d'un proveïdor de despatx duaner; a Libèria, uns 2,7 milions es van evaporar en preus inflats d'articles de socors, nòmines i incentius de voluntaris [5]. L'honestedat mereix ser dita: va ser la mateixa Federació qui ho va destapar i qui es va declarar disposada a renunciar a immunitats per perseguir els responsables [5].

Somàlia, 2010: el Grup de Monitoratge de l'ONU va informar que «fins a la meitat» de l'ajuda alimentària del Programa Mundial d'Aliments es desviava cap a una xarxa de contractistes corruptes, milícies i personal local, i va assenyalar la família Adaani — un dels tres grans contractistes del programa — com a financera de grups armats. El WFP ho va negar en rodó: «no se'ns ha presentat cap evidència», va dir la seva directora executiva, Josette Sheeran, i una auditoria pròpia no va trobar res [6]. I aquí hi ha la lliçó probatòria central d'aquest capítol: la disputa era irresoluble. Sense registres de custòdia verificables, ni

l'acusació podia provar el desviament ni la defensa podia provar la innocència — i el dubte es va menjar la confiança igualment, en totes dues direccions.

I Espanya, 2007: segons la Fiscalia Anticorrupció, els directius d'Intervida — una de les grans ONG d'apadrinament del país — van desviar més de 45 milions d'euros camuflats com a «despeses per apadrinament»; quan la investigació es va fer pública, unes 10.000 persones es van donar de baixa com a donants. Aquell mateix abril, el president d'Anesvad era detingut, denunciat pels treballadors de la seva pròpia organització, acusat d'apropiació indeguda de fons [7]. El sector sencer va pagar la factura de confiança.

El patró comú és el que importa: el forat mai no és a la foto de l'arribada del vaixell, ni a la del repartiment amb les caixes ben apilades. És a les baules fosques del mig — el canvi de divises, el despatx duaner, el contractista local, la comptabilitat entre l'origen i el destí. (El cas més cèlebre de tots, els 500 milions de dòlars que la Creu Roja americana va recaptar per Haití, pertany al costat del donant i s'explica al capítol 73.)

La segona catàstrofe

Després d'un desastre, l'ajuda es pot perdre de tres maneres documentades — i Veneçuela, per una amarga coincidència, les il·lustra totes tres.

La primera és **el desviament i la captura política**. El paradigma verificat és el programa CLAP: les caixes de menjar subvencionades que el govern veneçolà va crear el 2016 i que van esdevenir un vehicle de corrupció a gran escala. Segons les investigacions, l'empresari Alex Saab i el seu soci van muntar una estructura per comprar aliments a l'estranger amb sobrepreus de fins a 30 dòlars per caixa — uns 360 milions de dòlars defraudats en dos anys, a través de societats com Group Grand Ltd, que va subministrar més d'11,5 milions de caixes. El Tresor dels EUA va sancionar la xarxa el juliol de 2019 per «robar al programa de distribució d'aliments»; una anàlisi de laboratori va trobar que la llet de les caixes tenia una composició nutricional inferior a l'etiquetada; i el menjar es va fer servir com a instrument de control social — premiar afins, castigar opositors [3]. Amb aquest historial, les denúncies de subministraments retinguts i centres d'acopi capturats després del terratrèmol [1] no són una sorpresa: són la mateixa lògica en versió d'emergència.

La segona és **el bloqueig**. El febrer de 2019, l'ajuda arribada a Cúcuta, a la banda colombiana de la frontera, es va trobar el pont de Tienditas barrat amb un camió cisterna i dos contenidors soldats entre si; el 23 de febrer, catorze camions amb 280 tones d'aliments van intentar passar — dos van acabar cremats en els incidents, cap càrrega no va entrar, i la frontera es va tancar del tot [4]. Cal dir-ho amb la neutralitat que aquest llibre es deu: aquell enviament era també un instrument en plena disputa política, i el govern al·legava que l'«ajuda» encobria altres fins. La lliçó probatòria no és qui tenia raó; és que, sense un registre neutral i verificable del contingut d'aquells camions, cada bàndol tenia el seu relat — i el ciutadà, cap manera de saber-ho. La prova d'existència hauria servit exactament igual per demostrar que la càrrega era el que deia ser, o que no ho era.

I la tercera és **el «segon desastre»**. No tot el que es perd, es roba: molt es malbarata. Segons l'expert en logística humanitària José Holguín-Veras, entre el 50 i el 70 % dels béns que arriben en una emergència no són necessaris ni apropiats; les donacions no sol·licitades col·lapsen pistes d'aeroport, refugis i magatzems, i drenen els voluntaris que haurien de fer coses més útils — hi ha documentat el cas d'un avió que va descarregar tones de joguines a la pista d'un aeroport en plena emergència, on van quedar mesos [8]. El corol·lari honest, coherent amb el capítol 49: la millor donació particular sol ser el donatiu econòmic. Però l'ajuda en espècie institucional — els estocs preposicionats, les càrregues d'agència — existirà sempre, i és exactament la que necessita custòdia.

Per mar, per aire, per terra: les baules

La maquinària real de l'ajuda en espècie és més sofisticada del que sembla des de fora. La xarxa UNHRD, gestionada pel Programa Mundial d'Aliments, manté dipòsits humanitaris preposicionats a Bríndisi, Accra, Kuala Lumpur, Ciutat de Panamà i Dubai, amb kits mèdics, material de refugi i aliments a punt per ser despatxats en 48 hores per a moltes organitzacions alhora; i quan esclata una crisi, el Clúster Logístic liderat pel WFP coordina les cadenes de subministrament humanitàries i omple els buits comuns — transport compartit, magatzems, rutes [9].

Seguim ara un palet concret. Al dipòsit d'origen s'empaqueta i s'emet la documentació: el manifest, la llista de contingut. El palet puja a un vaixell o a un avió. Arriba a un port o a un aeroport — en el cas veneçolà, amb l'aeroport principal suspès els primers dies [1], cada via alternativa compta. Passa el despatx duaner. Entra en un magatzem nacional. En surt en camions, sovint en comboi, cap a l'interior. I acaba, si tot va bé, en un punt de repartiment on algú el converteix en paquets per a famílies.

El diagnòstic probatori: cada fletxa d'aquest trajecte és un canvi de mans, i cada canvi de mans sense registre verificable és un lloc on les coses «es perden», es reetiqueten, es revenen o es reparteixen per criteris que no són la necessitat. Papers, n'hi ha — manifestos, albarans, actes de recepció —, però són papers de cada part: modificables, extraviables, contradictoris. Quan arriba l'escàndol, com a Somàlia [6], no hi ha manera de reconstruir la veritat; quan arriba el frau, com al despatx duaner de Guinea [5], la facturació fraudulenta es confon amb la legítima. El que falta no són més papers: és que els papers tinguin data certa, autor cert i una integritat que un tercer pugui verificar sense demanar permís a ningú.

La prova d'existència aplicada

El mateix palet, la mateixa cadena — i a cada baula, trenta segons d'un gest amb el mòbil [11].

1. El contenidor amb pedigrí

Al dipòsit d'origen, el responsable obre t2p, gira la roda de modes fins a Document i escaneja el manifest i la llista de contingut: l'escàner detecta les vores, corregeix la perspectiva i admet fins a 50 pàgines en un únic PDF; un toc a «Certificar a la blockchain» i l'empremta SHA-512 — calculada al dispositiu, dels bytes exactes del fitxer — rep el seu segell de temps RFC 3161/eIDAS i queda ancorada a la blockchain pública, amb el certificat PDF i el seu codi QR generats automàticament [11]. Des d'aquest instant, què conté el palet i quan ha sortit és un fet amb data certa: el «hi faltaven caixes» i el reetiquetatge posterior es contrasten contra l'empremta d'origen. És el pedigrí del capítol 29, aplicat al socors; i el manifest segellat dialoga amb els documents del comerç del capítol 54.

2. La duana i el magatzem

A cada canvi de mans — la descàrrega al port, el despatx duaner, l'entrada i la sortida del magatzem — una foto o un escaneig de l'acta amb t2p. La barra de GPS forense mostra en viu la qualitat de la ubicació: perquè la coordenada se segelli amb grau forense cal un fix GPS genuí, amb precisió d'uns 50 metres i una antiguitat màxima d'uns 30 segons; una ubicació simulada és l'única condició que bloqueja la certificació del tot, i si no hi ha senyal es pot capturar igualment — el certificat registra honestament que no s'hi va incrustar coordenada, i per què [11]. El resultat és una cronologia ancorada d'entrades i sortides on els buits queden datats: el palet que va entrar dilluns i mai no va sortir deixa de ser una boira per esdevenir una pregunta concreta a una persona concreta. El frau duaner de Guinea [5] hauria deixat exactament aquest rastre.

3. El comboi

Els camions surten amb la càrrega fotografiada — i filmada, si cal, amb la superposició de data i hora activada [11] — i en ruta es fan captures puntuals amb GPS forense. El detall operatiu que importa en una zona de desastre: la certificació de t2p treballa en segon pla i, si no hi ha cobertura, la cua es reprèn sola quan torna la connexió — es captura ara, se certifica quan es pot, i el segell acredita el moment de la captura [11]. El comboi que es desvia, el remolc que canvia de contingut, la càrrega que «es redistribueix» en un control de carretera: tot topa amb una cadena de captures ancorades que ningú no pot reescriure. La posició real dels vaixells que porten l'ajuda gran, per cert, és la matèria del capítol 103.

4. El repartiment

Al punt final, el cercle es tanca en les dues direccions. Cap avall: el repartiment es documenta amb rebuts que no exposen els vulnerables — la lògica del capítol 49: identificadors anònims, cap base de dades biomètrica centralitzada. Cap amunt: el responsable local signa la recepció amb la signatura més forta de t2p — la càmera frontal grava, l'app planteja dos reptes de vida aleatoris (girar el cap, somriure), la verificació biomètrica del dispositiu confirma, i apareix «IDENTITAT VERIFICADA» [11] — verificada en el sentit que el capítol 88 precisa: una persona real i present, amb el compte i la biometria del dispositiu, no un nom en un registre civil. I l'ONG exporta el paquet d'evidència .asice — un contenidor estàndard (ETSI EN 319 162) amb la còpia byte a byte, el certificat, el segell de temps i les instruccions de verificació

— que l'auditor del donant, a deu mil quilòmetres, pot verificar sense connexió, sense l'app i sense haver de confiar en ningú [11].

Els límits, amb la mateixa franquesa: el segell acredita fets logístics — què, quan, on, qui signa —, no bondat. Una caixa amb llet per sota de l'etiquetatge [3] es pot certificar perfectament: per a la qualitat calen anàlisis i auditories, no només empremtes. Cap segell no aixeca un contenidor soldat en un pont [4] ni desarma qui reté l'ajuda per la força. I la traça és proporcional: es documenta la càrrega i el tràmit, mai les persones que reben — aquí mana el capítol 49.

La promesa i el perill

La promesa: el donant que pot seguir el seu palet baula a baula; la disputa de Somàlia [6], resoluble en hores contra registres en lloc d'irresoluble per sempre; l'ONG honesta que respon al proper escàndol amb evidència en lloc de comunicats. I el sector ja camina en aquesta direcció: StaTwig traça vials de vacunes del dipòsit al centre de salut amb el suport d'UNICEF, l'IFRC ha pilotat blockchain amb les Creus Roges irlandesa i libanesa, i el WFP explora la traçabilitat d'aliments d'origen a destí [10]. El que hi afegeix t2p és la capa neutral i transversal: la mateixa eina per a l'agència gran i per a l'ONG petita, sense infraestructura pròpia [11].

Els perills, amb la mateixa serietat.

El primer és **la vigilància dels més vulnerables**. Aquest capítol hereta, sencer, el perill del capítol 49: la traça és per a la càrrega i els tràmits, mai per convertir les víctimes en fitxers. Cap biometria centralitzada, cap llista de beneficiaris exposada, cap condició de «si vols menjar, registra't». Es documenta el palet, no la persona que l'obre.

El segon és **el segell que no atura tancs**. Tienditas [4] ho diu tot: cap empremta no desmunta un contenidor soldat. La prova d'existència fa el bloqueig i el desviament visibles i datats — i això és molt: converteix el rumor en expedient —, però la resposta a un bloqueig armat és política i diplomàtica. Vendre criptografia com a solució d'un pont barrat seria mentir.

El tercer és **la criminalització de qui documenta**. En entorns hostils, fotografiar un magatzem o un control de carretera pot costar una detenció, o coses pitjors. El disseny protegeix qui certifica — només empremtes a la cadena, contingut al dispositiu, revelació voluntària [11] —, però cap protocol no ha d'obligar el treballador humanitari a triar entre la traça i la seva seguretat. La captura es fa quan és segur fer-la; el segell acredita el moment, no exigeix l'heroisme. I quan l'entorn hostil és directament una guerra — quan qui documenta és el periodista a qui no deixen entrar, o la víctima que grava amb el mòbil el que li està passant —, aquest dilema arriba al seu extrem: hi tornem de ple al capítol 113.

I el quart és **el tecnosolucionisme logístic**. El segell no cura el «segon desastre»: si el 50-70 % del que arriba no cal [8], certificar-ho només documenta el malbaratament amb més precisió. La custòdia verificable funciona dins d'una logística professional — la dels dipòsits i el clúster [9] — i amb la donació correcta, que sovint són diners [8]. I la neutralitat final: la mateixa traça que delata el funcionari corrupte exonera el diligent. Si només serveix per acusar, morirà; si serveix per demostrar, s'adoptarà.

És hora d'actuar

Que la generositat viatgi amb la seva prova.

Per als donants — persones, empreses, governs: exigiu la cadena de custòdia verificable com a condició de la donació en espècie; i si sou particulars, recordeu que sovint la millor ajuda és el donatiu econòmic a organitzacions amb traça [8][11].

Per a les ONG i agències: segelleu el manifest a l'origen, l'acta a cada canvi de mans i la recepció al punt final [11]; publiqueu per empremta, no per nota de premsa — el proper escàndol el respondreu amb registres [5][6].

Per al clúster logístic i els organismes ONU: incorporeu l'ancoratge neutral als estàndards de la cadena humanitària — manifest, despatx, magatzem, repartiment [9][10] — perquè la traça viatgi amb el palet entre organitzacions.

Per a les duanes i els governs receptors: despatx d'emergència amb actes ancorades — la vostra diligència quedarà tan datada com qualsevol abús [5]; i cap requisit que converteixi la traça en eina de

control de qui ajuda.

Per als transportistes i les navilieres: càrrega documentada a la sortida i a l'arribada [11]; la vostra protecció contra l'acusació de desviament és la mateixa traça.

Per als legisladors i reguladors de la cooperació: valor probatori a la custòdia ancorada en la justificació de subvencions; i protecció legal explícita per a qui documenta [7].

Mentre s'escriu aquest capítol, encara surten palets cap a Veneçuela. Que cada un porti el seu pedigrí — i que d'aquí a un any el donant, la família i el jutge puguin respondre la mateixa pregunta amb la mateixa evidència: què hi havia, on va passar, a qui va arribar. Perquè el socors arribi sencer, **time2act**.

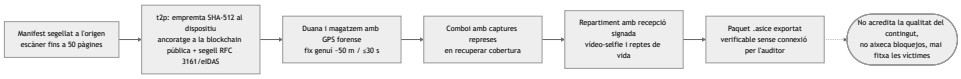


Figura 50.1 — La cadena de custòdia del socors amb prova d'existència (t2p: empremta SHA-512 al dispositiu, segell RFC 3161/eIDAS, blockchain pública, .asice): el manifest segellat a l'origen (escàner de fins a 50 pàgines), les actes de duana i magatzem amb GPS forense (fix genuí ~50 m / ≤30 s; la ubicació simulada bloqueja la certificació), el comboi amb captures represes en recuperar cobertura, i la recepció signada amb vídeo-selfie i reptes de vida — exportable com a paquet .asice verificable sense connexió per l'auditor del donant. Límits: el segell no acredita la qualitat del contingut, no aixeca bloquejos i mai no fitxa les víctimes. Fonts: IFRC (frau Ebola autodivulgat); ONU/WFP (Somàlia 2010); OFAC (xarxa CLAP); terratrèmol de Veneçuela 2026.

---

[1] Wikipedia (ES) — *Terremotos de Venezuela de 2026* (doblet M7,2 San Felipe + M7,5 Yumare, 24-6-2026, 39 s de diferència; >3.342 morts, >16.840 ferits, >68.000 desapareguts; aeroport Simón Bolívar suspès; conflictes de distribució: subministraments retinguts a Altamira, centres d'acopi civils prohibits a Charallave i Campo Elías, distribució impedida a El Limón, accés restringit a La Guaira; resposta: >30 països, >3.600 rescatistes, >1.000 tones); 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* (context humanitari; donacions: José Andrés/World Central Kitchen 1 M$, Rosalía 2 M$ a UNICEF, Metallica 100.000 $). https://ayudaenaccion.org/blog/ayuda-humanitaria/terremotos-venezuela/ ↩

[3] Departament del Tresor dels EUA — *Treasury Disrupts Corruption Network Stealing From Venezuela's Food Distribution Program (CLAP)* (25-7-2019; xarxa d'Alex Saab; Group Grand Ltd; sobrepreus); 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 caixes des de Mèxic, ~30 $/caixa de sobrepreu, ~360 M$; llet per sota d'etiquetatge — 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* (pont de Tienditas bloquejat amb cisterna i contenidors; 23-2-2019: 14 camions/280 tones, 2 camions cremats; tancament de frontera); CNN en Español — *Venezuela bloquea puente en frontera con Colombia* (6-2-2019); Infobae — *Maduro ordenó retirar los contenedores del puente Tienditas* (des. 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 Leone ~2,13 M col·lusió amb banc sobre el tipus de canvi; Guinea ~1,17 M facturació fraudulenta d'un proveïdor de despatx duaner; Libèria ~2,7 M preus inflats d'articles de socors, nòmines i incentius); 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; Grup de Monitoratge: «fins a la meitat» desviada; contractistes/milícies/personal local; família Adaani); VOA — *WFP Report says No Evidence of Food Diversion in Somalia* (negació del WFP — Josette Sheeran; auditoria pròpia sense evidència); 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€ desviats segons la Fiscalia Anticorrupció, ~10.000 donants de baixa; Anesvad: president detingut el 5-4-2007 per apropiació indeguda, denunciat pels treballadors). 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* (convergència material; donacions no sol·licitades col·lapsen pistes i magatzems); TED Ideas — *After a disaster, don't send toys or clothing — send money* (José Holguín-Veras: 50-70 % dels béns que arriben no són necessaris ni apropiats; el cas de l'avió de joguines). 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)* (dipòsits a Bríndisi, Accra, Kuala Lumpur, Ciutat de Panamà i Dubai; despatx en 48 h; estocs per a múltiples organitzacions); UNHRD — *Our Services*; World Economic Forum — *Logistics Emergency Team: 20 years* (Clúster Logístic liderat pel 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: traçabilitat de vials de vacunes del dipòsit al centre de salut); WFP Innovation Accelerator — *3 ways blockchain innovation is enhancing humanitarian work* (traçabilitat d'aliments; Building Blocks); LSE — *How Blockchain is Contributing to the Humanitarian Sector as of 2025* (pilot IFRC/AID:Tech amb la Creu Roja irlandesa i 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 producte (roda de modes; escàner de documents fins a 50 pàgines en un PDF; empremta SHA-512 calculada al dispositiu; certificació en segon pla que es reprèn en recuperar cobertura; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; GPS forense — fix genuí ~50 m / ≤30 s, la ubicació simulada bloqueja la certificació; comprovació d'integritat del dispositiu i attestation de maquinari; superposició de data/hora al vídeo; signatura amb vídeo-selfie, reptes de vida i biometria; paquet d'evidència .asice ETSI EN 319 162 verificable sense connexió; només empremtes a la cadena). Vegeu els capítols 13 i 15; l'entrega d'efectiu i la deduplicació, al capítol 49; l'euro del donant, al capítol 73. ↩

Fronteres i asil: l'evidència de qui fuig

«Vam perdre la llar, que vol dir la familiaritat de la vida diària. Vam perdre l'ofici, que vol dir la confiança de ser d'alguna utilitat en aquest món.»

— Hannah Arendt, «We Refugees» (1943)

La matinada del 14 de juny de 2023, el pesquer Adriana — sortit de Líbia cinc dies abans amb unes 750 persones a bord, la majoria de Síria, el Pakistan i Egipte, amb infants — va bolcar i es va enfonsar en aigües internacionals davant de Pylos, Grècia. Van morir més de 600 persones; van sobreviure 104; es van recuperar 82 cossos [1]. La guàrdia costanera grega va negar tota responsabilitat: els migrants haurien rebutjat l'ajuda, i el vaixell hauria bolcat sol. Les investigacions de Human Rights Watch, d'Amnistia Internacional i de desenes de periodistes van apuntar en una altra direcció: errors greus en les hores prèvies i al·legacions serioses que la patrullera grega va fer bolcar l'Adriana en intentar remolcar-la [1][2]. Dos anys després, el maig de 2025, la justícia grega va imputar 17 membres de la guàrdia costanera, inclòs el capità de la patrullera, acusat de causar un naufragi amb resultat de mort d'almenys 82 persones [3]. Mentrestant, nou supervivents havien estat processats — s'enfrontaven a cadenes perpètues — enmig de la denúncia de les organitzacions de drets humans, que advertien que el judici als supervivents no podia servir d'escut davant les responsabilitats de les autoritats [2].

Aquest capítol tracta l'evidència a les fronteres: els naufragis, les devolucions sumàries i el procediment d'asil. El lliurament de l'ajuda humanitària és al capítol 49; l'evidència de crims de guerra, al capítol 20; la identitat digital de qui no té papers, al capítol 47; la posició real dels vaixells, al capítol 103. Pregunta clau: com es proven els fets quan una de les parts ho ha perdut tot — sovint fins al telèfon — i l'altra escriu l'informe oficial? Resposta: anivellant amb prova d'existència — el rastre segellat de qui fuig, la documentació ancorada dels observadors i els registres igualment ancorats de les autoritats (**t2p**: empremta SHA-512, segell de temps RFC 3161/eIDAS, ancoratge a la blockchain pública, contenidor .asice [5]). A la frontera, la neutralitat de la prova no és una virtut abstracta: és l'única manera que la veritat no depengui de qui la conta.

Pylos: la versió oficial contra la reconstrucció

Val la pena mirar de prop com es va reconstruir la veritat d'aquella nit, perquè és una lliçó sencera sobre l'evidència a les fronteres. La primera versió la va posar qui tenia la ràdio i l'informe: segons la guàrdia costanera, l'Adriana navegava pel seu compte i els seus ocupants no volien assistència [1]. Contra aquesta versió no hi havia, d'entrada, res més que 104 supervivents traumatitzats i un vaixell al fons del mar.

La reconstrucció va arribar per convergència de fonts independents, i va costar mesos de feina: periodistes i organitzacions van creuar les dades de trànsit marítim de les embarcacions properes, els testimonis dels supervivents — recollits un a un — i el material dels seus telèfons, per contrastar la cronologia oficial amb la dels fets [4]. D'aquell periodisme forense, i de les investigacions de Human Rights Watch i Amnistia Internacional, van sortir les discrepàncies que la instrucció grega acabaria recollint: hores sense rescat amb el vaixell a la vista, i les al·legacions sobre el remolc fatal [1][2]. El resultat processal va trigar gairebé dos anys: el 26 de maig de 2025, la fiscalia va presentar càrrecs contra 17 membres de la guàrdia costanera — el capità de la patrullera ΠΠΛΣ-920, acusat de causar el naufragi; tots, d'exposar persones a perill malgrat el deure legal de rescatar-les —, després que una coalició d'ONG jurídiques presentés querella en nom de 40 supervivents [3].

La lliçó probatòria és el nucli d'aquest capítol: en un naufragi sense ancoratge, la primera versió la posa qui té l'informe, la reconstrucció triga anys, depèn d'heroïcitats periodístiques [4] i arriba quan les portades ja han passat. Si les posicions, les comunicacions i les imatges d'aquella nit haguessin estat segellades en origen — les de la patrullera i les dels telèfons dels passatgers per igual [5] —, la cronologia hauria estat un fet des del primer dia: què va fer cadascú, quan, i a quina distància. El capítol 103 va mostrar com es falsifica la posició d'un vaixell; aquí es veu què costa quan ningú no pot demostrar la seva.

La devolució que oficialment no va passar

El segon front són les devolucions sumàries — les expulsions sense procediment que, oficialment, no existeixen. La feina de documentar-les l'ha feta durant anys la societat civil: la Border Violence Monitoring Network, una coalició de més de dotze organitzacions fundada el 2017, recull testimonis de devolucions

il·legals i violència a les fronteres dels Balcans i Grècia; el seu «Black Book of Pushbacks» (2020) compilava els testimonis de 12.654 persones, i l'edició ampliada de 2022 supera les 3.000 pàgines en quatre volums [6]. En aquests milers de relats, un detall es repeteix amb una regularitat esfereïdora: la confiscació o destrucció dels telèfons. La prova de la víctima desapareix amb el seu únic testimoni.

I el desembre de 2025 va arribar el gir jurídic. El Tribunal de Justícia de la UE (assumpte C-136/24 P, sentència del 18 de desembre de 2025) va resoldre el cas d'un nacional sirià que al·legava que, després de desembarcar en una illa grega amb la intenció de demanar asil, havia estat detingut, despullat del telèfon i forçat a reembarcar cap al mar fins a ser traslladat a Turquia — amb Frontex present a l'operació. El Tribunal va establir que cal adaptar la càrrega de la prova: exigir proves concloents a víctimes en situació d'extrema vulnerabilitat faria «il·lusori» l'accés a la justícia, i és Frontex — responsable de les operacions — qui sol disposar de la documentació capaç d'aclarir els fets [7].

Llegit amb els ulls d'aquest llibre, el màxim tribunal europeu acaba de reconèixer l'asimetria probatòria com a problema jurídic central — i de constatar que la primera cosa que es pren a la víctima és, precisament, la seva prova. La resposta estructural no pot ser només processal. Si els observadors segellen els incidents en el moment [5][6], si el rastre de la víctima existeix ancorat abans que li prenguin el telèfon [5], i si els registres de les operacions oficials estan igualment ancorats i són exigibles [7], la devolució «que oficialment no va passar» esdevé impossible de sostenir — i la que de debò no va passar, impossible d'inventar. El segell no té bàndol: per això pot funcionar al territori més polaritzat d'Europa.

L'asil: demostrar la por amb el que et queda

El tercer front és el més silenciós. Qui demana protecció internacional ha d'acreditar una persecució — la militància, l'amenaça, la detenció, l'agressió — amb allò que ha pogut endur-se d'una fugida. Els documents es perden pel camí; els telèfons es confisquen o s'enfonsen [6][7]; els records es contradiuen sota l'estrès; i la credibilitat del relat esdevé l'eix de tota la resolució. És, probablement, el procediment jurídic amb més distància entre el que cal provar i el que es pot provar.

La prova d'existència s'hi aplica des del país d'origen. Qui tem haver de fugir pot segellar el seu rastre abans i durant: l'amenaça rebuda, la foto de la detenció del germà, el carnet del partit, l'article publicat — cada element amb la seva empremta SHA-512 i la seva data certa, ancorades des del primer moment [5]. Pel camí, pot ancorar els moments crítics sense publicar res ni revelar-se.

I aquí és on el disseny mostra la seva força: si el telèfon es perd al mar o el confisquen a la frontera [7], el contingut pot desaparèixer — però l'existència i la data del material queden acreditades per sempre. Recuperada una còpia — del núvol, d'un familiar, d'una organització —, la seva integritat i la seva antiguitat es verifiquen contra l'empremta ancorada. El relat de persecució deixa de dependre només de la memòria: porta annexos amb data certa.

El matís imprescindible, dit des d'ara: el segell no fa cert el contingut. Un document fals segellat continua sent fals, i la valoració de credibilitat continua corresponent a qui instrueix. El que el segell fa impossible és la fabricació retroactiva — crear avui «proves» datades d'ahir —, que és exactament el dubte que enverina aquests procediments i que cap entrevista no pot resoldre.

La prova d'existència aplicada

Una frontera qualsevol, de nit. Tres relats del mateix moment — el de qui fuig, el de qui vigila, el de qui observa — i, per primera vegada, cap dels tres no es pot reescriure.

1. El rastre de qui fuig

La persona que es prepara per demanar asil segella al seu dispositiu, des del país d'origen, l'evidència de la seva persecució [5]: cada document, cada amenaça, cada foto, amb empremta i data certa. Pel camí, pot ancorar els moments crítics — on era, quan — sense publicar res ni revelar-se. Si li prenen el telèfon [7], la prova no mor amb ell: només l'empremta és a la cadena — mai el contingut —, i espera la còpia recuperable per acreditar-ne la integritat i l'antiguitat. A l'entrevista d'asil, el seu relat porta una cronologia verificable que cap instructor no pot despatxar com a «fabricada per a l'ocasió».

2. L'observador a la frontera

Les organitzacions que documenten incidents fronterers — la feina que el Black Book compila a posteriori [6] — poden segellar cada testimoni i cada evidència en el moment de recollir-los [5]: la data certa del testimoni pres l'endemà dels fets val processalment molt més que el mateix testimoni publicat dos anys després en un informe. És el model del capítol 20 — l'evidència de drets humans amb cadena de custòdia — aplicat a la frontera europea: primer l'empremta, la publicació quan sigui segur, i un arxiu que els tribunals — que ja demanen a Frontex la seva documentació [7] — puguin contrastar amb la versió oficial.

3. La nit del naufragi, ancorada

Un rescat marítim amb prova d'existència: les posicions, les comunicacions i les imatges de totes les embarcacions — patrulleres, mercants, vaixells d'ONG — segellades en temps real [5], en la línia de la integritat marítima del capítol 103. Quan arribi la disputa — hi va haver remolc? quan es va avisar? qui era on? —, la cronologia existirà des del primer minut: ni la instrucció necessitarà dos anys [3], ni la veritat dependrà que 104 supervivents puguin testificar contra un informe [1][4]. Qui va actuar bé tindrà la millor defensa possible; qui no, cap escapatòria narrativa.

4. La simetria que protegeix tothom

Cal dir-ho amb tota la claredat: l'ancoratge també empara les autoritats. La patrulla acusada falsament d'una violència que no va exercir, l'agent que va seguir el protocol, l'operació de rescat impecable — tots tenen en els seus propis registres ancorats la defensa definitiva [5]. I les institucions hi guanyen el que més escasseja a les fronteres: credibilitat. Una guàrdia costanera amb bitàcoles segellades no necessita que la creguin — pot demostrar-ho.

Els límits, amb la mateixa serietat: el segell no decideix qui té dret a asil ni quina política migratòria és justa — això correspon a les lleis i als tribunals; no fa cert el contingut d'un document, només la seva existència i data; no substitueix el testimoni humà ni la valoració de credibilitat; i a la frontera, la seguretat de les persones passa per davant de la documentació — ningú no ha de segellar res que posi en perill qui fuig.

La promesa i el perill

La promesa: fronteres on els fets tenen cronologia des del primer minut [3][4], víctimes que no depenen de la memòria ni del telèfon que els van prendre [7], observadors amb arxius inatacables [6] i autoritats que poden demostrar la seva diligència en lloc de només afirmar-la. El TJUE ha obert la porta jurídica [7]; la infraestructura de prova és el que pot travessar-la.

Els perills, amb la màxima serietat.

El primer és **la vigilància dels vulnerables**. Cap eina d'evidència no pot esdevenir un registre de persones en moviment. El rastre segellat és de la persona: al seu dispositiu, només empremtes a la cadena, revelació voluntària davant de qui ella triï [5]. Qualsevol deriva cap a bases de dades biomètriques de migrants seria la perversió exacta del que aquest capítol proposa — el llibre ja ho ha advertit als capítols 47 i 49.

El segon és **el segell com a frontera nova**. Si l'asil acabés exigint «cronologia ancorada o no et crec», hauríem aixecat un mur probatori contra els més desposseïts — qui fuig d'un bombardeig no segella res. La prova d'existència suma credibilitat a qui la té; la seva absència no pot restar-ne mai. Això ha de quedar escrit a les normes.

El tercer és **el perill físic de la prova**. Documentar pot matar. Un telèfon amb evidència segellada és un risc en un control hostil; els protocols han de prioritzar la seguretat — segellar i esborrar el contingut local, recuperar-lo després des d'un lloc segur — i cap organització no ha de demanar a ningú que es converteixi en màrtir probatori [5][6].

I el quart és **la coartada tecnològica**. Cap empremta no rescata ningú del mar. Les obligacions de rescat, les vies legals i la política migratòria són decisions humanes i polítiques [1][2][7]; el segell només garanteix que, després, la veritat sigui recuperable. Que ningú no vengui criptografia on calen salvavides.

És hora d'actuar

A la frontera, la veritat no pot dependre de qui escriu l'informe.

Per a les persones que temen haver de fugir: segella el teu rastre — documents, amenaces, fets — des d'ara, al teu dispositiu [5]; si un dia et prenen el telèfon [7], la teva prova t'esperarà.

Per a les ONG i els observadors de fronteres: segelleu testimonis i evidències en el moment de recollir-los [5][6]; la data certa multiplica el pes processal de cada pàgina dels vostres informes.

Per a les operacions de rescat i les guàrdies costaneres: ancoreu bitàcoles, posicions i comunicacions [5] — la vostra millor defensa és una cronologia que no es pugui discutir (capítol 103).

Per a Frontex i les institucions europees: el TJUE ja us assenyala com a custodis de la documentació [7]; que aquesta documentació neixi ancorada i sigui exigible — la credibilitat de les fronteres europees en depèn.

Per als jutges i les oficines d'asil: valoreu la cronologia segellada com a suport de credibilitat [7], i no convertiu mai la seva absència en presumpció en contra.

Per als legisladors: escriviu la regla d'or — l'evidència ancorada suma, la seva absència no resta — i garantiu que cap sistema d'evidència no esdevingui registre de vigilància dels qui fugen [5].

Més de 600 persones van morir davant de Pylos, i va caldre esperar gairebé dos anys perquè la instrucció apuntés cap als qui tenien el deure de rescatar-les [1][3]. Que la pròxima nit fosca al mar tingui, des del primer minut, una cronologia que ningú no pugui reescriure. Pels qui només porten la veritat a sobre, **time2act**.

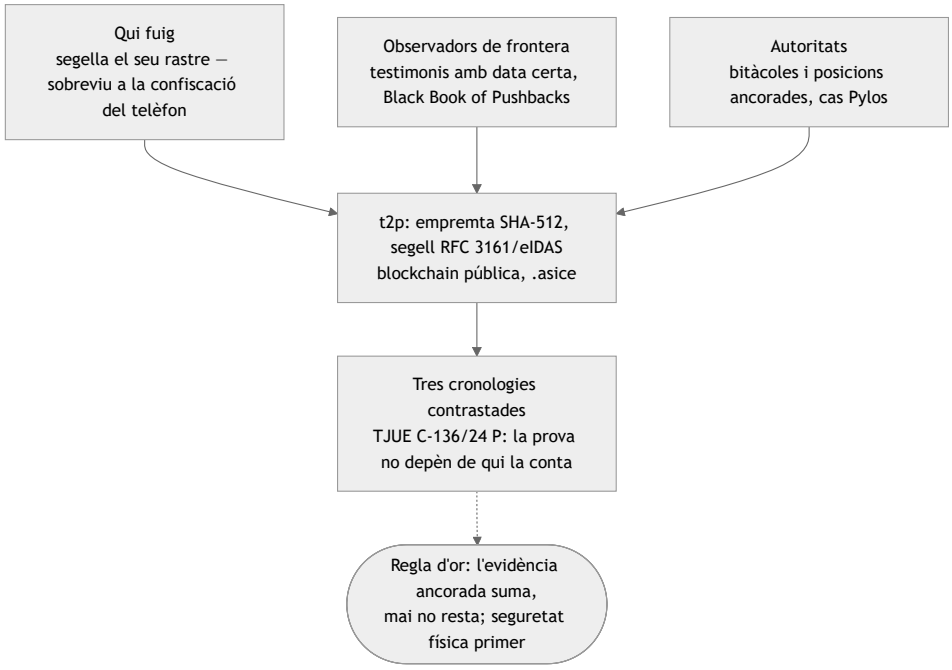


Figura 51.1 — Tres cronologies ancorades que es contrasten (empremta SHA-512 al dispositiu, segell de temps RFC 3161/eIDAS, blockchain pública, .asice): el rastre segellat de qui fuig (sobreviu a la confiscació del telèfon; TJUE C-136/24 P), la documentació dels observadors (testimonis amb data certa; Black Book of Pushbacks) i els registres ancorats de les autoritats (bitàcoles i posicions; el cas Pylos). La regla d'or: l'evidència ancorada suma credibilitat; la seva absència mai no resta. Límits: cap registre de persones, seguretat física primer, i el segell no decideix l'asil ni la política migratòria. Fonts: HRW/Amnistia (Pylos); RSA (imputació de 17 guardacostes); BVMN; TJUE C-136/24 P.

---

[1] Wikipedia — *2023 Pylos migrant boat disaster* (l'Adriana; sortida de Líbia; ≈750 persones a bord; més de 600 morts; 104 supervivents; 82 cossos; versió de la guàrdia costanera); Human Rights Watch — *Greece: Disparities in Accounts of Pylos Shipwreck Underscore the Need for Human Rights Compliant Inquiry* (errors de les autoritats; al·legacions sobre el remolc). 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] Amnistia Internacional — *Greece: Trial of Pylos shipwreck survivors must not be a shield in the investigation of the alleged responsibilities of the Greek authorities* (maig de 2024; nou supervivents processats; crítica de les organitzacions de drets humans). 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 maig de 2025; capità de la ΠΠΛΣ-920 acusat de causar naufragi amb resultat de mort d'almenys 82 persones; querella en

nom de 40 supervivents). 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* (reconstrucció periodística amb dades de trànsit marítim, testimonis de supervivents i material dels seus telèfons). https://gijn.org/stories/investigating-pylos-shipwreck/ ↩

[5] t2p — manual de producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; només empremtes a la cadena; publicació opcional; recuperació de còpies verificables contra l'empremta). Vegeu els capítols 13 i 15; l'evidència de drets humans, al capítol 20; la posició dels vaixells, al capítol 103. ↩

[6] Wikipedia — *Border Violence Monitoring Network* (coalició de més de 12 organitzacions, fundada el 2017); Statewatch — *The 'Black Book of Pushbacks': testimonies of pushbacks affecting over 12,000 people* (desembre de 2020; 12.654 persones); Balkan Insight — *Study Reports 25,000 Violent Pushbacks at EU Borders* (edició ampliada de 2022: més de 3.000 pàgines, 4 volums). 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* (assumpte C-136/24 P, sentència de 18 de desembre de 2025; nacional sirià despullat del telèfon i retornat a Turquia amb Frontex present; adaptació de la càrrega de la prova; Frontex com a posseïdora de la documentació). https://www.iberley.es/noticias/el-tjue-refuerza-tutela-judicial-efectiva-casos-devoluciones-sumarias-migrantes-35841 ↩

Testaments i herència: l'última voluntat, demostrable

«No moriré del tot.»

— Horaci, Odes, III, 30 (23 aC)

Maureen Renny, una antiga directora d'escola anglesa, va morir el gener de 2020 als vuitanta-dos anys. Poc després va aparèixer un testament que ho deixava tot a Leigh Voysey, una coneguda seva, i que desplaçava un testament anterior de 2016 a favor dels seus familiars. El document estava «atestat» per dues amigues de Voysey. Era fals. Voysey havia falsificat l'última voluntat de Renny per reclamar una herència de **4,2 milions de lliures**, i amb prou feines li van caldre dues testimonis còmplices per fabricar-lo. La justícia britànica la va condemnar el 2024 per frau i falsificació, i va empresonar també les seves dues còmplices; la condemna penal va permetre als hereus legítims recuperar el patrimoni [1].

El cas conté la dificultat singular d'aquest capítol, que cap altre comparteix: **quan un testament es disputa als tribunals, l'única persona que podria aclarir-ho —qui el va atorgar— ja és morta**. La seva veu s'ha apagat per sempre, i el document ha de parlar per ell. Aquest capítol tracta de com fer que aquella veu, en l'instant en què s'expressa, quedi gravada de manera que ningú la pugui falsificar ni silenciar.

La voluntat que ningú no pot defensar

El que hi ha en joc és immens. La consultora Cerulli Associates ha calculat que als Estats Units es transferiran **84,4 bilions de dòlars** a hereus i causes benèfiques d'aquí al 2045, en l'anomenada «gran transferència de riquesa» —la més gran de la història [2]. I tanmateix, la base sobre la qual descansa aquesta transferència és sorprenentment fràgil. Segons l'estudi anual de Caring.com, només el **24 % dels adults nord-americans** tenia testament el 2025, una xifra que ha baixat des del 33 % de tres anys abans [3]. Quan no hi ha testament, decideix la llei; i quan n'hi ha, comença el problema de provar que aquell és el bo.

Com hem vist, al Regne Unit les sol·licituds de bloqueig d'una herència —els *caveats*— van passar de 7.268 el 2019 a 11.362 el 2024, un augment del 56 % en cinc anys [4]. Els tres motius clàssics per anul·lar un testament són sempre els mateixos: la falta de **capacitat testamentària** (el testador no estava lúcid), la **influència indeguda** (algú el va pressionar) i la **falsificació** —exactament el que va fer Voysey [5]. Els testimonis hològrafs, escrits a mà, són els més vulnerables, perquè sovint no porten data ni testimonis que puguin declarar sobre l'estat del testador en el moment de redactar-los.

El forat de l'herència digital

A aquest problema antic, l'era digital n'hi afegeix un de nou. Al desembre del 2018, **Gerald Cotten**, fundador de la major casa de canvi de criptomonedes del Canadà, QuadrigaCX, va morir als trenta anys durant un viatge a l'Índia. Només ell coneixia les contrasenyes de les carteres fredes de l'empresa. Uns **137 milions de dòlars** van quedar bloquejats per sempre, afectant més de cent mil clients; la seva vídua va declarar sota jurament que no havia pogut trobar les claus escrites enlloc [6]. No és un cas aïllat: l'anàlisi de Chainalysis estimava el 2020 que prop d'un **20 % dels bitcoins** estan perduts i són irrecuperables, sovint perquè el titular mor sense compartir l'accés [7]. Com adverteix la secció de dret successori de l'**American Bar Association**, la persona mitjana té més de cent comptes en línia però menys d'una de cada quatre té un pla per a després de morir; sense les claus privades, la criptomoneda queda «permanentment bloquejada, sense cap servei d'atenció al client a qui trucar» [8]. El patrimoni digital, literalment, s'enterra viu.

Estònia ho va veure primer

Hi ha un país que va entendre tot això abans que ningú. El 2012, quan la resta del món encara veia la cadena de blocs com una cosa de bitcoin, Estònia va posar en producció el primer servei estatal del planeta ancorat en blockchain. No va ser un banc ni una borsa: va ser el **Registre de Successions**, el registre de testaments del seu Ministeri de Justícia [9]. Amb la tecnologia KSI de l'empresa Guardtime,

desenvolupada arran dels ciberatacs de 2007, el sistema segella cada testament ancorant-ne només l'empremta —el document mai no surt del servidor de l'Estat— de manera que qualsevol alteració posterior queda detectada matemàticament. Un petit país bàltic va decidir que el document que més mereix protecció contra la manipulació és l'última voluntat dels seus ciutadans. Tenia raó.

La prova d'existència: l'última voluntat demostrable

És aquí on **t2p** porta aquella intuïció a l'abast de qualsevol persona, i ho fa amb una peça que en aquest capítol brilla com en cap altre: la **prova de vida**. En el moment de signar o de gravar la voluntat, es calcula al dispositiu l'**empremta SHA-512** del document testamentari, s'ancora a la **blockchain pública** i s'hi afegeixen un **segell de temps RFC 3161** conforme a eIDAS, un **GPS forense** i el contenidor **.asice verificable fora de línia**. Però la clau de volta és la **gravació de vida** —un vídeo-selfie amb reptes—, que demostra tres coses decisives: que el testador *estava viu*, que *estava present* i que *és qui diu ser*, en l'instant exacte d'atorgar.

Pensem què significa això contra les dues amenaces més comunes. Contra la **influència indeguda**: es veu i se sent el testador declarar la seva voluntat lliurement, sense un tercer dirigint-lo fora de càmera de manera evident. Contra la **falsificació**: el signant real queda lligat biomètricament al document, de manera que ja no n'hi ha prou amb copiar una firma i aportar dues testimonis còmplices, com en el cas Voysey. I el **segell de temps** resol l'eterna disputa de «existeix un testament posterior»: la cadena d'empremtes datades estableix un ordre incontrovertible de versions, revocacions i codicils. Fins i tot el forat de l'herència digital té solució: el mateix contenidor pot segellar —xifrades— les instruccions d'accés als actius digitals, evitant un nou QuadrigaCX sense exposar les claus.

Cal dir el límit amb tota la honestedat, perquè aquí és subtil. El segell **no substitueix** les formalitats legals —testimonis, intervenció notarial, homologació successòria— ni la validesa segons cada jurisdicció: un testament segellat però sense les solemnitats exigides pot continuar sent nul. I, sobretot, la **capacitat testamentària és un judici legal i mèdic** que el vídeo de vida *recolza* —mostra lucidesa aparent, absència de coacció visible— però **no determina**: algú pot semblar perfectament lúcid davant la càmera i mancar, tanmateix, de capacitat jurídica. «Escombraries a l'entrada, escombraries a la cadena»: la prova demostra integritat, moment, lloc i persona, no la veritat de fons de les disposicions ni que ningú no exercís pressió fora de pla.

La promesa i el perill

La promesa és serena i poderosa. Donar a cada persona una manera de deixar la seva última voluntat de forma que es pugui demostrar —que era ella, viva i present, i que aquella és la versió definitiva— estalviaria anys de litigi a famílies en dol, protegiria els 84 bilions de dòlars que canviaran de mans i tancaria el forat de l'herència digital. És fer que la veu apagada del testador continue parlant amb autoritat.

El perill demana matís. El primer, ja dit: el segell no atorga validesa legal per si sol ni decideix la capacitat; confondre-ho seria perillós. El segon, la privacitat d'un document íntim per definició, que ha de quedar en mans del titular fins que arribi el moment. I el tercer, no convertir la tecnologia en una barrera per a qui no hi té accés: la manera més senzilla de fer testament —anar al notari— ha de seguir oberta a tothom. La prova d'existència és un reforç de l'última voluntat, no un substitut del dret successori ni del notari.

És hora d'actuar

Per a les persones: deixar testament —la majoria encara no ho fa— i, quan el facin, segellar-lo amb prova de vida i data certa. Per als notaris i advocats: incorporar la gravació de vida com a reforç contra la influència indeguda i la falsificació, les disputes més comunes. Per als registres successoris: seguir l'exemple d'Estònia i garantir la integritat de cada testament. Per als legisladors: tancar el buit legal de l'herència digital, perquè cap patrimoni torni a quedar enterrat amb una contrasenya. I per a tothom: recordar que l'última voluntat és l'únic document que el seu autor mai no podrà defensar en persona.

Una falsificadora va estar a punt de reescriure el destí d'aquell 4,2 milions de lliures amb dues testimonis còmplices. Donar a cada testador una prova que parli per ell quan ja no hi sigui —vivent, present i inconfusible— és, en aquest front profundament humà, time2act.

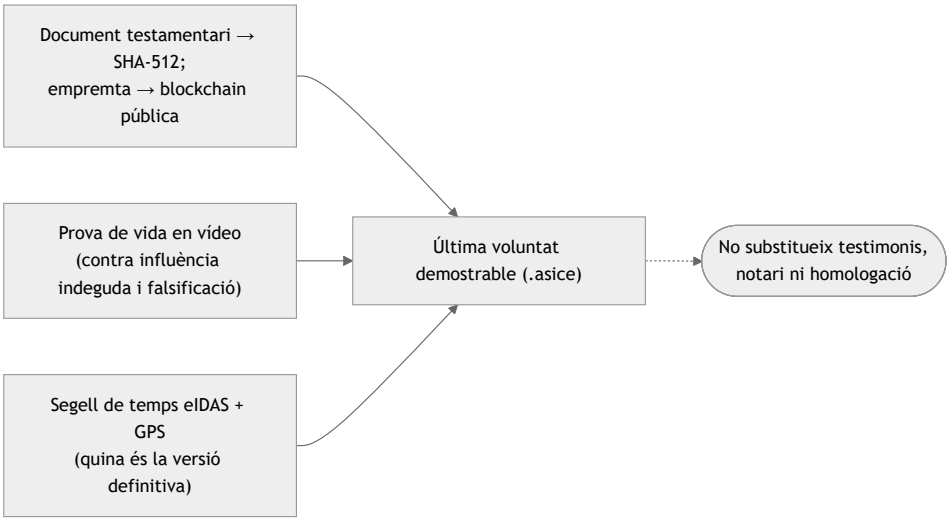


Figura 52.1 — Tres entrades convergeixen en un testament incontestable: el document, l'empremta SHA-512 del qual s'ancora a la blockchain pública (integritat); la prova de vida en vídeo, que lliga identitat, presència i voluntat (contra la influència indeguda i la falsificació); i el segell de temps eIDAS amb GPS, que fixa quina és la versió definitiva (contra «existeix un testament posterior»). El resultat és un .asice verificable fora de línia. Límit: no substitueix testimonis, notari ni homologació, i la capacitat la decideix el jutge o el metge. Fonts: Cerulli Associates; e-Estonia/Guardtime; cas Voysey.

---

[1] Hertfordshire Constabulary — *Three jailed for £4m inheritance fraud* (cas Leigh Voysey i el testament 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 transferència de riquesa»). 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* (només el 24 % dels adults té testament). https://www.caring.com/resources/wills-survey ↩

[4] Dutton Gregory / Probate Registry — *Inheritance dispute statistics* (11.362 caveats el 2024, +56 % en cinc anys). https://www.duttongregory.co.uk/site/blog/personalnews/inheritance-dispute-statistics ↩

[5] Justia — *Will contests: testamentary capacity, undue influence, forgery* (motius de nul·litat). https://www.justia.com/estate-planning/wills/will-contests/ ↩

[6] CBS News — *QuadrigaCX CEO took password to his grave* (Gerald Cotten; ~137 M$ bloquejats). https://www.cbsnews.com/news/gerald-cotten-quadrigacx-ceo-took-password-to-his-grave-leaving-company-unable-to-access-137-million/ ↩

[7] Chainalysis (via Decrypt) — *~3,7 milions de bitcoins perduts per sempre* (2020; ~20 % de l'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 es perd sense les claus). https://www.americanbar.org/groups/real_property_trust_estate/resources/estate-planning/digital-property/ ↩

[9] Comissió Europea (Interoperable Europe) / e-Estonia — *Estonia's KSI blockchain: the Succession Registry* (primer servei estatal sobre blockchain, 2012). https://e-estonia.com/blockchain-security-control-for-government-registers/ ↩

[10] eSignGlobal — *Electronic wills legislation and remote notarization* (eIDAS QES; els testaments sovint exclosos de la notarització electrònica). https://www.esignglobal.com/blog/electronic-wills-legislation-remote-notary

Dret de família: la coparentalitat amb data certa

«Els vostres fills no són els vostres fills. […] Venen a través vostre, però no de vosaltres.»

— Khalil Gibran, El Profeta (1923)

Un divendres a la tarda, a la porta d'una escola qualsevol. Dos adults que un dia es van estimar es passen una motxilla i un nen, amb la cordialitat justa. Fins aquí, la rutina de milers de famílies. La tensió és al que no es veu: si el lliurament era a les cinc o a dos quarts de sis; si l'abric que falta el tenia l'un o l'altra; si la factura del dentista s'havia comunicat; si el canvi de cap de setmana es va acordar o es va imposar. Cada detall minúscul pot acabar, mesos després, en un jutjat de família convertit en «la teva paraula contra la meva» — amb un menor al mig.

I cada cop són més famílies en aquesta coreografia. A Espanya, el 2024 hi va haver 82.991 divorcis — un 8,2 % més que l'any anterior — i la custòdia compartida es va atorgar en el 49,7 % dels casos amb fills, superant per primera vegada la custòdia materna; el 2010 era només el 12,6 % [1]. La custòdia compartida és la nova normalitat, i és una bona notícia — però multiplica la coordinació quotidiana entre persones que sovint ja no es fan confiança: dos calendaris, dues llars, un pla de parentalitat [3] i centenars de microacords l'any.

Aquest capítol tracta l'evidència de la coparentalitat. L'herència i l'última voluntat són al capítol 52; la cadena de custòdia judicial, al capítol 77; la gravació legal de converses pròpies, al capítol 75. Pregunta clau: com es documenta la vida compartida d'un menor entre dues llars sense convertir la família en un camp de vigilància mútua? Resposta: amb data certa neutral sobre els fets acordables — missatges, lliuraments, despeses, plans — mitjançant **t2p**: l'empremta SHA-512 al dispositiu, l'ancoratge de l'empremta a la blockchain pública i el segell de temps RFC 3161/eIDAS complementari, dins d'un contenidor .asice [4]. I sota un principi que mana sobre tots els altres: l'interès superior del menor. La prova no és per guanyar la guerra; és perquè no n'hi hagi.

La paraula contra la paraula, amb un menor al mig

La matèria primera dels conflictes postruptura és quotidiana i minúscula: horaris de lliurament, despeses extraordinàries, decisions escolars i mèdiques, canvis de plans. Quan la relació és serena, res d'això no importa; quan es deteriora, tot esdevé disputable — i el sistema judicial de família, sobrecarregat i lent, es troba resolent amb anys de retard discussions sobre qui va arribar tard un divendres de fa dos anys, amb proves fragmentàries: captures de pantalla, testimonis familiars i records carregats de biaix.

El cost de la prova fràgil el paguen tres parts alhora. Els progenitors, que acumulen captures i correus que mai no acaben de ser verificables. El jutjat, que ha de reconstruir la vida quotidiana d'una família des de fora, decidint quin fragment pesa més sense cap capa neutral que n'acrediti la integritat. I, sobretot, el menor: cada hora de litigi sobre fets discutibles és tensió que li arriba, i les decisions sobre la seva vida es prenen sobre versions en lloc de fets.

I el matís que aquest llibre no pot esquivar, dit amb tot l'equilibri: en els conflictes greus — els incompliments reiterats, les acusacions creuades — la falta d'evidència neutral perjudica tothom alhora. El progenitor que compleix i no ho pot demostrar; el que és acusat injustament i no es pot defensar; i el menor, la realitat del qual queda enterrada sota les versions. La resposta no és més sospita: és un registre objectiu dels fets que totes dues parts han acceptat documentar. Ni més, ni menys.

El que els tribunals ja demanen

El món judicial ja ha fet mig camí. OurFamilyWizard — l'aplicació de coparentalitat de referència — és usada i recomanada per tribunals i professionals del dret de família als 50 estats dels Estats Units i al Canadà, el Regne Unit, Austràlia i Nova Zelanda; la seva proposta és exactament la d'un registre: missatgeria amb marca de temps a cada missatge i sense possibilitat d'esborrar res, confirmacions de lectura, calendaris de custòdia amb historial de canvis, registre de despeses i informes descarregables per a judicis i mediacions — fins i tot un mesurador de to que assenyala el llenguatge encès abans d'enviar [2]. A Espanya, la peça equivalent en l'àmbit de l'acord és el pla de parentalitat: el document que fixa el marc comú de criança més enllà del conveni regulador [3].

La lliçó és clara: els jutjats ja no volen batalles de records — volen registres. Però les eines actuals tenen una dependència estructural: l'evidència viu als servidors del proveïdor, subjecta a les seves polítiques, a la seva jurisdicció i a la seva continuïtat com a única garantia. Si l'empresa canvia les condicions o desapareix, el registre pot perdre's sense que cap tribunal disposi d'una còpia verificable independent — el capítol 75 ja va mostrar què passa quan la prova depèn d'un contractista.

La capa que falta és la neutralitat criptogràfica: que cada missatge, cada acta de lliurament i cada versió del pla porti la seva empremta SHA-512 amb segell de temps, ancorada a la blockchain pública [4] — verificable per qualsevol jutjat sense dependre de cap empresa, ni de cap de les dues parts. La confiança deixa de ser una esperança per esdevenir un fet documentat, i la justícia pot dedicar-se a resoldre conflictes reals en lloc de qüestionar registres.

La prova d'existència aplicada

La mateixa porta d'escola, un divendres qualsevol; els mateixos dos adults; i una diferència invisible: els fets del dia queden fixats, i cap dels dos no haurà de recordar-los mai més.

1. La comunicació coparental amb data certa

Els missatges entre progenitors — els acords, els avisos, els canvis de plans — se segellen en enviar-se: empremta SHA-512, data certa, ancoratge [4]. És el que les aplicacions judicials ja ofereixen [2], amb la capa neutral afegida: la integritat no depèn del proveïdor, i el registre és verificable per qualsevol jutjat encara que l'empresa desaparegui. L'acord de canviar el cap de setmana existeix amb hora; l'avís de la despesa mèdica, també; i la conversa que mai no va existir no es pot inventar a posteriori.

2. El lliurament acreditat

El moment més delicat de la setmana — el lliurament i la recollida — pot quedar acreditat amb un gest de deu segons acordat per totes dues parts: la confirmació segellada des dels dos dispositius (som aquí, és aquesta hora) [4]. Cap càmera, cap gravació de l'altre, cap menor fotografiat: només el fet i l'hora, signats per tots dos. El retard reiterat queda datat; la puntualitat sistemàtica, també; i la discussió de fa dos anys sobre un divendres concret desapareix de l'expedient perquè la resposta ja hi és.

3. La despesa compartida sense guerra

Les despeses extraordinàries — el dentista, les ulleres, el campament — són el focus clàssic: es va comunicar? es va acceptar? es va pagar? Amb justificants segellats i avisos amb data certa [4], el circuit sencer queda acreditat: la factura existeix, es va comunicar tal dia, es va respondre — o no — tal altre. El progenitor que paga i comunica queda protegit; el que respon a temps, també. I el silenci no és un buit: és un registre datat que parla sol, amb la mateixa neutralitat per a tothom.

4. El pla de parentalitat versionat

El pla de parentalitat [3] és un document viu: es modifica quan els fills creixen, quan canvien les feines, quan la vida mana. Cada versió segellada amb data certa [4] fa indiscutible què estava vigent quan: l'acord de l'estiu passat, la modificació pactada al setembre, la proposta que l'altra part mai no va acceptar. Els acords evolucionen; la seva història, no. I quan calgui mediació o jutjat, la discussió començarà des dels textos datats, no des de les memòries enfrontades.

Els límits, dits amb cura: el segell acredita fets — hores, textos, justificants —, no la qualitat de la criança ni l'amor de ningú; no decideix custòdies — això ho fan els jutges, amb molts més elements —; no ha de convertir la família en un expedient permanent — es documenta l'objectivable i acordat, mai la intimitat de cap llar ni la vida del menor —; i en situacions de violència, la prioritat és la protecció immediata pels canals especialitzats, no cap aplicació.

La promesa i el perill

La promesa: famílies separades que discuteixen menys perquè els fets no es discuteixen [2][4]; jutjats de família que resolen sobre registres i no sobre versions; i menors que creixen amb menys guerra al voltant — la logística en pau, perquè l'energia dels adults vagi on toca.

Els perills, tractats amb la màxima cura.

El primer és **la família sota vigilància**. Documentar els fets acordats no pot degenerar en vigilar l'altre progenitor — ni gravar-lo, ni fotografiar-ne la llar, ni convertir el menor en informador o en portador de dispositius de control. La línia és nítida: se segella el que totes dues parts han acordat documentar — missatges, lliuraments, despeses, plans — i res més. El menor no és mai objecte de registre; és la raó per la qual els adults es documenten a si mateixos.

El segon és **l'arsenal processal**. Si el registre es fa per acumular munició, la tecnologia haurà empitjorat el que volia curar. El disseny bilateral — les dues parts segellen, les dues parts veuen — i la simetria radical de la prova (protegeix el que compleix, sigui qui sigui) desincentiven l'ús bèl·lic: contra un registre neutral, la millor estratègia és complir.

El tercer és **la desigualtat d'armes**. Si només una part domina l'eina, la data certa esdevé avantatge processal. Com al lloguer i al treball de plataforma, la resposta és el disseny: gratuïtat o cost negligible, simplicitat, i el jutjat valorant el registre bilateral per sobre de l'unilateral.

I el quart és **el tecnosolucionisme afectiu**. Cap segell no cura una ruptura mal digerida ni substitueix la mediació, la teràpia o el temps. La prova d'existència pacifica la capa dels fets; la capa de les emocions és feina d'humans. Confondre-les seria vendre criptografia on calen acords — i, sovint, una mica de generositat.

És hora d'actuar

Que els fets quedin en pau perquè les persones puguin estar-hi.

Per als progenitors separats: acordeu al pla de parentalitat [3] què documentareu — missatges, lliuraments, despeses — i segelleu-ho bilateralment [4]; que la logística tingui data certa perquè la relació no hagi de tenir memòria de greuges.

Per a advocats de família i mediadors: proposeu el registre segellat bilateral com a clàusula estàndard del conveni [2][3]; cada fet indiscutible és una batalla que no es lliura.

Per als jutjats de família: valoreu els registres ancorats bilaterals per sobre de les captures i els testimonis creuats [2][4]; i recordeu a les parts que el registre és escut, no arma.

Per a les aplicacions de coparentalitat: incorporeu l'ancoratge neutral [2][4] — que la vostra evidència no depengui de la vostra continuïtat com a empresa.

Per als legisladors: reconeixeu valor probatori qualificat al registre coparental segellat bilateral, i garantiu que cap eina no esdevingui obligatòria ni vehicle de vigilància dins de la família [4].

A la porta de l'escola, el divendres que ve, hi haurà els mateixos dos adults i el mateix nen amb la seva motxilla. Que tot el que és discutible quedi fixat en deu segons — i que tota l'energia que abans es cremava en discussions vagi allà on toca: a la criatura que se'ls mira. Per les famílies que continuen, **time2act**.

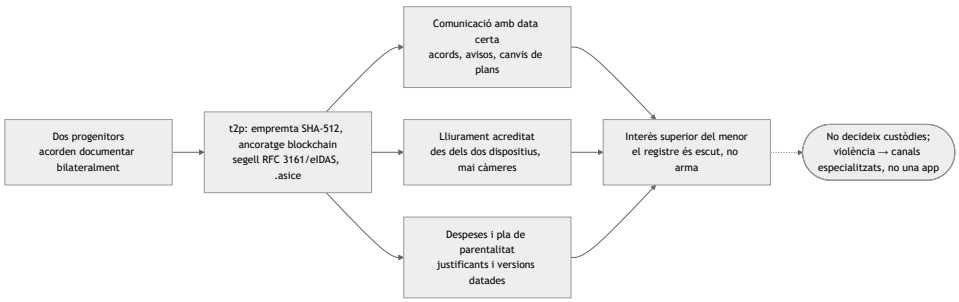


Figura 53.1 — La logística coparental amb prova d'existència (empremta SHA-512 al dispositiu, segell de temps RFC 3161/eIDAS, blockchain pública, .asice), sempre bilateral i acordada: la comunicació amb data certa, el lliurament acreditat des dels dos dispositius (mai càmeres ni menors fotografiats), les despeses amb justificants ancorats i el pla de parentalitat versionat. El nord: l'interès superior del menor; el registre és escut, no arma. Límits: no decideix custòdies, no mesura la criança, i en situacions de violència la prioritat són els canals especialitzats. Fonts: INE (custòdia compartida 49,7 %, 2024); OurFamilyWizard (tribunals de 50 estats); pla de parentalitat.

[1] INE / Gracia Carrión (anàlisi) — *Custodia compartida supera a la materna en España (INE 2024)* (49,7 % dels divorcis amb fills, +1,3 punts; primera vegada per sobre de la custòdia materna; 12,6 % el 2010); APFS — *Separaciones y divorcios en España 2024* (82.991 divorcis, +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* (aplicació de coparentalitat de referència per a tribunals i professionals als 50 estats dels EUA, Canadà, Regne Unit, Austràlia i Nova Zelanda; missatges amb marca de temps i sense esborrat; confirmacions de lectura; calendaris amb historial; informes per a judicis; 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 pla de parentalitat com a marc comú de criança més enllà del conveni regulador). https://www.elespanol.com/mujer/relaciones/20251214/abogada-solicitar-custodia-compartida-despues-anos-necesitas-plan-parentalidad/1003744039064_0.html ↩

[4] t2p — manual de producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; registre bilateral; contingut als dispositius, només empremtes a la cadena; revelació davant del jutjat). Vegeu els capítols 13 i 15; la gravació legal de converses pròpies, al capítol 75. ↩

Trade finance: el mateix carregament finançat dues vegades

«El fonament de la justícia és la bona fe, és a dir, la constància i la veritat en allò dit i convingut.»

— Ciceró, De Officiis, I, 23 (44 aC)

El juny del 2014, al port xinès de Qingdao, uns inspectors de banc van intentar entrar als magatzems per verificar una cosa que hauria de ser elemental: que el metall que figurava a les factures hi era de debò. No els van deixar passar. L'empresa Citic Resources va denunciar que no aconseguia localitzar més de cent mil tones d'alúmina que haurien d'estar allà [4]. Aviat es va descobrir per què: el mateix coure i el mateix alumini havien estat pignorats, mitjançant **rebuts de magatzem duplicats**, a desenes de bancs xinesos i internacionals alhora. L'empresari darrere de l'engany, Chen Jihong, va aixecar uns 12.300 milions de iuans —prop de 1.800 milions de dòlars— amb documents falsos, i va acabar condemnat a vint-i-tres anys de presó [4]. L'exposició dels bancs va superar els 3.000 milions de dòlars.

Aquell escàndol té un nom propi en el sector —«metall fantasma»— i conté la doble lliçó d'aquest capítol. La primera: el frau més car del comerç internacional no és falsificar la mercaderia, sinó **finançar el mateix carregament moltes vegades** amb documents que ningú no pot creuar. La segona, més incòmoda, la deixarem per al final: a Qingdao, el problema no era que els documents fossin falsos —alguns eren ben reals—, sinó que el coure no hi era.

El comerç que viu del paper

Per entendre la vulnerabilitat cal comprendre l'escala. Entre el 80 i el 90 % del comerç mundial depèn d'instruments de finançament —cartes de crèdit, coneixements d'embarcament, rebuts de magatzem—, i la immensa majoria continua essent **de paper** [10]. La Cambra de Comerç Internacional (**ICC**), que redacta les regles que governen les cartes de crèdit, calcula que cada dia circulen uns **4.000 milions de documents** pel sistema comercial global [10]. Tanmateix, la digitalització avança a pas de tortuga: malgrat que el coneixement d'embarcament electrònic existeix des de fa anys, només havia penetrat en un **5,7 %** dels transportistes marítims a principis del 2025 [3].

Aquesta dependència del paper té un cost brutal, i el paguen sobretot els més febles. El **Banc Asiàtic de Desenvolupament** (ADB), que pren el pols mundial al sector amb la seva enquesta de referència, va calcular que la **bretxa de finançament del comerç** —la diferència entre el que les empreses demanen i el que els bancs aproven— va arribar a un rècord de **2,5 bilions de dòlars el 2022**, des d'1,7 bilions dos anys abans [1]. Les petites i mitjanes empreses, que són menys d'una quarta part de la demanda, concentren el 40 % dels rebuigs. Com resumeix l'ADB, el finançament no falta per manca de béns, sinó per manca de **confiança verificable** en els documents i en la contrapart. McKinsey ha estimat que només digitalitzar el coneixement d'embarcament estalviaria 6.500 milions de dòlars i habilitaria desenes de milers de milions de comerç nou [2].

El mateix carregament, finançat dues vegades

Qingdao no va ser un cas aïllat; va ser el patró. El 2020, a Singapur, el gegant del comerç de cru Hin Leong es va esfondrar amb **3.850 milions de dòlars** de deute davant de vint-i-tres bancs. Els administradors judicials van destapar una falsificació de documents «a escala massiva»: vendes inventades a altres empreses per treure gairebé **112 milions de dòlars** a HSBC per barrils de petroli que mai no van canviar de mans, i va generar una empremta profunda en el sector. El seu fundador, Lim Oon Kuin —«OK Lim»—, de vuitanta-dos anys, va ser condemnat el novembre del 2024 a disset anys i mig de presó; la pena es va reduir a tretze anys i mig en apel·lació el març del 2026 [5]. I el 2021, l'imperi de finançament de **Greensill Capital** va caure en insolvència, arrossegant Credit Suisse, els clients del qual tenien uns **10.000 milions de dòlars** en fons recolzats per factures —algunes de les quals, segons el regulador suís **FINMA**, es basaven en operacions que encara no havien passat o eren presumptament fictícies [6]. Com va concloure la FINMA, l'opacitat documental, no l'instrument, va ser allò letal.

En tots els casos, el mecanisme és el mateix: un document —un rebut, una factura, un coneixement d'embarcament— que ningú no pot contrastar contra els altres financers, i que per tant es pot presentar a deu bancs alhora o fabricar després per tapar un forat.

La prova d'existència contra la doble financiació

És aquí on **t2p** ataca el cor del problema. En el moment d'emetre-s, el coneixement d'embarcament, la factura comercial, el rebut de magatzem o la carta de crèdit reben una **empremta SHA-512** calculada al dispositiu, s'ancreuen a la **blockchain pública**, i hi afegeixen un **segell de temps RFC 3161** conforme a eIDAS i un **GPS forense** de la ubicació del port o el magatzem, tot en un contenidor **.asice verificable fora de línia**.

El cop a la doble financiació és directe: abans de prestar, el banc B pot comprovar si l'empremta d'aquell coneixement d'embarcament **ja havia estat segellada i pignorada** pel banc A. Si el document ja està «gastat», la segona financiació es bloqueja —exactament el que hauria aturat els rebuts duplicats de Qingdao. El segell de temps, a més, impedeix la **retrodatació**, evitant que ningú pugui fabricar després un document «anterior» a una pèrdua, com va fer Hin Leong. D'aquesta manera es distingeix una factura real emesa en un moment d'una de «predita» o inventada posteriorment, el problema de Greensill. Tot plegat s'enforteix amb la **prova de vida** del comerciant en el moment de la firma.

Cal posar límit a la cruesa: la prova d'existència **no verifica que la mercaderia física existeixi**. A Qingdao, el document era real i podria haver estat perfectament segellat; el que no hi havia era el coure. «Escombraries a l'entrada, escombraries a la cadena»: la cadena demostra la integritat, el moment, el lloc i la persona del *registre*, no la veritat física del magatzem. Per això calen oracles físics —inspeccions, sensors, custodis independents— que **t2p** no substitueix. A més, perquè un document electrònic segellat tingui «possessió» i «singularitat» executables, cal reconeixement legal: la **Llei Model de les Nacions Unides sobre Registres Electrònics Transferibles** (MLETR) ho fa possible, però com hem vist, el 2025 només l'han adoptada tretze jurisdiccions, entre elles el Regne Unit [8]. I la lliçó dels consorcis fracassats —TradeLens, we.trade, Marco Polo, tots tancats entre 2022 i 2023— mostra que bloquejar la doble financiació exigeix que **tots** els financers consultin el mateix registre. Una prova oberta i verificable fora de línia redueix aquesta necessitat de coordinació, però no l'elimina.

La promesa i el perill

La promesa és quantificable: una capa de prova d'existència sobre els documents comercials dificultaria enormement finançar el mateix carregament dues vegades, retrodatar vendes fantasma o inventar factures futures, i ajudaria a tancar la bretxa de finançament que, com hem vist, afecta sobretot les petites empreses dels països emergents. En un sector on la confiança documental ho és tot, segellar la integritat i el moment de cada document restaura el fonament del comerç.

El perill demana el matís de sempre. Primer, el segell no fa aparèixer el metall al magatzem; confondre la integritat del document amb l'existència de la mercaderia és precisament l'error que va costar milers de milions a Qingdao. Segon, sense MLETR un document segellat no és executable. Tercer, la coordinació: la tecnologia no serveix de res si els bancs no la consulten en comú. La prova d'existència és una capa necessària dins d'una arquitectura que inclou, sempre, la inspecció física i el marc legal.

És hora d'actuar

Per als exportadors i comerciants: segellar els documents comercials a l'origen, de manera que la seva integritat i el moment siguin demostrables. Per als bancs i financers: comprovar l'empremta d'un document abans de prestar, per impedir que el mateix carregament es financi dues vegades. Per als reguladors: adoptar la MLETR, com ja han fet el Regne Unit i una dotzena de jurisdiccions, perquè el document electrònic segellat tingui plena força legal. I per als organismes del sector (ICC, bancs): aprendre dels consorcis fracassats i convergir en estàndards oberts, no en silos tancats.

A Qingdao, el mateix metall va finançar desenes de préstecs perquè ningú no podia creuar els documents. Assignar a cada coneixement d'embarcament una empremta única, segellada en el temps i comprovable per tothom —sense oblidar mai que cal anar al magatzem a comptar el coure— és, en aquest front del comerç global, time2act.

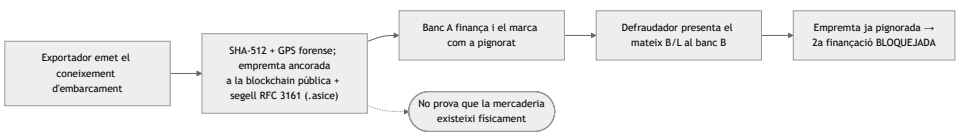


Figura 54.1 — L'exportador emet un coneixement d'embarcament que se segella amb empremta SHA-512, segell de temps RFC 3161/eIDAS i GPS, ancorat a la blockchain pública (.asice). El banc A el finança i el marca com a pignorat. Quan un defraudador presenta el «mateix» document al banc B, l'empremta coincideix i consta com ja pignorat: la segona financiació es bloqueja. Límit: el segell no prova que la mercaderia existeixi físicament al magatzem (el «metall fantasma» de Qingdao). Context: bretxa de finançament del comerç de 2,5 bilions de dòlars; coneixement d'embarcament electrònic real, només el 5,7 %. Fonts: Banc Asiàtic de Desenvolupament; ICC; cas Qingdao.

---

[1] Banc Asiàtic de Desenvolupament (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; estalvi de 6.500 M$ + comerç nou). 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* (penetració real del coneixement d'embarcament electrònic: 5,7 %, gener 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 anys; ~12.300 M iuans amb rebuts 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 anys, reduïts a 13,5 en apel·lació el març 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* (insolvència 2021; ~10.000 M$ en quatre fons; factures fictícies). https://www.finma.ch/en/news/2023/02/20230228-mm-greensill/ ↩

[7] Maersk — *Maersk and IBM to discontinue TradeLens* (tancament del consorci, 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 jurisdiccions; inclou el Regne Unit). https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records/status ↩

[9] Clifford Chance — *UK Electronic Trade Documents Act 2023* (equivalència legal del coneixement d'embarcament electrònic). 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 documents/dia; regles UCP 600). https://iccwbo.org/news-publications/news/survey-shows-steady-rise-of-global-adoption-of-electronic-bills-of-lading/ ↩

Auditoria: comptes i informes a prova de manipulació

«Quins avantatges dona al comerciant la partida doble! És una de les invencions més belles de l'esperit humà.»

— Goethe, Els anys d'aprenentatge de Wilhelm Meister (1796)

Hi havia un compte fiduciari que no existia. Durant anys, l'empresa alemanya de pagaments Wirecard va declarar que tenia **1.900 milions d'euros** —gairebé una quarta part del seu balanç— dipositats en comptes de garantia a bancs de Filipines. Quan els auditors d'EY van preguntar al fiduciari de Singapur, Shan Rajaratnam, aquest els va dir la veritat: no custodiava cap diner de Wirecard. Però uns gestors de Wirecard van intervenir, i Shan va «corregir» la seva resposta i va confirmar els 1.900 milions. EY es va acontentar amb captures de pantalla i documents aportats pel mateix client, i **mai no va escriure directament als bancs** [1]. Dos anys més tard, els bancs van confirmar que aquells extractes eren falsos i que el compte no havia existit mai. Wirecard va fer fallida el juny de 2020, en el major frau de la postguerra alemanya.

El detall que ho fa tan dolorós és la seva simplicitat: hauria bastat una **carta de confirmació directa del banc** —el que un auditor rival va descriure com «la formació del primer dia a l'escola d'auditoria»— per fer caure tot l'engany. Aquest capítol tracta d'això: de com fer que les proves sobre les quals descansa la confiança en els comptes d'una empresa siguin impossibles de fabricar.

El frau que els auditors no van veure

Wirecard no és una excepció; és l'últim baula d'una cadena tristament famosa. El 2001, Enron va esfondrar-se i va evaporar més de **74.000 milions de dòlars** dels seus accionistes; la seva auditora, Arthur Andersen —una de les cinc grans del món, amb més de **85.000 empleats**—, va ser declarada culpable de destruir documents i va desaparèixer, donant origen a la llei Sarbanes-Oxley [4]. El 2020, la cadena de cafè Luckin Coffee va admetre haver fabricat uns **311 milions de dòlars** en vendes [5], i el cas indi de Satyam ja havia mostrat el patró exacte de Wirecard: factures falses i **confirmacions bancàries forjades**. Segons l'Associació de Examinadors de Frau Certificats, les organitzacions perden de mitjana un 5 % dels seus ingressos per frau, i el frau d'estats financers, tot i ser només el 5 % dels casos, és el més costós, amb una pèrdua mediana de **766.000 dòlars** per cas [7].

El fil comú de tots aquests escàndols és que l'auditor treballa amb documents que han passat per les mans de l'auditat; quan aquest és el defraudador, la prova ja arriba contaminada. Cal recordar qui va destapar Wirecard: el periodista **Dan McCrum**, del *Financial Times*, que al seu llibre *Money Men* (2022) explica com va ser vigilat, piratejat i fins i tot investigat penalment per «manipulació de mercat» —**per tenir raó** — mentre l'empresa continuava cotitzant a l'índex alemany [3]. El sistema va castigar el missatger abans que el frau.

El regulador respon, i el nou front de l'ESG

La resposta reguladora ha anat, precisament, cap a la prova. El supervisor d'auditoria nord-americà, el **PCAOB**, va adoptar el 2023 una norma específica —l'AS 2310, «L'ús de la confirmació per l'auditor»— que reforça que les confirmacions arribin directament de fonts externes fiables i s'avaluïn amb escepticisme [6]. És, en el fons, un reconeixement que la confirmació bancària directa és el baula que combat el frau corporatiu.

I s'obre un front nou i encara més fràgil: la sostenibilitat. La directiva europea **CSRD** va néixer per obligar desenes de milers d'empreses a presentar un informe de sostenibilitat amb **asseguració externa** —verificació independent— segons les normes ESRS desenvolupades per **EFRAG** [8]. El 2025-26, el paquet «Omnibus» en va retallar l'abast en un 80 %, limitant-lo a les empreses de més de mil empleats i 450 milions d'euros de facturació, però va mantenir l'asseguració limitada com a obligatòria [9]. I el consell mundial de normes d'auditoria, l'**IAASB**, va aprovar el 2024 la primera norma global per verificar la informació de sostenibilitat, la ISSA 5000 [10]. El problema de fons és que les dades ESG —emissions, dades de la cadena de subministrament— són el terreny on la **procedència de la dada** és més feble de totes. Verificar-les exigeix saber d'on venen.

La prova d'existència: segellar en origen

És aquí on **t2p** ofereix el complement tècnic natural a tota aquesta regulació. La idea és aplicar el segellat **en el punt de captura**, no quan el document ja ha passat per l'auditat. Una confirmació bancària signada i segellada **al mateix banc** —amb empremta SHA-512, ancoratge a la blockchain pública i segell de temps RFC 3161 conforme a eIDAS, en un contenidor .asice verificable fora de línia— no es pot substituir per una captura de pantalla fabricada ni redirigir a un fiduciari còmplice. L'auditor deixa de fiar-se d'un paper intermediat i verifica una **cadena de custòdia inalterable** des de la font.

El mateix s'aplica als llibres comptables, a les factures, als recomptes físics d'inventari —amb GPS i prova de vida de qui els fa— i, sobretot, als **papers de treball de l'auditor**, segellats en el moment de crear-se. Contra el cas Andersen, això fa **impossible destruir-los o retrodatar-ne el contingut** sense que l'ancoratge ho delati. I per al front més fràgil de la CSRD, segellar la dada ESG en origen —la lectura del sensor d'emissions, la factura del proveïdor— és l'única manera de donar una procedència sòlida al que avui es verifica gairebé a cegues.

Cal dir el límit amb tota la cruesa, perquè en auditoria és essencial. La prova d'existència demostra **integritat, moment, lloc i persona** d'un registre, no la **veritat econòmica** de fons. Si tots els inputs es fabriquen aigües amunt —un banc còmplice que segella un extracte fals des de l'origen, vendes inventades com a Luckin, una entitat de propòsit especial com a Enron—, el segell només certificarà que **una mentida es va capturar de forma inalterable**: «escombraries a l'entrada, escombraries a la cadena». t2p redueix dràsticament la falsificació posterior i elimina la coartada del «document perdut o alterat», però **no substitueix el judici de l'auditor ni la confirmació amb una font externa genuïnament independent**. Un segell no converteix una dada falsa en veritable.

La promesa i el perill

La promesa és sòlida i quantificable. Una capa de prova d'existència sobre les confirmacions, els llibres i els papers de treball dificultaria molt més el frau d'estats financers —que costa milers de milions i destrueix llocs de treball i estalvis—; donaria a l'auditor una cadena de custòdia fiable en comptes de documents intermediats i posaria un fonament sòlid a l'asseguració de la sostenibilitat, on la procedència de la dada és més feble. En un sistema que es basa en la confiança en els comptes, fer la prova inalterable reforça tot l'edifici.

El perill demana el matís de sempre. El primer, ja hem dit: el segell no converteix una dada falsa en veritable; si la font ja és còmplice, la cadena immortalitza la mentida. Confondre la integritat documental amb la veritat econòmica seria precisament l'error fonamental de Wirecard. El segon, l'excés de confiança: cap tecnologia substitueix l'escepticisme professional de l'auditor. La prova d'existència és una eina que enforteix la confirmació externa i protegeix els papers de treball, no un substitut del judici humà ni de la independència de la font.

És hora d'actuar

Per als auditors: exigir confirmacions segellades en origen i segellar els propis papers de treball en crear-los, perquè ningú no els pugui fabricar ni destruir. Per als bancs i fonts externes: emetre les confirmacions amb un segell criptogràfic des de la font, no a través del client. Per als reguladors (PCAOB, IAASB, EFRAG): reconèixer el segell d'origen com a reforç de l'AS 2310 i de l'asseguració de sostenibilitat. I per a les empreses: segellar la dada ESG en origen, abans que cap auditor l'hagi de verificar a cegues.

Un compte que no existia va estar a punt de passar desapercebut perquè ningú no va escriure al banc. Assignar a cada confirmació, a cada llibre i a cada paper de treball una prova segellada en origen —i recordar sempre la necessitat d'escepticisme professional— és, en aquest front que sosté la confiança en els mercats, **time2act**.

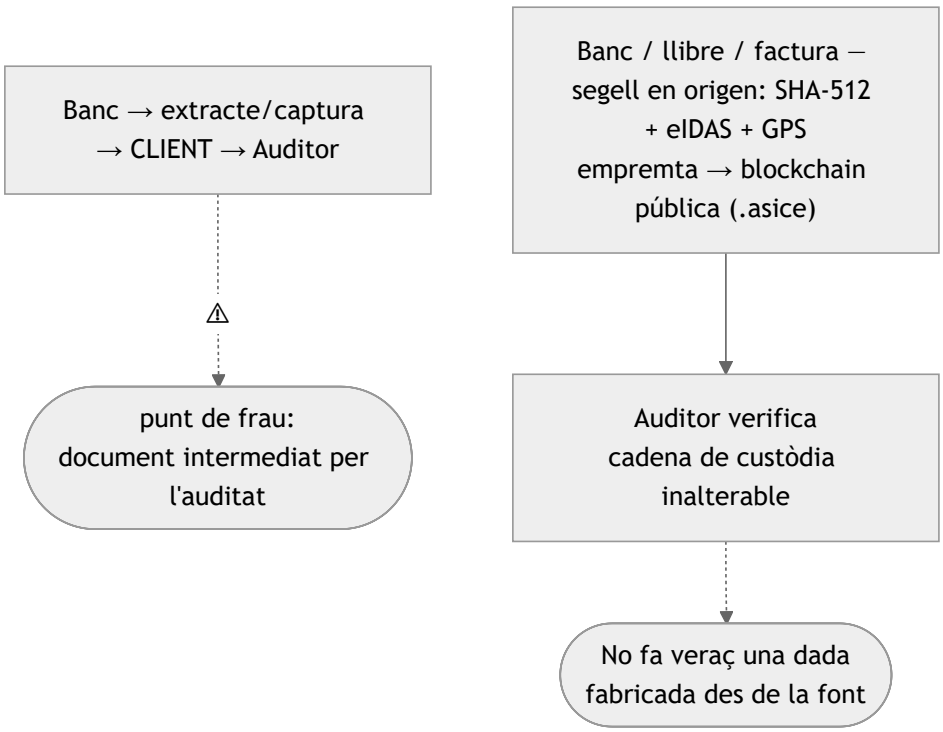


Figura 55.1 — En el model tradicional vulnerable, l'extracte bancari passa pel client (Wirecard) abans d'arribar a l'auditor: és el punt on s'hi cola la falsificació. Amb t2p, la confirmació bancària, el llibre major o la factura se segellen en origen —empremta SHA-512, segell de temps eIDAS, GPS, ancoratge a la blockchain pública— i l'auditor verifica una cadena de custòdia inalterable (.asice). Límit: el segell no fa veritable una dada fabricada des de la font (Wirecard, Luckin, Enron). Context: Wirecard, 1.900 M€ inexistents; frau d'estats financers, mediana de 766.000 $ per cas. Fonts: Financial Times; PCAOB; ACFE.

---

[1] Financial Times (via S&P Global) — *Wirecard auditor did not independently verify its bank balance* (EY; comptes de garantia inexistents; extractes fabricats). 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: «negligència greu»; multa de 500.000 € i prohibició de 2 anys). 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$ perduts; Arthur Andersen, ~85.000 empleats; 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 vendes fabricades). https://www.sec.gov/newsroom/press-releases/2020-319 ↩

[6] PCAOB — *AS 2310, The Auditor's Use of Confirmation* (adoptada el setembre de 2023; confirmació externa directa). https://pcaobus.org/oversight/standards/auditing-standards/details/AS2310 ↩

[7] Association of Certified Fraud Examiners (ACFE) — *Report to the Nations 2024* (5 % dels ingressos; frau d'estats financers, mediana de 766.000 $ per cas). https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf ↩

[8] Comissió Europea — *Corporate sustainability reporting (CSRD)* (asseguració limitada obligatòria; normes ESRS d'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* (llindar de >1.000 empleats i >450 M€; l'asseguració limitada es manté). 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 d'asseguració de sostenibilitat). https://www.iaasb.org/publications/international-standard-sustainability-assurance-5000-general-requirements-sustainability-assurance ↩

Frau publicitari: l'anunci que ningú va veure

«La promesa, la gran promesa, és l'ànima d'un anunci.»

— Samuel Johnson, The Idler, núm. 40 (1759)

L'octubre de 2016, una granja de bots dirigida des de Rússia fingia veure fins a **tres-cents milions de vídeos publicitaris al dia**. No hi havia ningú mirant: el programari simulava cursors de rató que es movien, sessions iniciades a xarxes socials i visites a pàgines; així va generar cobrament dels anunciants. L'operació, batejada Methbot, ingressava entre tres i cinc milions de dòlars diaris [6]. El seu successor, una xarxa anomenada 3ve, va anar més enllà: va infectar **1,7 milions d'ordinadors domèstics** sense que els seus amos ho sabessin, va suplantar deu mil dominis legítims i va costar als anunciants més de **29 milions de dòlars** en anuncis que cap ésser humà mai va veure [5]. Al darrere hi havia un rus que es feia dir «el Rei del Frau»; condemnat a deu anys de presó, va escriure en la seva defensa: «sóc un soldat sense armes davant d'un tanc que es diu FBI» [7].

Aquell cas il·lustra un problema massiu i sorprenentment invisible: una bona part del que gastem en publicitat digital es perd en anuncis que ningú no veu. Aquest capítol tracta de com tornar a fer demostrable la pregunta més bàsica de tot el negoci: **un anunci es va servir de debò a una persona real?**

L'anunci que ningú va veure

La magnitud és estremidora. L'empresa d'anàlisi Juniper Research calcula que el frau publicitari digital va costar 84.000 milions de dòlars el 2023 —un 22 % de tota la inversió publicitària en línia, i fins al 30 % en mòbil—, i projecta que arribarà a 172.000 milions el 2028 [1]. No és estrany si considerem un fet que esgarrifa: segons l'empresa de seguretat Imperva, el 2023 els bots van representar el 49,6 % del tràfic d'Internet, i els bots maliciosos, un 32 %, van créixer per cinquè any consecutiu i van imitar el comportament humà per evadir la detecció [4]. Quan la meitat del trànsit no és humà, saber qui veu de debò un anunci deixa de ser un detall tècnic i es converteix en el problema central del sector.

El dòlar que s'evapora

Però el frau criminal és només una part. L'altra és l'**opacitat de la cadena**. L'associació nord-americana d'anunciants, l'**ANA**, dirigida per Bob Liodice, va publicar al desembre del 2023 un estudi que mostrava que, de cada dòlar que un anunciant posa al sistema, només **36 cèntims** arriben realment al consumidor; la resta s'esfuma en costos de transacció i en «pèrdua de productivitat mediàtica», un eufemisme que inclou els llocs anomenats *made-for-advertising* —webs escombraria creades només per captar anuncis—, que van arribar a emportar-se el 15 % de la inversió [2]. L'ANA calcula que els anunciants podrien recuperar uns **22.000 milions de dòlars** només depurant la seva cadena [2]. Com adverteix l'investigador independent **Augustine Fou**, una de les veus més crítiques del sector, les pròpies plataformes donen una imatge incompleta de l'èxit de les campanyes i les xifres de frau que la indústria reporta tendeixen a subestimar el problema.

...i aquest nus de tot plegat és, una vegada més, un problema de **prova**: ningú no pot demostrar de manera independent que una impressió es va servir a un humà real, en un lloc i un moment concrets. Existeixen estàndards de transparència —l'ads.txt de l'IAB Tech Lab, que declara quins venedors estan autoritzats— i mètriques de visibilitat, però tots descansen en la confiança i en dades que controla qui ven l'inventari.

La prova d'existència: l'ull humà demostrable

És aquí on **t2p** omple el buit. Cada esdeveniment d'impressió genera un registre —anunci servit, identificador de dispositiu atestat, visibilitat segons l'estàndard del sector, geolocalització— i el **SHA-512** corresponent s'ancora a la **blockchain pública** amb un **segell de temps RFC 3161** conforme a eIDAS. El registre queda inalterable: ningú no pot inflar després les xifres ni reescriure quantes vegades s'ha vist un anunci. A més, igual que l'ads.txt declara *qui* pot vendre, **t2p** pot **encadenar i segellar criptogràficament cada salt** de la cadena —de l'editor a la plataforma de venda, a l'intercanvi, a la plataforma de compra—, de manera que cada revenda quedi amb la seva empremta, hora i origen

verificables. Així, com hem vist, aquests imports perduts es converteixen en una cadena traçable. I per validar l'abast real d'un influencer, una campanya amb **prova de vida** i **GPS forense** pot demostrar que darrere d'un visionat hi ha una persona viva en un lloc real, no una granja de seguidors falsos —un frau que costa centenars de milions a les marques. Tot s'empaqueta en un **.asice verificable fora de línia** que un tercer independent pot auditar sense dependre de qui ven l'inventari, precisament la «imatge incompleta» que denuncia Fou.

Cal dir el límit sense embuts, perquè aquí és triple. La prova d'existència demostra integritat, hora, lloc i —amb prova de vida— presència humana d'un registre, però no resol per si sola tres qüestions. La primera, la **privacitat**: verificar que darrere de cada impressió hi ha un humà real implica, per definició, recollir senyals del dispositiu o de la persona —la mateixa tensió entre vigilància i transparència que recorre tot el llibre—, i exigeix minimitzar les dades i atestar sense identificar l'usuari. La segona, que **els bots evolucionen**: Methbot ja falsejava cursors, i una atestació d'avui serà evadida demà; la prova redueix el frau, no l'elimina. I la tercera, que **no corregeix el desalineament d'incentius**: mentre els intermediaris cobrin per impressió servida i no per valor lliurat, hi haurà pressió per inflar. «Escombraries a l'entrada, escombraries a la cadena»: la criptografia fa el registre inviolable, però no garanteix honestament què s'ha de registrar.

La promesa i el perill

La promesa es pot quantificar en desenes de milers de milions; una capa de prova d'existència sobre les impressions i la cadena programàtica dificultaria cobrar per anuncis invisibles, oferiria als anunciants una evidència auditable a un tercer i recuperaria part d'aquestes xifres, com hem vist. En un mercat on la meitat del trànsit no és humà, demostrar l'ull humà real restaura el fonament de tot el negoci.

El perill demana el matís de sempre. Primer, la privacitat: cal evitar que la lluita contra el frau es converteixi en vigilància de l'usuari. Segon, l'excés de confiança: cap atestació és definitiva davant bots que innoven sense parar. I tercer, l'incentiu: la tecnologia registra inviolablement, però l'honestedat de la cadena depèn de qui la vol. La prova d'existència és una eina poderosa per a la transparència, no una bala de plata contra el frau ni un substitut per arreglar els incentius del sector.

És hora d'actuar

Per als anunciants: exigir una evidència segellada i auditable per a cada impressió, en lloc de confiar en les xifres del venedor d'inventari. Per a la cadena programàtica (plataformes de venda i compra, intercanvis): segellar cada salt perquè cada revenda sigui traçable. Per als organismes d'estàndards (IAB, mètriques de visibilitat): integrar la prova d'existència com a reforç de l'ads.txt i de la viewability. I per a les plataformes: deixar d'oferir una imatge incompleta i obrir-se a la verificació independent.

Una granja de bots va cobrar per tres-cents milions de vídeos que ningú no va mirar. Assignar a cada impressió i a cada salt de la cadena una prova segellada de l'ull humà real —sense oblidar mai la privacitat ni els incentius— és, en aquest front del comerç de l'atenció, time2act.

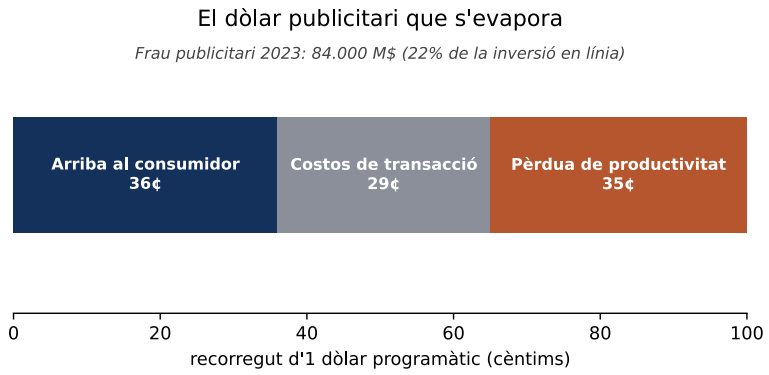


Figura 56.1 — De cada dòlar que un anunciant posa a la compra programàtica, només 36 cèntims arriben al consumidor: 29 es perden en costos de transacció i 35 en «pèrdua de productivitat mediàtica» (webs escombraria i inventari de baixa qualitat). El frau publicitari digital va costar 84.000 milions de

dòlars el 2023 —un 22 % de la inversió en línia— i els bots ja són la meitat del trànsit d'internet. Fonts: ANA (2023); Juniper Research; Imperva.

---

[1] Juniper Research (via PR Newswire) — *22% of online ad spend is wasted due to ad fraud in 2023* (84.000 M$ el 2023 → 172.000 M$ el 2028; mòbil 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* (desembre 2023; 36 cèntims per dòlar; ~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* (els bots, el 49,6 % del tràfic d'internet el 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 i 3ve)* (novembre 2018; 1,7 M d'ordinadors; >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 visionats/dia). 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 suplantació de dominis). 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) — recerca independent sobre el frau publicitari digital. https://www.linkedin.com/pulse/how-do-we-un-fu-digital-advertising-dr-augustine-fou

Ciberseguretat: registres que l'atacant no pot reescriure

«Qui controla el passat controla el futur: qui controla el present controla el passat.»

— George Orwell, 1984 (1949)

Quan un atacant aconsegueix entrar en una xarxa, la primera acció que realitza no és robar; **esborra el seu rastre**. Executa una ordre tan senzilla com `wevtutil cl Security` per buidar el registre de seguretat de Windows i eliminar les proves del seu pas. La maniobra té un nom catalogat —la tècnica **T1070, «Indicator Removal»**, del marc MITRE ATT&CK— i és tan esperada que els defensors la consideren un pas previsible, no una sorpresa [2]. Però amaga una ironia reveladora: en buidar aquell registre, Windows escriu automàticament un nou esdeveniment, l'**Event ID 1102** —«el registre d'auditoria s'ha esborrat»—, amb el compte que ho va fer [2]. Esborrar l'evidència *crea* evidència... **sempre que aquella evidència hagi sortit a temps del sistema compromès**.

I aquí hi ha el problema.

Segons l'informe anual de la unitat de resposta a incidents de Google i Mandiant, el temps mitjà que un atacant opera dins d'una xarxa sense ser detectat —el *dwell time*— va empitjorar fins als **catorze dies el 2025** [1]. Catorze dies són una eternitat: temps de sobra per manipular els registres si aquests viuen només en els sistemes que l'atacant ja controla. Aquest capítol explica com convertir la història d'un atac en un registre que **ni l'atacant pugui reescriure**.

L'atacant ataca l'evidència primer

La ciberseguretat ha après una lliçó dura: l'adversari ataca la prova abans que tu. Les conseqüències de no poder demostrar què va passar són cada cop més greus, perquè avui no responen només els tècnics, sinó també reguladors, tribunals i asseguradores. Com hem vist, aquell any el cost mitjà global d'una bretxa de dades va ser de 4,44 milions de dòlars, amb 10,22 milions als Estats Units i una mitjana de 241 dies per identificar-la i contenir-la [4]. La pressió reguladora s'ha disparat: el reglament europeu de protecció de dades obliga a notificar una bretxa en 72 hores; la directiva NIS2 i el reglament DORA imposen terminis estrictes de notificació d'incidents; i la comissió de valors nord-americana exigeix divulgar un incident material en quatre dies hàbils [5][6][7][8].

El cas de la ciutat de Hamilton, a l'Ontario, mostra fins on arriba. Després d'un atac de ransomware el febrer del 2024 que va paralitzar bona part de la seva xarxa, l'asseguradora va denegar la cobertura perquè la ciutat no tenia plenament desplegada l'autenticació de doble factor, i va deixar els contribuents amb una factura de fins a 18,3 milions de dòlars canadencs [9]. El que els registres i les atestacions de la ciutat podien demostrar — o no — va decidir qui pagava. En ciberseguretat, la integritat de l'evidència ja no és només una qüestió tècnica: és una qüestió de milions.

Treure l'evidència del sistema atacat

La defensa estàndard contra l'esborrament de registres consisteix a treure'ls del sistema: **reenviar-los en temps real** cap a un magatzem extern o a un sistema de gestió d'esdeveniments de seguretat, perquè sobrevisquin la buidada local. És una bona pràctica, però presenta un forat: un atacant prou hàbil pot **desactivar el reenviament abans d'actuar**. I encara que els registres arribin a un servidor extern, qui garanteix que algú —un intern o l'atacant amb accés privilegiat— no els alteri allí? Cal una garantia més forta: que la història registrada quedi amb ancoratge en un lloc que ningú no pugui reescriure. És exactament el que descriu l'estàndard forense de referència, la guia **NIST SP 800-86**: la utilitat d'una prova digital depèn de poder demostrar que no s'ha alterat i d'una cadena de custòdia que aguanti davant d'un tribunal [3].

La prova d'existència: registres que no es poden reescriure

És aquí on **t2p** aporta aquella ancoratge. Un centre d'operacions de seguretat no pot ancorar cada línia de registre —el volum seria inviable—; el que ancorat periòdicament és l'arrel d'un arbre de Merkle que resumeix tot un lot de registres. **t2p** pren l'**empremta SHA-512** d'aquella arrel, junt amb la capçalera

del lot (rang temporal, font, nombre d'esdeveniments), la **segella amb un segell de temps RFC 3161** conforme a eIDAS i l'**ancora a la blockchain pública**. La cadena d'arrels forma una història que només es pot afegir, mai modificar: cada arrel incorpora l'estat anterior, de manera que reescriure un esdeveniment passat obligaria a reescriure totes les arrels posteriors ja ancorades en una cadena pública —cosa impossible sense que la verificació falli.

Això frustra exactament la tècnica descrita; si l'atacant esborra o altera registres *després* que la seva empremta ja estigui ancorada, la discrepància entre el registre reconstruït i l'arrel ancorada el delata. I si esborra registres que **encara no** s'havien ancorat, el forat en la continuïtat de la cadena d'arrels és una prova de manipulació. Per a l'evidència d'una bretxa —captures, bolcats de memòria, cronologies de la resposta a l'incident—, **t2p** genera un contenidor **.asice** verificable fora de línia amb empremta, segell de temps, **GPS forense** del lloc de captura i **prova de vida** de l'analista que la va recollir: una cadena de custòdia alineada amb l'estàndard que serveix davant d'un regulador, d'una asseguradora —el cas Hamilton— i d'un tribunal, demostrant *quan*, *on* i *qui* va preservar cada artefacte, sense dependre de la paraula de la víctima.

Cal dir el límit amb tota claredat, perquè aquí és essencial. L'ancoratge **no impedeix la bretxa**: no atura l'atacant ni tanca la vulnerabilitat. Només protegeix **el que s'ha registrat**; si el registre tenia forats, estava mal configurat o l'atacant va desactivar el reenviament abans d'actuar, no hi ha res per ancorar —«escombraries a l'entrada, escombraries a la cadena». La integritat és tan bona com la **immediatesa del reenviament** fora del sistema compromès: si l'arrel s'ancora cada hora i l'atacant esborra dins d'aquella finestra abans de la sincronització, aquell tram no queda protegit. I resta el cost de rendiment: un centre d'operacions genera milions d'esdeveniments, i cal triar la freqüència d'ancoratge. **t2p** garanteix que **ningú no va reescriure el registre sense deixar rastre**, no que el registre sigui complet ni que reflecteixi tota la veritat de l'atac.

La promesa i el perill

Així, la promesa és tangible: una capa d'ancoratge sobre els registres convertiria el clàssic «la teva paraula contra la meva» en una cronologia que ningú pot tocar, faria inútil l'esborrament de rastres i donaria a l'equip de resposta una evidència admissible davant reguladors i asseguradores. A més, podria estalviar els milions perduts per Hamilton; quan una bretxa costa de mitjana més de quatre milions de dòlars, una prova inalterable del que ha succeït esdevé un actiu de primer ordre.

El perill requereix el matís habitual. Primer, no confondre l'ancoratge amb la prevenció: segellar els registres no atura cap atac. Segon, evitar l'excés de confiança; la prova només val tant com el reenviament immediat i la qualitat del registre. Tercer, protegir la privacitat dels propis registres, que poden contenir dades sensibles i necessiten un disseny que ancori l'empremta, no el contingut en clar. La prova d'existència és una eina poderosa per a la fase posterior a l'incident, però no substitueix la defensa ni la bona higiene de seguretat.

A més, cal reconèixer que la immutabilitat de la cadena protegeix la integritat dels registres sense garantir la confidencialitat. Un cop un arxiu es puja a una blockchain pública, qualsevol node pot validar-lo i, si disposa d'informació addicional, des-anonimitzar-lo. Les agències federals nord-americanes com ICE, IRS o FBI ja compren analítica de cadena per enlairar adreces IP amb identitats reals, convertint el que hauria de ser una prova anònima en un rastre directe cap a persones concretes [12]. Aquest escenari esdevé especialment perillós quan la càrrega útil és sensible: documents mèdics, informes financers o dades personals. Un atacador que comprometi el punt d'entrada inicial pot exposar tot el contingut, i la immutabilitat només assegura que l'explotació persisteixi indefinidament. Com avisa Carissa Véliz, «és possible que la ciberseguretat no s'assoleixi mai», perquè les defenses evolucionen a la mateixa velocitat que les tècniques d'anàlisi i des-anonimització [11].

És hora d'actuar

Per als centres d'operacions de seguretat i els responsables: aplicar ancoratge a les arrels de Merkle dels registres en temps gairebé real, de manera que l'esborrament de rastres deixi de funcionar. Per als equips de resposta a incidents: segellar l'evidència amb cadena de custòdia i fer-la admissible davant reguladors, asseguradores i tribunals. Per a les asseguradores: reconèixer l'evidència ancorada com a base per a les decisions de cobertura. I per als reguladors (NIS2, DORA, la Comissió de valors): valorar el segell d'origen com a reforç de les obligacions de notificació.

Un atacant intenta esborrar els registres per eliminar el seu rastre, però el buidat deixa una empremta —si aquesta apareix a temps. Assignar a cada registre i a cada peça d'evidència una àncora inalterable que converteixi la història d'un atac en quelcom que ningú no pugui reescriure és, en aquest front, cada cop més car, time2act.

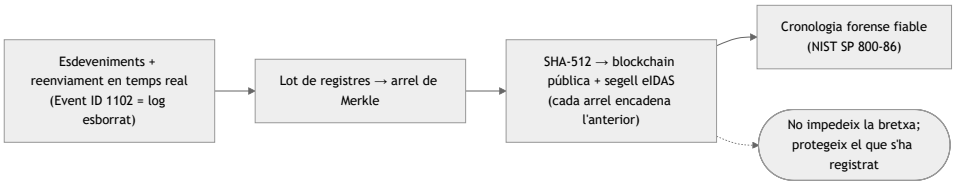


Figura 57.1 — Els esdeveniments del sistema (inclòs l'Event ID 1102, «s'ha esborrat el registre») es reenvien en temps real fora del sistema atacat; els lots de registres es resumeixen en una arrel de Merkle que se segella amb empremta SHA-512 i segell de temps RFC 3161/eIDAS i s'ancora a la blockchain pública, encadenant cada arrel amb l'anterior (només s'hi pot afegir). Qualsevol alteració posterior trenca l'empremta i delata l'atacant. Límit: l'ancoratge no impedeix la bretxa; només protegeix el que s'ha registrat i reenviat a temps. Context: dwell time mitjà de 14 dies el 2025; cost mitjà d'una bretxa, 4,44 M$. Fonts: MITRE ATT&CK; Mandiant M-Trends; NIST SP 800-86.

---

[1] Mandiant / Google Cloud — *M-Trends 2026* (dwell time mitjà de 14 dies el 2025; traspàs d'accés en 22 segons). https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026 ↩

[2] MITRE ATT&CK — *T1070 Indicator Removal / T1070.001 Clear Windows Event Logs* (l'esborrament deixa l'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 i cadena de custòdia). https://csrc.nist.gov/pubs/sp/800/86/final ↩

[4] IBM — *Cost of a Data Breach 2025* (cost mitjà global de 4,44 M$ / 10,22 M$ als EUA; 241 dies per identificar i contenir). https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai ↩

[5] Comissió Europea — *NIS2 Directive (UE 2022/2555)* (notificació en 24 h / 72 h; 23 estats en procediment d'infracció). https://digital-strategy.ec.europa.eu/en/policies/nis2-directive ↩

[6] EUR-Lex — *DORA, Reglament (UE) 2022/2554* (aplicable des del 17-gen-2025; reporting d'incidents TIC greus). 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 dies hàbils). https://www.sec.gov/newsroom/press-releases/2023-139 ↩

[8] GDPR-info — *Article 33 GDPR* (notificació de bretxa de dades en 72 hores). https://gdpr-info.eu/art-33-gdpr/ ↩

[9] Global News — *Hamilton cyberattack cost* (l'asseguradora denega la cobertura per MFA incomplet; 18,3 M CAD). https://globalnews.ca/news/11313018/hamilton-cyberattack-cost/ ↩

[10] Richard Bejtlich (TaoSecurity) — *Mandiant global median dwell time* (dos anys consecutius de deteriorament). 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/ ↩

Les teves dades filtrades: la reclamació del ciutadà

«Dir que no t'importa la privadesa perquè no tens res a amagar no és gaire diferent de dir que no t'importa la llibertat d'expressió perquè no tens res a dir.»

— Edward Snowden, Permanent Record (2019)

El correu comença amb la frase de sempre: «La seguretat de les teves dades és la nostra prioritat». Tres paràgrafs més avall, en lletra una mica més petita, admet que el teu nom, el teu telèfon i el teu DNI han estat «potencialment afectats per un incident». I a partir d'aquell dia, la pluja fina: l'SMS del «teu banc» que no és el teu banc, la trucada que en sap coses que no hauria de saber, l'intent d'entrar als teus comptes, la sol·licitud de duplicat de SIM que tu no vas fer. La bretxa no és un fet puntual: és un degoteig que dura mesos i anys — i que gairebé ningú no pot facturar a qui el va provocar.

El marc hi és, a mitges [2]: el RGPD obliga les empreses a notificar les bretxes a l'autoritat en 72 hores i, si el risc per als afectats és alt, a comunicar-la directament als afectats — les obligacions que el capítol 57 explica des del costat de l'empresa. I eines públiques com Have I Been Pwned permeten a qualsevol comprovar si el seu correu apareix en filtracions conegudes. El que faltava era la peça econòmica: qui paga el mal que això fa?

Aquest capítol és el mirall ciutadà del capítol 57: allà, els registres de l'empresa atacada; aquí, la vida de la persona les dades de la qual ara corren pel mercat negre. La identitat digital és al capítol 47; l'estafa que usa dades filtrades contra la gent gran, al capítol 85; el SIM-swap, al capítol 68. Pregunta clau: es pot cobrar pel dany d'una filtració? Resposta: el Tribunal de Justícia europeu ha dit que sí — sense llindar mínim de gravetat — però amb tres condicions que s'han de PROVAR [1]. I provar-les és, exactament, una qüestió de cronologia: la que es construeix amb **t2p** — empremta calculada al dispositiu i hora certa ancorada a la cadena pública (capítol 13) [3] — des del dia que arriba l'avís.

El TJUE obre la porta — i hi posa un llindar de prova

El 4 de maig de 2023, el Tribunal de Justícia de la Unió Europea va dictar sentència en l'assumpte C-300/21 — el cas del servei postal austríac que, mitjançant un algorisme, inferia l'afinitat política dels ciutadans sense el seu consentiment — i va fixar la doctrina de l'article 82 del RGPD [1]: el dret a indemnització exigeix tres condicions acumulatives — una infracció del reglament, un dany (material o immaterial) i una relació de causalitat entre l'una i l'altre.

La sentència conté dues tensions que defineixen aquest capítol. La favorable al ciutadà: el dany moral és indemnitzable sense cap llindar mínim de gravetat — sentir-se exposat, humiliat o angoixat compta. La dura: la mera infracció no basta — el dany s'ha de provar, i la causalitat també; i la quantificació queda en mans dels tribunals nacionals [1].

Europa ha dit, doncs, que el teu malestar val diners — si el proves. I aquí és on el ciutadà perd sempre: la bretxa passa un dia, el phishing arriba durant mesos, l'intent de suplantació al cap d'un any — i quan la reclamació es presenta, tot són records dispersos en carpetes de correu brossa esborrades. La lectura pràctica és la d'aquest llibre: la causalitat que el TJUE demana és, exactament, una cronologia — i les cronologies es construeixen amb dates certes, no amb memòria.

La prova d'existència aplicada

El diari comença el dia que arriba l'avís [3].

1. La notificació capturada

El correu o la carta que t'informa de la bretxa — o la pàgina on l'empresa ho admet —, capturats amb data certa [3]. És la primera baula de la causalitat: quan es va saber, què es va admetre, quines dades es van reconèixer afectades. I si l'empresa no et va notificar quan tocava [2], l'absència també es documenta: la data en què ho vas saber per la premsa o per una eina pública, segellada.

2. El certificat de presència

La comprovació a Have I Been Pwned — el teu correu, en quines filtracions apareix — capturada amb el navegador certificat de t2p: la imatge completa i el codi font, amb data [3]. La teva presència a la filtració deixa de ser una afirmació teva: és una consulta datada d'una font pública reconeguda.

3. El diari del dany

Cada conseqüència, segellada al moment: l'SMS de phishing que cita el teu nom complet, la trucada que sabia el teu DNI — gravació de conversa pròpia, com explica el capítol 75 —, l'avís d'intent d'accés, la sol·licitud de duplicat de SIM que tu no vas fer (capítol 68) [3]. Trenta segons per peça. Al cap d'un any, no tens records: tens una sèrie datada que comença just després de la bretxa — la relació de causalitat que el TJUE demana [1], feta de fets.

4. La reclamació que arriba armada

L'expedient sencer — notificació, presència, diari del dany — exportat com a paquet .asice verificable sense connexió [3]: per a la reclamació a l'empresa, la denúncia davant l'autoritat de protecció de dades o la demanda civil de l'article 82 [1][2]. I la simetria de sempre: l'empresa que va notificar bé i a temps — i que té els seus registres del capítol 57 ancorats — pot acreditar la seva diligència amb la mateixa moneda.

Els límits, com sempre, per endavant: el segell acredita la cronologia — no la valoració del dany, que és del jutge amb el dret nacional a la mà [1]. La correlació no sempre és causalitat: el phishing existia abans de la bretxa, i el pèrit haurà de valorar la connexió — la sèrie datada l'ajuda, no el substitueix. I el diari del dany és teu: al dispositiu, només empremtes a la cadena, revelació selectiva [3].

La promesa i el perill

La promesa: ciutadans que reclamen amb cronologies en lloc de queixes [1][3]; empreses que responen amb diligència demostrable en lloc de plantilles; el dany moral de les filtracions — reconegut pel TJUE sense llindar [1] — convertit en reclamacions viables; i un incentiu nou i potent perquè les dades es protegeixin abans: quan el dany es pot provar, la negligència surt cara.

Els perills, que no són pocs.

El primer és **la indústria de la reclamació**: despatxos massificant demandes idèntiques amb danys de plantilla. El contrapès és la mateixa doctrina: el TJUE exigeix dany i causalitat provats [1] — la reclamació de plantilla mor on la cronologia personal comença.

El segon és **la revictimització documental**. Demanar a la víctima que ho segelli tot pot ser una segona càrrega. El gest ha de ser mínim — la captura de deu segons — i l'eina, un aliat: qui no documenta no perd els seus drets, només la seva millor prova.

El tercer és **el diari com a nou botí**: l'expedient del teu dany conté... més dades teves. Per això la regla d'or: al dispositiu, només empremtes a la cadena [3], i revelació selectiva davant de qui toqui.

El quart perill és confondre el rescabalament amb la protecció. Cap segell no evita la bretxa ni retorna les dades al pot. La prevenció és feina de les empreses — el capítol 57 — i del regulador; la prova d'existència només fa que, quan fallin, el cost no el pagui en silenci la víctima.

És hora d'actuar

El diari es comença el dia u — perquè el dia mil serà tard.

Per a tu, ciutadà: quan arribi l'avís d'una bretxa — o la sospita —, comença el diari: la notificació, la presència, cada símptoma datat [3]; la reclamació de demà es construeix el dia u.

Per a les associacions de consumidors i els despatxos: exigiu i aporteu cronologies ancorades — el TJUE us ha donat la porta [1]; la clau és la causalitat datada, no el volum.

Per a les empreses que custodien dades: notifiqueu bé i ancoreu-ho — la vostra diligència demostrable és la diferència entre un incident i una condemna; el capítol 57 és el vostre.

Per a les autoritats de protecció de dades: valoreu l'expedient datat del ciutadà com el que és — la causalitat feta cronologia [1]; i publiqueu guies perquè documentar el dany sigui a l'abast de tothom.

Per als legisladors: l'article 82 ja hi és [1][2]; el pas pendent és processal — reconèixer la cronologia ancorada com a prova qualificada del dany moral, perquè reclamar no exigeixi ser pèrit.

Les teves dades poden córrer per llocs que mai no veuràs; que almenys el dany que et facin deixi un rastre que sí. Per la intimitat que es defensa amb fets, **time2act**.

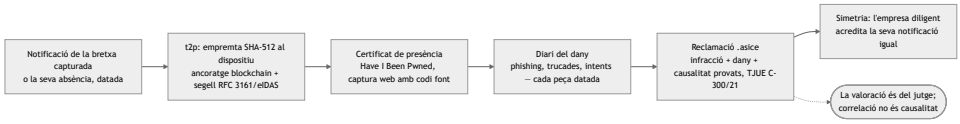


Figura 58.1 — La bretxa vista des del ciutadà, amb prova d'existència (segellat amb t2p — capítol 13): la notificació capturada (o la seva absència, datada), el certificat de presència a la filtració (captura web amb codi font), el diari del dany (phishing, trucades, intents — cada peça segellada al moment) i la reclamació .asice. Fonament: TJUE C-300/21 — dany moral indemnitzable sense llindar, però amb infracció + dany + causalitat PROVATS. Simetria: l'empresa diligent acredita la seva notificació. Límits: la valoració és del jutge; correlació ≠ causalitat; el diari queda al dispositiu. Fonts: TJUE; RGPD art. 82.

---

[1] TJUE — *Sentència de 4 de maig de 2023, assumpte C-300/21 (UI c. Österreichische Post)* (article 82 RGPD: tres condicions acumulatives — infracció, dany i relació de causalitat; la mera infracció no dona dret a indemnització; el dany immaterial és indemnitzable sense llindar mínim de gravetat; quantificació segons el dret nacional amb equivalència i efectivitat); anàlisis de Cuatrecasas, finReg360 i 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: notificació de bretxes a l'autoritat en 72 h i als afectats en cas d'alt risc; art. 82: dret a indemnització); Have I Been Pwned com a eina pública de comprovació de filtracions. Vegeu el capítol 57 per al costat de l'empresa. ↩

[3] t2p — manual de producte (captura de pantalla i de pàgina web certificades — imatge completa + codi font; gravació d'àudio de converses pròpies; certificar qualsevol fitxer; projectes per al diari d'un incident; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió; només empremtes a la cadena). Vegeu els capítols 13 i 15; el SIM-swap, al capítol 68; l'estafa amb dades filtrades, al capítol 85. ↩

La caiguda documentada: SLA, núvol i continuïtat

«Cap home no és una illa, complet en si mateix; cada home és un tros del continent, una part del tot.»

— John Donne, Devocions, Meditació XVII (1624)

El 19 de juliol de 2024, una actualització defectuosa del programari de seguretat Falcon Sensor, de CrowdStrike, va tombar uns 8,5 milions d'ordinadors Windows arreu del món — la caiguda informàtica més gran de la història [1]. Pantalles blaves a les terminals dels aeroports, als quiròfans, a les sucursals bancàries, als sistemes ferroviaris. Delta Air Lines va cancel·lar més de 7.000 vols en cinc dies, amb més d'1,3 milions de passatgers afectats — i a l'octubre va demandar CrowdStrike reclamant uns 550 milions de dòlars; les dues companyies van acabar demandant-se mútuament [1].

Aquell dia, milers d'empreses van descobrir alhora tres coses que donaven per fetes. Que tot el seu negoci penja d'un proveïdor. Que el contracte promet «99,9 % de disponibilitat» amb crèdits de servei com a únic remei. I que, quan toca reclamar, la caiguda l'ha de provar el client — sobre les pàgines d'estat, els panells i els mesuraments del mateix proveïdor que ha fallat. Qui va caure, quan exactament, durant quant de temps, amb quin impacte? Les respostes oficials les escriu una de les parts.

Aquest capítol tracta la disponibilitat — el germà oblidat de la seguretat. Els registres que un atacant no pot reescriure són al capítol 57; les telecomunicacions i la veu, al capítol 68; la reclamació a l'assegurança, al capítol 28. Pregunta clau: de qui és el rellotge quan el núvol cau? Resposta: de qui l'ha provocada — llevat que el client tingui el seu, amb data certa oposable: el monitoratge independent segellat amb **t2p** — empremta, hora certa i àncora pública, la maquinària del capítol 13 [3]. I amb la simetria de sempre: el proveïdor que compleix té, en els seus propis registres ancorats, el millor argument comercial del sector.

El rellotge del proveïdor

L'anatomia del problema, peça a peça. El SLA — l'acord de nivell de servei — promet un percentatge de disponibilitat i ofereix crèdits quan s'incompleix; però els crèdits no són automàtics: exigeixen que el client reclami dins d'un termini, i la càrrega de la prova és seva. El mesurament oficial és del proveïdor: les seves pàgines d'estat — que durant els incidents sovint van per darrere de la realitat —, els seus panells, les seves mètriques. I les eines de mesura del client, per acabar-ho d'adobar, sovint corren al mateix núvol que s'està enfonsant.

El crèdit, a més, cobreix una fracció de la factura mensual. El dany real — les vendes perdudes, el TPV parat, la reputació — queda fora, i exigeix prova pericial del lucre cessant. Sense una cronologia fiable i verificable, la negociació amb el proveïdor i amb l'asseguradora és un joc de versions.

I el context regulador puja el llistó: DORA obliga el sector financer europeu a gestionar el risc TIC dels seus proveïdors i a reportar incidents amb precisió, i la NIS2 estén les obligacions de notificació a molts més sectors — totes dues demanen, en el fons, cronologies fiables [2]. El registre del temps ja no és només una qüestió contractual: és un requisit legal.

La conclusió és la d'aquest llibre: la disputa de la caiguda és una disputa de rellotges — i avui gairebé tots els rellotges admissibles són de la mateixa banda. El que falta no és més monitoratge: és que el monitoratge del client tingui data certa oposable.

La prova d'existència aplicada

El moment en què el servei cau és l'únic instant que el client no es pot permetre perdre [3].

1. La sonda independent segellada

L'empresa munta les seves sondes — comprovacions periòdiques del servei des de fora del núvol vigilat — i en segella els resultats amb t2p: el fitxer de registres de cada interval, certificat per empremta amb data certa; només l'empremta s'ancora, el registre queda a casa [3]. La cadència la tria cada negoci; el que importa és la cadena: quan arriba la caiguda, la seqüència «responia — responia — no respon — no respon» té segells de temps que cap de les dues parts no pot moure. El rellotge del client, per fi, existeix.

2. La pàgina d'estat, congelada

Durant l'incident, la pàgina d'estat del proveïdor es captura amb el navegador certificat de t2p — la imatge completa i el codi font, empaquetats amb data certa [3]. El que el proveïdor deia a les 10:42 — «tot operatiu» o «incident en investigació» — queda congelat. Si després la narrativa oficial canvia, la discrepància és un fet datat, no un record.

3. L'impacte documentat

La transacció que falla, gravada en pantalla i certificada [3]: el carret que no cobra, el TPV que no respon, la cua de comandes aturada. Les exportacions de mètriques de negoci — vendes per hora, transaccions completades —, segellades per empremta. Quan calgui quantificar el lucre cessant davant l'asseguradora o el jutjat, el pèrit treballarà sobre una cronologia ancorada, no sobre reconstruccions.

4. La reclamació que es sosté

El paquet .asice de l'incident [3]: sondes, captures d'estat, impacte, comunicacions amb el proveïdor — cada peça verificable sense connexió i sense confiar en ningú. Per als crèdits del SLA, per a la ciberassegurança, per al report regulador de DORA o NIS2 [2]: la mateixa evidència serveix tots els fronts. I la simetria: el proveïdor seriós que publica els seus propis registres de disponibilitat ancorats converteix el seu SLA en el seu millor argument — contra la reclamació oportunista, els seus segells; contra la competència, la seva transparència.

Els límits, d'entrada: el segell acredita quan el servei no responia des d'on mesurava la sonda — no diagnostica la causa ni reparteix culpes entre proveïdor, xarxa i client: això és feina de pèrits. Una sonda mal dissenyada segella la seva pròpia confusió — metodologia primer, criptografia després. I cap empremta no aixeca un servei caigut: la continuïtat es construeix amb redundància i plans de contingència — la prova només fa que el dany, quan arribi, no sigui també una disputa de cronologies.

La promesa i el perill

La promesa: crèdits de SLA que es reclamen amb cronologies pròpies [3]; disputes com les del juliol de 2024 [1] que es podrien dirimir sobre registres ancorats de les dues parts en lloc d'anys de litigi; asseguradores i reguladors [2] treballant sobre fets datats; i proveïdors que competeixen publicant la seva disponibilitat verificable.

I ara, els perills, sense edulcorar.

El primer és **la guerra de sondes**: cada part mesurant des d'on més li convé. La resposta és metodològica — sondes des de punts representatius, metodologia declarada i segellada per endavant, com el compromís previ del capítol 45, i pèrits que valorin la qualitat del mesurament, no només la seva data.

El segon és **el proveïdor a la defensiva**. Si la traça del client només serveix per litigar, la relació es tensa. La sortida és la simetria: el proveïdor que ancora els seus registres guanya la presumpció de serietat — la transparència verificable com a estàndard del sector, no com a arma.

El tercer és **el paper mullat regulador**. DORA i NIS2 [2] demanen reports; si els reports es fabriquen a posteriori, tot l'edifici és decoratiu. La cronologia ancorada és el mínim perquè el compliment signifiqui alguna cosa.

El quart és brutal de tan simple: la prova no aixeca servidors. Cap segell no substitueix la redundància, el multi-proveïdor ni el pla de contingència. Primer, que el negoci sobrevisqui la caiguda; després, que la pugui provar.

És hora d'actuar

Que la pròxima caiguda trobi cada empresa amb rellotge propi.

Per a les empreses que viuen al núvol: monteu la sonda independent i segelleu-ne la cadena [3]; el dia de la pròxima gran caiguda [1], la cronologia serà vostra.

Per als proveïdors de núvol i hosting: ancoreu els vostres registres de disponibilitat i publiqueu-los per empremta — el SLA verificable és màrqueting que cap competidor no pot copiar sense complir.

Per a les asseguradores de cyber i lucre cessant: exigiu cronologies ancorades a la pòlissa; pagareu més de pressa els sinistres reals i menys els fabricats.

Per als reguladors financers i de ciberseguretat: DORA i NIS2 [2] ja demanen cronologies d'incidents — que siguin verificables, no narratives.

Per als legisladors: els crèdits de SLA amb mesurament unilateral són una clàusula coixa; el reconeixement del mesurament independent amb data certa equilibraria el contracte més asimètric de l'economia digital.

La pròxima pantalla blava global arribarà. Que trobi cada empresa amb el seu rellotge segellat — i que la discussió sigui de causes, no de cronologies. Per l'economia que no pot aturar-se, **time2act**.

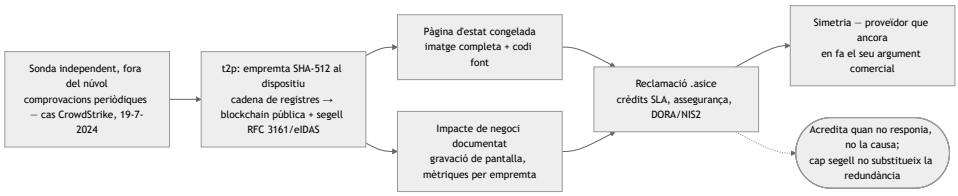


Figura 59.1 — La caiguda documentada amb prova d'existència (segellat amb t2p — capítol 13): la sonda independent amb cadena de registres segellats (el rellotge del client), la pàgina d'estat del proveïdor congelada amb codi font, l'impacte de negoci documentat (gravació de pantalla, mètriques per empremta) i la reclamació .asice — per als crèdits del SLA, l'asseguradora i els reports DORA/NIS2. Simetria: el proveïdor que ancora la seva disponibilitat en fa el seu argument comercial. Límits: la sonda acredita quan no responia, no la causa; metodologia primer; cap segell no substitueix la redundància. Fonts: 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: actualització defectuosa de Falcon Sensor; ~8,5 milions de Windows; la caiguda informàtica més gran de la història; impacte en aerolínies, hospitals, bancs, emergències); CNBC — *Delta, CrowdStrike sue each other over widespread IT outage* (Delta: >7.000 vols cancel·lats en cinc dies, >1,3 M de passatgers; demanda d'octubre de 2024 per ~550 M$; demandes creuades). 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] Reglament (UE) 2022/2554 (DORA — resiliència operativa digital del sector financer: gestió del risc TIC de tercers, report d'incidents; aplicable des de l'11-1-2025) i Directiva NIS2 (obligacions ampliades de notificació d'incidents). Vegeu el capítol 57 per al context de seguretat i terminis de notificació. ↩

[3] t2p — manual de producte (certificar qualsevol fitxer — només l'empremta viatja; captura de pàgina web amb imatge completa + codi font; captura i gravació de pantalla certificades; projectes per agrupar l'expedient d'un incident; certificació en segon pla; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; els registres d'un atac, al capítol 57; la reclamació d'assegurança, al capítol 28. ↩

Art i antiguitats: la procedència contra la falsificació i l'espoli

«Fins i tot a la reproducció més perfecta d'una obra d'art li manca un element: la seva presència en el temps i l'espai, la seva existència única al lloc on es troba.»

— Walter Benjamin, L'obra d'art a l'època de la seva reproductibilitat tècnica (1935)

En un garatge del barri de Queens, a Nova York, un pintor immigrant xinès anomenat Pei-Shen Qian fabricava obres mestres. Pintava «Rothkos» i «Pollocks» que envellia amb te i amb pols d'una aspiradora per simular dècades de brutícia, i cobrava menys de **nou mil dòlars** per llenç. La galeria més antiga de Nova York, Knoedler & Company — fundada el 1846 —, els venia per milions a col·leccionistes que confiaven en el seu prestigi de cent seixanta-cinc anys. El frau, d'uns **vuitanta milions de dòlars** en una quarantena de falsificacions, va enganyar els experts durant gairebé quinze anys, fins que la galeria va tancar les portes de cop el 2011 [1].

Ara bé, com es va destapar el major falsificador alemany de la postguerra? No va ser un expert ni un document, sinó un **pot de pintura**. El falsificador Wolfgang Beltracchi havia venut un suposat Campendonk per 2,88 milions d'euros, però l'anàlisi de laboratori hi va detectar **blanc de titani**, un pigment que no existia en la vida de l'artista [2]. Aquella molècula va desencadenar una carrera de centenars de falsificacions. La lliçó, que posem al davant perquè és el cor d'aquest capítol, és aquesta: el que autentica una obra és la **ciència i l'ull expert**, no el paper. Però el que decideix si es pot vendre, robar o restituir és una altra cosa: la **procedència**, el seu historial d'origen i propietat. I aquí la mentida campa lliure.

La mentida sobre l'origen

Si la falsificació ataca *qui* va fer una obra, l'espoli ataca *d'on* ve. El cas més emblemàtic és el del marxant Subhash Kapoor, propietari d'una galeria de Manhattan, que dirigí una xarxa internacional de tràfic d'antiguitats valorada en uns cent milions de dòlars. Un dels seus objectes era un Shiva dansant de bronze del segle XI, arrencat d'un temple en desús de Tamil Nadu i venut el 2008 a la Galeria Nacional d'Austràlia per 5,6 milions de dòlars amb papers de procedència falsos. La unitat antitràfic de la fiscalia de Manhattan va acabar confiscant més de 2.500 peces vinculades a Kapoor, valorades en uns 143 milions, i ell fou condemnat a deu anys de presó a l'Índia el 2022 [3]. Com explica l'arqueòleg forense Christos Tsirogiannis, de la Universitat de Cambridge, que ha identificat milers d'antiguitats espoliades creuant-les amb arxius confiscats a traficants, la «procedència» que exhibeixen cases de subhastes i museus sovint és un relat fabricat que comença just després de l'espoli: el problema no és la falta de papers, sinó que els papers menteixen.

La magnitud és tan gran com opaca. INTERPOL estima el comerç il·lícit d'antiguitats entre 225 milions i 6.000 milions de dòlars l'any —l'enorme forquilla reflecteix l'opacitat del mercat [8]. A Síria, com hem vist, s'han robat desenes de milers de peces de jaciments i museus. I el problema té una versió històrica que encara cou: l'art espoliat pels nazis, com les 1.406 obres —Picasso, Matisse, Chagall— que un control duaner rutinari va descobrir el 2012 amagades a l'apartament de Munic de Cornelius Gurlitt, fill d'un dels marxants de Hitler [5]. Davant d'això, la comunitat internacional ha bastit defenses: la Convenció de la UNESCO de 1970 contra el tràfic il·lícit, ratificada per prop de 150 estats [7]; els Principis de Washington de 1998 sobre la restitució de l'art nazi [6]; i bases de dades com l'Art Loss Register, fundat per Julian Radcliffe el 1991, que té registrats uns 700.000 objectes robats i n'ha recuperat per valor de més de cent milions de dòlars [9]. La tesi de Radcliffe és lluminosa: si tot l'art robat es registra en un sol lloc i tothom qui compra o ven el consulta, robar deixa de ser rendible perquè la peça no es pot revendre netament.

La prova d'existència: la procedència des del segon zero

És aquí on **t2p** aporta el que falta: una **cadena de procedència** com a successió d'esdeveniments verificables. Cada nou baula —un certificat d'autenticitat, un informe de condició, una factura, un dictamen d'expert, un canvi de propietari, una fotografia d'alta resolució— es resumeix en una **empremta SHA-512** al dispositiu, s'ancora a la **blockchain pública** amb un **segell de temps RFC 3161** conforme a eIDAS i s'empaqueta en un contenidor **.asice verificable fora de línia**.

Però l'aplicació més potent és arqueològica. En una excavació legal, l'arqueòleg pot segellar *in situ* la fotografia del **lloc exacte de la troballa** —amb GPS forense i segell de temps— abans de moure la peça. Això crea una prova digital d'excavació regulada que distingeix el descobriment legítim de l'espoli: és exactament la diferència entre el Shiva de Kapoor, amb papers inventats anys després, i un objecte amb el seu **origen documentat des del segon zero**. I la **prova de vida** lliga el perit o l'excavador que signa el dictamen a una persona real i viva en aquell moment, dificultant els «experts fantasma» i els certificats signats a posteriori que apareixen en casos com el de Knoedler. Contra el patró de Kapoor i Tsirogiannis, un registre segellat i datat fa que inventar un historial **després** del moment del segellat sigui detectable.

Cal dir el límit amb tota la cruesa, perquè aquí és absolut. La prova d'existència **no autentica l'objecte**. Segellar la fotografia d'un Beltracchi no el converteix en un Campendonk autèntic: una foto segellada d'una falsificació continua sent una falsificació. L'autenticació continua exigint l'ull expert i l'anàlisi científica —els pigments, la datació— que va ser el que de debò va enxampar Beltracchi. I, encara més important, **tota procedència fabricada *abans* del segell queda fabricada per sempre**: la cadena hereta i petrifica la mentida. «Escombraries a l'entrada, escombraries a la cadena.» El valor real de t2p no és segellar historials antics i dubtosos, sinó segellar l'origen **en el moment exacte** en què neix la prova —el find-spot d'una excavació, el dictamen d'un perit identificat—, perquè a partir d'aquell instant la mentida ja no s'hi pugui colar.

La promesa i el perill

La promesa és gran per a un mercat corcat per l'opacitat. Una cadena de procedència segellada des de l'origen faria molt més difícil l'espoli —perquè una antiguitat sense find-spot documentat seria immediatament sospitosa—, dificultaria les procedències «blanquejades» a posteriori i donaria a museus, compradors i jutges una evidència incontestable de l'historial d'una obra. En un comerç on robar un temple pot rendir milions, la procedència verificable és la millor defensa del patrimoni de la humanitat.

El perill demana el matís de sempre, i aquí és especialment important. El primer, ja dit: confondre la procedència amb l'autenticitat seria fatal; el segell no fa autèntic res, i la ciència ha de continuar sent insubstituïble. El segon, que la cadena petrifica el que se li doni: una procedència falsa segellada avui serà una mentida immutable demà. I el tercer, que la part que de debò importa —la inspecció física, l'ull de l'expert, el context històric— viu fora de la cadena. La prova d'existència és una eina poderosa per documentar l'origen des del segon zero, no un certificat d'autenticitat ni un substitut del coneixement expert.

És hora d'actuar

Per als museus i cases de subhastes: exigir una procedència segellada i, sobretot, punts de troballa documentats des de l'excavació, evitant comprar peces amb historials que comencen sospitosament tard. Per als arqueòlegs i les excavacions legals: segellar el lloc de la troballa *in situ* per generar una prova que distingeixi el descobriment de l'espoli. Per als mercants i compradors: consultar registres com l'Art Loss Register i no confiar en documents enganyosos. Per als reguladors i la UNESCO: reconèixer la cadena de procedència segellada com a estàndard del comerç legítim. I per a tothom, recordar que cap segell **NO** substitueix l'ull de l'expert ni el laboratori.

Un pot de blanc de titani va revelar el falsificador més destacat d'Europa; uns documents falsos van permetre vendre un déu robat per milions. Assignar a cada obra una procedència segellada des del seu origen —sense oblidar mai que l'autenticació requereix ciència, no només una empremta— és el front que custodia la memòria i la bellesa, time2act.

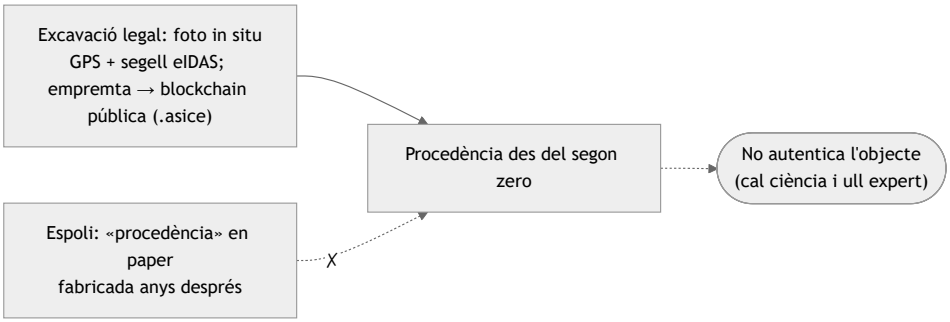


Figura 60.1 — En una excavació legal (esquerra), la peça es fotografia in situ amb coordenades GPS i segell de temps eIDAS abans de moure-la: la procedència queda documentada des del segon zero i s'ancora a la blockchain pública (.asice). En l'espoli (dreta), la «procedència» en paper comença anys després de la troballa i és fàcil de fabricar —com el Shiva Chola venut a Austràlia per 5,6 M$ amb papers falsos. Límit: el segell prova integritat, data, lloc i persona, però NO autentica l'objecte (una foto segellada d'una falsificació continua sent una falsificació). Context: comerç il·lícit d'antiguitats de 225 M$ a 6.000 M$/any. Fonts: INTERPOL; fiscalia de Manhattan; Art Loss Register.

---

[1] CNBC — *This $80 million art scam fooled experts* (galeria Knoedler; Pei-Shen Qian; <9.000 $ per 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 pigment impossible). 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 peces, ~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 antiguitats de 29 països, >460 M$ recuperats). 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 obres). 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 països). https://www.state.gov/washington-conference-principles-on-nazi-confiscated-art ↩

[7] UNESCO — *1970 Convention against the illicit trafficking of cultural property* (~149 estats). https://www.unesco.org/en/fight-illicit-trafficking/about ↩

[8] INTERPOL — *Cultural heritage crime: the issues* (comerç il·lícit de 225 M$ a 6.000 M$/any). https://www.interpol.int/en/Crimes/Cultural-heritage-crime/The-issues-cultural-property ↩

[9] Art Loss Register — *~700.000 objectes registrats; fundat per Julian Radcliffe (1991); >100 M$ recuperats.* https://www.artloss.com/ ↩

[10] CNN — *The forensic archaeologist hunting trafficked antiquities* (Christos Tsirogiannis; «els papers menteixen»). https://edition.cnn.com/2025/12/13/style/forensic-archaeologist-trafficked-antiquities-scli-intl

Memòria històrica: els arxius contra el negacionisme

«Els qui no poden recordar el passat estan condemnats a repetir-lo.»

— George Santayana, The Life of Reason (1905)

El juny de 2024, la UNESCO i el Congrés Jueu Mundial van publicar un informe que hauria de treure la son a qualsevol historiador: la IA generativa amenaça la memòria de l'Holocaust. No és una advertència abstracta — porta exemples: ChatGPT havia inventat campanyes d'un «Holocaust per ofegament», amb nazis ofegant jueus als rius, un episodi que mai no va existir; Bard havia fabricat cites falses de testimonis per apuntalar narracions distorsionades de massacres reals [1]. Pensem un moment què significa: la màquina no es limita a equivocar-se — inventa atrocitats amb aparença d'història i testimonis amb aparença de veu humana, a escala industrial i amb to d'enciclopèdia. I mentrestant, els últims supervivents s'apaguen: aviat, tota la memòria viva serà arxiu — i l'arxiu, atacable.

Aquest llibre ha defensat fins aquí el present: provar què passa ara, mentre passa. Aquest capítol estén la mateixa lògica cap enrere. La procedència dels objectes d'art es tracta al capítol 60; la fotografia del present, al capítol 17; la crisi general de la veritat, al capítol 10. Aquí la pregunta és una altra: com es protegeix el passat, quan fabricar-ne «proves» costa un prompt? Resposta: ancorant la memòria abans que arribi la riuada — arxius amb manifests segellats, testimonis empremtats en vida, exhumacions amb cadena de custòdia ancorada i col·leccions fotogràfiques amb data certa, amb **t2p**: l'empremta SHA-512, l'ancoratge de l'empremta a la blockchain pública i el segell de temps RFC 3161/eIDAS complementari, dins d'un contenidor .asice [5]. El passat no es pot canviar; la seva prova, sí — i per això s'ha de segellar.

La història, reescrita a màquina

L'informe de la UNESCO no es limita als exemples: fa un diagnòstic estructural. Els models generatius tendeixen a simplificar en excés la complexitat històrica i prioritzen una petita selecció de fonts i esdeveniments, deixant fora matisos i contextos sencers; les recomanacions apunten en dues direccions — que les tecnològiques treballin amb supervivents, descendents, educadors i historiadors, i que els sistemes educatius equipin el jovent amb alfabetització digital i pensament crític [1].

I el fenomen ja parla català i castellà. El febrer de 2025, Maldita.es documentava com webs i revistes publicaven en portada imatges generades amb IA de personatges i fets reals — el papa, la científica Margarita Salas, escenes de la Guerra Civil espanyola —, sovint sense cap etiqueta que les identifiqués com a sintètiques; el risc descrit: alterar la percepció de personatges i fets històrics, generar falsos relats i aprofundir la desconfiança en els mitjans [2]. La imatge «d'època» fabricada ja no és un exercici de laboratori: és contingut editorial en circulació.

La mecànica del dany és el dividend del mentider aplicat a la història. Quan les imatges d'època fabricades són indistingibles de les autèntiques, passa el pitjor dels dos móns alhora: la foto falsa troba creients, i la foto verídica troba negacionistes — «això és un muntatge» esdevé resposta universal. I el negacionisme, que sempre havia hagut de treballar contra els documents, ara pot fabricar-ne de favorables. La batalla de la memòria deixa de ser només interpretativa per esdevenir probatòria: quins documents existien, des de quan, i qui ho pot demostrar.

L'arxiu que va tremolar

El 9 d'octubre de 2024 es va saber que l'Internet Archive — la biblioteca digital que custodia la memòria del web — havia patit una intrusió majúscula: 7 terabytes sostrets, amb el codi font de la institució i les adreces i contrasenyes amb hash de 31 milions d'usuaris, a partir d'un token de GitLab que havia quedat exposat des de finals de 2022. Simultàniament, atacs de denegació de servei van deixar fora de línia la Wayback Machine, i una segona bretxa el mateix mes va exposar més de 800.000 tiquets de suport, alguns amb documents d'identitat. El servei va tornar a mitjan octubre, amb funcions limitades [3].

Per què això és més que un incident tècnic? Perquè la Wayback Machine és la memòria de facto d'internet: l'eina amb què periodistes, jutges i investigadors demostren que una pàgina deia una cosa abans que algú l'edités en silenci. Cada citació judicial o acadèmica d'una captura confia en la integritat i la disponibilitat

d'una infraestructura sostinguda per una sola organització sense ànim de lucre — atacable, com es va veure, per un token oblidat i una allau de trànsit.

La lliçó no és culpar l'Archive, una institució venerable i essencial: és entendre que cap institució de memòria, per sòlida que sigui, no pot garantir sola la integritat del que custodia. La resposta estructural són els manifests ancorats: l'empremta de cada col·lecció i de cada captura, amb segell de temps, publicada a una cadena que cap atac a cap servidor no pot reescriure [5]. Si els continguts es perden, l'existència i la integritat del que hi havia queden acreditades; si algú els altera, la discrepància canta. La memòria necessita còpies; la confiança en la memòria necessita ancoratges.

Les fosses que encara parlen

El front espanyol d'aquest capítol es diu Llei 14/2022, de Memòria Democràtica: l'Administració General de l'Estat va assumir la responsabilitat de cercar les persones desaparegudes durant la Guerra Civil i la dictadura, es va crear el Banc Estatal d'ADN de víctimes i es va impulsar el Mapa Integrat de Fosses, que registra 5.848 fosses localitzades, de les quals al voltant de 1.500 han estat obertes [4]. El balanç conegut el novembre de 2025: 8.941 restes localitzades i recuperades i unes 9.000 víctimes reparades — però només 70 restes plenament identificades i lliurades a les famílies, i més de 10.000 cossos encara per recuperar [4]. Cada xifra és una família que espera.

L'angle d'aquest llibre és el probatori, i és rigorosament neutral. Una exhumació és ciència forense — estratigrafia, fotografies, objectes, mostres, ADN — i la seva força depèn de la cadena de custòdia. I és, alhora, un acte exposat a tres amenaces: el dubte revisionista futur («aquestes restes no són el que diuen»), l'acusació de manipulació política i l'error humà.

La documentació ancorada protegeix el procés de totes tres. Cada estadi de l'excavació pot quedar segellat en el moment — la fotografia de cada troballa amb data certa, el registre de mostres, la cadena de custòdia fins al Banc Estatal d'ADN [4][5] —, i el resultat és un expedient que cap negacionisme futur no podrà despatxar com a «fabricat» sense negar la matemàtica, i que cap sospita de manipulació no podrà tacar sense proves. El segell no serveix una memòria contra una altra: serveix els fets contra l'oblit i contra la mentida, vinguin d'on vinguin.

La prova d'existència aplicada

Un arxiu comarcal qualsevol, una tarda de digitalització: el so dels escàners, pàgines groguenques d'un diari antic — i cada full, en néixer digital, rep la seva data certa.

1. L'arxiu ancorat

Biblioteques, hemeroteques i arxius — públics, comunitaris, d'exili — publiquen manifests ancorats de les seves col·leccions: l'empremta SHA-512 de cada document i de cada lot, amb segell de temps, a la blockchain pública [5]. L'edició silenciosa d'una notícia antiga esdevé detectable per qualsevol; la pèrdua d'un servidor no esborra l'evidència del que existia [3]; i la cita acadèmica o judicial d'un document pot verificar-se contra l'empremta original. És la mateixa lògica que el llibre ha aplicat als comunicats oficials (capítol 86), estesa al temps profund: no un arxiu únic i oficial, sinó tots els arxius, cadascun amb la seva integritat acreditada. Quan aparegui un «article de 1940» acabat de fabricar, la seva absència del corpus ancorat parlarà per ell.

2. El testimoni segellat

La generació dels supervivents s'acaba, i la UNESCO recomana treballar amb ells mentre hi són [1]. Cada testimoni enregistrat — veu, vídeo, transcripció — pot quedar segellat en vida del testimoni: empremta i data certa que acrediten que aquelles paraules existien, exactament així, en aquell moment [5]. Quan d'aquí a vint anys un negacionista digui que un testimoni «va ser fabricat a posteriori», o quan una IA generi testimonis falsos amb veu clonada [1], la diferència serà verificable: els testimonis reals tindran prioritat temporal ancorada; els fabricats, no. I el mateix val per a la memòria oral de la Guerra Civil: cada entrevista d'història oral segellada avui és un document blindat demà.

3. La fossa documentada

Cada exhumació emparada per la Llei 14/2022 [4] pot ancorar el seu expedient: fotografies de cada estrat amb data certa, actes de l'equip forense, registre de troballes, cadena de custòdia de les mostres fins al Banc Estatal d'ADN [4][5]. El resultat serveix tres causes alhora: la judicial (una cadena de custòdia impecable), la familiar (una identificació traçable — que les 70 famílies que ja han rebut les seves restes [4] esdevinguin milers, amb la mateixa certesa) i la històrica (un registre que digui, per sempre i amb matemàtica al darrere: aquí hi havia una fossa, això s'hi va trobar, i aquest n'és el registre).

4. L'horitzó pre-IA

Hi ha una finestra que es tanca: tot allò digitalitzat i ancorat abans de la maduresa de la imatge sintètica queda acreditat com a anterior — un horitzó pre-IA que separa el corpus fotogràfic verificable de tot el que vingui després. Museus, arxius fotogràfics i col·leccions familiars que ancorin avui les seves digitalitzacions [5] creen el cànon de referència contra el qual les futures imatges «d'època» fabricades [2] es podran contrastar: si una foto «de 1937» no apareix enlloc del corpus ancorat i emergeix d'aquí a uns anys, la seva absència d'història parlarà per ella. Cada any que passa sense ancorar, l'horitzó es difumina una mica més.

Els límits, dits amb claredat: el segell acredita quan es va digitalitzar o registrar un document i que no s'ha alterat des d'aleshores — no acredita que el document digui la veritat, ni substitueix la crítica de fonts, que continua sent ofici d'historiadors; no pot recuperar allò que mai no es va documentar; i la història és també interpretació — el segell protegeix els documents i els fets, no cap relat únic sobre els fets.

La promesa i el perill

La promesa és una memòria col·lectiva amb integritat verificable: arxius que no es poden editar en silenci [3], testimonis amb prioritat temporal sobre les seves falsificacions [1], fosses amb expedients inatacables [4] i un cànon fotogràfic pre-IA contra la història fabricada [2]. La veritat del passat deixaria de dependre d'una sola veu o d'un sol servidor: es validaria contra un teixit d'empremtes obert a qualsevol.

Els perills demanen la mateixa claredat.

El primer és **l'arxiu únic**. Si l'ancoratge esdevé monopoli d'un «arxiu oficial de la veritat», haurem creat el ministeri que Orwell temia. La resposta és la pluralitat: totes les memòries — institucionals, comunitàries, d'exili, dissidents — han de poder ancorar els seus fons. El segell acredita integritat i data; mai autoritat, mai versió única.

El segon és **la memòria contra l'oblit personal**. Els arxius contenen dades de persones vives i de famílies. Ancorar no és publicar: només empremtes a la cadena, amb l'accés regulat pels marcs de cada arxiu i pels drets de les persones esmentades. La immutabilitat protegeix la integritat del document; no pot servir per negar drets a ningú.

El tercer és **el fetitxe de la immutabilitat**. La història es corregeix: apareixen documents nous i es reinterpreten els vells. L'ancoratge documenta versions i dates; no congela el coneixement. Confondre «segellat» amb «definitiu» seria trair l'ofici que es vol protegir — cada nova troballa s'ancora com a nova versió, i el debat continua.

I el quart és **el tecnosolucionisme memorial**. Cap cadena de blocs no ensenya història. Contra el negacionisme, la primera línia són l'escola, els historiadors i l'alfabetització crítica que reclama la UNESCO [1]; el segell només garanteix que, quan calgui demostrar què existia, es pugui. Una societat que no vulgui recordar no se salvarà per criptografia.

És hora d'actuar

El passat no es pot canviar; la seva prova, sí — i per això cal segellar-la ara.

Per a arxius, biblioteques i hemeroteques: publiqueu manifests ancorats de les col·leccions [3][5]; que cada edició silenciosa sigui detectable i que cap servidor caigut no s'endugui l'evidència.

Per a les institucions de memòria i els equips forenses: ancoreu els expedients d'exhumació — fotos, troballes, cadena d'ADN [4][5]; les famílies mereixen certesa, i la història, un registre inatacable.

Per a supervivents, famílies i projectes d'història oral: enregistreu i segelleu els testimonis ara, en vida [1][5]; la prioritat temporal serà el seu escut quan arribin les falsificacions.

Per a museus i col·leccions fotogràfiques: ancoreu les digitalitzacions — l'horitzó pre-IA es tanca cada dia una mica més [2][5].

Per als mitjans: etiqueteu tota imatge sintètica de fets o personatges reals [2] i ancoreu les hemeroteques — la vostra credibilitat retrospectiva també és patrimoni.

Per a les empreses d'IA i els legisladors: seguiu les recomanacions de la UNESCO — treballar amb supervivents, educadors i historiadors [1] — i doteu la Llei de Memòria Democràtica [4] dels mitjans forenses i d'ancoratge que facin la seva feina irreversible.

Una màquina va inventar un «Holocaust per ofegament» que mai no va existir [1]. Que quan algú el «documenti», el món pugui respondre amb un corpus ancorat que demostri què és memòria i què és fabricació. Pels qui ja no poden testificar, **time2act**.

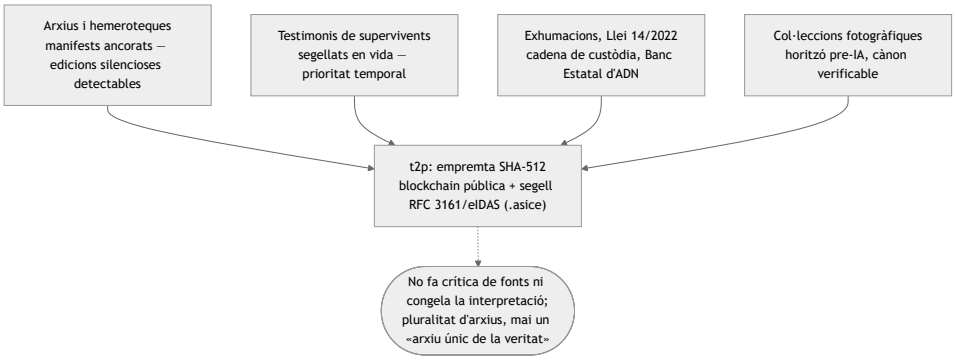


Figura 61.1 — Quatre fronts d'una mateixa defensa (empremta SHA-512, segell de temps RFC 3161/eIDAS, ancoratge a la blockchain pública, .asice): els manifests ancorats dels arxius i hemeroteques (edicions silencioses detectables), els testimonis de supervivents segellats en vida (prioritat temporal contra la fabricació), els expedients d'exhumació amb cadena de custòdia ancorada (Llei 14/2022, Banc Estatal d'ADN) i l'horitzó pre-IA de les col·leccions fotogràfiques (el cànon verificable contra la història sintètica). Límits: el segell no fa crítica de fonts ni congela la interpretació; pluralitat d'arxius, mai un «arxiu únic de la veritat». Fonts: UNESCO/CJM; Maldita.es; Internet Archive (bretxa 2024); Llei 14/2022.

---

[1] UNESCO — *New UNESCO report warns that Generative AI threatens Holocaust memory* (juny de 2024, amb el Congrés Jueu Mundial; ChatGPT i el fals «Holocaust per ofegament»; cites de testimonis fabricades per Bard; simplificació excessiva; recomanacions a tecnològiques i sistemes educatius); comunicat de premsa en castellà (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 febrer de 2025; imatges sintètiques de fets i personatges reals publicades sense etiqueta; alteració de la percepció històrica i desconfiança en els mitjans). 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 filtrats; token de GitLab exposat des de finals de 2022; DDoS simultani sobre la Wayback Machine); NPR — *Hackers steal information from 31 million Internet Archive users*; Hispasec — *Internet Archive sufre su segunda brecha* (més de 800.000 tiquets de suport exposats). 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 novembre de 2025; 8.941 restes localitzades i recuperades; només 70 identificades i lliurades; Mapa Integrat de Fosses: 5.848 fosses, ≈1.500 obertes; Banc Estatal d'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 producte (empremta SHA-512 a l'origen; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; manifests per lots; contingut als sistemes de cada arxiu, només empremtes a la cadena). Vegeu els capítols 13 i 15; els comunicats oficials, al capítol 86; l'evidència de crims de guerra, al capítol 20. ↩

Whistleblowing: provar sense delatar-se

«Una paraula de veritat pesa més que el món sencer.»

— Aleksandr Soljenitsin, conferència Nobel (1970)

El juny de 2017, una contractista de la NSA de vint-i-cinc anys anomenada Reality Winner va imprimir un informe classificat sobre la ingerència russa en les eleccions nord-americanes i el va enviar per correu al mitjà *The Intercept*. La redacció en va publicar un **escaneig de la còpia impresa**. Pocs dies després, l'FBI trucava a la seva porta. El document la va delatar amb una traïció invisible: uns **punts grocs minúsculs** que gairebé totes les impressores làser de color incrusten en cada full —el codi d'identificació de la màquina—, i que, descodificats amb l'eina de la Electronic Frontier Foundation, revelaven el model de la impressora, el seu número de sèrie (29535218) i **la data i l'hora exactes d'impressió: 9 de maig de 2017, a les 6:20** [6][8]. Els registres interns de la NSA mostraven que només sis persones havien accedit a l'informe, i només una l'havia imprès. Reality Winner va ser condemnada a seixanta-tres mesos de presó, la pena més llarga mai imposada als Estats Units a una font periodística [7].

El seu cas conté l'advertència que vertebra aquest capítol i el converteix en un mirall de tot el llibre: **l'anonimat és difícil, i cap tecnologia NO pot salvar un denunciant descuidat**. Però també planteja el repte més delicat de tots: com pot algú provar que un document és autèntic —perquè el poder no el pugui descartar com una falsificació— **sense, alhora, delatar-se a si mateix**?

La tensió irreductible

La societat ha reconegut que els denunciants són essencials i ha construït defenses. La **Directiva europea de protecció dels denunciants** de 2019 va convertir la confidencialitat de la identitat de qui denuncia en una **obligació jurídica**, amb canals segurs i protecció contra les represàlies; el 2025, el Tribunal de Justícia de la UE va multar amb uns 39 milions d'euros cinc estats per no transposar-la a temps —Alemanya amb 34 milions [2]. I la **Freedom of the Press Foundation**, l'ONG nord-americana, manté **SecureDrop**, un sistema de lliurament anònim de documents a través de la xarxa Tor que fan servir més de seixanta redaccions —el *New York Times*, el *Guardian*, el *Washington Post*. La seva filosofia és reveladora: la protecció de la font no és només legal, sinó **arquitectònica** —el sistema està dissenyat perquè el periodista mai no conegui la identitat ni les dades de xarxa de l'informant [3].

Però l'arquitectura de la vigilància és igual d'omnipresent. Com va demostrar la EFF al descodificar els punts de les impressores, el paper que surt d'una màquina ja «signa» qui i quan el va imprimir. I no és l'únic vector: l'**estilometria** —l'empremta de l'estil d'escriptura— pot atribuir l'autoria d'un text amb una precisió del 80 al 95 % [9]. La tensió, doncs, és irreductible: provar **què** sense revelar **qui**.

Que la veritat sobrevisqui sense la font

I tanmateix, es pot fer. La prova més gran de la història ho demostra. Els **Panama Papers** — 11,5 milions de documents, 2,6 terabytes del despatx Mossack Fonseca — van ser lliurats per una font que només es va identificar com a «John Doe», i va imposar una regla absoluta: únicament canals xifrats, mai cap trobada cara a cara [4]. Més de tres-cents cinquanta periodistes de vuitanta països, coordinats pel consorci internacional ICIJ, van verificar-ne l'autenticitat i van publicar les revelacions, que van fer caure un primer ministre i van guanyar un premi Pulitzer. Després d'una dècada, la identitat de John Doe continua sent desconeguda. En el seu manifest, va reclamar per als denunciants legítims «immunitat davant de la represàlia governamental, sense excepcions» [5]. La lliçó és poderosa: la verificabilitat i l'anonimat poden coexistir. Es va poder provar que 2,6 terabytes de documents eren genuïns sense necessitat d'identificar qui els havia filtrat.

La prova d'existència com a escut: el que NO se segella

És aquí on **t2p** ofereix una eina amb un disseny invertit respecte a tota la resta del llibre. El denunciant calcula l'**empremta SHA-512** del document **al seu propi dispositiu** i ancora *només* aquella empremta a la **blockchain pública**, amb un **segell de temps RFC 3161** conforme a eIDAS. Això prova dues coses verificables per qualsevol —que el document **és autèntic i no s'ha alterat**, i que **existia abans d'un instant determinat**— sense pujar el document ni cap dada personal.

I aquí entra la peça clau d'aquest capítol: la **divulgació selectiva**. Mitjançant proves de coneixement zero, un periodista o un tribunal poden verificar que el document que han rebut coincideix amb l'empremta segellada —és a dir, que és genuí i anterior a la filtració— **sense aprendre qui el va segellar**. Es prova una propietat del document, no la identitat de l'autor. Això desmunta la defensa del «document fals o manipulat»: l'organització acusada no pot al·legar que el filtrador el va fabricar després dels fets, perquè l'empremta i el segell l'ancoren a una data anterior.

Però el més important és el que **no** se segella. A diferència del flux forense de la resta del llibre, aquí s'ometen deliberadament el GPS, la prova de vida i les metadades del dispositiu —precisament allò que delataria. El contenidor **.asice** es pot lliurar al periodista **fora de línia**, sense que la identitat real del filtrador toqui mai la xarxa. És el gir conceptual d'aquesta obra: la **mateixa** tecnologia que als capítols sobre fotoperiodisme i drets humans era un **risc** —ancorar metadades pot delatar una font—, configurada amb divulgació selectiva i omissió de metadades, es converteix en un **escut**. La diferència no és la cadena de blocs, sinó el disseny de què hi entra i què es prova sense revelar.

I cal dir el límit amb tota la cruesa, perquè aquí és vital i tanca el cercle del llibre. **L'anonimat és difícil, i la tecnologia no salva un filtrador descuidat.** El cas de Reality Winner ho crida: ni el xifratge més fort no hauria servit quan la van trair els punts de la impressora, els plecs del paper i els registres d'accés interns. Una empremta prova existència, integritat i moment —**no** que el contingut sigui veritat ni que s'obtingués lícitament: «escombraries a l'entrada, escombraries a la cadena». I queden vectors de desanonimització que t2p no resol: les metadades de xarxa (cal usar Tor o SecureDrop a banda), l'estilometria, les marques físiques del suport. La regla d'or d'aquest front és la més contraintuïtiva de tot el llibre: el que protegeix **és el que es decideix no segellar**.

La promesa i el perill

La promesa és preciosa per a la democràcia. Una eina que permeti a un denunciant provar que un document és autèntic i anterior a una data, sense revelar qui és, donaria al periodisme d'investigació i als tribunals una evidència incontestable i protegiria alhora la persona que va arriscar-ho tot per dir la veritat. És fer que la veritat sobrevisqui sense que la font caigui.

El perill, aquí, és sobretot el de la **falsa seguretat**. Vendre la prova d'existència com una garantia d'anonimat seria irresponsable i podria costar la llibertat d'algú: l'anonimat depèn d'una disciplina —Tor, dispositius nets, cura amb el suport físic i l'estil— que cap segell no substitueix. El segell tampoc no fa veritable un document fals ni legitima una obtenció il·lícita. La prova d'existència és una capa que protegeix *si i només si* es dissenya per ometre el que delata; mai una bala de plata contra una maquinària de vigilància que el cas Winner va mostrar implacable.

A més, el segell amb hora esdevé una **àncora temporal** que pot ser explotada com a instrument de coacció. En un procés d'investigació, aquell que controla l'horari del segell pot demostrar que un document va ser «segellat» en un moment concret, i aquest rastre pot servir per identificar el moment exacte en què una persona va exposar informació sensible. Carissa Véliz ha mostrat com aquesta pressió es tradueix en autoinhibició: «entre un terç i dos terços dels escriptors van evitar certs temes per por de la vigilància governamental»[11]. El registre immutable, que suposadament protegeix la veritat, pot acabar convertint-se en una amenaça per a la llibertat d'expressió: el simple fet de saber que el segell deixa constància del moment pot dissuadir la denúncia legítima i obligar els potencials informants a autocensurar-se, minant així l'objectiu mateix de preservar la veritat.

És hora d'actuar

Per tant, per als denunciants: comprovar l'autenticitat del que revelen sense fer ancoratge del que els delata i combinar-ho amb canals segurs com SecureDrop i una disciplina estricta. Per a periodistes i plataformes de filtració: oferir divulgació selectiva perquè es pugui verificar un document sense conèixer-ne la font. Per als legisladors: complir i reforçar la directiva de protecció dels denunciants, que massa estats van transposar tard. I per a la ciutadania: recordar que, sense qui s'atreveix a parlar —i sense eines que el protegeixin—, molta corrupció no es destaparia mai.

Uns punts grocs invisibles van enviar Reality Winner a la presó; un anònim anomenat John Doe va sacsejar el món i continua sent lliure. La diferència, sovint, és el que es revela sense voler.

Donar a qui denuncia la manera de provar la veritat **sense delatar-se** —segellant el document i amagant la persona— és, en el front que tanca aquesta part, time2act.

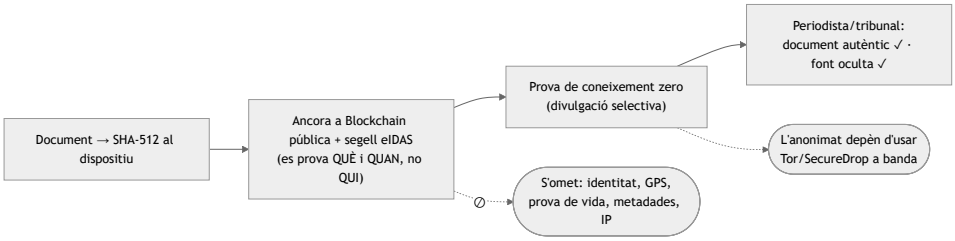


Figura 62.1 — El denunciant calcula l'empremta SHA-512 del document al seu dispositiu i l'ancora a la blockchain pública amb segell de temps eIDAS: es prova QUÈ i QUAN, no QUI. La capa que delataria — identitat, GPS, prova de vida, metadades, IP— s'omet deliberadament: el que protegeix és el que no se segella. Amb una prova de coneixement zero, el periodista o el tribunal verifiquen que el document és autèntic i anterior a una data, sense conèixer la font. Límit: la cadena no bloqueja els punts de rastreig de la impressora (cas Winner), l'estilometria ni les metadades de xarxa. Fonts: ICIJ (Panama Papers); EFF; Freedom of the Press Foundation.

---

[1] EUR-Lex — *Directiva (UE) 2019/1937 sobre la protecció dels denunciants* (confidencialitat de la identitat; canals segurs; terminis). 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* (març 2025; ~39 M€; Alemanya 34 M€; Estònia 500.000 € + 1.500 €/dia). 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* (més de 60 redaccions; servei ocult de Tor; protecció arquitectònica de la font). https://securedrop.org/overview/ ↩

[4] ICIJ — *Panama Papers* (11,5 milions de documents; 2,6 TB; >350 periodistes; la font «John Doe»). https://www.icij.org/investigations/panama-papers/ ↩

[5] OCCRP — *John Doe: «The Revolution Will Be Digitized»* (manifest de la font dels 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* (punts de rastreig de la impressora; sèrie 29535218; 9-maig-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 més llarga als EUA per a una font de premsa). 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* (codi d'identificació de la màquina). https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots ↩

[9] Wikipedia — *Stylometry / Adversarial stylometry* (atribució d'autoria amb un 80-95 % de precisió). https://en.wikipedia.org/wiki/Stylometry ↩

[10] Wikipedia — *Frances Haugen* (filtració de Facebook; va decidir revelar la seva identitat). https://en.wikipedia.org/wiki/Frances_Haugen

[11] Carissa Véliz — *The Ethics of Privacy and Surveillance* (Oxford UP, 2024). ↩

Integritat de la recerca: la dada que ningú pot repetir

«El primer principi és que no t'has d'enganyar a tu mateix — i tu ets la persona més fàcil d'enganyar.»

— Richard Feynman, «Cargo Cult Science», Caltech (1974)

L'abril del 2002, la física Lydia Sohn, llavors a Princeton, comparava les gràfiques d'un jove investigador dels Bell Labs anomenat Jan Hendrik Schön. Les mesures es presentaven com preses en dispositius diferents i a temperatures molt diverses; però mostraven una característica impossible: **exactament el mateix soroll**. El soroll d'una mesura electrònica és aleatori, únic com una empremta dactilar; que dues mesures independents comparteixin el mateix patró només podia indicar una cosa. Sohn, junt amb Paul McEuen de Cornell, acabava de destapar el major frau de la física moderna: Schön havia copiat i enganxat les dades. El comitè Beasley va confirmar una mala conducta en setze de vint-i-quatre càrrecs i es van retirar prop de vint-i-nou articles, vuit d'ells a *Science* i set a *Nature* [6]. L'any anterior, Schön havia arribat a publicar, de mitjana, un article nou cada vuit dies.

Aquell soroll copiat planteja la pregunta central d'aquest capítol. No es tracta de qui va tenir primer la idea ni si un títol és autèntic —això correspon al capítol 19—, sinó d'una qüestió més fonamental: **aquesta dada, aquesta imatge, existia sense manipular en el moment d'adquirir-la?** Perquè la ciència, el sistema de coneixement més fiable que hem construït, es recolza en una cadena de proves —píxels, blots, fitxers crus— que, com les del frau, poden ser fabricades.

La factura de la ciència que no es pot repetir

L'escala del problema és vertiginosa. El 2023 es van retractar **més de deu mil articles científics**, un rècord històric; el gruix el va aportar l'editorial Hindawi, filial de Wiley, que en va retirar més de vuit mil de números especials infiltrats per *paper mills* —empreses que fabriquen i venen articles falsos [1]. Com adverteixen **Ivan Oransky i Adam Marcus**, cofundadors de **Retraction Watch**, la base de dades de referència sobre retractacions, aquesta xifra és «només la punta de l'iceberg»: el sistema de correcció va molt per darrere del frau industrialitzat.

I el que no és frau directe sovint tampoc no es pot repetir. L'empresa Amgen va aconseguir reproduir només l'**11 %** de cinquanta-tres estudis oncològics de referència; el Reproducibility Project: Cancer Biology, publicat a *eLife* el 2021 després de gairebé una dècada de feina, va trobar que els efectes replicats eren de **mediana un 85 % més petits** que els originals [10]. A tot això s'hi suma la manipulació deliberada: el psicòleg Diederik Stapel acumula cinquanta-vuit articles retractats per haver-se inventat conjunts de dades sencers —quan li van preguntar pels col·legis on suposadament havia fet els experiments, va admetre que **aquells col·legis no existien**—, i el rècord individual l'ostentava el juliol de 2023 l'anestesiòleg Joachim Boldt, amb cent vuitanta-quatre retractacions. Quan la prova és fàcil de fabricar i difícil de verificar, tot l'edifici trontolla.

El frau abans i després de prémer «capturar»

El frau de dades entra per dues portes. La primera és la **manipulació de la imatge** un cop feta. La microbiòloga **Elisabeth Bik**, en el seu estudi fundacional amb Arturo Casadevall i Ferric Fang (*The Prevalence of Inappropriate Image Duplication in Biomedical Research Publications*, mBio, 2016), va inspeccionar visualment **20.621 articles** de quaranta revistes i va trobar que el **3,8 %** contenien figures problemàtiques, la meitat amb senyals de manipulació deliberada: bandes de Western blot duplicades, girades, retallades i enganxades [2]. I com adverteix Bik, com que només va mirar un tipus de dada, la prevalença real és gairebé segur més alta. La bona notícia és que el cribratge automàtic funciona: en un pilot d'un any, la American Society for Microbiology va passar 2.627 manuscrits acceptats per l'eina ImageTwin i en va detectar 410 amb problemes d'imatge, fins al punt de revocar l'acceptació a sis [3]. El cas més sonat el va destapar des d'un poble de Gal·les el biòleg **Sholto David**, que el gener de 2024 va publicar al seu blog imatges de papers del Dana-Farber Cancer Institute, de Harvard, que semblaven retallades i enganxades; l'institut va demanar retractar sis estudis i corregir-ne trenta-un. Gairebé dos anys després, el desembre de 2025, el Dana-Farber pagava **quinze milions de dòlars** per tancar una demanda federal, admetent que imatges i dades s'havien «tergiversat o duplicat» en sol·licituds de subvenció als instituts nacionals de salut [4].

La segona porta és més subtil: el **canvi de variables**. L'equip de **Ben Goldacre**, a la Universitat d'Oxford, va monitorar amb el projecte COMPare seixanta-set assaigs clínics publicats a les cinc grans revistes mèdiques i va descobrir que, de mitjana, només el **76,3 %** dels desenllaços primaris preespecificats es reportaven correctament, mentre s'hi afegien 365 desenllaços nous que ningú no havia anunciat abans [8]. És el que es coneix com a *outcome-switching*: mesurar una cosa, no trobar res i reportar una altra com si fos el que es buscava. La defensa contra això és el **pre-registre**: dipositar el protocol abans de començar. Quan els Estats Units el van fer obligatori per als assaigs de fàrmacs el 2007, el registre va passar del 64 % al 100 % i el report de resultats, del 10 % al 100 %. I el **Center for Open Science**, impulsat per Brian Nosek, ha estès els *Registered Reports* —on la revista accepta l'estudi pels seus mètodes, abans de conèixer els resultats— de noranta-una revistes el 2018 a més de tres-centes el 2022. La idea de fons és lluminosa: si la decisió de publicar es pren *abans* de veure els resultats, desapareix l'incentiu per maquillar-los.

La prova d'existència: segellar la dada en l'adquisició

És aquí on **t2p** actua amb precisió quirúrgica, perquè ataca el problema en el seu origen exacte. En l'instant de l'**adquisició** —quan el microscopi confocal, el lector de gels, el citòmetre o el seqüenciador genera el fitxer cru—, es calcula al propi dispositiu l'**empremta SHA-512** del fitxer original i s'ancora a la **blockchain pública** amb un **segell de temps RFC 3161** conforme a eIDAS. Queda un registre inalterable: «aquest píxel exacte existia en aquesta data i hora». Qualsevol retall, gir, còpia de banda o ajust de contrast posterior produeix una empremta diferent que ja no coincideix amb la segellada en origen: la manipulació es torna **matemàticament detectable i datable**. El soroll copiat de Schön no hauria sobreviscut a aquesta comprovació.

El mateix s'aplica al **pre-registre amb data certa**: el protocol, els desenllaços primaris i el pla d'anàlisi se segellen *abans* de recollir cap dada, de manera que si després apareixen desenllaços nous, la data del contenidor **.asice** demostra que no estaven preespecificats —és l'equivalent criptogràfic del que COMPare necessita per caçar l'*outcome-switching*, però verificable sense dependre d'un registre central. I la combinació de **GPS forense** i **prova de vida** ancora la captura a un lloc, un moment i un operador humà reals: contra el frau de Stapel, exigiria coordenades i hora autèntiques en lloc d'una full inventada en un despatx.

Cal dir el límit amb tota la cruesa, perquè aquí és el cor de la qüestió. «Escombraries a l'entrada, escombraries a la cadena»: el segell garanteix que un fitxer existia sense alterar en una data i un lloc, però **no garanteix que la dada sigui veritat ni que l'experiment sigui bo**. Un investigador deshonest pot segellar en origen una dada **fabricada per endavant** —números inventats al mateix instrument, una mostra falsa, un control trucat—: l'empremta serà perfecta i la procedència, impecable, i tanmateix la ciència serà frau. El segell tampoc no detecta els errors honestos ni els problemes de reproductibilitat —un resultat pot estar perfectament datat i ser irreproduïble per mala metodologia—, ni substitueix l'ull expert de Bik o de David, que cacen la manipulació *anterior* a prémer «capturar». La prova d'existència trasllada el punt de confiança del «em crec la teva figura» al «em crec la teva adquisició», un avenç real contra la manipulació posterior, però **no tanca la fabricació en origen**.

La promesa i el perill

Així, la promesa és immensa per a un sistema que mou bilions en finançament i del qual depenen la medicina i la tecnologia. Segellar la dada crua en l'adquisició i el protocol abans de l'experiment faria molt més difícil duplicar una banda, reutilitzar soroll o afegir desenllaços posteriorment, i donaria als revisors i als comitès d'integritat una cadena de custòdia verificable en lloc d'una figura que cal creure's. En una ciència corcada per les *paper mills*, fer la prova inalterable és protegir el fonament del coneixement.

El perill demana el matís habitual. Primer, ja dit: el segell no fa veritable una dada falsa; si la fabricació passa abans de la captura, la cadena immortalitza la mentida amb procedència impecable. Segon, l'excés de confiança: cap empremta substitueix la reproducció independent ni l'ull expert. I tercer, l'adopció: si el segellat és opcional o posterior a l'adquisició, perd gairebé tot el seu valor, i l'absència de segell no prova frau per si sola. La prova d'existència és una eina poderosa contra la manipulació i el canvi de variables, però no constitueix un certificat de veritat científica.

És hora d'actuar

Segellar el fitxer cru en capturar-lo i pre-registrar el protocol amb data certa garanteix la integritat demostrable de les dades.

Les revistes han d'exigir la dada crua segellada i comparar-ne l'empremta, tal com es fa amb el cribatge automàtic d'imatges.

Els finançadors han de condicionar les subvencions a una cadena de custòdia verificable de les dades, cosa que hauria impedit el cas Dana-Farber.

Les institucions han de protegir els que, com Sholto David, destapin la manipulació i no penalitzar-los.

Un soroll copiat va fer caure el principal frau de la física quan algú va comparar dues empremtes. Assignar a cada dada científica una empremta segellada al néixer —sense oblidar que la veritat final requereix repetir l'experiment— és, en aquest front del coneixement, time2act.

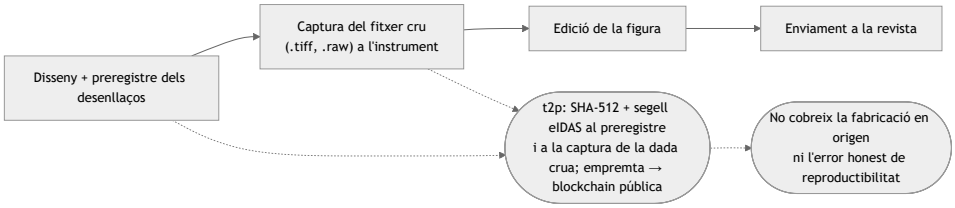


Figura 63.1 — Al llarg de la vida d'un experiment, el frau pot entrar al disseny (canvi de variables: COMPare va trobar que només el 76,3 % dels desenllaços primaris es reportaven bé), a la mostra (fabricació en origen, com Stapel), a la captura del fitxer cru o a l'edició de la figura (duplicació de bandes: Bik va trobar-ne en el 3,8 % de 20.621 articles). El segell en l'adquisició —empremta SHA-512 + segell eIDAS— cobreix el pre-registre del protocol i la captura de la dada crua, i fa detectable qualsevol edició posterior; però no demostra que la dada fabricada en origen sigui veritat. Fonts: 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 i Ferric Fang — *The Prevalence of Inappropriate Image Duplication in Biomedical Research Publications* (mBio, 2016; 20.621 articles, 3,8 %). https://journals.asm.org/doi/10.1128/mbio.00809-16 ↩

[3] American Society for Microbiology / mBio — *Pilot d'ImageTwin* (2.627 manuscrits; 410 amb problemes d'imatge; 6 acceptacions revocades). 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* (imatges/dades tergiversades en subvencions als 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; dimissió del president). https://boardoftrustees.stanford.edu/news/board-trustees-statement-release-report-and-announcements

[6] American Physical Society — *The Schön scandal* (comitè Beasley; mala conducta en 16 de 24 càrrecs). https://www.aps.org/apsnews/2022/08/september-2002-schon-scandal-report ↩

[7] Retraction Watch (Ivan Oransky i Adam Marcus) — *The new retraction record holder* (Joachim Boldt, 184 retractacions, juliol 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, Universitat d'Oxford) — *COMPare: outcome-switching en assaigs clínics* (Trials, 2019; 76,3 % de desenllaços primaris ben reportats). https://pmc.ncbi.nlm.nih.gov/articles/PMC6375128/ ↩

[9] Center for Open Science (Brian Nosek) — *Registered Reports* (de 91 a més de 300 revistes; el protocol abans dels resultats). https://www.cos.io/initiatives/registered-reports

[10] eLife — *Reproducibility Project: Cancer Biology* (Amgen, 11 % de 53 estudis; efectes replicats un 85 % més petits). https://elifesciences.org/articles/71601 ↩

Pensions: provar que encara hi ets, avui

«La vellesa només és honorada a condició que es defensi, mantingui els seus drets, no se sotmeti a ningú i governi fins a l'últim alè el seu propi domini.»

— Ciceró, De Senectute, §38 (44 aC)

El 28 de juliol de 2010, uns funcionaris de Tòquio van anar a casa de Sogen Kato per felicitar-lo: segons el registre, era l'home més vell de la ciutat, amb cent onze anys, i s'acostava el Dia del Respecte als Grans. Quan van obrir la seva habitació, hi van trobar un cos momificat en pijama, envoltat de diaris de 1978. Kato feia trenta-dos anys que era mort dins de casa seva mentre la seva **pensió de supervivència** seguia caient, mes rere mes, al compte familiar. La família havia cobrat indegudament uns 9,5 milions de iens; la seva neta va ser condemnada [1]. El cas va destapar un forat nacional: la policia japonesa no va poder confirmar si **234.354 persones** que figuraven com a centenàries seguien vives —77.118 d'elles haurien superat els cent vint anys—, perquè els registres familiars portaven dècades sense actualitzar [2].

Aquell cos momificat conté la pregunta d'aquest capítol, que no és la del capítol 47 —«qui ets?», que es respon un cop— ni la del capítol 49 —«ha arribat l'ajuda?»—, sinó una de més persistent: **segueixes viu, avui, i ho tornaràs a estar d'aquí a tres mesos?** Perquè una pensió no és un acte únic, sinó un dret que es cobra durant anys, i el frau més silenciós no és un esdeveniment, sinó un **no-esdeveniment**: una mort que ningú no declara.

L'Estat que no sap qui ha mort

El problema és universal i car. Als Estats Units, un informe de l'inspector general de la Seguretat Social de 2025 va trobar que el rebuig automàtic d'avisos de defunció va provocar **327 milions de dòlars** en pagaments a persones mortes; un altre informe ja havia detectat **6,5 milions** de titulars de número de Seguretat Social amb cent dotze anys o més **sense data de defunció** als seus registres [3]. A Grècia, sota la pressió de la troica, un cens de pensionistes va suspendre prestacions a unes **200.000 persones** que no hi tenien dret o ja eren mortes —entre elles, unes nou mil que figuraven com a «centenàries» cobrant jubilació—, amb un estalvi de fins a **800 milions d'euros l'any** [4]. I a Sud-àfrica, l'agència de subsidis SASSA va admetre haver pagat uns **140 milions de rands a prop de 75.000 beneficiaris difunts** [5]. L'arrel de tot és la mateixa: un **registre civil que no sap de manera fiable qui ha mort**.

I hi ha un matís incòmode que cal dir: bona part del frau no el comet el mort, sinó qui controla el sistema. A Sud-àfrica, una anàlisi de l'Institute for Economic Justice atribueix prop del 75 % del frau de subsidis a funcionaris i intermediaris, no als beneficiaris: insiders que creen «beneficiaris fantasma», dupliquen targetes i canvien dades bancàries. Per això, com adverteix l'Associació Internacional de la Seguretat Social (ISSA) en la seva anàlisi *Proof of life in international social security* [9], la prova de vida ha d'evitar dependre d'un repositori central que es pugui manipular des de dins.

Provar que segueixes viu, avui i d'aquí a tres mesos

La resposta tradicional —fer venir el pensionista a una finestreta un cop l'any— és humiliant per als grans i impossible per als qui viuen lluny. Diversos països han buscat alternatives digitals. L'Índia va crear el certificat digital de vida **Jeevan Pramaan**, que l'any passat va generar uns 19 milions de certificats, més d'onze milions mitjançant autenticació facial, estalviant la compareixença física [6]. El Brasil va invertir la lògica amb la seva *prova de vida*, creuant bases de dades públiques. I Espanya, amb l'app **VIVESS**, permet als pensionistes residents a l'estranger acreditar que segueixen vius sense viatjar.

Però aquí apareix una amenaça nova. Com adverteix la revista jurídica brasilera **Conjur** en el seu article *Deepfakes, provas digitais e fraudes no INSS* [10], els deepfakes amenacen amb un «apocalipsi epistèmic» en què un vídeo deixa de servir com a prova; ja hi ha falsos agents que recullen la cara i la veu dels jubilats «per a la prova de vida». La lliçó connecta amb tot aquest llibre: no n'hi ha prou amb «un vídeo creïble»; cal una prova **verificable criptogràficament**.

La prova d'existència recurrent: el repte que el mort no pot respondre

És aquí on **t2p** ofereix una mecànica feta a mida d'aquest problema. En cada cicle d'atestació —mensual, trimestral o anual—, el pensionista fa un **gest de vivacitat** al seu dispositiu: girar el cap, dir una frase, respondre un repte actiu anti-suplantació. El dispositiu calcula localment l'**empremta SHA-512** del paquet format per {prova de vivacitat + **repte del dia** + marca de temps + GPS forense}, l'ancora a la **blockchain pública** amb un **segell RFC 3161** conforme a eIDAS i ho tanca en un contenidor **.asice** verificable fora de línia. El que queda registrat a la cadena no és la cara, sinó **la prova que un humà viu va respondre a un repte irrepetible en un instant i un lloc concrets**.

La clau és el **repte fresc**, un valor aleatori del dia que actua com a antídot contra la reutilització: una gravació de fa sis mesos no conté la frase d'avui, i la seva empremta no coincidirà. Això ataca de ple el frau del pensionista fantasma —**el mort no pot respondre al repte d'avui**—, mentre el GPS i la marca de temps detecten patrons impossibles, com un mateix dispositiu atestant cinquanta beneficiaris el mateix minut. I tot això **sense base biomètrica central**: a diferència d'Aadhaar o de les bases del sistema brasiler, la plantilla biomètrica **no surt mai del dispositiu**; a la cadena només hi viu una empremta. No hi ha cap honeypot per robar. A més, el contenidor es genera fora de línia i s'ancora quan hi ha xarxa, just el que necessiten els pensionistes rurals o a l'estranger que avui fracassen en els sistemes presencials.

Cal dir el límit amb tota la cruesa, perquè aquí és delicat. «Escombraries a l'entrada, escombraries a la cadena»: t2p pot certificar de manera infalsificable que un humà viu va respondre a un repte únic, però **no garanteix que aquest humà sigui el beneficiari legítim** si l'alta inicial va ser fraudulenta o si un cuidador coacciona la persona. Si un familiar obliga un ancià viu a fer el gest per seguir cobrant una pensió a la qual no té dret, la cadena registrarà una prova de vida perfectament vàlida: l'empremta és honesta sobre el que va veure el sensor, no sobre la legitimitat jurídica del cobrament. Segon, **no resol el problema invers**: com mostra l'operació LEAP del sistema britànic —**119.050 pagaments insuficients per 736 milions de lliures** [8], amb més de quinze mil persones que ja no es podran localitzar perquè han mort—, sovint el dany real és l'Estat que **deu diners i no els paga**. Provar que segueixes viu no obliga l'administració a calcular bé el teu dret. I tercer, la vivacitat no és infal·lible i la barrera tecnològica **exclou**: com documenta el diari indi **The Wire** [7], hi ha ancians a qui es nega la pensió perquè les seves empremtes desgastades no casen amb la base biomètrica —un cas, el d'una dona de vuitanta-tres anys, va acabar en mort després de setze mesos sense pensió ni ració. Per això l'autenticació per empremta es va acabar fent **no obligatòria**. Exigir un gest digital a qui té demència, no té telèfon o no té cobertura reprodueix la bretxa digital; la prova periòdica ha de conviure amb una via assistida i no punitiva, o es converteix en una màquina de suspendre pensions als més febles.

La promesa i el perill

La promesa és humana i quantificable. Una prova de vida recurrent, verificable i sense base central faria gairebé impossible el cobrament després d'una mort no declarada —el forat de Tòquio, d'Atenes, de Pretòria—, sense convertir els grans en una població fitxada ni obligar-los a fer cua. En sistemes que paguen pensions a centenars de milions de persones, segellar la vivacitat en el temps és protegir alhora les arques públiques i la dignitat de qui cobra.

El perill demana els matisos que hem dit. El primer, la coacció i l'alta fraudulenta, que cap segell no resol. El segon, no confondre la prova de vida amb el control d'elegibilitat ni amb la qualitat del registre de defuncions, que és l'arrel del problema. I el tercer, sobretot, la inclusió: una eina pensada contra el frau no pot acabar excloent precisament els més vulnerables. La prova d'existència endureix l'esglaó «segueix viu i present, avui?», que és exactament on fallen els pensionistes fantasma, però no substitueix ni la política d'inclusió ni un registre civil que sàpiga qui ha mort.

És hora d'actuar

Per als **fons de pensions i la seguretat social**: adoptar una prova de vida recurrent amb repte fresc i sense base biomètrica central, perquè el mort no pugui cobrar i el viu no hagi de viatjar. Per als **registres civils**: tancar el forat d'origen —saber de manera fiable qui ha mort—, que és la causa dels fons. Per als **reguladors**: exigir una via assistida i no punitiva per a qui no pot fer el gest, i vigilar que la prova de vida no es converteixi en exclusió. I per als **mateixos pensionistes i les seves famílies**: una eina que demostri que segueixen vius sense lliurar la seva biometria a cap servidor.

Un home va seguir cobrant la pensió trenta-dos anys després de morir perquè ningú no el va obligar a provar que era viu. Donar a cada pensionista una manera de demostrar, una vegada i una altra, que encara

hi és —amb un repte que el mort no pot respondre i sense fitxar el viu— és, en aquest front que toca la vellesa de tots, time2act.

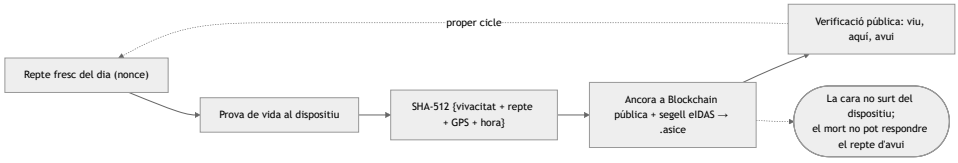


Figura 64.1 — Cada cicle d'atestació parteix d'un repte fresc del dia (nonce); el pensionista fa el gest de vivacitat al dispositiu; es calcula localment l'empremta SHA-512 de {vivacitat + repte + GPS + hora}, s'ancora a la blockchain pública amb segell eIDAS i es tanca en un .asice verificable fora de línia. El repte irrepetible impedeix reutilitzar gravacions antigues: el mort no pot respondre al repte d'avui. La cara no surt mai del dispositiu; a la cadena només hi viatja una empremta. Cost de no saber qui segueix viu: Japó, 234.354 centenaris sense confirmar; els EUA, 327 M$ a difunts; Sud-àfrica, 140 M de rands a 75.000 morts. Fonts: France 24; SSA OIG; SASSA/Moneyweb.

---

[1] Wikipedia (amb BBC / AFP / Japan Times) — *Sogen Kato* (momificat 32 anys; pensió de supervivència cobrada; ~9,5 M de iens). https://en.wikipedia.org/wiki/Sogen_Kato ↩

[2] France 24 — *Over 230,000 listed centenarians missing in Japan* (234.354 sense confirmar; 77.118 amb 120+ anys). 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) i *6,5 M de titulars de ≥112 anys sense data de defunció al 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 (via HuffPost) — *Greece stops pensions and benefits for 200,000 people* (~9.000 «centenaris»; fins a 800 M€/any d'estalvi). 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 frau, de funcionaris, segons l'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 certificats; ~11,5 M per autenticació 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 (Índia) — *Digital Exclusion: Poor, Elderly Face the Brunt of Aadhaar-Based Authentication Errors* (empremtes desgastades; pensions denegades; huella no obligatòria). 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 (operació LEAP)* (119.050 pagaments insuficients, 736 M£; >15.000 ja morts). 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* i la bona pràctica VIVESS (pensionistes espanyols a l'estranger). 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/ ↩

Prova de vida: segrestos virtuals, desapareguts i la veu que no era

«Era la veu de la meva filla. Eren els seus plors. Eren els seus sanglots. Era la seva manera de parlar.»

— Jennifer DeStefano, testimoni davant el Senat dels EUA (13-6-2023)

Arizona, 20 de gener de 2023, quarts de cinc de la tarda. Jennifer DeStefano contesta el telèfon i sent la veu de la seva filla de quinze anys — que és fora, en una competició esportiva — plorant i demanant ajuda. Un home pren la línia: exigeix un milió de dòlars, després rebaixa el rescat a cinquanta mil i comença a dictar instruccions de transferència. Ella no creu els qui, al seu voltant, li diuen que pot ser una estafa: «la veu era tan real, i el seu plor, tan real». El «segrest» es va desfer d'un cop quan la filla, perplexa, va trucar per dir que estava bé: mai no havia estat en perill. No hi havia cap segrestador — només una veu clonada amb intel·ligència artificial. DeStefano va acabar testificant davant d'un subcomitè del Senat dels Estats Units perquè cap altra família no hagués de passar per aquell infern [1].

Aquest capítol tracta la prova de vida quan algú l'ataca. La fe de vida rutinària — demostrar cada any que segueixes viu per cobrar la pensió — és al capítol 64; la tecnologia de la veu clonada, al capítol 68; les rèpliques digitals, al capítol 81. Aquí la pregunta és la del pitjor dia possible: com saps que la persona a l'altra banda és real, és viva i és ara? La resposta de sempre — la foto amb el diari del dia — ha mort: la pot fabricar qualsevol. La nova resposta és criptogràfica: un repte imprevisible, respost en el moment i segellat amb **t2p** — l'empremta SHA-512 al dispositiu, el segell de temps RFC 3161/eIDAS, l'ancoratge a la blockchain pública dins d'un contenidor .asice [4]. La veu es pot clonar; el present, no.

El segrest que no existeix

La mecànica del segrest virtual, tal com la descriu l'FBI, és una màquina de pànic perfectament calibrada: una trucada — sovint des d'un número internacional — assegura que un familiar ha estat segrestat; s'hi barregen crits o una veu que sona com la de l'ésser estimat; s'exigeix un rescat immediat, només per transferència; i s'impedeix que la víctima pengi o intenti contactar amb el suposat segrestat. Tot l'engany depèn de la velocitat, perquè no hi ha cap segrest: només cal que la família pagui abans que la mentida caigui pel seu propi pes [2]. Les recomanacions oficials són les contràries a l'instint: mantenir la calma, guanyar temps, intentar contactar amb el familiar per una altra via i fer preguntes que només la persona real sabria respondre [2].

I el 2025 va arribar l'esglaó següent. L'alerta de l'IC3 — el centre de denúncies de ciberdelictes de l'FBI — documenta criminals que usen «prova de vida» alterada: fotos i vídeos manipulats o generats amb IA a partir d'imatges públiques de la víctima, fabricats per fer versemblant el segrest inexistent. Les incoherències que l'FBI recomana buscar-hi — un tatuatge que falta, una cicatriu que no hi és — són exactament la mena de detall que cada generació de síntesi esborra una mica millor [3].

Llegiu-ho bé, perquè és el nucli del capítol: l'ofici del segrestador virtual ja inclou fabricar la prova de vida. El ritual probatori més antic del crim — «demostra'm que és viu» — s'ha convertit en un camp de deepfakes, i la família, en el moment de màxim pànic de la seva vida, ha de fer de pèrit forense en trenta segons. Cap família no hauria de jugar aquesta partida amb les regles velles.

La contraprova: repte, frescor i segell

La resposta estructural es construeix sobre una asimetria que juga a favor de la família: el clonador pot imitar una veu [1], però només pot dir el que el seu operador sap; i pot fabricar una imatge [3], però no pot respondre l'imprevisible. D'aquí la contraprova en tres peces [4].

La primera és **el repte**: una pregunta que només la persona real pot respondre — el record compartit, la paraula de seguretat familiar —, la mateixa lògica que l'FBI ja recomana [2] i que hem vist a la verificació familiar del capítol 85. Prou personal perquè cap algorisme no pugui anticipar-la; prou simple perquè la persona real la respongui sense pensar.

La segona és **la frescor**: la resposta ha de ser d'ara — un vídeo o àudio curt que inclogui el repte acabat de formular, no material reciclat ni preparat. El contingut del present no es pot haver sintetitzat al passat.

I la tercera és **el segell**: la resposta queda empremtada i ancorada al minut — SHA-512, segell de temps RFC 3161/eIDAS, blockchain pública [4] —, de manera que ni es pot haver fabricat abans ni es pot alterar després.

Contra aquest triple mur, el clonador està perdut: pot imitar el timbre [1], però no coneix el repte; pot generar una imatge convincent [3], però no la frescor del moment; i encara que ho tingués tot, no pot fabricar un segell criptogràfic del present amb data d'ahir. La família, per la seva banda, té un protocol en lloc d'un pànic: davant de qualsevol trucada de rescat, exigir la prova de vida segellada amb repte; si no arriba, és l'estafa que l'FBI descriu [2][3]. És el mateix principi de repte i frescor que el capítol 64 aplica a la fe de vida rutinària de les pensions — traslladat al minut més fosc.

L'ostatge real i el desaparegut

Hi ha dos escenaris més greus que l'estafa, i tots dos necessiten el mateix instrument.

El primer és l'ostatge real. Quan un segrest existeix de debò, la prova de vida és moneda de negociació — i la seva autenticitat, qüestió de vida o mort en les decisions de famílies i negociadors. En l'era del deepfake, el dubte talla en dos sentits: un vídeo autèntic pot ser despatxat com a fals, i un de fabricat pot mantenir viva una negociació per una persona que ja no hi és. La contribució del segell és la datació: un vídeo que respon una informació que només existia després d'una data — i que arriba amb empremta ancorada [4] — acredita, com a mínim, que la persona era viva després d'aquella data. No resol la negociació; li treu la boira que la enverina. I la mateixa lògica serveix els qui verifiquen des de fora — el periodisme i les organitzacions del capítol 20 —: material datat i íntegre en lloc de fragments incontrastables.

El segon és el desaparegut. A Espanya, el Centre Nacional de Persones Desaparegudes — pioner a Europa — coordina la resposta a milers de desaparicions cada any: 16.147 persones investigades el 2024 (un 6 % més que l'any anterior, amb el 72 % dels casos esclarits en menys d'una setmana) i 16.024 el 2025, amb un esclariment del 90,7 %; aquell any el CNDES va publicar 928 alertes, 132 de les quals continuaven actives [5]. Darrere de cada alerta activa hi ha una família buscant un rastre.

L'aportació de la prova d'existència és aquí delicada, i cal dir-la amb el límit al davant: voluntària o res. La persona que, per decisió pròpia, manté un rastre segellat de moments i llocs al seu dispositiu [4] pot donar a una eventual investigació l'últim punt verificable del mapa; i la «tornada» — real, o simulada amb la veu i la cara de l'absent [3] — es pot contrastar amb reptes i segells. Un rastre imposat, en canvi, seria vigilància i no protecció: aquesta frontera no es creua.

La prova d'existència aplicada

El telèfon sona amb la pitjor notícia possible. Per primera vegada, la família té alguna cosa a fer que no sigui creure o pagar.

1. El protocol familiar contra el segrest virtual

La família acorda el protocol abans que passi res: paraula de seguretat, retrucada al número de sempre [2] i, davant de qualsevol exigència de rescat, una petició única — prova de vida segellada amb repte [4]. La trucada de l'estafador s'estavella contra tres murs: no coneix el repte, no controla la persona real i no pot fabricar el segell del present [3]. En el cas d'Arizona [1], trenta segons de protocol haurien substituït els minuts de terror: la filla, localitzada per l'altra línia, hauria respost el repte des del vestidor de la competició — segellat, datat, inequívoc.

2. La negociació amb datació

En el segrest real, els negociadors exigeixen als captors proves de vida datables: la resposta a una pregunta formulada avui, segellada avui [4]. El material que arriba amb empremta i frescor acreditades permet decisions — pagar, esperar, actuar — sobre fets i no sobre esperances; i el material sense cap ancoratge es tracta amb la sospita que mereix, perquè l'FBI ja ha documentat la indústria de la prova de vida fabricada [3]. La datació no estova el drama; li treu la boira.

3. L'últim punt del mapa

Una persona que ho decideix lliurement — el senderista solitari, la professional que viatja a zones de risc, l'adolescent que vol tranquil·litzar els pares sense sentir-se vigilat — manté un rastre segellat mínim:

moments triats, empremtats al seu dispositiu, sense cap registre central ni seguiment en temps real [4]. Si mai desapareix, la família pot oferir a la investigació [5] una cronologia verificable de l'última normalitat: no on és ara — això el segell no ho sap ni ho ha de saber —, sinó on i quan va ser per última vegada, amb data certa. En una cerca, les primeres hores i l'últim punt fiable ho són gairebé tot.

4. La tornada que s'ha de creure

El retorn també necessita prova. Qui reapareix després d'una desaparició — i qui reapareix només digitalment: la veu al telèfon, el missatge «soc jo, estic bé» — pot acreditar continuïtat responent reptes i segellant les respostes al moment [4]; una suplantació construïda amb la veu i la cara de la persona absent [3] no pot fer cap de les dues coses. Per a les famílies, és la diferència entre l'esperança fundada i la crueltat d'un engany que es pot allargar mesos; per a les investigacions [5], un filtre contra les pistes falses que consumeixen recursos i esperances.

Els límits, dits sense embuts: el segell no troba ningú, no allibera ningú i no substitueix ni la policia ni els negociadors professionals; la prova de vida segellada exigeix que la persona tingui accés a un dispositiu i una llibertat mínima per respondre — condicions que el segrest real sovint nega; el rastre voluntari mai no pot esdevenir obligació ni vigilància; i cap protocol no estalvia a una família la por — només li dona, enmig de la por, un fet on agafar-se.

La promesa i el perill

La promesa: famílies amb un protocol en lloc d'un pànic [1][2], negociacions sobre fets datats [3], investigacions amb últims punts fiables [5] i tornades que es poden creure. La prova de vida, tornada a la vida.

Els perills, amb la mateixa gravetat.

El primer és **el rastre imposat**. De l'«últim punt del mapa» voluntari a la geolocalització permanent de fills, parelles o empleats hi ha un pendent que aquest llibre es nega a baixar. La prova de vida és un acte de la persona, no sobre la persona: dispositiu propi, moments triats, revocabilitat total, cap registre central [4]. Tot allò que s'assembli a un collar digital és el contrari exacte d'aquest capítol.

El segon és **la coacció sobre el protocol**. Un segrestador real pot forçar la víctima a respondre reptes i segellar respostes. El segell acredita frescor, no llibertat: una prova de vida autèntica pot ser el producte d'una pistola. Els protocols seriosos ho saben — la datació informa la negociació, no la substitueix, i cap família no hauria de gestionar això sense professionals [2].

El tercer és **la falsa seguretat**. Cap protocol no cobreix tots els casos: la persona sense dispositiu, el repte oblidat, el pànic que ho esborra tot. Vendre la prova de vida segellada com a garantia seria cruel; és una eina que millora probabilitats, no un talismà.

I el quart és el més delicat: tecnificar la por. Darrere de cada alerta activa [5] hi ha famílies vulnerables — i un mercat potencial de falses esperances tecnològiques. La primera resposta a una desaparició són la policia, els protocols públics i el suport a les famílies; el segell és infraestructura de prova al seu servei, mai un producte per vendre'ls por.

És hora d'actuar

La pregunta «és viu?» mereix una resposta millor que una foto falsificable.

Per a les famílies: acordeu el protocol abans que calgui — paraula de seguretat, retrucada, prova de vida segellada amb repte [1][2][4]; i si arriba la trucada, guanyeu temps: l'estafa viu de la pressa [2].

Per a policies i negociadors: incorporeu la datació criptogràfica als protocols de prova de vida [3][4]; el material sense frescor acreditada mereix sospita per defecte.

Per al CNDES i les unitats de desapareguts: accepteu i valoreu les cronologies voluntàries segellades que aportin les famílies [4][5]; l'últim punt fiable escurça cerques.

Per a les plataformes i operadores: faciliteu el canal de verificació — el repte segellat d'un clic — i col·laboreu amb les alertes oficials [2][5].

Per a tu: si viatges sol, si t'exposes, si vols que els teus puguin saber sense vigilar-te — el rastre mínim, voluntari i segellat és teu [4]; i parla del protocol a casa: la conversa incòmoda d'avui és la calma de demà.

Per als legisladors: reconeixeu la prova de vida segellada en els protocols oficials i blindeu-la contra tota deriva de vigilància — voluntària, revocable i sense registres centrals [4].

Jennifer DeStefano va sentir la veu exacta de la seva filla suplicant, i la veu mentia [1]. Que la pròxima família que rebi aquella trucada tingui una pregunta preparada i un segell per exigir — i que la pròxima veritat, la del retorn o la de l'última ubicació, arribi amb data certa. Per la pregunta més antiga — «és viu?» —, **time2act**.

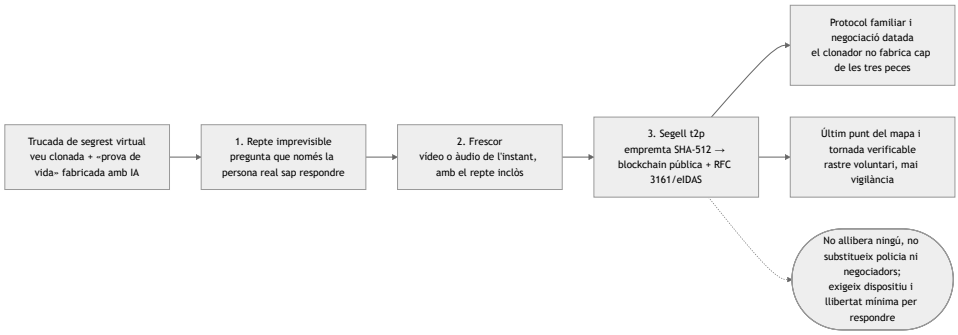


Figura 65.1 — La prova de vida en l'era del deepfake: contra el segrest virtual amb veu clonada i la «prova de vida» fabricada amb IA (alerta FBI/IC3 2025), el protocol de tres peces — repte imprevisible, frescor del moment i segell t2p (empremta SHA-512 al dispositiu, RFC 3161/eIDAS, blockchain pública, .asice). Aplicacions: el protocol familiar, la negociació amb datació, l'últim punt del mapa voluntari i la tornada verificable (CNDES: 132 alertes actives el 2025). Límits: el segell acredita frescor, no llibertat; voluntari o res; mai un substitut de la policia i els negociadors. Fonts: CNN (cas DeStefano); FBI/IC3; Ministeri de l'Interior/CNDES.

---

[1] CNN en Español — *Una mujer cree que estafadores clonaron la voz de su hija en un falso secuestro* (cas Jennifer DeStefano, Arizona; trucada del 20 de gener cap a les 16:55; filla de 15 anys en una competició; rescat d'1 milió rebaixat a 50.000 dòlars; «la voz era tan real»; testimoni posterior davant d'un subcomitè del Senat dels EUA); 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* (mecànica de l'estafa; números internacionals; impediment de contacte; rescat per transferència; recomanacions: calma, contactar per una altra via, preguntes que només la persona real sap respondre); 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 i vídeos alterats o generats amb IA com a falsa «prova de vida», sovint a partir d'imatges públiques; incoherències com tatuatges o cicatrius absents; denúncia a ic3.gov amb el material rebut); Axios — *AI-generated videos, photos used in new virtual kidnapping scams, FBI warns* (5 de desembre 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 producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; prova de vida amb repte i frescor — nonce imprevisible respost i segellat al minut; rastre voluntari amb moments triats; cap registre central; revocabilitat). Vegeu els capítols 13, 15 i 64; la veu clonada, al capítol 68. ↩

[5] La Moncloa / Ministeri de l'Interior — *Las Fuerzas de Seguridad investigaron la desaparición de 16.147 personas en 2024* (+6 %; el 72 % dels casos esclarits en menys d'una setmana; CNDES pioner a Europa); Ministeri de l'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 denúncies; 928 alertes publicades, 132 actives; 11.461 episodis únics, mitjana de 3 denúncies en reincidents). 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/ ↩

Integritat esportiva: la mostra que algú va canviar de nit

«Quan el Gran Anotador vingui a escriure al costat del teu nom, no hi posarà si vas guanyar o perdre, sinó com vas jugar el Joc.»

— Grantland Rice, «Alumnus Football» (1908)

Al laboratori antidopatge dels Jocs Olímpics d'hivern de Sotxi, una nit de febrer de 2014, un agent del servei secret rus rebia per un forat de la mida d'un puny —un «forat de ratolí» perforat a la paret— les ampolles d'orina «bruta» dels esportistes russos. A la sala del costat, l'equip del director del laboratori, Grigori Rodtxenkov, obria les ampolles Berlinger suposadament inviolables, en buidava l'orina dopada i la substituïa per orina neta del mateix atleta, congelada mesos abans, ajustant-ne la densitat amb **sal de taula**. Aquell engany va funcionar perquè el guardià de la integritat —l'Estat, el laboratori acreditat, el servei secret— era qui la corrompia. Mesos després, el laboratori de Londres trobaria que vuit mostres de Sotxi tenien un contingut de sal **fisiològicament impossible** en un ésser humà sa, i que dues mostres de jugadores d'hoquei contenien **ADN masculí** [4].

Aquell forat a la paret conté la pregunta d'aquest capítol: com es prova que una mostra biològica, una sèrie de valors o el resultat d'un partit no han estat manipulats, quan de vegades qui els hauria de custodiar és precisament qui els altera? Aquí no segellem un document, com als capítols 20 i 29, sinó **el contingut físic d'un cos i la seva cadena de custòdia**.

Quan el guardià és el corruptor

L'escàndol rus va ser d'una escala industrial. El jurista canadenc **Richard McLaren**, designat per l'Agència Mundial Antidopatge (WADA) com a Persona Independent, va documentar en el seu *Informe McLaren* (2016) la «metodologia del positiu que desapareix»: almenys **643 mostres positives** reportades com a negatives entre finals de 2011 i l'agost de 2015, una xifra que ell mateix va qualificar de mínima. La segona part de l'informe concloïa que **més de mil atletes russos**, en més de trenta esports, s'havien beneficiat de l'encobriment [1][2]. I el detall més incòmode és que les famoses ampolles «a prova de manipulació» no ho eren: el servei secret va descobrir com obrir-ne els taps sense trencar el segell visible, i una investigació posterior de la revista *Republik* va demostrar que el redisseny tampoc resistia —tres de cada vint-i-quatre kits es descargolaven a mà després de tres dies a la nevera, i una especialista no va trobar «ni una sola mesura de seguretat insuperable» [5]. La cobertura de l'Informe McLaren va revelar que quaranta-quatre mostres, dotze d'elles de medallistes, tenien marques de manipulació als taps [3].

La lliçó és duríssima i és el cor d'aquest front: **un precinte físic, per sofisticat que sigui, no val res si qui el controla és còmplice**. La cadena de custòdia —que la WADA defineix com la seqüència de responsables d'una mostra des que s'obté fins que arriba al laboratori— es pot trencar des de dins.

Del laboratori al mercat d'apostes

El dopatge no és l'únic frau que corca l'esport; també hi ha l'amanyament de partits, detectat indirectament per les empremtes que deixa als mercats d'apostes. L'operació VETO d'Europol ja va identificar més de 380 partits sospitosos a Europa i 425 persones implicades en una xarxa transnacional de crim organitzat [8]. Sportradar, al seu informe d'integritat del 2024, va monitorar més de 850.000 partits en setanta esports i va detectar 1.108 casos sospitosos, la meitat gràcies a les dades d'apostes de compte [9]. La prova, segons Sportradar, ja no és la confessió ni el suborn visible, sinó el moviment anòmal de les quotes. El cas més gran el va protagonitzar Grigor Sargsyan, «el Mestre», condemnat a cinc anys a Bèlgica el 2023 per dirigir una xarxa d'uns cent vuitanta tenistes de més de trenta-cinc països, als quals va pagar uns set milions d'euros en suborns via mòbil [10].

Aquesta lògica indirecta també impregna l'antidopatge modern: el Passaport Biològic de l'Atleta no «veu» la substància prohibida, sinó que rastreja biomarcadors al llarg del temps i n'individualitza els llindars. El ciclista Franco Pellizotti va ser sancionat amb dos anys el 2011 sense cap control positiu, només per valors anòmals del seu passaport —el primer cas validat pel Tribunal d'Arbitratge de l'Esport sobre aquesta base [7]. En tots dos casos, el frau es demostra per un patró, no per un flagrant.

La prova d'existència: segellar la mostra i datar l'evidència

És aquí on **t2p** reforça la baula més feble. En el moment de la presa, l'oficial de control i l'atleta firmen amb **prova de vida** un acte d'obtenció que captura l'empremta SHA-512 del formulari, el **número del kit** llegit, el **GPS forense** de la sala, el segell de temps RFC 3161/eIDAS i la cara de l'atleta; tot s'ancora a la **blockchain pública** i es tanca en un contenidor **.asice**. A partir d'aquí, cada **transferència de custòdia** —de l'atleta a l'oficial, al missatger, al laboratori— genera un esdeveniment segellat amb hora i lloc. Qualsevol obertura, substitució o «forat de ratolí» trencaria la continuïtat de la cadena ancorada, que **no es pot reescriure retroactivament** des del propi laboratori: el banc d'orina neta congelada o l'intercanvi nocturn deixarien una discontinuïtat temporal i geogràfica detectable. El mateix s'aplica al passaport biològic, on cada lectura es pot ancorar amb data certa per blindar la sèrie contra la inserció posterior de valors «nets». I en l'amanyament, t2p no segella cap mostra, sinó **l'evidència**: les alertes de Sportradar, les comunicacions dels oficials d'integritat i les decisions arbitrals se segellen perquè la prova presentada davant del Tribunal d'Arbitratge o d'un jutge penal sigui demostrablement anterior a qualsevol filtració.

Cal dir el límit amb tota la cruesa, perquè aquí és especialment fort. «Escombraries a l'entrada, escombraries a la cadena»: el segell garanteix que la mostra precintada al minut zero és la mateixa que arriba al laboratori, però **no pot certificar que el seu contingut sigui orina pròpia i no manipulada *abans* del segellat**. Si l'atleta orina ja amb orina d'un altre, o si el sistema de dopatge opera en el mateix acte d'obtenció amb complicitat de l'oficial, el segell inalterable només certificarà un frau ben custodiat. Tampoc no resol el **dopatge fisiològicament indetectable** —les microdosis, les substàncies sense marcador—: el passaport biològic és indirecte i probabilístic, i la cadena de custòdia no hi afegeix poder analític. En l'amanyament, segella la sospita però no prova la intenció: un patró d'apostes anòmal ancorat no demostra per si sol que hi hagués suborn; això encara exigeix la investigació criminal. I, sobretot, el cas rus ensenya la lliçó més dura: **quan el custodi és el corruptor —l'Estat, el laboratori acreditat—, el problema no és tecnològic sinó de captura institucional**, i un segell criptogràfic només desplaça la confiança, no l'elimina, si qui firma l'acte de segellat és còmplice.

La promesa i el perill

La promesa és real i valuosa. Una cadena de custòdia segellada, amb hora i lloc a cada transferència, hauria fet molt més difícil l'intercanvi nocturn de Sotxi, perquè la discontinuïtat hauria quedat registrada en un lloc que el laboratori no pot reescriure. I datar l'evidència de l'amanyament donaria als tribunals esportius una prova incontestablement anterior. En un món on el frau es prova per patrons, fer la prova inalterable i datada és reforçar tot l'edifici de la integritat.

El perill demana els matisos que hem dit. El primer, la substitució prèvia al segellat, que cap precinte no resol. El segon, la captura institucional: cap tecnologia no salva un sistema on el guardià mateix és el tramposo, i per això la **independència de qui custodia** continua sent insubstituïble. I el tercer, no confondre segellar l'evidència amb provar la intenció. La prova d'existència endureix la cadena de custòdia i l'anterioritat probatòria, no substitueix ni la independència institucional ni la investigació criminal.

És hora d'actuar

Per a les **agències antidopatge** (la WADA, els laboratoris): segellar l'acte d'obtenció i cada transferència de custòdia amb hora i lloc, perquè cap «forat de ratolí» pugui trencar la cadena sense deixar rastre. Per a les **federacions i unitats d'integritat**: datar les alertes d'amanyament perquè la prova sigui anterior a qualsevol filtració. Per als **reguladors i tribunals esportius**: exigir una independència real de qui custòdia, ja que cap precinte no val res en mans còmplices. I per als **atletes nets**: una cadena de custòdia que els protegeixi tant del trampós com del sistema que el va emparar.

Una mostra va canviar de mans de nit per un forat a la paret perquè ningú no podia provar què havia passat entre el precinte i l'anàlisi. Donar a cada mostra i a cada evidència una empremta segellada amb hora i lloc —sense oblidar mai que cap segell no salva un guardià corrupte— és, en aquest front que defensa el joc net, time2act.

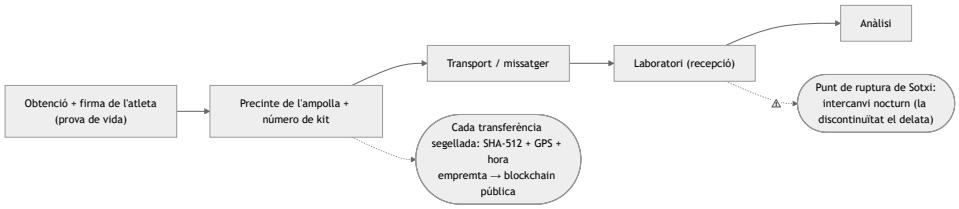


Figura 66.1 — La vida d'una mostra antidopatge passa per cinc nodes: obtenció i firma de l'atleta, precinte de les ampolles A i B, transport, recepció al laboratori i anàlisi. A Sotxi, el frau va entrar al node del laboratori (el «forat de ratolí» per on el servei secret intercanviava l'orina de nit). El segell de t2p —GPS forense, segell eIDAS i empremta del número de kit ancorats a la blockchain pública— fa que aquell intercanvi deixi una discontinuïtat temporal i geogràfica detectable. L'evidència forense que va delatar el frau malgrat les ampolles «inviolables»: 44 taps amb marques de manipulació (12 de medallistes), 8 mostres amb sal impossible, 2 amb ADN masculí, ≥643 positius «desapareguts». Límit: el segell no demostra què hi havia a l'ampolla abans de precintar-la. Fonts: Informe McLaren; CNN; Chemistry World.

---

[1] Wikipedia (síntesi de l'*Informe McLaren*) — *McLaren Report* (≥643 positius «desapareguts»; ADN masculí en mostres femenines). https://en.wikipedia.org/wiki/McLaren_Report ↩

[2] World Anti-Doping Agency — *Independent investigation confirms Russian state manipulation of doping control* (McLaren, Persona Independent; >1.000 atletes). 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 mostres amb marques als taps, 12 de medallistes; Part 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 mostres amb sal fisiològicament impossible). https://www.chemistryworld.com/news/anti-doping-scientists-expose-cheating-russian-athletes/2500159.article ↩

[5] Republik — *Bad bottles* (les ampolles «inviolables» Berlinger, vulnerades). https://www.republik.ch/2018/02/21/bad-bottles ↩

[6] World Anti-Doping Agency — *Athlete Biological Passport* (detecció indirecta; mòdul hematològic 2009, esteroide 2014). https://www.wada-ama.org/en/athlete-biological-passport

[7] ESPN — *Pellizotti banned in landmark biological-passport ruling* (2 anys sense positiu; primer cas validat pel 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 partits; 425 persones; >15 països). 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 partits; 1.108 sospitosos; 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 anys; ~180 tenistes de >35 països; ~7 M€). https://www.washingtonpost.com/world/interactive/2023/tennis-match-fixing-itf-grigor-sargsyan/ ↩

Música i espectacles: l'humà real darrere del play

«El cant del rossinyol és deliciós perquè és el mateix rossinyol qui el dona.»

— John Philip Sousa, «The Menace of Mechanical Music» (1906)

A finals de 2018, des de Cornelius, a Carolina del Nord, un músic de mitjana edat anomenat Michael Smith va escriure als seus dos socis un correu revelador: «necessitem un MUNTÓ de cançons ràpid per esquivar les polítiques antifrau que fan servir ara». No buscava cap èxit; buscava **soroll estadístic**. Al seu soterrani digital, mil quaranta comptes-bot —aviat en serien deu mil— reproduïen sense descans sis-centes trenta-sis cançons al dia cadascun: pistes amb noms sense sentit i artistes inventats, fabricades en massa per una empresa de música amb intel·ligència artificial. Mig cèntim per escolta, **661.440 escoltes al dia**. Ningú no les sentia. Durant set anys ningú no se'n va adonar, fins que l'organització que gestiona els drets mecànics als Estats Units, The MLC, va veure el patró. El març de 2026, Smith es declarava culpable; el botí superava els deu milions de dòlars [1][2].

Aquell soroll fabricat conté la pregunta d'aquest capítol. No és la del capítol 40 —«ho va crear un humà o una IA?»—, perquè aquí les cançons eren clarament d'IA i no importa: la pregunta és una altra, **un humà real va escoltar de debò això, o va comprar de debò aquesta entrada?** És el frau de la *presència humana* en un acte de consum.

El frau que no crea diners, els reparteix

El que fa especial aquest frau és com fa mal. La música en *streaming* reparteix un **fons de suma fixa**: el 2025, segons la federació discogràfica internacional **IFPI**, va generar més de 22.000 milions de dòlars [6]. Cada escolta falsa no inventa diners nous; **roba la seva part a la resta d'artistes** que sí que tenen públic. L'empresa de detecció **Beatdapp** estima que el frau de *streaming* desvia uns dos mil milions de dòlars l'any —almenys un 10 % de tota l'activitat—, tot i que, com a part interessada, convé prendre la xifra com una estimació del sector amb un marge ampli [3]. La resposta de les plataformes ha estat posar llindars: Spotify va decidir que una pista ha de superar les mil reproduccions anuals per entrar al repartiment, justament per frustrar la tàctica de Smith de diluir poques escoltes entre centenars de milers de pistes escombraria [4].

I hi ha un segon problema d'identitat, encara més subtil. The MLC va rebre **424 milions de dòlars** en drets mecànics històrics **no aparellats** —la «caixa negra»: diners generats per reproduccions el titular de les quals no es va poder determinar [5]. La pregunta, doncs, no és només «hi va haver una escolta real?», sinó «de qui és la cançó que es va escoltar?».

Del play fals a l'entrada fantasma

El mateix frau de presència humana corca el món de les entrades. En la preventa de la gira *Eras* de Taylor Swift, el 15-de-novembre-2022, la web de Ticketmaster va rebre **3.500 milions de peticions** —quatre vegades el rècord anterior—, amb uns dotze milions d'«entitats», moltes d'elles bots de revenda, que van sobrecarregar el sistema fins al col·lapse [10]. No és un accident, sinó un model de negoci. La comissió federal de comerç nord-americana (**FTC**) ja havia portat als tribunals, sota la llei BOTS de 2016, revenedors que havien comprat més de cent cinquanta mil entrades amb programari automatitzat i centenars de comptes ficticis [8]. Com hem vist, el 2025 es va presentar una prova demolidora: cinc revenedors controlaven 6.345 comptes i acaparaven **246.407 entrades** per a 2.594 esdeveniments, gestionades des d'una sola pantalla; un executiu va admetre per correu que l'empresa «feia la vista grossa com a política» [9]. El límit de «quatre entrades per persona» que veia el fan era, a la pràctica, ficció.

La prova d'existència: l'humà real darrere del play i de l'entrada

És aquí on **t2p** ataca el buit, certificant no qui va crear l'obra, sinó que **un humà real, en un dispositiu real, en un moment i un lloc reals, va executar una acció real**. En el costat del consum: al dispositiu de l'oient, en l'instant de la reproducció, es genera una empremta SHA-512 d'un esdeveniment d'escolta —pista, dispositiu, **prova de vida**, GPS forens i durada realment reproduïda—, s'ancora a la

blockchain pública i se segella amb el segell de temps eIDAS; el reproductor exigeix un senyal de vivacitat perquè l'escolta compti. En el costat de les entrades: en el moment de la compra i, de nou, en l'accés al recinte, se segella un contenidor **.asice** que lliga la identitat verificada amb prova de vida, l'entrada, el GPS del recinte i l'hora d'entrada física.

L'efecte és directe. Una escolta **sense prova de vida no entra al còmput** que reparteix els drets, cosa que enfonsa el model de Smith: deu mil comptes-bot deixen de cobrar. Vincular cada compra a una identitat amb vivacitat **anul·la els centenars de comptes per revenedor** documentats per la FTC. I el segell de GPS i hora a la porta prova que qui entra és qui va comprar, no un comprador massiu automatitzat. La presència humana torna a ser la unitat de compte.

Cal dir-ho amb tota cruesa, perquè aquí és matisat. «Escombraries a l'entrada, escombraries a la cadena»: **t2p** pot provar que un humà viu va prémer «play» o va creuar la porta, però **no pot provar que aquella escolta fos genuïna ni honesta**. Si en lloc de bots es contracten **humans reals** —cadascun superant la prova de vida— per escoltar pistes escombraries, el segell els certificarà com a «humans reals» i el frau persistirà: la prova de vida derrota els bots, no les granges humanes ni l'*streaming* pagat. Tampoc jutja el mèrit: una escolta humana de trenta segons de soroll d'IA, feta només per cobrar, queda segellada com a vàlida. La «caixa negra» dels 424 milions tampoc no es resol amb un segell; l'esdeveniment va existir, però no se sap **de qui** és la composició, i això exigeix metadades netes, no només un segell. I, sobretot, el segell només serveix si les plataformes l'integren i l'honoren: l'expedient de la FTC demostra que l'intermediari dominant pot «fer la vista grossa per política», i cap criptografia corregeix l'incentiu econòmic del propi guardià. En la revenda legítima, a més, lligar l'entrada a la identitat no impedeix que algú revengui o regali la seva entrada a una altra persona real.

La promesa i el perill

La promesa és quantificable en milers de milions. Una capa de presència humana sobre el *streaming* i les entrades faria molt més difícil drenar el fons de drets amb bots, anul·laria els exèrcits de comptes ficticis dels revenedors i tornaria els diners als artistes amb públic real i les entrades als fans. En un mercat on el frau no crea diners sinó que els reparteix malament, demostrar l'humà real és restaurar la justícia del repartiment.

El perill requereix els matisos que hem dit. El primer, les presències humanes i el *streaming* incentivat, ja que la prova de vida no atura. El segon, no confondre presència amb legitimitat ni amb identitat de l'obra. El tercer, la captura de plataforma: cap segell NO val res si el guardià decideix no honorar-lo. I el quart, la privacitat i el dret del fan a revendre o regalar la seva entrada, que la mecànica anti-bot ha de respectar. La prova d'existència és una eina poderosa per restaurar la presència humana, no una bala de plata contra tots els fraus del sector ni un substitut d'arreglar-ne els incentius.

És hora d'actuar

Per a les plataformes (Spotify, Apple Music) cal integrar la prova de presència humana al còmput dels drets, de manera que una escolta sense humà deixi d'estar facturada. Per als organismes de drets (IFPI, The MLC) s'ha d'exigir el segell i netejar les metadades que buiden la «caixa negra». Per a la indústria de les entrades (Live Nation/Ticketmaster) i els reguladors (la FTC) cal vincular la compra i l'accés a una identitat real i deixar de fer la vista grossa. I per als artistes i els fans, el sistema ha de garantir que tant l'escolta com l'entrada siguin d'humans, no de bots.

Una granja de bots va cobrar per 661.440 escoltes diàries que ningú no va sentir; oferir a cada escolta i a cada entrada una prova segellada de l'humà real —sense vulnerar la privacitat ni el dret a revendre— és, en aquest front del comerç de l'atenció i l'oci, **time2act**.

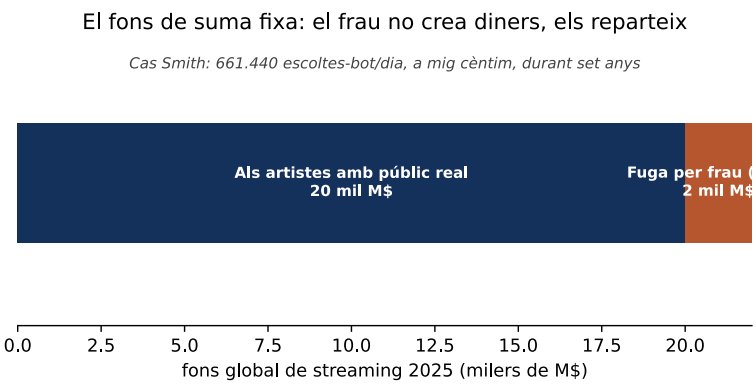


Figura 67.1 — La música en streaming reparteix un fons de suma fixa: el 2025, més de 22.000 milions de dòlars (IFPI). Cada escolta falsa no inventa diners nous; roba la seva part als artistes amb públic real. L'estimació de la indústria xifra la fuga per frau en uns 2.000 milions de dòlars l'any —almenys un 10 % de l'activitat (Beatdapp). El cas Smith: 661.440 escoltes-bot al dia, a mig cèntim, durant set anys. Amb prova de vida, les escoltes sense humà no entren al repartiment i el fons torna als artistes reals. Fonts: IFPI Global Music Report 2026; Beatdapp; acusació de la fiscalia de Nova York.

---

[1] U.S. Department of Justice / SDNY (via Music Business Worldwide) — *North Carolina man pleads guilty to AI-assisted music streaming fraud* (Michael Smith; decomís 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 comptes-bot; 661.440 reproduccions/dia; els correus). 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 l'activitat; estimació de part). 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* (anunciat nov-2023; vigent 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 «caixa 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 entrades; >31 M$ en sancions). 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 revenedors, 6.345 comptes, 246.407 entrades; «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 peticions; ~12 M d'«entitats» amb bots). https://en.wikipedia.org/wiki/Taylor_Swift%E2%80%93Ticketmaster_controversy ↩

Telecom i veu: autenticar qui truca de debò

«Senyor Watson, vingui: el vull veure.»

— Alexander Graham Bell, quadern de laboratori (10-3-1876)

A finals de gener de 2024, dos dies abans de les primàries demòcrates de Nou Hampshire, milers de telèfons van sonar. En despenjar, una veu inconfusible —la de Joe Biden— demanava als votants que *no* anessin a votar i «guardessin el seu vot» per al novembre. L'identificador de trucada mostrava un número conegut del partit. Tot era fals: la veu estava clonada amb intel·ligència artificial i l'identificador, falsificat. L'operador polític que ho va encarregar, Steve Kramer, va rebre una multa de **sis milions de dòlars**, i la comissió federal de comunicacions nord-americana (**FCC**) va dictar la primera norma que declara il·legals els *robocalls* amb veu d'IA [2][3]. No era ni la primera vegada: ja el 2019, el director d'una filial energètica britànica havia transferit uns 243.000 dòlars després d'una trucada del seu «cap», amb l'accent alemany de sempre —una veu sintètica, el primer frau de veu clonada conegut [10].

Aquell vespre de Nou Hampshire conté la paradoxa d'aquest capítol: una veu d'autoritat, **perfectament autenticada per a l'oïda humana, completament falsa al cable**. A diferència del capítol 16, que narrava la suplantació visual d'un executiu en una videotrucada, aquí l'atac és a la **infraestructura mateixa de les telecomunicacions** —la SIM, la xarxa de senyalització, l'identificador— i a la prova de **qui origina de debò una veu**.

El número, l'esglaó feble

El frau més silenciós no toca la veu, sinó el número. En el **SIM-swap**, l'atacant aconsegueix que l'operadora porti el teu número de mòbil a una SIM que ell controla i, amb això, intercepta els codis d'un sol ús que protegeixen els teus comptes. Només el 2023, l'oficina de delictes informàtics de l'FBI va registrar més de mil denúncies amb pèrdues de **48,8 milions de dòlars** [1], i al Regne Unit el servei antifrau **Cifas** va reportar un augment del **1.055 %** de SIM-swaps no autoritzats en un sol any [6]. Les xifres individuals fan vertigen: T-Mobile va ser condemnada a pagar uns **33 milions de dòlars** —el laudo es va fer públic el 2025— després que un SIM-swap permetés robar uns 38 millions en criptomonedes a l'emprenedor Josh Jones, eludint la verificació per SMS [7]. Com resumeix Cifas, el número de mòbil s'ha convertit en **l'esglaó feble** de tota la identitat digital basada en codis per SMS. I les víctimes preferides són els grans: la comissió de comerç nord-americana va trobar que el 41 % dels adults grans que van perdre deu mil dòlars o més en estafes de suplantació —com hem vist— deien que el primer contacte havia estat **una trucada de telèfon**.

STIR/SHAKEN: una capa, no la solució

La indústria ha respost autenticant l'identificador de trucada amb el sistema **STIR/SHAKEN**, que firma criptogràficament el número d'origen perquè les operadores puguin bloquejar o etiquetar les trucades falsificades. Però hi ha un forat enorme: l'abril de 2025 només el **42,5 %** de les trucades arribaven firmades, ja que el sistema **només funciona en xarxes IP** i qualsevol tram antic trenca la firma [5]. Com hem vist, els consumidors nord-americans van rebre **52.800 milions de robocalls** el 2024, unes dues-centes per adult [referència de YouMail]. Per això la defensa s'està desplaçant a la **capa de xarxa**: segons la **GSMA**, l'associació mundial d'operadors, la seva iniciativa Open Gateway exposa senyals com «temps des de l'últim canvi de SIM» perquè un banc no es fiï cegament d'un SMS [9]. Però cap d'aquestes capes no respon la pregunta fonamental: **qui ha originat realment aquesta veu?**

La prova d'existència: autenticar l'origen humà de la veu

És aquí on **t2p** aporta una capa complementària. No impedeix que algú cloni una veu ni que es faci amb una SIM; **segella l'autenticitat i l'origen d'un acte d'identitat en el moment en què passa**. Quan una persona grava una instrucció o autoritza una operació sensible —autoritzar una transferència, confirmar la identitat davant d'un banc, registrar un consentiment—, l'aplicació calcula al dispositiu l'**empremta SHA-512** del clip més les metadades, l'ancora a la **blockchain pública** i hi adjunta un **segell de temps RFC 3161** conforme a eIDAS i un **GPS forense**, tot en un contenidor **.asice**.

La peça decisiva és la **prova de vida**, que ataca exactament el forat que assenyalen els reguladors: distingir una veu humana real, capturada en viu, d'una síntesi. És el mateix principi del concepte premiat per la pròpia comissió de comerç en el seu *Voice Cloning Challenge*, **OriginStory**, que mesura les bioseñals de la gola i la boca per autenticar l'**origen humà de la veu en el punt de creació**. Així, una autorització legítima queda segellada amb vivacitat, hora i lloc, de manera que un àudio clonat posterior no pot fer-se passar per la «gravació original» ni reclamar precedència temporal; la víctima pot demostrar que **no** va emetre certa instrucció perquè no existeix cap segell vàlid seu; i el segell de temps fixa un ordre incontrovertible davant d'un clip fabricat. STIR/SHAKEN autentica el *número* a la xarxa; t2p autentica el *contingut i l'origen humà* a l'extrem. Són capes que es completen.

Cal dir el límit amb tota la cruesa. «Escombraries a l'entrada, escombraries a la cadena»: t2p segella la integritat i el moment d'una captura, però **no certifica que el seu contingut sigui veritat ni que la persona no estigui sent enganyada en aquell instant**. No detecta la clonació dins de la trucada entrant: si un estafador et truca amb veu clonada, t2p no l'analitza; només serveix si la contrapart legítima **segella proactivament** el seu propi acte d'identitat —no és un filtre de robocalls ni un substitut de STIR/SHAKEN. Tampoc no impedeix el SIM-swap, que passa a l'operadora; com a molt, permet que un sistema **no depengui** d'un SMS com a única prova. I si l'atacant enganya la víctima perquè ella mateixa gravi i segelli una autorització, la cadena dirà la veritat sobre una mentida: el segell serà vàlid i l'acte, fraudulent. Finalment, com STIR/SHAKEN, només protegeix qui l'usa als dos extrems, i no recupera els diners d'una transferència ja executada.

La promesa i el perill

La promesa és real en un terreny on la veu ha deixat de ser una prova. Una capa que autentiqui l'origen humà i el moment d'un acte d'identitat donaria a bancs, empreses i ciutadans una contraprova verificable davant de la veu clonada, i trencaria la dependència malsana del SMS com a única clau. Combinada amb STIR/SHAKEN a la xarxa i les API de la GSMA, completaria una defensa per capes que avui té forats arreu.

El perill demana els matisos que hem dit. El primer: no confondre t2p amb un filtre de trucades; protegeix l'acte propi, però no analitza l'aliè. El segon: no atura ni el SIM-swap ni la coacció de la víctima. I el tercer: l'adopció. Sense ús als dos extrems, no hi ha efecte de xarxa. La prova d'existència és una capa complementària potent contra la suplantació de veu, però no és una bala de plata contra tot el frau telefònic.

És hora d'actuar

Per a les **operadores**: completar STIR/SHAKEN, tancar els trams no-IP i aplicar els principis de conèixer el client i el proveïdor que la FCC va imposar a Lingo.

Per als **bancs i les apps**: deixar de dependre del SMS com a única prova i fer servir senyals de xarxa, com l'API de canvi de SIM de la GSMA.

Per als **reguladors** (la FCC): perseguir la veu clonada il·legal, com en el cas de Nou Hampshire. I per als **usuaris**, sobretot els grans: disposar d'una prova segellada que acrediti l'origen humà de la pròpia veu, perquè cap clon pugui parlar en nom seu.

Una veu clonada de Biden va demanar a milers de persones que no votessin, perfectament creïble per a l'oïda i del tot falsa al cable. Donar a cada acte de veu una prova segellada del seu origen humà —sense oblidar que no atura ni la SIM robada ni l'engany— és, en aquest front on ja no podem creure el que sentim, time2act.

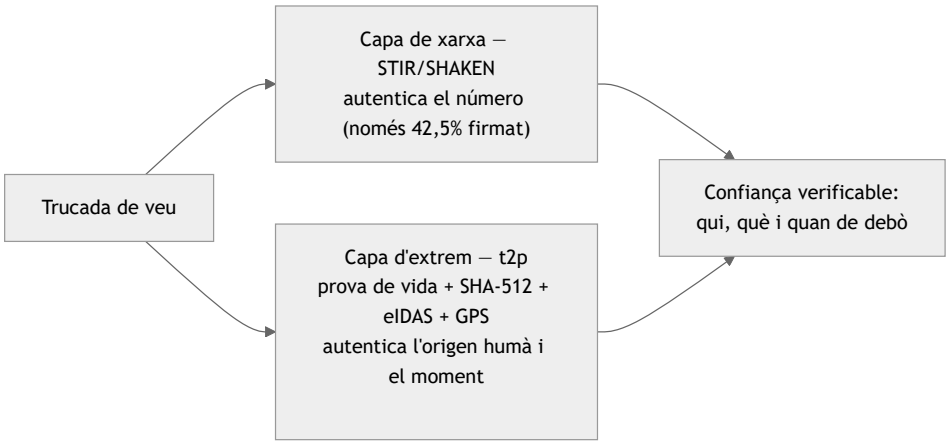


Figura 68.1 — La capa de xarxa (STIR/SHAKEN) autentica el número d'origen —«des de quin número truca?»—, però només el 42,5 % de les trucades arriben firmades (abril de 2025), perquè qualsevol tram no-IP trenca la firma. La capa d'extrem (t2p: prova de vida + SHA-512 + segell eIDAS + GPS) autentica l'origen humà i el moment de l'acte —«qui, què i quan, de debò?». Són complementàries. Context: 52.800 milions de robocalls als EUA el 2024; 48,8 M$ robats per SIM-swap (FBI, 2023). Fonts: TransNexus; FCC; FBI IC3.

---

[1] FBI Internet Crime Complaint Center (IC3) — *2023 Internet Crime Report* (SIM-swapping: 1.075 denúncies, 48,8 M$ de pèrdues). https://www.ic3.gov/AnnualReport/Reports ↩

[2] NPR — *The AI deepfake Biden robocall and the FCC* (Nou 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, febrer 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 + conèixer el client i el proveïdor). https://www.fcc.gov/document/fcc-settles-lingo-telecom-robocall-investigation

[5] TransNexus — *SHAKEN statistics, April 2025* (només el 42,5 % de trucades firmades; la bretxa no-IP). https://transnexus.com/blog/2025/shaken-statistics-april/ ↩

[6] Cifas — *Fraudscape 2025* (+1.055 % de SIM-swaps no autoritzats al Regne Unit). 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 criptomonedes). 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 l'origen humà de la veu al punt de creació). 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 xarxa). 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 frau de veu sintètica conegut). http://thenextweb.com/news/fraudsters-deepfake-ceos-voice-to-trick-manager-into-transferring-243000 ↩

El frau bancari del pagament «autoritzat»

«La confiança és la base indispensable de tota mena de transaccions. Sense ella, el comerç [...] s'aturaria com un rellotge sense corda.»

— Herman Melville, The Confidence-Man (1857)

La trucada arriba d'un número que sembla el del banc. La veu — professional, tranquil·la — avisa d'un «càrrec sospitós» i guia la víctima, pas a pas, «per protegir els estalvis»: una transferència «al compte segur». O el missatge del «fill»: «papa, se m'ha trencat el mòbil, fes-me un Bizum a aquest número». Quan la persona s'adona, els diners han sortit — i els ha enviat ella, amb la seva app, les seves claus i la seva empremta.

El nus jurídic és exactament aquest [2]. La normativa europea de pagaments — la PSD2, transposada a Espanya pel RDL 19/2018 — distingeix dos mons. En l'operació no autoritzada — algú altre mou els teus diners —, el banc ha de retornar l'import llevat que provi frau o negligència greu del client, i la càrrega de provar que l'operació es va autenticar correctament és seva. Però en el pagament autoritzat sota engany — el que els britànics anomenen frau APP —, la resposta clàssica del sistema és demolidora: «vas autoritzar tu». La víctima perfecta del frau modern no és qui perd les claus: és qui les fa servir convençuda.

Aquest capítol tracta el frau que no força la porta: convenç la víctima perquè l'obri. La SIM clonada i la veu falsificada — els vehicles de l'engany — són al capítol 68; el director financer suplantat que ordena transferències d'empresa, al capítol 87; la relació amb la companyia de serveis, al capítol 33; el compliance institucional, al capítol 16; l'estafa a la gent gran, al capítol 85; el pagament fora de plataforma de la compravenda entre particulars, al capítol 31. Pregunta clau: quan el pagament el vas fer tu, enganyat, què queda per discutir? Resposta: diligències — què et van mostrar, què et van advertir, què vas veure — i les diligències són fets datats: la data certa als dos costats de la pantalla, amb **t2p** — la tríada del capítol 13: empremta, hora certa, àncora [3]. El Regne Unit acaba de convertir aquesta batalla de proves en llei.

El Regne Unit capgira el tauler

Des del 7 d'octubre de 2024, el Regne Unit és el primer país del món amb un règim de reemborsament obligatori del frau del pagament autoritzat [1]. El règim — del Payment Systems Regulator — obliga els proveïdors de pagament a reemborsar les víctimes: particulars, microempreses i entitats benèfiques, en transferències dels sistemes Faster Payments i CHAPS, fins a un límit de 85.000 lliures — rebaixat de les 415.000 inicials per alinear-lo amb el fons de garantia britànic. El reemborsament, en cinc dies hàbils — o fins a trenta-cinc si cal investigar. I la peça més enginyosa: el cost es reparteix al 50 % entre el banc emissor i el banc receptor — el banc que va acollir el compte mula també paga [1]. El règim substitueix un codi voluntari que s'havia demostrat insuficient.

La lectura d'aquest llibre: quan el reemborsament és la norma, tot el sistema esdevé una disputa de diligències. El client va ignorar advertències clares? El banc les va mostrar de debò — i quan? El banc receptor va obrir el compte mula amb la mà trencada? Cada resposta és un fet datat en una pantalla o en un registre. El règim britànic, sense dir-ho, ha creat la necessitat de la prova d'existència a banda i banda: qui pugui acreditar què es va mostrar, què es va advertir i què es va fer — i quan — tindrà la seva part de la raó; qui no, pagarà.

I a Europa continental, amb la reforma dels pagaments en tramitació [2], la pregunta no és si aquest model arriba, sinó quan.

La prova d'existència aplicada

L'engany es desplega com una cadena de moments — i cada moment es pot datar [3].

1. L'engany documentat

La trucada del fals tècnic, gravada — conversa pròpia, lícita, com explica el capítol 75 —; l'SMS del «compte segur» i el xat del «fill», capturats amb data certa [3]. L'engany deixa de ser una història que la víctima explica avergonyida: és una seqüència datada que un analista pot resseguir — i que, davant del banc o del jutge, estableix el context del pagament «autoritzat»: autoritzat, sí; lliure, no.

2. La sessió capturada

El que la víctima veia quan va pagar: la pantalla de l'app amb el beneficiari i l'avís — o l'absència d'avís —, el web que suplantava el banc, capturat amb imatge completa i codi font [3]. En un règim de diligències compartides, aquest és el camp de batalla exacte: el banc dirà que va advertir; el client, que no va veure res. La pantalla d'aquell moment, amb data certa, respon per tots dos.

3. La reclamació datada

El rellotge corre des del primer minut: la comunicació al banc, capturada en enviar-se; la denúncia policial, escanejada; cada resposta i cada silenci, amb la seva data [3]. Els terminis del règim britànic — el reemborsament en 5 dies, o 35 amb investigació [1] — i els de qualsevol reclamació europea es mesuren sobre aquestes dates; i l'expedient .asice sencer, verificable sense connexió, arriba al servei de reclamacions, al supervisor o al jutjat amb la cronologia tancada.

4. La simetria del banc diligent

El mateix mecanisme protegeix l'entitat que ho fa bé: els avisos mostrats — la fricció aplicada al pagament inusual, l'advertència del beneficiari nou — ancorats per lots encadenats, amb la mateixa lògica que VeriFactu imposa a les factures [3]; i el registre de l'alta del compte receptor, amb les seves comprovacions. Quan el règim reparteix costos segons diligències [1], el banc que pot provar que va advertir — i el receptor que pot provar que va verificar — tenen la seva defensa; el que no pot provar res, paga. La prova no tria bàndol: obliga tothom.

Els límits, dits clarament: el segell acredita pantalles, converses i dates — no decideix si la negligència era greu ni si l'avís era prou clar: això ho diuen la llei i el jutge [2]. No recupera diners ja moguts — la velocitat de reacció i la cooperació entre bancs continuen sent decisives. I la prevenció segueix sent la primera línia: el banc no truca mai per demanar transferències, i cap pressa és bona senyal.

La promesa i el perill

La promesa: víctimes que no han de triar entre la vergonya i la indefensió — l'engany documentat és reclamable [1][3]; bancs diligents que acrediten els seus avisos i no paguen pels pecats dels descuidats; comptes mula més cars d'obrir, perquè el receptor també respon [1]; i un model — el britànic — que demostra que el frau APP no és una fatalitat, sinó un problema de repartiment d'incentius i de prova.

Ara toca mirar els perills.

El primer és **el frau del frau**. Si el reemborsament és automàtic, apareixerà qui simuli ser víctima. El contrapès és el mateix expedient: la víctima real té una seqüència d'engany datada i coherent; el simulador ha de fabricar-la sencera contra un GPS forense i uns segells que no es deixen backdatar [3].

El segon és **la fortalesa del banc**: l'entitat amb registres perfectes contra el client amb memòria. Si només una part pot provar, el règim es desequilibra — per això la capa del client, les seves captures i el seu diari, és tan important com la del banc, i el supervisor ha de valorar totes dues.

El tercer és **la por que paralitza**. Un règim massa dur per als bancs pot acabar en friccions infinites per a tothom: pagaments bloquejats, sospita universal. L'equilibri és fi — advertències clares i datades, no obstacles; protecció, no paternalisme.

I el quart és **el tecnosolucionisme del reemborsament**. Recuperar els diners no desfà l'engany ni atrapa l'estafador. La persecució del delicte — i de les xarxes de mules — continua sent feina policial; la prova d'existència hi ajuda: cada expedient datat és un mapa del modus operandi.

És hora d'actuar

Que qui va confiar no hagi de provar la seva innocència amb les mans buides.

Per a tu, client: si l'engany arriba, documenta mentre reacciones — la trucada, l'SMS, la pantalla [3]; i recorda la regla d'or: el banc no truca mai per demanar-te una transferència.

Per als bancs emissors: ancoreu els vostres avisos i friccions [3] — en un règim de diligències compartides [1], l'advertència que no podeu provar no existeix.

Per als bancs receptors: l'alta de comptes amb verificació demostrable — quan el compte mula també us costa diners [1], la vostra porta d'entrada és la vostra primera defensa.

Per als supervisors i legisladors europeus: el model britànic [1] ja funciona; que la reforma europea dels pagaments [2] incorpori el reemborsament del frau APP — i que el repartiment de costos es decideixi sobre evidència datada de les dues parts, no sobre la paraula del més gran.

Per a la policia i les fiscalies: l'expedient .asice de cada víctima [3] és un mapa datat de la xarxa — agregats, els mapes atrapen mules i estafadors.

El frau modern no roba claus: roba confiança. Que almenys cada engany deixi la seva cronologia — i que qui va confiar no hagi de provar la seva innocència amb les mans buides. Pels estalvis de tothom, **time2act**.

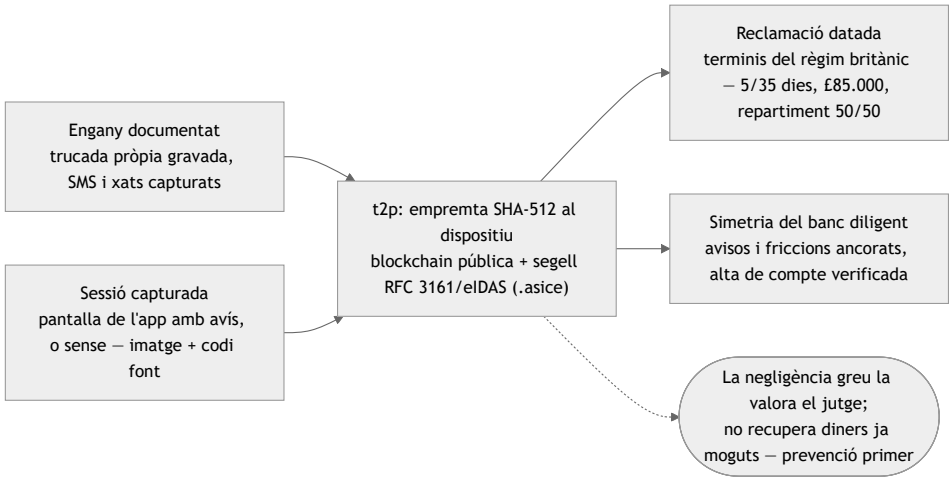


Figura 69.1 — El frau del pagament «autoritzat» amb prova d'existència (segellat amb t2p — capítol 13): l'engany documentat (trucada pròpia gravada, SMS i xats capturats), la sessió capturada (la pantalla amb l'avís — o sense), la reclamació datada (terminis) i la simetria del banc diligent (avisos i friccions ancorats per lots; l'alta del compte receptor verificada). Context: Regne Unit, primer reemborsament obligatori del món (7-10-2024; £85.000; 50/50 emissor-receptor; 5/35 dies); PSD2: en operacions no autoritzades, la càrrega de la prova és del banc. Límits: la negligència greu la valora el jutge; la prevenció primer. Fonts: PSR; PSD2/RDL 19/2018.

---

[1] Payment Systems Regulator (Regne Unit) — *APP fraud reimbursement protections* (règim obligatori des del 7-10-2024, primer del món; particulars, microempreses i entitats benèfiques; Faster Payments i CHAPS; límit 85.000 £ — rebaixat de 415.000 per alinear-lo amb l'FSCS; cost compartit 50/50 entre proveïdor emissor i receptor; reemborsament en 5 dies hàbils o fins a 35 amb investigació; substitueix el codi voluntari CRM); anàlisis de Freshfields, A&O Shearman i 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, transposada a Espanya pel RDL 19/2018): en operacions de pagament no autoritzades, devolució per part del proveïdor llevat de frau o negligència greu del client; càrrega de la prova de l'autenticació correcta sobre el proveïdor; autenticació reforçada (SCA); reforma europea dels pagaments (PSD3/PSR) en tramitació. ↩

[3] t2p — manual de producte (gravació d'àudio de converses pròpies; captura de pantalla i de pàgina web certificades — imatge completa + codi font; certificar qualsevol fitxer per lots; projectes per a l'expedient d'un incident; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió; només empremtes a la cadena). Vegeu els capítols 13 i 15; la veu clonada i la SIM, al capítol 68; el CFO suplantat, al capítol 87; la caixa negra personal, al capítol 75. ↩

Maquinari: el pedigrí d'un xip que no podia fallar

«El disseny d'enginyeria té com a primer i principal objectiu evitar la fallada.»

— Henry Petroski, To Engineer Is Human (1985)

En un magatzem de Clearwater, a Florida, entre 2006 i 2010, una empresa anomenada VisionTech importava circuits integrats d'una sola fàbrica xinesa, fets amb materials «inferiors i reciclats», i els reetiquetava amb les marques d'Intel, Texas Instruments i Motorola. Els fiscals hi van trobar un detall que ho diu tot: **fotografies del fill del propietari aplicant abrillantador de cotxes a xips bruts** perquè semblessin nous. L'empresa deia fer «proves internes», però no tenia ni un sol expert en control de qualitat. Va vendre **15,8 milions de dòlars** en components etiquetats com a «aptes per a ús militar», i la seva administradora va acabar amb trenta-vuit mesos de presó —la primera condemna penal federal als Estats Units per tràfic de circuits integrats falsificats [3].

Aquells xips reciclats no anaven a joguines. El 2010, la mateixa mena de memòries falses van aparèixer als ordinadors de missió del míssil antimíssils **THAAD**; segons l'agència de defensa, si haguessin fallat, **el mateix míssil probablement hauria fallat** [1]. I un xip de memòria falsificat es va instal·lar en més de quatre-centes unitats de pantalla de cabina dels avions de transport C-27J i C-130J, on una avaria podia deixar la pantalla del pilot **en blanc en ple vol** [4]. Aquest capítol no tracta de la falsificació de béns de consum del capítol 29, sinó d'una mentida més tècnica i més perillosa: la del **pedigrí** d'un component electrònic —el seu origen, la seva data, la seva cadena de custòdia— que viatja en etiquetes i certificats falsificables fins al cor d'un sistema d'armes.

El mercat gris i la mentida del pedigrí

L'escala del problema és nacional. Una investigació d'un any del **Comitè de Serveis Armats del Senat** dels Estats Units va identificar el 2012 unes mil vuit-centes ocurrències de peces sospitoses de ser falsificades a la cadena de subministrament de defensa, amb **més d'un milió de peces** individuals i més de sis-centes cinquanta empreses implicades; més del **70 % es va rastrejar fins a la Xina** [1]. Per demostrar com de fàcil era, l'oficina de fiscalització del Congrés (**GAO**) va crear una empresa ficticia i va comprar setze components de grau militar per internet: **els setze van resultar falsos** [2]. La majoria d'aquestes falsificacions —al voltant del **80 %, segons les bases de dades del sector** com IHS i ERAI — no són còpies fabricades de zero, sinó xips usats arrencats de plaques rebutjades, polits i remarcats. Un sol proveïdor de Shenzhen, Hong Dark, va introduir unes **84.000 peces** sospitoses que van arribar a sistemes anticol·lisió d'avions militars i a projectils d'artilleria [1]. L'associació de la indústria de semiconductors calcula que tot plegat costa més de **7.500 milions de dòlars** l'any [5], i el problema no remet: l'organització de seguiment ERAI va registrar el 2024 el nombre més alt de peces sospitoses des de 2015 [6].

Per què detectar és car i prevenir per l'origen és barat

El que fa diabòlic aquest frau és que un xip reciclat pot ser, per fora, **idèntic** a un d'autèntic. Com explica el centre de recerca CALCE de la Universitat de Maryland, detectar-lo exigeix un laboratori físic-químic car —raigs X, obertura de la càpsula, proves elèctriques—, perquè la falsificació viu a dins. La norma aeroespacial **AS6171** estandarditza aquests assajos per a les peces que arriben **sense una cadena de custòdia coneguda** fins al fabricant original, i la legislació nord-americana fa responsable el contractista de defensa **sigui quin sigui el punt on va entrar la peça falsa**. Però com adverteix l'organització ERAI en el seu informe anual, el frau és atomitzat i ocult, i la majoria de casos són ocurrències noves. La lliçó del sector és clara: **prevenir per l'origen és molt més barat que detectar per assaig**. El problema és que aquell origen viatja en un PDF que es pot reescriure.

La prova d'existència: un pedigrí inalterable

És aquí on **t2p** ataca el cor del frau, que no és (només) un xip dolent, sinó **una mentida sobre el pedigrí**. La idea és segellar cada **esdeveniment de custòdia** —el marcatge pel fabricant original, la inspecció d'entrada, l'assaig AS6171, la sentència d'acceptació— calculant al dispositiu l'**empremta SHA-**

512 dels artefactes d'evidència: informe d'assaig amb les seves imatges de raigs X, certificat de conformitat, foto del codi de data i número de lot. Aquesta empremta s'ancora a la **blockchain pública** amb un **segell de temps RFC 3161** conforme a eIDAS. La **prova de vida**, en capturar la imatge del component, impedeix reutilitzar una **foto antiga d'una peça autèntica** per emparar un lot fals, i el **GPS forense** fixa **on** s'ha inspeccionat —el laboratori acreditat real, no un «laboratori fantasma». Tot viatja en un contenidor **.asice** que qualsevol actor de la cadena pot verificar sense connexió; si un codi de data o un certificat són alterats, l'empremta es trenca. La cadena de custòdia deixa d'ésser un PDF reescriptible i es converteix en un **registre de pedigrí inalterable, datat i geolocalitzat**.

Cal dir el límit amb tota la cruesa, perquè aquí és literal: «Escombraries a l'entrada, escombraries a la cadena». **t2p** segella l'evidència i el seu moment, **no la veritat física del silici**. Si un laboratori acreditat assaja correctament un xip autèntic i després, aigües avall, algú **substitueix físicament** aquell xip per un de reciclat amb el mateix marcatge, la cadena continuarà apuntant al segell legítim: l'atestat és honest, la peça no. La prova garanteix que *aquest informe existia i no s'ha alterat*, no que *l'assaig es va fer bé* ni que *la peça que tinc a la mà és la que es va assajar*. Per això aquest front depèn d'un **ancoratge físic fiable** —un marcatge d'ADN, una empremta física no clonable al mateix xip, una serialització indeleble— que lligui criptogràficament l'àtom al bit. Sense aquest vincle físic, un actor malintencionat pot **certificar de bona fe el lot A i lliurar el lot B**. La prova d'existència apuja el cost de l'engany i deixa rastre forense de qui va signar què i quan —inestimable en un litigi—, però **no detecta per si sola un xip reciclat**: això continua sent feina de l'assaig físic, i un laboratori corrupte o un segell sobre la peça equivocada derroten el sistema.

La promesa i el perill

La promesa és de seguretat nacional. Un pedigrí segellat, datat i geolocalitzat a cada baula faria molt més difícil col·locar un xip reciclat al cor d'un míssil o d'una pantalla de cabina, perquè cada certificat fals trencaria l'empremta i cada responsabilitat quedaria atada a qui la va signar. Combinat amb l'assaig físic i amb un ancoratge al silici, donaria a la cadena de defensa la traçabilitat que la llei ja exigeix però que avui descansa sobre papers falsificables.

El perill demana els matisos que hem dit. El primer, no confondre el segell amb la prova física: el pedigrí inalterable no fa autèntic un xip fals, i sense ancoratge al silici la substitució posterior continua sent possible. El segon, l'assaig continua sent insubstituïble, i un laboratori corrupte derrota qualsevol cadena. I el tercer, l'adopció a tota la cadena, des del fabricant original fins a l'últim subcontractista. La prova d'existència és una capa poderosa per al pedigrí documental, no un substitut de l'assaig físic ni de l'ancoratge al component.

És hora d'actuar

Per als fabricants originals i distribuïdors autoritzats: segellar el marcatge i el codi de data en origen, perquè el pedigrí neixi inalterable. Per als contractistes principals i subcontractistes: exigir el pedigrí segellat com a condició, ja que la llei els fa responsables d'on sigui que entri la peça falsa. Per als laboratoris acreditats: segellar els informes d'assaig amb prova de vida i GPS, perquè ningú no en reutilitzi un de vell. I per al Departament de Defensa i les seves agències: lligar el pedigrí criptogràfic a un ancoratge físic al silici, perquè l'àtom i el bit no es puguin separar.

Uns xips polits amb abrillantador van acabar dins d'un míssil que no podia fallar. Donar a cada component una prova segellada del seu pedigrí —sense oblidar mai que cal l'assaig físic i un ancoratge al silici— és, en aquest front que toca la seguretat de tots, time2act.

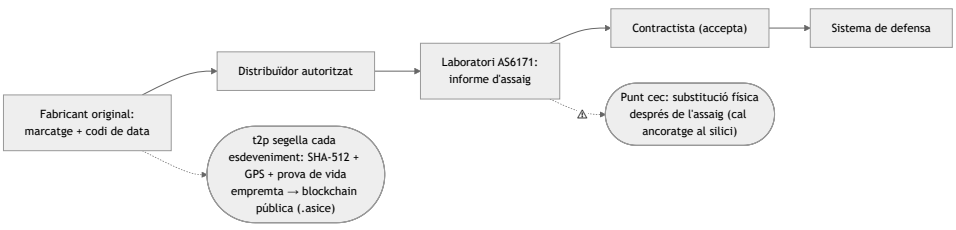


Figura 70.1 — Cada esdeveniment de custòdia d'un component de grau defensa —marcatge pel fabricant original, recepció al distribuïdor, «origen» declarat pel broker, informe d'assaig AS6171, acceptació del

contractista, instal·lació— es pot segellar amb empremta SHA-512, segell eIDAS, GPS forense i prova de vida, ancorats a la blockchain pública. El punt cec (en vermell): la substitució física de la peça després *de l'assaig, que el segell no detecta sense un ancoratge al silici (ADN, empremta física no clonable). Context: ~80 % dels xips falsos són reciclats o remarcats; la GAO va comprar 16 peces militars en línia i les 16 eren falses; un sol broker en va introduir 84.000. Fonts: Senat dels EUA (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 peces; >70 % rastrejades a la Xina; 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 peces falses). https://www.gao.gov/products/gao-12-375 ↩

[3] Center for Public Integrity — *Counterfeit chips plague Pentagon weapons systems* (VisionTech; l'abrillantador als xips; McCloskey, 38 mesos). 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 blanc; defectes del 27 %). https://www.airandspaceforces.com/c-27jandc-130jpartslinkedtocounterfeitmills/ ↩

[5] Semiconductor Industry Association — *Winning the battle against counterfeit semiconductor products* (>7.500 M$/any; ~11.000 llocs de treball). https://www.semiconductors.org/resources/winning-the-battle-against-counterfeit-semiconductor-products/ ↩

[6] ERAI — *2024 Annual Report* (1.055 peces sospitoses; el màxim des de 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 mesos; submarí nuclear, sistema de míssils). 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* (laboratoris acreditats ISO/IEC 17025). https://www.sae.org/standards/content/as6171/7/

[9] CALCE (University of Maryland) — *Counterfeit electronics detection and avoidance* (un xip reciclat pot semblar idèntic a l'autèntic). https://calce.umd.edu/counterfeit-electronics-detection-and-avoidance

[10] Defense Microelectronics Activity (DMEA) — *Trusted Foundry / Trusted IC* (proveïdors de confiança amb pedigrí controlat; 2003, amb la NSA). https://www.dmea.osd.mil/TrustedIC.aspx

Programari: el pedigrí del codi que tot ho fa anar

«La moral és òbvia: no pots confiar en codi que no hagis creat totalment tu mateix.»

— Ken Thompson, «Reflections on Trusting Trust», lliçó del Premi Turing (1984)

Finals de març de 2024. Andres Freund — enginyer de Microsoft i desenvolupador de PostgreSQL — investiga una minúcia que gairebé tothom hauria deixat passar: els inicis de sessió SSH d'una màquina de proves triguen uns 500 mil·lisegons més del compte. Mig segon. Estirant aquell fil, Freund troba el que ningú no volia trobar: una porta del darrere sofisticadíssima dins de XZ Utils — una biblioteca de compressió present a gairebé tot Linux —, dissenyada per permetre l'execució remota de codi a través del servidor SSH. La reporta el 28-29 de març a la llista de seguretat Openwall; rep l'identificador CVE-2024-3094 i la severitat màxima: 10,0 sobre 10 [1].

Els analistes coincideixen en el diagnòstic retrospectiu: si aquell mig segon de curiositat no hagués disparat la investigació, la porta del darrere hauria pogut ser un facilitador d'intrusions més gran que el cèlebre atac SolarWinds — accés potencial a qualsevol màquina Linux exposada del planeta [1]. Bancs, hospitals, xarxes elèctriques: tot el que funciona sobre Linux havia estat a un pas de tenir una cambra secreta oberta. El món digital es va salvar per 500 mil·lisegons i un enginyer tossut.

Aquest capítol tracta la cadena de subministrament del programari: les biblioteques de codi que ho sostenen tot, les seves versions i els voluntaris que les mantenen. El pedigrí del maquinari — els xips falsificats — és al capítol 70; els registres que l'atacant no pot esborrar, al capítol 57; la procedència dels models d'IA, al capítol 79. Pregunta clau: com saps que el codi que executes — tu, el teu banc, el teu hospital — és exactament el que els seus autors van publicar? Resposta: amb el pedigrí del codi — els registres de transparència públics com Sigstore/Rekor, que ja són prova d'existència en producció [3], i la capa d'ancoratge neutral de **t2p**: l'empremta SHA-512 de cada versió publicada, amb segell de temps RFC 3161/eIDAS i ancoratge a la blockchain pública, dins d'un contenidor .asice [5]. La indústria del programari ha arribat pel seu compte a la tesi d'aquest llibre; aquest capítol explica per què — i què hi falta.

El paleta infiltrat

Quan obres l'aplicació del banc i veus la icona de la connexió xifrada, no et preguntes qui ha escrit el codi que xifra. La resposta és: desconeguts. El programari modern és una torre de peces — «biblioteques» — que ningú no escriu de zero: cada aplicació pren blocs de projectes oberts, mantinguts sovint per voluntaris amb pressupost zero. XZ Utils era això: una peça humil de compressió, present a gairebé totes les distribucions de Linux, cuidada durant anys per un únic mantenidor.

L'atac va ser una obra mestra d'enginyeria social, teixida al llarg de diversos anys [1]. Un personatge que es feia dir «Jia Tan» va aparèixer aportant correccions útils; comptes falsos van començar a pressionar el mantenidor original amb queixes i exigències fins que, esgotat, va acceptar ajuda; i «Jia Tan» va anar guanyant permisos — primer de modificar codi, després de publicar versions.

Aleshores va col·locar el maó enverinat, amb una subtilesa decisiva: el codi maliciós no era visible al repositori públic que qualsevol pot revisar. S'amagava en un fitxer del procés de construcció i en fitxers de prova binaris ofuscats, dins dels paquets de distribució — els «tarballs» — que les distribucions es descarreguen per instal·lar el programari [1]. Traducció: la versió publicada no coincidia amb el codi font visible, i cap revisió estàndard del repositori no podia detectar-ho.

La lliçó probatòria és el gir del capítol: l'atac va explotar exactament un buit de prova d'existència — ningú no verificava que allò publicat fos allò visible. Amb l'empremta ancorada de cada paquet publicat, contrastable amb l'empremta del codi font [5], la discrepància hauria estat detectable per qualsevol màquina del món en el moment de la descàrrega. No hauria calgut cap heroi del mig segon.

El cuc amb les claus del regne

Un any i mig després va arribar la industrialització. El 14 de setembre de 2025, l'ecosistema npm — el repositori del qual es nodreixen milions d'aplicacions web — va patir el primer cuc autoreplicant amb èxit

de la seva història: «Shai-Hulud», batejat per la comunitat de ciberseguretat amb el nom dels cucs de sorra de *Dune*. Més de 500 paquets compromesos, incloent-hi @ctrl/tinycolor — més de 2,2 milions de descàrregues setmanals — i, en una ironia perfecta, paquets del compte npm de CrowdStrike, un dels grans proveïdors mundials de ciberseguretat [2].

La mecànica era tan sofisticada com sinistra: el cuc collia credencials dels desenvolupadors infectats — claus d'Amazon, Google i Microsoft, localitzades amb eines de cerca de secrets —, s'instal·lava a les seves automatitzacions de GitHub i, la novetat letal, usava els drets de publicació de cada mantenidor infectat per publicar-se dins dels seus propis paquets: cada víctima esdevenia propagador. Un paquet legítim dilluns podia portar el cuc dimarts, publicat amb les mateixes credencials. La CISA — l'agència nord-americana de ciberseguretat — va emetre alerta el 23 de setembre; el novembre va arribar una segona onada [2].

El diagnòstic, en clau d'aquest llibre: si xz va ser el paleta infiltrat que va trigar anys, Shai-Hulud és el robatori de la identitat de publicació a escala. El problema ja no és només qui és el mantenidor — la identitat, que el capítol 91 tracta —, sinó què es publica amb les seves claus i quan. La pregunta de la cadena de subministrament del programari és, literalment, la pregunta d'aquest llibre: què existia, exactament, i en quin moment?

La resposta que ja és prova d'existència

La bona notícia mereix ser dita amb totes les lletres: la indústria ha començat a respondre amb la mateixa arquitectura que aquest llibre defensa. Sigstore — la infraestructura oberta de signatura de programari — s'ha convertit en el mètode per defecte d'ecosistemes com Kubernetes i de registres com npm, Maven i PyPI; i el seu cor és Rekor: un registre de transparència públic i d'única escriptura — no s'hi pot esborrar ni reescriure res — que ja conté més de 101 milions d'entrades de signatures de més de 33.000 projectes de codi obert, de Kubernetes a CPython [3]. Cada publicació signada hi deixa constància pública i datada, i npm i PyPI ja admeten atestacions de procedència signades així [3].

L'ús defensiu més elegant és la monitorització del registre: un mantenidor pot vigilar Rekor i rebre alerta si hi apareix una signatura de publicació del seu paquet que ell no ha fet — la detecció del robatori de claus pel rastre públic que deixa, tal com van demostrar Trail of Bits i l'OpenSSF el desembre de 2025 [3]. Contra un cuc com Shai-Hulud [2], és exactament l'alarma que faltava: la publicació fraudulenta queda registrada on tothom la pot veure — inclòs el legítim propietari, en minuts.

I aquí el moment de tesi: un registre de transparència d'única escriptura amb entrades datades és, per definició, prova d'existència. La comunitat del programari, empesa pels seus atacants, ha arribat pel seu compte a la solució que aquest llibre proposa per a la resta de la societat. El que t2p hi afegeix és la capa d'ancoratge neutral i transversal: empremtes SHA-512 de cada versió publicada — tarballs inclosos, la lliçó de xz [1] —, amb segell de temps RFC 3161/eIDAS i ancoratge a una cadena pública [5], de manera que el pedigrí del codi no depengui de cap infraestructura única i sigui verificable amb la mateixa eina que el pedigrí d'un document, d'una foto o d'un xip (capítol 70).

El context regulador tanca el cercle: el Reglament europeu de Ciberresiliència — Reglament (UE) 2024/2847, en vigor des del desembre de 2024 — imposa als fabricants seguretat durant tot el cicle de vida del producte digital, amb les obligacions de notificació de vulnerabilitats aplicables des de l'11 de setembre de 2026 i l'aplicació plena l'11 de desembre de 2027 [4]. La traçabilitat del programari deixa de ser bona pràctica per esdevenir llei.

La prova d'existència aplicada

Una actualització qualsevol, un servidor qualsevol — i, abans d'instal·lar-la, una comprovació d'un segon contra un registre que ningú no pot reescriure.

1. La versió amb pedigrí

Cada versió publicada d'una biblioteca — el paquet complet, el tarball — rep la seva empremta SHA-512 ancorada amb data certa [5], contrastable amb l'empremta del codi font visible. En el moment d'instal·lar, l'eina de gestió compara l'empremta del que ha descarregat amb l'ancorada: si no coincideixen — la discrepància que va amagar la porta del darrere de xz [1] —, no s'instal·la, i l'alarma sona sola. El pedigrí

del codi, com el del xip al capítol 70: no una promesa del venedor, sinó una cadena verificable per qualsevol abans de confiar-hi.

2. La publicació vigilada

El mantenidor ancora la seva cadena de publicació — quines versions ha publicat, quan, amb quines claus — i monitoritza els registres públics [3]: qualsevol publicació amb les seves credencials que ell no hagi fet dispara l'alarma en minuts, no en setmanes. Contra el cuc que es publica amb claus robades [2], la finestra d'infecció es redueix de dies a l'instant de la detecció — i la comunitat sencera pot veure, al registre, quines versions són legítimes i quines no. El vigilant deixa de ser una empresa: és tothom.

3. L'inventari segellat

Cada producte digital porta — i el marc europeu ho anirà exigint [4] — el seu inventari de components: quines biblioteques, quines versions (l'anomenat SBOM, la llista d'ingredients del programari). Un inventari segellat per versió, amb data certa [5], converteix la resposta a incidents en una consulta: quan esclata el pròxim xz o el pròxim Shai-Hulud [1][2], cada organització pot saber en minuts — i demostrar davant del regulador [4] — si executa o no la peça enverinada, i des de quan. La conjectura es torna verificació.

4. La línia de temps forense

Després d'un atac, la pregunta val milions: quan va entrar el codi maliciós, quines versions el porten, qui el va publicar? Amb cadenes de publicació i inventaris ancorats [3][5], la investigació forense treballa sobre una línia de temps no repudiable — la mateixa lògica dels registres del capítol 57, aplicada al codi. I la responsabilitat es reparteix amb justícia: el fabricant que va desplegar la versió neta pot demostrar-ho; el que va ignorar l'alerta datada queda igualment retratat.

Els límits, dits sense embuts: el segell acredita que un paquet existia i no s'ha alterat — no acredita que el codi sigui bo ni segur. La porta del darrere que l'autor legítim publica amb la seva pròpia clau queda perfectament ancorada — xz n'és mig exemple: «Jia Tan» era mantenidor [1]. La revisió de codi, l'auditoria i la seguretat de les claus continuen sent la primera línia; i el registre de transparència detecta la publicació fraudulenta, no la impedeix — la resposta ràpida continua sent humana.

La promesa i el perill

La promesa: una cadena de subministrament del programari on cada peça porta pedigrí verificable [3][5], les discrepàncies com la de xz canten soles [1], els cucs com Shai-Hulud troben alarmes en minuts [2] i la resposta a incidents és una consulta en lloc d'una arqueologia [4]. El món que funciona sobre codi, funcionant sobre codi acreditat.

Els perills, amb la mateixa claredat.

El primer és **la falsa seguretat del segell**. Ancorat no vol dir innocu. El codi maliciós publicat pel seu autor legítim amb les seves claus legítimes queda impecablement ancorat [1]; el pedigrí acredita origen i integritat, no bondat. Qui vengui el segell com a auditoria de seguretat estarà creant la pitjor vulnerabilitat: la confiança injustificada.

El segon és **la càrrega sobre els voluntaris**. La infraestructura digital mundial descansa sobre mantenidors sense sou — el mantenidor únic i esgotat de xz és el patró, no l'excepció [1]. Si el pedigrí esdevé una obligació burocràtica més sobre les seves esquenes, abandonaran — i el problema empitjorarà. Les eines han de ser automàtiques i gratuïtes per al codi obert, i el finançament dels comuns digitals és part de la solució de seguretat [4].

El tercer és **la centralització del registre**. Si tot el pedigrí del programari mundial depèn d'un sol registre de transparència, hem creat un punt únic de fallada i de poder [3]. La resposta és la de tot el llibre: pluralitat de registres, ancoratge creuat a cadenes públiques neutrals [5] i cap guardià únic de la veritat del codi.

I el quart és **el tecnosolucionisme de cadena**. Cap empremta no arregla l'economia política del problema: atacants estatals pacients [1], ecosistemes que premien publicar de pressa, dependències infinites que ningú no revisa. El pedigrí fa el frau visible; reduir-lo exigeix també revisió, finançament i cultura. La criptografia és la bastida, no l'edifici.

És hora d'actuar

Si tot funciona sobre codi, que el codi tingui pedigrí.

Per als mantenidors de codi obert: signeu i ancoreu cada versió — tarball inclòs [1][3][5] — i monitoritzeu el registre: que cap publicació amb les vostres claus no us agafi per sorpresa [2][3].

Per a les empreses que despleguen programari: exigiu pedigrí verificable a cada peça, mantingueu l'inventari segellat per versió [4][5] i comproveu empremtes abans d'instal·lar — el mig segon d'Andres Freund [1], automatitzat.

Per als registres i ecosistemes (npm, PyPI i companyia): atestacions de procedència per defecte [3], verificació d'empremtes a la descàrrega i alarmes públiques de publicació anòmala [2].

Per als reguladors europeus: el Reglament de Ciberresiliència [4] arriba en el moment just — que la seva aplicació reconegui el registre de transparència i l'empremta ancorada com a mitjans de compliment.

Per als governs i les grans tecnològiques: financeu els comuns digitals — el mantenidor esgotat és la vulnerabilitat número u [1]; cap criptografia no substitueix un sou digne per a qui sosté la infraestructura de tothom.

El món es va salvar una matinada de març per mig segon de latència i la tossuderia d'un enginyer [1]. Que la pròxima porta del darrere no depengui de la sort: que topi amb un pedigrí que la delati a la primera descàrrega. Pel codi que tot ho sosté, **time2act**.

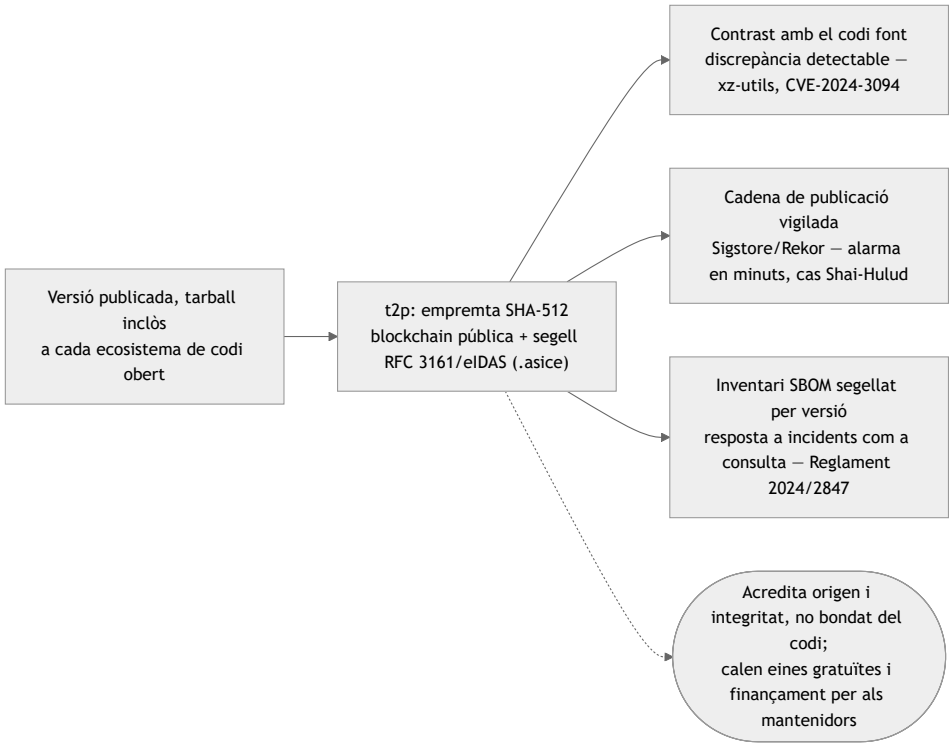


Figura 71.1 — La cadena de subministrament del programari amb prova d'existència: cada versió publicada s'ancora (empremta SHA-512 del tarball, segell de temps RFC 3161/eIDAS, blockchain pública, .asice) i es contrasta amb el codi font (la discrepància de xz-utils, detectable); la cadena de publicació vigilada als registres de transparència (Sigstore/Rekor: >101 milions d'entrades — prova d'existència en producció) dispara l'alarma davant de publicacions amb claus robades (el cuc Shai-Hulud); l'inventari (SBOM) segellat per versió fa la resposta a incidents una consulta (Reglament (UE) 2024/2847). Límits: el segell acredita origen i integritat, no bondat del codi; els mantenidors necessiten eines gratuïtes i finançament. Fonts: CVE-2024-3094; CISA (Shai-Hulud); Sigstore/Rekor; CRA.

[1] Wikipedia — *XZ Utils backdoor* (CVE-2024-3094; CVSS 10,0; Andres Freund, enginyer de Microsoft i desenvolupador de PostgreSQL, investigant ~500 ms de latència extra a SSH; report a Openwall el 28-29 de març de 2024; campanya d'enginyeria social de «Jia Tan» amb comptes falsos pressionant el mantenidor; codi ocult a build-to-host.m4 i fitxers de test binaris dins dels tarballs — invisible a la revisió del repositori; potencial superior a SolarWinds; caçat abans del desplegament massiu); 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 setembre de 2025; primer cuc autoreplicant a npm; >500 paquets; @ctrl/tinycolor amb >2,2 milions de descàrregues setmanals; paquets de CrowdStrike; collita de credencials AWS/GCP/Azure amb TruffleHog; persistència via GitHub Actions; propagació amb els drets de publicació dels mantenidors); CISA — *Widespread Supply Chain Compromise Impacting npm Ecosystem* (alerta del 23 de setembre de 2025); StepSecurity — *Shai-Hulud: Self-Replicating Worm Compromises 500+ NPM Packages*; Datadog — *The Shai-Hulud 2.0 npm worm* (segona onada, novembre). 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* (registre públic append-only; >101 milions d'entrades de >33.000 projectes: Kubernetes, CPython, Istio, urllib3; mètode de signatura per defecte per a Kubernetes, npm, Maven i PyPI; atestacions de procedència a npm i PyPI); OpenSSF / Trail of Bits — *Catching malicious package releases using a transparency log* (desembre de 2025; monitorització de Rekor per detectar publicacions fraudulentes amb credencials robades). 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 — *Reglament (UE) 2024/2847, de 23 d'octubre de 2024* (Cyber Resilience Act: requisits horitzontals de ciberseguretat per a productes amb elements digitals; en vigor el desembre de 2024; obligacions de notificació des de l'11 de setembre de 2026; aplicació plena l'11 de desembre de 2027; seguretat durant tot el cicle 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 producte (empremta SHA-512; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; empremtes de versions i manifests per lots; ancoratge neutral i transversal, complementari als registres de transparència sectorials). Vegeu els capítols 13 i 15; el pedigrí del maquinari, al capítol 70; els registres inesborrables, al capítol 57. ↩

Pesca i minerals: l'origen que es va enfonsar amb el vaixell

«Perquè tot, al final, retorna al mar — a Oceà, el riu oceànic, com el corrent sempre fluent del temps, el començament i la fi.»

— Rachel Carson, The Sea Around Us (1951), frase final

El 17 de desembre de 2014, dos vaixells de l'organització Sea Shepherd van començar a perseguir un pesquer furtiu anomenat *Thunder*, que feia anys que pescava il·legalment austromerluza a les aigües antàrtiques. La persecució va durar **cent deu dies i deu mil milles nàutiques**, fins a la zona econòmica de São Tomé i Príncipe. I allà, en lloc de rendir-se, la tripulació va fer una cosa reveladora: **van enfonsar deliberadament el seu propi vaixell**, amb les escotilles lligades en obert, per destruir les proves de la captura il·legal. Tres oficials van ser condemnats per falsificació i delictes ambientals, amb una multa de quinze milions d'euros [referència del cas Thunder]. La prova de l'origen, literalment, es va enfonsar amb el vaixell.

Aquell vaixell que s'enfonsa per esborrar el seu rastre conté la pregunta d'aquest capítol. Al capítol 29 vam veure la traçabilitat de productes agrícoles a terra contra la desforestació; aquí el patró és el mateix — segellar l'origen— però en dos dominis nous i de vegades sagnants: el **mar** i les **mines de minerals de conflicte**. La pregunta ja no és «aquest cafè ve de terra desforestada?», sinó «aquest peix es va pescar en una zona vedada i per qui?» i «aquest tàntal va finançar una milícia?».

Un de cada cinc peixos, i el 90 % de mineral «net»

L'escala del frau marí és immensa. La pesca il·legal, no declarada i no reglamentada mou entre **onze i vint-i-sis milions de tones** l'any —prop d'un de cada cinc peixos salvatges— per un valor d'entre 10.000 i 23.500 milions de dòlars [1]. I és gairebé invisible: un estudi de **Global Fishing Watch** publicat a *Nature* el 2024 va demostrar, creuant imatges de satèl·lit amb intel·ligència artificial, que **tres de cada quatre vaixells pesquers industrials del món no emeten cap senyal públic de posició** [3]. Quan el peix arriba al plat, a més, sovint no és el que diu: l'organització **Oceana** va trobar que un terç del marisc dels Estats Units estava mal etiquetat, i fins al **87 %** del que es venia com a «pargo vermell» era una altra espècie [2]. I darrere de tot plegat hi ha l'horror: la investigació de la Environmental Justice Foundation va documentar pescadors birmans **tancats en gàbies** a l'illa indonèsia de Benjina, esclaus d'una flota el peix de la qual acabava als supermercats occidentals [7].

El paral·lel mineral és igual de fosc. Els **minerals de conflicte 3TG** —estany, tàntal, wolframi i or— financen grups armats a la República Democràtica del Congo, regulats per la llei nord-americana Dodd-Frank i el reglament europeu de 2017. Els diamants tenen el seu propi sistema, el **Procés de Kimberley**, creat el 2003, que va reduir el comerç de diamants de conflicte de prop d'un 15 % als anys noranta a menys de l'1 % [6]. Però el problema és present, no històric: el grup armat M23 va prendre el 2024 la mina de coltan de Rubaya, obtenint-ne uns **800.000 dòlars al mes** [10].

Quan la traçabilitat es torna una rentadora

I aquí arriba l'advertència més important d'aquest capítol, perquè afecta el cor de la solució. Un sistema de traçabilitat no és infal·lible; pot convertir-se en una **rentadora**. L'organització **Global Witness**, en el seu informe *The ITSCI Laundromat* de 2022, va demostrar que en dues zones mineres del Kivu del Sud entre el **80 % i el 90 %** dels minerals etiquetats com a «nets» per l'únic proveïdor de traçabilitat de la zona procedien en realitat de fonts il·lícites [5]. El truc era senzill i devastador: l'etiqueta «neta» s'aplicava a mineral **ja barrejat**. Una etiqueta de bona procedència sobre mineral de mala procedència és pitjor que cap etiqueta, perquè dona una falsa confiança. I el risc de centralitzar la traçabilitat en una sola empresa també és real: Everledger, pionera a rastrejar diamants amb blockchain, va entrar en concurs el 2023 [9]. La lliçó és clara: **el problema no és tenir un certificat, sinó on i quan neix**.

La prova d'existència: segellar l'origen en el punt d'extracció

És aquí on **t2p** ataca el frau al seu origen exacte. La idea és segellar la captura o el lot **en el moment i el lloc de l'extracció**, abans que es pugui barrejar o reetiquetar. A bord, amb la xarxa acabada de pujar, o a la boca de la mina artesanal, l'operari fa una foto de la captura amb **prova de vida** del pescador o del miner; el dispositiu calcula localment l'**empremta SHA-512** de la imatge i les metadades —espècie declarada, pes, art de pesca, identificador del vaixell o de la mina—, hi incrusta el **GPS forense** i un **segell de temps RFC 3161** conforme a eIDAS, i ancorat l'empremta a la **blockchain pública**, generant un contenidor **.asice** que sobreviu sense cobertura en alta mar o en una galeria.

L'efecte és directe contra els tres fraus. Contra la **retrodatació**: ningú no pot afirmar que un peix capturat en una zona vedada es va pescar en una de legal, perquè el segell de GPS i hora és anterior i inalterable. Contra el **canvi d'espècie**: la foto segellada lliga una identitat visual al lot en origen. I contra el **rentat de lot** —el cas de la rentadora—: cada sac de coltan queda segellat amb la geolocalització de la seva mina **abans** de qualsevol barreja, de manera que mesclar mineral d'una milícia trenca la cadena d'empremtes en lloc d'heretar una etiqueta neta. El certificat de captura europeu o el de Kimberley deixen de ser un PDF validat tard i guanyen una àncora criptogràfica d'origen.

Cal dir el límit amb tota la cruesa, perquè aquí és el més perillós de tots. «Escombraries a l'entrada, escombraries a la cadena», en la seva forma extrema: el **rentat en el punt de segellat**. t2p no resol per si sol el que va destapar Global Witness. No verifica l'espècie ni la legalitat de la zona: l'empremta garanteix que *aquesta foto, en aquestes coordenades, a aquesta hora, feta per aquesta persona viva* va existir, no que el peix sigui l'espècie declarada —això exigeix ADN— ni que les coordenades estiguin fora d'una veda —això exigeix creuar-les amb mapes d'àrees protegides. No impedeix la **corrupció del segellador**: si qui segella és l'operador del vaixell furtiu o el comprador de la mina amb milícia, pot segellar captures il·legals amb metadades veritables però declaracions falses. No cobreix el **vaixell fosc**: el 75 % de la flota que no emet senyal simplement no segellaria res, i contra qui decideix no participar segueix calent la vigilància per satèl·lit. I no fixa l'atribució física de la foto a l'objecte —una foto pot mostrar un lot i enviar-se'n un altre—, per la qual cosa aporta més combinada amb un marcatge físic, com nanotraçadors o ADN, ancorat a la mateixa empremta. El seu valor real és **tancar la finestra de la retrodatació i del canvi documental**, no garantir per si sol que l'origen declarat sigui veritat.

La promesa i el perill

La promesa toca el medi ambient i els drets humans alhora. Segellar l'origen en el punt d'extracció, abans de cap barreja, faria molt més difícil colar peix d'una veda o coltan d'una milícia dins d'una cadena de subministrament global, i donaria als certificats de captura i de Kimberley una àncora que avui els falta. En un món on un de cada cinc peixos és il·legal i on una etiqueta «neta» pot amagar mineral de sang, segellar l'origen és protegir alhora el mar i les persones.

El perill demana els matisos que hem dit, i aquí són especialment greus. El primer, la rentadora: un segell sobre mineral ja barrejat dona una falsa confiança, i per això el segellat ha de ser **en origen i abans de la barreja**, mai després. El segon, la corrupció del segellador, que cap criptografia no resol sense auditoria independent. I el tercer, el vaixell fosc, contra el qual segueix calent el satèl·lit. La prova d'existència és una capa poderosa per ancorar l'origen, no un substitut ni de l'ADN, ni de la verificació geoespacial, ni de l'auditoria de qui segella.

És hora d'actuar

Per als **estats de pavelló i la Unió Europea**: exigir el certificat de captura amb un ancoratge d'origen segellat al punt de pesca, no validat tard en un despatx. Per als **importadors de minerals**: segellar cada lot a la boca de la mina, abans de cap barreja, per impedir la rentadora. Per al **Procés de Kimberley i les marques** (electrònica, joieria): reconèixer el segell d'origen com a prova primària. I per als **auditors independents i la vigilància per satèl·lit**: continuar sent vigilant el vaixell fosc i la honestedat de qui segella, perquè cap etiqueta no val res sense ells.

Un vaixell furtiu es va enfonsar a si mateix per esborrar l'origen de la seva captura. Donar a cada captura i a cada lot de mineral una prova segellada al punt d'extracció —sense oblidar mai que cal l'ADN, el satèl·lit i l'auditoria— és, en aquest front que toca el mar i la dignitat, time2act.

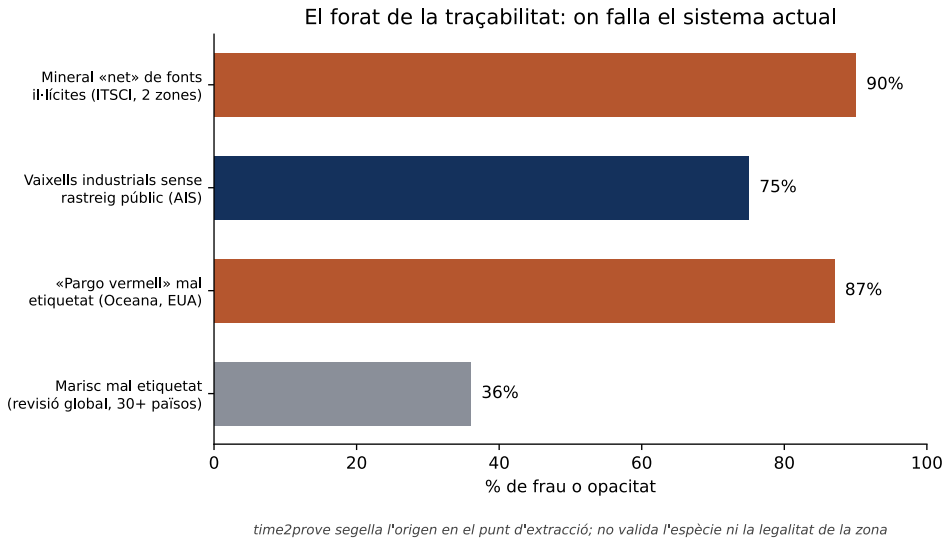


Figura 72.1 — El frau i l'opacitat per vertical: tres de cada quatre vaixells pesquers industrials no emeten senyal públic de posició (75 %, Global Fishing Watch); un terç del marisc dels EUA està mal etiquetat —fins al 87 % del «pargo vermell» (Oceana); una revisió global de més de trenta països troba un 36 % de mal etiquetatge; i fins al 90 % del mineral «etiquetat net» en dues zones del Kivu del Sud procedia de fonts il·lícites (Global Witness). t2p segella l'origen en el punt d'extracció, abans de la barreja o el canvi d'etiqueta; el que el segell NO valida és l'espècie ni la legalitat de la zona. Fonts: Global Fishing Watch; Oceana; Global Witness.

---

[1] Agnew et al. (PLOS ONE) — *Estimating the worldwide extent of illegal fishing* (11-26 milions de tones; 10.000-23.500 M$/any). https://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0004570 ↩

[2] Oceana — *Oceana study reveals seafood fraud nationwide* (33 % mal etiquetat; «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 vaixells sense rastreig públic). https://globalfishingwatch.org/press-release/new-research-harnesses-ai-and-satellite-imagery-to-reveal-the-expanding-footprint-of-human-activity-at-sea/ ↩

[4] Comissió Europea — *Illegal fishing (IUU): catch certificates i CATCH* (Reg. (CE) 1005/2008; CATCH obligatori des del 10-gen-2026). https://oceans-and-fisheries.ec.europa.eu/fisheries/rules/illegal-fishing_en

[5] Global Witness — *The ITSCI Laundromat* (fins al 80-90 % de mineral «net» procedent de fonts il·lícites). https://www.globalwitness.org/en/campaigns/natural-resource-governance/itsci-laundromat/ ↩

[6] Kimberley Process / World Diamond Council — *The Kimberley Process fact sheet* (de ~15 % als anys 90 a <1 %; ~99 % de la producció). 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 bord; l'illa de Benjina). https://ejfoundation.org/reports/thailands-seafood-slaves ↩

[8] Science Advances (Park et al.) — *Illuminating Dark Fishing Fleets in North Korea* (>900 vaixells; >164.000 t; >440 M$). https://www.science.org/doi/10.1126/sciadv.abb1197

[9] Ledger Insights — *Everledger bankruptcy* (el risc de centralitzar la traçabilitat de diamants 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 per a un grup armat). https://www.theafricareport.com/375904/drc-rwanda-rubaya-coltan-mine-at-the-heart-of-m23-financing/ ↩

Filantropia: on va el meu euro

«Qualsevol pot donar diners; però donar-los a qui cal, en la mesura que cal, quan cal, pel motiu que cal i com cal, això ja no és a l'abast de tothom, ni és fàcil.»

— Aristòtil, Ètica a Nicòmac, II, 9 (1109a)

Després del terratrèmol de Haití de 2010, la Creu Roja Americana va recaptar gairebé **cinc-cents milions de dòlars**, mentre prometia barris sencers de cases noves a un poble devastat. El 2015, els periodistes Justin Elliott, de ProPublica, i Laura Sullivan, de la ràdio pública NPR, van recórrer el terreny per veure el resultat. Van trobar **sis cases permanents** acabades a tot el país. Sobre el paper, l'organització deia haver «donat una llar a més de 130.000 persones», però aquella xifra incloïa gent que havia assistit a un seminari de reparació o que havia rebut un refugi temporal ja en runes [1]. Un detall ho resumia tot: un enginyer haitià sènior cobrava 42.000 dòlars mentre un cap de projecte expatriat en cobrava 140.000.

Aquelles sis cases contenen la pregunta d'aquest capítol, que és la del donant, no la del beneficiari. Al capítol 49 vam veure com provar que l'ajuda **arriba** a qui la necessita; aquí la pregunta és anterior i complementària: **on va el meu euro entre el clic i l'impacte, i és real l'impacte que em venen?** Perquè entre la donació i la causa hi ha un trajecte fosc —captadors, despeses, subcontractistes, xifres inflades— on es perd molt més del que es roba en el repartiment final.

On va el meu euro?

L'opacitat d'aquest trajecte és sistèmica i, de vegades, criminal. Com hem vist, el 2015 la comissió de comerç nord-americana i els cinquanta estats van demandar quatre organitzacions falses contra el càncer, controlades per la família Reynolds, per estafar **més de 187 milions de dòlars**: menys del **3 %** arribava als pacients, i els teleoperadors es quedaven el 85 % o més de cada donació, que es gastava en creuers, jet skis i entrades a concerts [2]. Però no cal arribar al frau per perdre-s-hi: segons l'informe anual de la fiscalia de Nova York, els captadors professionals es van quedar el **25 % de cada dòlar** el 2024, i en la meitat de les campanyes l'entitat va rebre **menys de la meitat** del que es va recaptar [4]. I el problema creix: l'oficina de delictes informàtics de l'FBI va xifrar en uns **96 milions de dòlars** el frau de falses caritats i campanyes de catàstrofe el 2024, amb la intel·ligència artificial fabricant aparença de legitimitat [3].

Davant d'això, el sector ha après una lliçó contraintuïtiva. El 2013 els responsables dels tres grans avaluadors d'ONG —**GuideStar, Charity Navigator i la BBB Wise Giving Alliance**— van firmar una carta oberta, *El mite de l'overhead*, advertint que fixar-se només en el percentatge de despeses administratives és un **mal indicador**: empeny les ONG a la «inanició», a no invertir en els sistemes que les farien eficaces [6]. La pregunta correcta, com defensa l'avaluador d'eficàcia **GiveWell**, no és quant gasta una ONG en si mateixa, sinó **quantes vides canvia per dòlar** —i calcula que les millors poden evitar una mort per entre tres mil i cinc mil cinc-cents dòlars [7]. Per al donant, com resumeix Daniel Borochoff, fundador de **CharityWatch**, el que ha de guiar no és el màrqueting, sinó la **transparència financera auditable**.

Quan la donació neteja una reputació

Hi ha un frau més subtil que el del diner: el de la **reputació**. El desembre de 2021, el Museu Metropolità de Nova York va retirar el nom de la família Sackler de set galeries. Els Sackler, propietaris de Purdue Pharma —el fabricant que va promoure agressivament l'OxyContin en plena epidèmia d'opioides—, havien estat «entre els nostres donants més generosos». Com documenta el periodista **Patrick Radden Keefe** en el seu llibre *Empire of Pain*, aquella filantropia va funcionar com un **rentat de reputació**: donacions milionàries a museus que compraven una façana de virtut mentre la família mai no va destinar fons a tractar l'addicció que la seva empresa havia escampat. La donació, aquí, no roba diners al donant; roba la veritat al públic.

La prova d'existència: segellar la promesa i l'evidència d'impacte

És aquí on **t2p** ofereix una capa que treu els *claims* de la paraula de l'organització i els ancora en evidència verificable. No certifica que una ONG sigui honesta, però segella **proves a cada node del recorregut del diner**. Primer, la **promesa**: en l'instant de donar, l'import, el propòsit restringit i la promesa publicada es resumeixen en una **empremta SHA-512**, s'ancoren a la **blockchain pública** i se segellen amb el segell de temps eIDAS. Això fixa de manera inalterable *què es va prometre* i *per a què* es va restringir el fons, impedint reescriure després la promesa —el patró de Haití, on una «comunitat nova» es va convertir en un «seminari». Segon, cada **desemborsament** —una factura pagada, una transferència a un subcontractista— se segella amb el seu import i la seva data, creant un rastre encadenat de l'overhead real davant del promès. I tercer, la **prova d'impacte** —la foto de l'obra, l'acta signada, el recompte d'entregables— es captura amb **GPS forense**, **segell de temps** i **prova de vida**, i s'empaqueta en un contenidor **.asice** verificable fora de línia.

L'efecte per al donant és que pot **auditar** si el 75 % que diu arribar a la causa coincideix amb els desemborsaments segellats, i que una foto d'impacte porta coordenades, hora i prova de captura en viu — no una imatge reciclada d'una altra catàstrofe. Un avaluador independent com CharityWatch, un regulador o el mateix donant poden verificar el contenidor sense dependre del servidor de l'ONG.

Cal dir el límit amb tota la cruesa, perquè aquí és subtil. «Escombraries a l'entrada, escombraries a la cadena»: el segell garanteix que una dada existia i quan, no que el diner es gastés bé. El **problema de l'última milla** és estructural: quan l'ONG paga en efectiu un proveïdor local, aquella transacció surt del rastre verificable. Una acta d'impacte pot estar **segellada, geolocalitzada i mentir alhora**; sis casos reals es poden fotografiar i presentar com a prova de «130.000 ajudats», si la mètrica declarada és tramposa —la prova d'existència no jutja la *definició* del *claim*, només la seva existència. No detecta el rentat de reputació ni l'origen brut del diner del donant: segellar una donació dels Sackler la fa més auditable, no més neta. I no substitueix el judici d'eficàcia —si són tres mil dòlars per vida o un projecte inútil—, que exigeix l'avaluació de GiveWell i l'auditoria humana. **t2p** aporta **integritat de l'expedient**, no **mèrit** del programa.

La promesa i el perill

La promesa és restaurar la confiança que sosté tota la filantropia. Una capa que segelli la promesa restringida, cada desemborsament i l'evidència d'impacte donaria al donant la capacitat d'auditar el seu euro, faria molt més difícil inflar beneficiaris o reciclar fotos, i premiaria les ONG honestes amb una transparència demostrable en lloc de penalitzar-les per un overhead mal entès. En un sector que viu de la confiança, fer l'expedient inalterable és protegir tant el donant com les organitzacions que fan bé la seva feina.

El perill demana els matisos que hem esmentat. El primer, l'última milla: el rastre s'acaba on algú deixa de capturar evidència honesta. El segon, no confondre integritat amb veritat: una mètrica tramposa segellada continua sent tramposa. El tercer, que el segell no neteja diners bruts ni jutja l'eficàcia. I el quart, la captura selectiva: si l'ONG tria què segella, el rastre tindrà forats. La prova d'existència és una eina poderosa per a la transparència del trajecte, no un certificat d'honestedat ni un substitut de l'avaluació d'impacte.

És hora d'actuar

Per als donants: exigir la promesa restringida i l'evidència d'impacte segellades, i centrar-se en el cost per resultat, no en l'overhead. Per a les ONG: segellar cada desemborsament i cada prova d'impacte, convertint la transparència en un avantatge demostrable. Per als avaluadors i reguladors (CharityWatch, les fiscalies): reconèixer el contenidor segellat com a base d'auditoria independent. I per a les plataformes de captació (el crowdfunding): lligar cada campanya a una promesa i una evidència verificables, perquè una pàgina falsa no pugui cobrar en nom d'una víctima.

Mig miler de milions de dòlars van produir sis casos, i ningú ho va saber fins que dos periodistes ho van comptar. Donar a cada donació una prova segellada del seu trajecte —sense oblidar mai que cal l'avaluació d'impacte i l'auditoria humana— és, en aquest front que sosté la generositat, time2act.

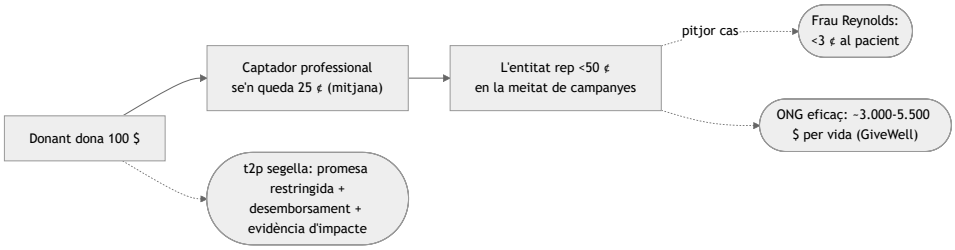


Figura 73.1 — El recorregut d'un dòlar donat, amb les seves fuites reals: el captador professional se'n queda 25 cèntims de mitjana (fiscalia de Nova York, 2024), i en la meitat de les campanyes l'entitat rep menys de la meitat; en el frau Reynolds, menys de 3 cèntims arribaven al pacient; en el projecte de Haití, un 40 % es perdia en overhead. Com a contrapunt, una ONG eficaç evita una mort per uns 3.000-5.500 dòlars (GiveWell). t2p segella tres nodes —la promesa restringida, cada desembors ament i l'evidència d'impacte (GPS + hora + prova de vida)—, convertint el «confia en l'informe» en evidència auditable. Límit: no jutja si la mètrica declarada és honesta ni l'eficàcia del programa. Fonts: fiscalia de Nova York; FTC; ProPublica; GiveWell.

---

[1] ProPublica / NPR (Justin Elliott i 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* (família Reynolds; <3 % als pacients). 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 augmenta la legitimitat aparent). https://www.ic3.gov/PSA/2025/PSA250116 ↩

[4] New York Attorney General (Letitia James) — *Pennies for Charity 2025* (els captadors es queden el 25 %; <50 % en la meitat de campanyes). 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 conferències; directius destituïts el març de 2016). https://www.cbsnews.com/news/cbs-news-investigates-wounded-warrior-project-spending/

[6] GuideStar, Charity Navigator i BBB Wise Giving Alliance — *The Overhead Myth* (2013; l'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 i 5.500 $ per 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 $ per recaptar 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 filantropia com a «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* (context del frau). https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

Caixes negres: la dada que el fabricant deia que no existia

«Els fets són tossuts; i siguin quins siguin els nostres desitjos, les nostres inclinacions o els dictats de les nostres passions, no poden alterar l'estat dels fets i de les proves.»

— John Adams, defensa als judicis de la Massacre de Boston (1770)

El 25 d'abril de 2019, a Key Largo (Florida), un Tesla amb l'Autopilot activat va causar un accident mortal. Quan els advocats de la víctima van reclamar les dades del cotxe, Tesla va respondre primer que **no existien**; després va dir a la policia que estaven «corruptes», i va invocar una funció d'**autoesborrat que no existia**. Tot era fals: els seus propis servidors havien rebut una **instantània de col·lisió** —vídeo, dades del bus del cotxe i del registrador— uns **tres minuts després de l'impacte**. Un perit extern, Alan Moore, ho va recuperar tot fent una **imatge bit a bit de la memòria** de la unitat de control. «Els enginyers de Tesla van dir que no es podia fer... i ho va fer gent de fora de Tesla.» L'agost de 2025, un jurat de Miami va condemnar Tesla a pagar **243 milions de dòlars**, dels quals 200 en danys punitius [1][2].

Aquell forcejament per una dada conté la pregunta d'aquest capítol, diferent de les del capítol 20 (l'evidència d'atrocitats per a un tribunal) i del capítol 57 (els registres d'una intrusió informàtica). Aquí la dada és **telemetria de màquina** —velocitat, frenada, classificació d'objectes, paràmetres de vol— i el conflicte típic no és «ens van piratejar», sinó **«el cotxe diu X, el conductor diu Y»** i, sobretot, **qui controla i retalla la dada del fabricant**. Perquè el problema, com veurem, no és que faltin dades: és que qui les custodia pot fer-les desaparèixer.

La caixa negra existeix; el problema és qui la controla

Els registradors moderns són prodigiosos. Una caixa negra d'avió sobreviu a un impacte de 3.400 g, a 1.100 graus de foc durant mitja hora i a la pressió de l'aigua a sis mil metres, i registra més de vuitanta-vuit paràmetres [5]. El registrador d'un cotxe captura ara els vint segons previs a un xoc deu vegades per segon [7]. La dada hi és. El problema és la **custòdia i la selecció**. En l'atropellament mortal d'Elaine Herzberg per un Uber autònom a Tempe el 2018, la telemetria va revelar que el sistema **va detectar la vianant 5,6 segons abans** però no la va saber classificar mai —objecte, vehicle, bicicleta— mentre el frenat d'emergència estava desactivat; la caixa negra no va captar una avaria, sinó una **indecisió algorítmica** mil·lisegon a mil·lisegon [3]. I el cas de Cruise a San Francisco va mostrar el perill en la seva forma més pura: després que un robotaxi arrossegués una vianant sis metres, l'empresa va ensenyar a l'autoritat de trànsit de Califòrnia un **vídeo retallat que acabava abans de l'arrossegament**; la **DMV li va suspendre els permisos** per tergiversar la informació de seguretat [4]. Quan qui controla la dada és el mateix que s'investiga, **la tria del que s'ensenya esdevé el problema central**.

Quan la caixa no arriba al final, o no resol la causa

Però la caixa negra té dos límits que cap tecnologia pot esborrar. El primer és que només serveix si grava fins al final. En l'accident de Jeju Air a Corea del Sud el desembre del 2024, amb 179 morts, tant la gravadora de veu com la de dades es van aturar uns quatre minuts abans de l'impacte i van deixar fora de la caixa la franja decisiva [9].

El segon límit és encara més profund: la caixa fixa els fets físics, però no resol la interpretació. En l'accident d'EgyptAir 990 del 1999, amb les mateixes dades autèntiques i íntegres, l'autoritat nord-americana va concloure una acció deliberada del copilot, mentre que l'autoritat egípcia la va atribuir a una avaria mecànica [10]. Els bits eren els mateixos; el seu significat, en disputa. La cadena de blocs no és perit.

La prova d'existència: segellar la caixa negra

És aquí on **t2p** aporta una capa d'**integritat probatòria**, no només de captura. Segella la caixa negra perquè ningú pugui dir després «aquesta no és la dada original». En el moment en què el registrador tanca un esdeveniment —una instantània de col·lisió, un bloc de dades de vol o un registre d'aterratge d'un dron

—, el dispositiu calcula l'**empremta SHA-512** i l'ancora a la **blockchain pública** amb un **segell de temps RFC 3161** conforme a eIDAS. Només es publica l'empremta; la dada crua resta privada, però queda provada la seva existència i el seu contingut exacte en aquell instant.

Això contraresta directament els casos que hem vist: si l'empremta de la instantània completa s'ancora tres minuts després de l'impacte, una dada posterior «diferent» no coincidirà amb el segell, i un vídeo truncat com el de Cruise mostrarà una empremta incompatible amb la del clip íntegre. El **GPS forense** i el segell de temps per a drons i vehicles permeten refutar l'afirmació «jo no era en zona restringida», com al cas de Cap Canyaveral, on els registres del propi dron contradeien l'operador [8]. La **prova de vida** en el moment de l'extracció certifica que una persona identificada va treure la dada en tal data, segellant la cadena de custòdia des del primer minut.

Cal assenyalar tres limitacions. Primer, «escombraries a l'entrada, escombraries a la cadena»: el segell no corregeix la dada d'origen; si un sistema classifica malament una vianant, només certifica que l'error va existir en aquell moment. Segon, **no resol la interpretació**: com demostra el cas de l'EgyptAir 990, la prova hauria blindat els bits però la disputa pericial sobre què signifiquen quedaria intacta. Tercer, **no grava el que la màquina mai no va captar**: a Jeju Air les caixes van deixar de registrar quatre minuts decisius i el segell només tanca el buit. Finalment, l'ancoratge **ha de passar al dispositiu i de manera immediata**; si el fabricant controla el moment del segellat —com avui controla la instantània— podria segellar una versió ja modificada. El valor és real només amb un **segellat automàtic, al dispositiu i instantani**, fora del control discrecional de qui s'investiga.

La promesa i el perill

La promesa és tancar l'asimetria que va costar a Tesla **243 milions de dòlars** provar en contra seva; una caixa negra segellada en origen faria impossible negar, corrompre o retallar la dada després del fet, i donaria als investigadors i als tribunals una cadena de custòdia inatacable des del minut zero, protegint tant les víctimes com els fabricants honestos, que podrien demostrar que la seva dada és l'original. En un món on els accidents els decideixen algoritmes, fer la caixa negra inalterable és restaurar la confiança en el que va passar de debò.

El perill demana els matisos que hem dit. Primer, no confondre integritat amb veritat ni amb causa: el segell blinda els bits, però no n'hi resol el significat. Segon, no rebleix els buits del que el sensor no va captar. I tercer, i més important, si el segellat no és immediat i al dispositiu, el fabricant pot seguir curant la dada abans de segellar-la. La prova d'existència és una capa poderosa d'integritat probatòria, no un perit ni un substitut d'una gravació completa.

És hora d'actuar

Per als fabricants (de cotxes, avions, drons): segellar cada bloc de dades al dispositiu i a l'instant del seu tancament, fora del seu propi control discrecional. Per als reguladors (organismes de seguretat del transport, aviació, trànsit): exigir el segellat en origen com a part de l'homologació dels registradors. Per als investigadors i tribunals: segellar l'extracció amb prova de vida, perquè la cadena de custòdia sigui inatacable. I per als operadors: una dada que els protegeixi tant si tenen raó com si no, perquè la veritat de l'accident no depengui de qui controla el servidor.

Un fabricant va dir que una dada no existeix, i un perit de fora la va trobar als seus servidors. Donar a cada caixa negra una prova segellada en el moment de néixer — sense oblidar mai que el segell no resol la causa ni rebleix el que no es va gravar — és, en aquest front on decideixen les màquines, time2act.



Figura 74.1 — Els registradors (la caixa negra d'avió amb més de 88 paràmetres i ara fins a 25 h de veu; el registrador del cotxe amb els 20 s previs al xoc; el registre de vol d'un dron) capturen la dada. t2p no millora la captura: en l'instant en què el registrador tanca un esdeveniment, en calcula l'empremta SHA-512 al dispositiu i l'ancora a la blockchain pública amb segell eIDAS, de manera que negar la dada (Tesla), retallar-la (Cruise) o alterar-la deixa una empremta que no quadra. Límit: el segell no corregeix una dada errònia, no resol la disputa pericial sobre la causa (EgyptAir 990), i no rebleix el que el sensor

no va gravar (Jeju Air, on la gravació es va tallar 4 minuts abans). Fonts: NTSB; California DMV; cas Benavides contra Tesla.

---

[1] NPR — *Tesla ordered to pay $243 million in fatal Autopilot crash* (Benavides contra Tesla; 200 M$ en danys punitius; 33 % de responsabilitat). 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 instantània de col·lisió a +3 min; la imatge NAND; el perit 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; frenat d'emergència desactivat). https://www.ntsb.gov/investigations/Pages/HWY18MH010.aspx ↩

[4] California DMV — *Statement on Cruise LLC suspension* (24-oct-2023; el metratge de l'arrossegament, omès). 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* (supervivència; ≥88 paràmetres). 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 hores). 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-xoc 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* (els registres de geofencing contradiuen l'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* (els 4 minuts decisius, fora de la caixa). 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)* (les mateixes dades, causes oposades). https://www.ntsb.gov/investigations/AccidentReports/Reports/AAB0201.pdf ↩

La caixa negra personal: evidència preventiva per a víctimes i per a innocents

«Val més una unça de prevenció que una lliura de remei.»

— Benjamin Franklin, Pennsylvania Gazette (1735)

El 20 de març de 2024 no va passar res que es veiés a simple vista. Cap sirena, cap titular. Aquell dia, el sistema Cometa —el servei estatal que registra cada moviment dels agressors amb polsera antimaltractament— canviava de mans: de Telefónica a la unió temporal d'empreses formada per Vodafone i Securitas. En la migració, els historials de posicionament anteriors a aquella data van quedar inaccessibles per als jutjats [1]. Els mesos següents, en sales de vistes de tot Espanya, fiscals que volien provar trencaments d'ordres d'allunyament es van trobar amb el buit: la memòria anual de la Fiscalia General de l'Estat, coneguda el setembre de 2025, reconeix «nombroses absolucions i sobreseïments provisionals» per la pèrdua d'aquelles dades, en un sistema amb unes 4.500 polseres actives, i parla d'una potencial desprotecció de les víctimes [1][2]. El Govern coneixia incidències des del gener de 2024 [3]. La caixa negra que havia de protegir milers de dones va fallar en silenci, i part de la prova va morir amb ella.

Aquest capítol tracta la caixa negra personal: la certificació preventiva de la teva pròpia vida —l'àudio d'una conversa amenaçadora, el clip de la càmera del cotxe, la foto datada— segellada al dispositiu per si un dia ets víctima o t'acusen falsament. Les caixes negres dels fabricants són al capítol 74; la cadena de custòdia judicial, al capítol 77; la reclamació d'assegurances, al capítol 28; la documentació del dany en línia, als capítols 83 i 84. La pregunta clau: com pot una persona corrent guardar-se la veritat sense convertir-se en espia de ningú? La resposta és **t2p**: el contingut no surt mai del telèfon; només l'empremta SHA-512, amb l'ancoratge de l'empremta a la blockchain pública i el segell de temps RFC 3161/eIDAS complementari dins d'un contenidor .asice, queda fixada per sempre [18]; i revelar-la o no és sempre decisió teva. La neutralitat és radical: la mateixa eina serveix la víctima que documenta —el cas de cada dia— i l'innocent que es defensa — el cas rar, però devastador. La prova no té bàndol.

Quan la caixa negra de l'Estat falla

Val la pena mirar de prop el cas Cometa, perquè és una paràbola sencera. La infraestructura probatòria més sensible del país —la que registra els moviments dels agressors per protegir víctimes de violència de gènere— depenia d'una migració de base de dades entre contractistes. En el canvi de Telefónica a la UTE de Vodafone i Securitas, els posicionaments anteriors al 20 de març de 2024 van esdevenir inaccessibles per a les autoritats judicials [1]. Quan un fiscal necessitava demostrar que un agressor s'havia acostat a la seva víctima abans d'aquella data, la dada ja no hi era: d'aquí les absolucions i els sobreseïments provisionals que la Fiscalia va acabar reconeixent a la seva memòria anual [2]. El Govern tenia constància d'incidències des del gener de 2024 [3]; la gestió va costar una reprovació parlamentària a la ministra i unes disculpes públiques a les víctimes, sense descartar penalitzacions al contractista [4]. L'anàlisi jurídica posterior ho va resumir sense embuts: un sistema «en crisi» [5].

La lliçó no és partidista, és estructural: quan la prova viu en un únic dipòsit centralitzat, un canvi de contracte, un error de migració o una decisió administrativa la poden esborrar. No cal cap malícia; n'hi ha prou amb la fragilitat. La prova d'existència inverteix el disseny: si cada posició i cada alerta s'hagués ancorat en origen —empremta SHA-512 i segell de temps, en el mateix instant de produir-se [18]—, el contingut s'hauria pogut perdre igualment, però hauria estat impossible discutir què existia, què es va registrar i quan. Cap defensa no hauria pogut fonamentar-se en el dubte sobre si les dades van existir mai.

I aquí neix la pregunta que dona sentit a tot el capítol: si això li pot passar a l'Estat, amb 4.500 polseres i un contracte milionari, què no li pot passar al ciutadà que, davant d'un conflicte, només té la seva paraula?

El dret a gravar la teva pròpia vida

La regla de base la va fixar el Tribunal Constitucional fa quatre dècades, i va néixer, precisament, d'una gravació aportada en un conflicte laboral. La STC 114/1984, de 29 de novembre, estableix que gravar una conversa en què participes no vulnera el secret de les comunicacions de l'article 18.3 de la Constitució —«no hi ha secret per a aquell a qui la comunicació va dirigida»— i que la gravació pròpia és admissible

com a prova documental, amb un límit: no envair l'esfera íntima de l'altre [6]. El Tribunal Suprem ho ha confirmat de manera constant [7]. El teu telèfon pot ser, legalment, el teu testimoni.

La línia vermella també és nítida. Gravar converses alienes —aquelles en què no participes— amb artificis tècnics d'escolta o gravació és delicte de descobriment i revelació de secrets: l'article 197.1 del Codi Penal el castiga amb presó d'un a quatre anys i multa, i si el material es difon, la pena puja de dos a cinc anys [8]. La caixa negra personal no és un micròfon ocult a casa d'altri: és el registre de la teva pròpia vida, de les converses que tu mantens i del que passa davant del teu parabrisa.

El subcas del parabrisa mereix el seu propi mapa, perquè el mosaic europeu és instructiu. A Espanya, l'Agència Espanyola de Protecció de Dades admet la càmera de bord (*dashcam*) amb condicions: gravació limitada a l'incident —uns vint segons abans i després—, preferiblement sense so i minimitzant les dades de tercers; amb aquests límits, la gravació val com a prova, emparada per l'interès legítim i la tutela judicial efectiva [13]. Alemanya n'admet la prova limitada al moment del sinistre; França fa el conductor responsable del tractament de les dades; i Portugal aplica la política més dura d'Europa: la Llei 58/2019 prohibeix les *dashcams* fins al punt que ni tan sols es poden portar al cotxe [14]. El dret a la teva pròpia prova existeix, doncs, però és estret i exigeix un respecte escrupolós per la intimitat aliena. És exactament el disseny de t2p: només empremtes a la cadena, contingut al dispositiu, revelació voluntària davant del jutge [18].

La gravació ja no es creu

Dues forces han xocat en aquesta dècada: mai no havia estat tan fàcil gravar-ho tot, i mai no havia estat tan fàcil falsificar-ho tot. Amb la tecnologia actual es clonen veus convincents a partir de tres a cinc minuts d'àudio net, i alguns sistemes en tenen prou amb trenta segons [9]: qualsevol fragment de conversa pot ser imitat per una màquina que reprodueix el timbre, el ritme i les imperfeccions del parlant.

Els tribunals ho saben, i han mogut fitxa. En el procés, impugnar l'autenticitat d'un àudio desplaça la càrrega de la prova cap a qui el presenta; i la jurisprudència recent del Tribunal Suprem ja no accepta la impugnació genèrica —el «podria ser fals»—, sinó que exigeix una impugnació tècnica i fonamentada, amb els criteris d'admissió cada cop més estrictes: anàlisi forense, cadena de custòdia completa, integritat acreditada, contrast amb altres proves [10].

Per al ciutadà, la conseqüència és incòmoda: la teva gravació verídica, per si sola, val cada dia menys. L'endemà d'un conflicte, l'altra part sempre podrà sembrar el dubte —«és un munt de bits, editats a saber quan»—, i el peritatge que ho resol és car, lent i cada generació de síntesi el fa més difícil [9][10].

La sortida estructural és la del capítol 15: no detectar la falsedat a posteriori, sinó acreditar l'autenticitat a priori. Una gravació amb l'empremta SHA-512 segellada en el moment de la captura i ancorada a la blockchain pública [18] arriba al jutjat amb la pregunta clau ja resolta: aquest fitxer, exactament aquest, existia en aquella data i no s'ha tocat des d'aleshores. El dubte raonable canvia de bàndol: qui vulgui negar-la haurà d'explicar com es falsifica un segell criptogràfic cap enrere en el temps.

La caixa negra que ja portes a sobre

La caixa negra personal no és vigilància: és memòria certificada pròpia, activada quan tu vols. Un botó abans d'una reunió tensa; un mode al cotxe que només conserva l'incident; una foto que se segella en fer-se. El contingut resta xifrat al dispositiu; només l'empremta viatja [18]. No es tracta de gravar la vida sencera, sinó d'obrir un canal controlat per a aquells fragments que poden decidir el teu destí.

L'Estat, de fet, ja apunta cap aquí. L'aplicació oficial AlertCops, de la Secretaria d'Estat de Seguretat, incorpora un botó SOS que, premut cinc vegades en menys de sis segons, envia a les forces de seguretat la ubicació i deu segons d'àudio; les víctimes de violència de gènere s'hi registren amb el codi AVDG per a l'avís automàtic als cossos competents [15]. És el reconeixement institucional que un àudio immediat i datat pot trencar el cercle de la paraula contra paraula.

La víctima d'assetjament —laboral, veïnal, domèstic— hi troba el primer ús: acumular durant mesos converses pròpies segellades, emparades per la STC 114/1984 [6]. Quan decideixi denunciar, no portarà records dispersos: portarà una cronologia verificable.

L'innocent acusat falsament hi troba el segon. És un cas estadísticament rar —les denúncies per violència de gènere que acaben en condemna ferma per denúncia falsa són el 0,0082 % de gairebé tres milions de

denúncies, segons la sèrie de la Fiscalia [11][12], i aquest llibre ho subratlla per no alimentar cap mite—, però per a qui el pateix és devastador. Una agenda segellada —on eres, què vas dir— pot ser l'única defensa possible contra una difamació o una acusació errònia.

I el conductor hi troba el tercer, davant les màfies del sinistre simulat: les asseguradores detecten uns 400.000 intents de frau l'any, amb un cost potencial de 2.000 milions d'euros; sis de cada cent lesions declarades amaguen frau, i els accidents simulats són el 3,2 % dels declarats però el 18 % del cost dels sinistres investigats [16]. El juliol de 2025, una sola trama va acabar amb 32 detinguts per set accidents simulats en vuit mesos [17]. La *dashcam* amb segell en origen, dins dels límits de l'AEPD [13], és la caixa negra sobre rodes del particular.

La prova d'existència aplicada

Una persona corrent, un telèfon corrent, i una decisió: guardar-se la veritat per si mai cal ensenyar-la.

1. La víctima que documenta

Una dona que pateix amenaces reiterades grava les converses en què participa, emparada per la STC 114/1984 [6]. Cada vespre, el mòbil calcula l'empremta SHA-512 dels fitxers, hi afegeix el segell de temps RFC 3161/eIDAS i l'ancora a la blockchain pública [18]. El contingut no surt del telèfon: ni núvols, ni tercers, ni risc de filtració. El dia que denuncia, la seva advocada aporta una cronologia d'evidència amb data certa que cap impugnació genèrica no pot tombar [10]. Si l'agressor esborra els seus missatges o nega les trucades, el registre d'ella continua existint — i no depèn de cap contractista ni de cap migració de bases de dades [1]. Complementa, no substitueix, els canals oficials: AlertCops i el 016 [15].

2. L'innocent que es defensa

Un home acusat d'haver dit o fet una cosa en un moment concret aporta la seva agenda segellada: l'àudio de la reunió real, la ubicació datada, el missatge original. No és una eina de sospita contra ningú —les condemnes fermes per denúncia falsa són ínfimes [11][12]—, sinó una assegurança de baix cost contra el pitjor dia d'una vida. La clau és tècnica: el segell es va crear abans del conflicte, i ningú no fabrica una coartada retroactiva contra una cadena de blocs [18].

3. La caixa negra sobre rodes

Un conductor amb la càmera configurada al mode que recomana l'AEPD —només l'incident, uns vint segons abans i després, sense so [13]— topa amb una frenada sospitosa: dos cotxes coordinats, quatre ocupants, lesions declarades l'endemà. El clip segellat en origen —empremta i hora ancorades en el mateix minut [18]— desmunta el guió de la trama [16][17]: contra un segell criptogràfic no hi ha versió coordinada que aguanti. Per a l'asseguradora, peritatge més ràpid; per al conductor honest, la fi del «tu contra quatre testimonis».

4. El contracte de paraula

L'autònoma que tanca un encàrrec per telèfon, el llogater que acorda una reparació amb el propietari, la família que pacta els torns de cura d'un pare gran: converses pròpies, gravades legalment [6] i segellades al moment [18]. Si tot va bé, ningú no les escoltarà mai. Si algú nega la seva paraula, la data certa converteix el «jo no vaig dir mai això» en una posició insostenible.

Cal dir també, amb la mateixa claredat, què no fa el segell: acredita quan existia un fitxer i que no s'ha alterat, però no acredita que el que s'hi diu sigui veritat; no converteix en lícita una gravació que no ho era —gravar converses alienes continua sent delicte de l'article 197 [8]—; i no allibera el jutge de valorar la prova en el seu context. La caixa negra personal és memòria blindada, no veredicte.

La promesa i el perill

La promesa és triple: que cap víctima no torni a perdre un judici perquè la prova vivia en un servidor aliè i va desaparèixer amb un contracte [1][2]; que cap innocent no depengui només de la seva paraula; i que la gravació verídica recuperi el valor probatori que la clonació de veu i la síntesi li estan erosionant [9][10]. Però aquest és, potser, el capítol on els perills demanen més franquesa de tot el llibre.

El primer és **la societat de la sospita**. Si tothom grava sempre tothom «per si de cas», la confiança íntima mor: una societat de caixes negres mútues és una societat vigilada des de dins. Per això la caixa negra personal ha de ser defensiva i excepcional: s'activa amb intenció, no per defecte; registra la teva vida, no la dels altres; i el disseny de només-empremtes [18] garanteix que res no es pot difondre que no s'hagi revelat formalment. L'eina és per a la sala de vistes, no per a les xarxes.

El segon és **la línia penal i l'esfera íntima**. El dret empara la gravació pròpia (STC 114/1984 [6]) i castiga la intercepció de la conversa aliena (article 197 del Codi Penal [8]). Cap segell no blanqueja una captació il·lícita, i la difusió fora del procés pot ser delicte encara que la gravació fos lícita. La frontera entre prova legal i exposició pública ha de quedar gravada al mateix disseny de l'eina.

El tercer és **la revocabilitat i l'oblit**. Les empremtes de la teva vida han de poder invalidar-se a petició teva, i no hi pot haver cap registre central d'empremtes personals. La immutabilitat protegeix la prova; no pot esdevenir una condemna perpètua de la pròpia memòria.

I el quart és **l'excusa per no arreglar l'Estat**. La caixa negra personal no eximeix l'Administració de fer funcionar Cometa, AlertCops o el 016 [1][15]. Que el ciutadà hagi de blindar-se la prova és un símptoma, no un ideal: la promesa només és justa si conviu amb institucions que també fan la seva feina.

És hora d'actuar

La prova de la teva vida no pot dependre ni de la memòria ni d'un contracte de manteniment.

Per a tu, ciutadà: coneix el teu dret — gravar les converses en què participes és legal des de la STC 114/1984 [6]; gravar les alienes, delicte [8]. Activa la caixa negra amb intenció — la reunió difícil, el trajecte en cotxe, l'incident — i segella al dispositiu [18]. I no difonguis mai: revela només davant del jutge.

Per a les víctimes de violència de gènere i d'assetjament: registreu-vos a AlertCops amb el codi AVDG [15]; documenteu amb gravacions pròpies segellades i cerqueu assessorament legal. Una cronologia verificable val més que mil records dolorosos.

Per a advocats, jutges i pèrits: exigiu i valoreu el segell de captura; una empremta ancorada resol d'entrada la impugnació d'autenticitat que avui encareix i allarga els procediments [10].

Per a les administracions: ancoreu en origen els sistemes probatoris públics — que cap migració no torni a esborrar la protecció de 4.500 dones [1][2][3] — i reconegueu valor probatori qualificat a l'evidència ciutadana segellada.

Per a les asseguradores: premieu la càmera de bord conforme a l'AEPD amb segell en origen [13]: menys frau [16][17], peritatges més curts i clients honestos més ben tractats.

Per als legisladors: estabiliu la presumpció d'autenticitat per a la prova segellada en captura; garantiu-ne la revocabilitat; i ni un pas cap a l'obligatorietat — la caixa negra personal és un dret, mai un deure.

La caixa negra de l'Estat va fallar un 20 de març sense que ningú no ho veiés [1]. La teva no depèn de cap contracte, de cap migració ni de cap empresa: només de tu i de la matemàtica. Per a la veritat de cadascú, **time2act**.

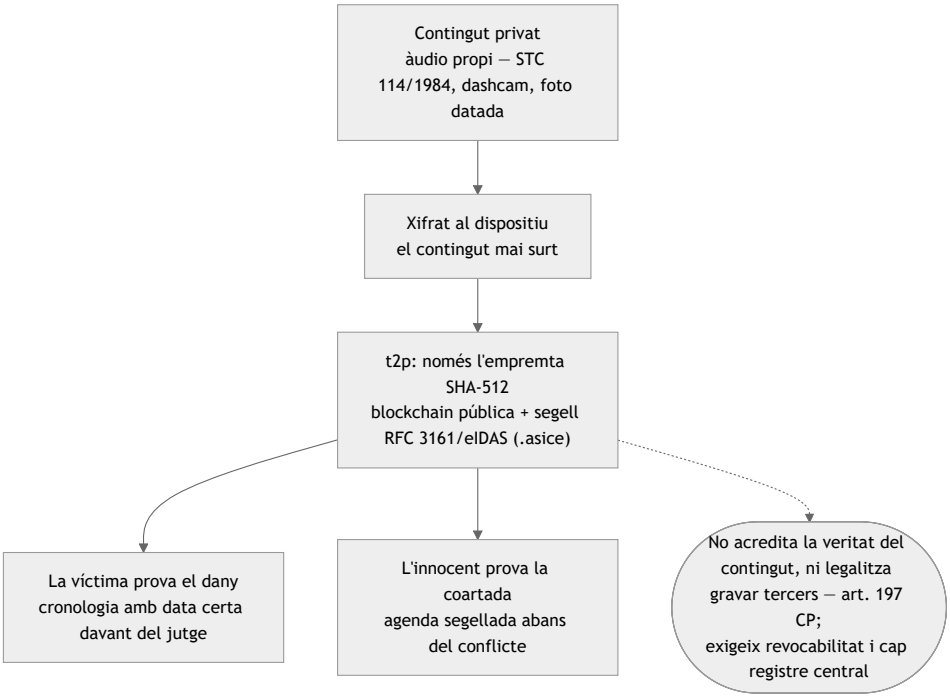


Figura 75.1 — La caixa negra personal: l'àudio d'una conversa pròpia (STC 114/1984), el clip de la dashcam (límits AEPD) o la foto datada es xifren i NO surten mai del dispositiu; només l'empremta SHA-512 amb segell de temps RFC 3161/eIDAS s'ancora a la blockchain pública (.asice). La revelació és decisió del titular, davant del jutge. Dues sortides simètriques: la víctima que prova el dany i l'innocent que prova la coartada. Límits: no acredita la veritat del contingut, no legalitza la gravació d'altri (art. 197 CP), exigeix revocabilitat i cap registre central. Fonts: STC 114/1984; Fiscalia General de l'Estat (Cometa; denúncies falses 0,0082 %); AEPD; UNESPA.

---

[1] Euronews — *Un fallo informático en las pulseras antimaltrato en España absuelve a decenas de agresores* (18 de setembre de 2025; migració Telefónica → UTE Vodafone+Securitas; dades anteriors al 20 de març de 2024 inaccessibles; memòria de la Fiscalia General de l'Estat; ≈4.500 polseres actives). 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 setembre de 2025; «nombroses absolucions i sobreseïments provisionals»). 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 (agències) — *Redondo aborda en el Senado la gestión de pulseras para maltratadores tras ser reprobada en el Congreso* (setembre de 2025; disculpes a les víctimes; possibles penalitzacions al contractista). 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 d'octubre de 2025). https://www.hayderecho.com/2025/10/08/pulseras-antimaltrato-analisis-juridico-politico/ ↩

[6] Tribunal Constitucional — *STC 114/1984, de 29 de novembre* (gravar una conversa pròpia no vulnera l'art. 18.3 CE; admissible com a prova documental; límit de l'esfera íntima; origen laboral del cas). 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 gravacions de participants); 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 (advocats) — *¿Es delito grabar una conversación sin consentimiento?* (art. 197.1 CP: presó d'1 a 4 anys i multa de 12 a 24 mesos; difusió: 2 a 5 anys); 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* (clons convincents amb 3-5 minuts d'àudio; alguns sistemes amb 30 segons; anàlisi d'espectrogrames i prosòdia). https://digitalperito.es/glosario/clonacion-voz/ ↩

[10] Economist & Jurist — *La prueba sintética en el proceso judicial: retos probatorios de los deepfakes* (impugnar desplaça la càrrega; el TS exigeix impugnació tècnica, no genèrica; criteris d'admissió reforçats); 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 condemnes fermes, 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* (sèrie 2009-2024); ANAVID — *¿De dónde sale la cifra del 0,01 %?* (matís metodològic: només falsedat acreditada amb dol). 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?* (criteris AEPD: gravació limitada a l'incident, ~20 segons abans i després, preferible sense so; vàlida com a prova per interès legítim i 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: Llei 58/2019, prohibit fins i tot portar-la; Alemanya: admissió limitada a l'incident; França: CNIL, conductor responsable del tractament). https://www.tododashcam.es/pages/blog-legislacion-dashcams-espana ↩

[15] AlertCops (Secretaria d'Estat de Seguretat, Ministeri de l'Interior) — *AlertCops incorpora un botón SOS* (5 pulsacions en menys de 6 segons; ubicació + 10 segons d'àudio a les FCSE; codi AVDG per a víctimes de violència de gènere). 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 intents de frau anuals; ≈2.000 M€; 6 de cada 100 lesions; accidents simulats: 3,2 % dels declarats, 18 % del cost investigat; Procediment Operatiu 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 juliol de 2025; set accidents simulats en vuit mesos). 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 producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; el contingut no surt mai del dispositiu; revelació voluntària). Vegeu els capítols 13 i 15. ↩

Dades genòmiques: el consentiment d'un exposa molts

«...una de les idees més poderoses i perilloses de la història de la ciència: el "gen", la unitat fonamental de l'herència.»

— Siddhartha Mukherjee, The Gene: An Intimate History (2016)

El 24 d'abril de 2018, la policia de Sacramento va detenir Joseph James DeAngelo, un expolicia de setanta-dos anys, com el «Golden State Killer», responsable de més de dotze assassinats i cinquanta violacions als anys setanta i vuitanta. La pista no va sortir de cap base de dades policial. Els investigadors van pujar un perfil d'ADN de l'escena del crim a una base genealògica pública, GEDmatch, i la genealogista forense Barbara Rae-Venter el va rastrejar a través de **cosins de tercer i quart grau** que sí que havien pujat el seu ADN voluntàriament [7]. L'assassí no el va delatar el seu propi ADN, sinó **l'arbre genealògic de la seva família**.

Aquell cas, alhora una victòria de la justícia i un malson de la privacitat, conté la paradoxa central d'aquest capítol, diferent de la del capítol 47 —«qui ets?»— i de la del capítol 49 —la biometria del refugiat vulnerable. Aquí el subjecte és el **consumidor** que paga voluntàriament per un test d'ADN, i la dada té una propietat que cap altra no té: **és teva i de la teva família alhora, és irrevocable i delata persones que mai no van consentir res**. El consentiment d'un exposa molts.

La dada que no pots canviar ni recuperar

La fragilitat d'aquesta dada va quedar nua l'octubre de 2023, quan 23andMe va patir una bretxa. Els atacants van entrar directament en només unes catorze mil comptes —el 0,1 %—, però des d'allà, a través de la funció que connecta parents, van exposar les dades de **6,9 milions d'usuaris** [1]. I van fer una cosa esgarrifosa: van publicar llistes segmentades per origen ètnic —un milió de perfils etiquetats com a jueus asquenazites, cent mil com a xinesos— a la venda per uns pocs dòlars. La dada genètica és, per construcció, una dada de **pertinença a un grup**. El pitjor és que no es pot desfer: a diferència d'una contrasenya, no pots «canviar el teu ADN» després d'una fuga.

I el 2025 va arribar el segon cop. 23andMe, que custodiava les dades de prop de **quinze milions de persones**, va fer fallida; en vint-i-quatre hores el trànsit a la seva web va pujar un 526 % i prop d'**1,9 milions de persones** van demanar esborrar el seu ADN, en descobrir que la genètica que havien confiat a una startup era ara un **actiu concursable** que se subhastaria [3]. Una coalició de **28 fiscals generals**, encapçalada per la de Nova York, Letitia James, va demandar l'empresa amb un argument contundent: «23andMe no pot subhastar la informació genètica de milions de persones sense el seu consentiment» [4]. Les dades van acabar en mans d'una fundació de la cofundadora per 305 milions de dòlars, i el regulador britànic va multar l'empresa amb 2,31 milions de lliures —castigant, com va subratllar, la **custòdia**, no el contingut [6]. I la llei nord-americana de no-discriminació genètica, recordem-ho, **no cobreix les assegurances de vida** [9].

La família que mai no va consentir

Aquí hi ha la veritat més incòmoda, i és matemàtica. Els investigadors **Yaniv Erlich i els seus col·legues** van demostrar, com hem vist, que n'hi ha prou que el **2 % d'una població** estigui en una base de dades genètica per identificar gairebé qualsevol persona a través d'un parent llunyà; ja avui, prop del 60 % dels nord-americans d'ascendència europea són identificables encara que **mai no s'hagin fet un test** [2]. La privacitat genètica, doncs, no és un dret individual, sinó **col·lectiu i familiar**. Com argumenta el jurista **Taner Kuru**, pujar el teu ADN no converteix l'ADN del teu cosí en «públic»: cap firma teva pot legitimar una dada que delata fills, cosins i descendents encara no nascuts. I el mateix val per a la biometria de consum —la cara, l'iris—, que tampoc no es pot canviar: sota la llei d'Illinois, Facebook va pagar 650 milions de dòlars per etiquetar cares sense consentiment.

La prova d'existència: segellar el consentiment, no el genoma

És aquí on **t2p** ha de ser especialment humil, perquè el que pot fer és valuós però limitat. No ancora **la seqüència d'ADN** —posar-la a la cadena seria catastròfic—, sinó **l'acte i els termes del consentiment**. El client signa un formulari que fixa exactament per a què autoritza l'ús —el test, la connexió amb parents, la recerca, l'accés policial—; al dispositiu es calcula l'**empremta SHA-512**, i només aquesta s'ancora a la **blockchain pública** amb un **segell de temps eIDAS** i **GPS forense**. El resultat és una prova inalterable de *què va consentir aquesta persona, quan i on*. La **prova de vida** lligarà el consentiment a una persona viva i present, i el **versionat** de cada política de privacitat —com el canvi de GEDmatch el 2019 o la transferència a la fundació el 2025— deixa un registre verificable de quina base de consentiment emparava realment cada transferència. El contenidor **.asice** es lliura al consumidor, que conserva així la **seva pròpia còpia probatòria** del que va autoritzar, sense dependre del servidor d'una empresa que pot fallir.

Cal dir el límit amb tota la cruesa, perquè aquí és el més dur de tot el llibre. «Escombraries a l'entrada, escombraries a la cadena», i pitjor: **la dada genètica no és de qui la segella**. Primer, la prova d'existència **no dona privacitat, dona traçabilitat**: segellar el consentiment demostra que va existir, però no impedeix que la dada es filtri, se subhasti en una fallida o l'usi una asseguradora de vida; la integritat no és confidencialitat. Segon, i el més greu, la dada és **irrevocable** i el consentiment és estructuralment impossible de donar del tot, perquè **el teu consentiment segella l'ADN de la teva família**; la prova pot demostrar que *tu* vas consentir, però no crea el consentiment del teu cosí tercer. Tercer, no resol l'asimetria de la lletra petita: un *opt-in* segellat a la perfecció continua sent el mateix que l'usuari va acceptar sense llegir —la cadena dona fe del clic, no que el clic fos informat. I quart, esborrar l'empremta **no esborra la mostra física**, ni els *backups*, ni les còpies ja compartides amb investigadors o atacants. **t2p** pot aportar **sobirania probatòria sobre el consentiment**, però no pot tornar la privacitat a una dada que, per naturalesa, ja pertany també a altres i no es pot desfer.

La promesa i el perill

La promesa, ben acotada, és real. Donar a cada persona una prova segellada i en mans pròpies de què va consentir exactament i quan faria molt més difícil que una empresa en fallida subhasti dades amb un consentiment que ningú no va donar o que reescrigués els termes a posteriori. En un món on la genètica que confies a una startup pot acabar en una subhasta, tenir la teva pròpia còpia del que vas autoritzar és un escut real contra el repudi corporatiu.

El perill, aquí, és prometre el que no es pot complir. Vendre la prova d'existència com una garantia de privacitat genètica seria una mentida perillosa: el segell dona traçabilitat, no confidencialitat, i no pot legitimar una dada que compromet la família. El consentiment veritablement informat, la prohibició de subhastar genomes, el tancament del forat de les assegurances de vida i la minimització de la dada són problemes de dret i de governança, no de criptografia. La prova d'existència és una eina per a la sobirania sobre el consentiment, no un substitut d'una llei que protegeixi una dada que no es pot canviar.

És hora d'actuar

Per als consumidors: pensar-s'hi dues vegades abans de lliurar una dada que també pertany als seus fills i cosins, i conservar una prova del que autoritzen. Per a les empreses de genòmica i biometria: segellar el consentiment i el seu versionat, i exigir un opt-in real abans de qualsevol venda o transferència. Per als reguladors: castigar la mala custòdia, com va fer el regulador britànic, i tancar el forat de les assegurances de vida. I per als legisladors: reconèixer que la privacitat genètica és familiar i col·lectiva, i que cap firma individual pot vendre l'ADN d'una nissaga sencera.

Un assassí va caure perquè un parent havia pujat el seu ADN; milions de persones van veure el seu genoma a la venda després que una empresa fos fallida. Donar a cada persona una prova del que ha consentit —sense oblidar mai que el segell no torna la privacitat en una dada irrevocable i compartida— és, en aquest front que toca el més íntim de tots, time2act.

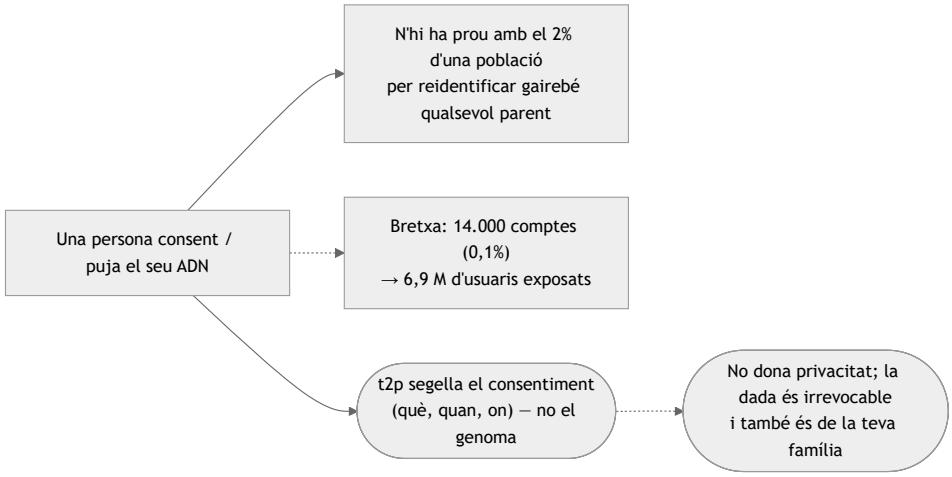


Figura 76.1 — Dues veritats de la dada genètica. A l'esquerra, l'efecte familiar: n'hi ha prou que el 2 % d'una població estigui en una base de dades per reidentificar gairebé qualsevol persona a través d'un parent llunyà, i prop del 60 % dels d'ascendència europea ja són identificables encara que mai no s'hagin fet un test (Erlich et al., 2018). A la dreta, l'efecte multiplicador de la bretxa: l'atac a 14.000 comptes (el 0,1 %) va exposar 6,9 milions d'usuaris a través de la funció que connecta parents. t2p pot segellar l'acte de consentiment —què, quan i on—, però no pot tornar la privacitat a una dada irrevocable que també és de la teva família. Fonts: Science (Erlich et al.); TechCrunch; fiscalia de Nova York.

---

[1] TechCrunch — *23andMe confirms hackers stole ancestry data on 6.9 million users* (2023; les llistes segmentades per origen ètnic). 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 i Shai Carmi (Science) — *Identity inference of genomic data using long-range familial searches* (2018; el 2 % de la població basta). https://www.science.org/doi/10.1126/science.aau4832 ↩

[3] CNBC — *23andMe bankruptcy: selling and deleting DNA* (2025; +526 % de trànsit; ~1,9 M de sol·licituds d'esborrament). 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* (coalició de 28 fiscals generals). 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$; tancament 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 (Regne Unit) — *ICO fines 23andMe £2.31 million* (155.592 residents britànics; la sanció castiga la custòdia). 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* (l'ADN el va pujar 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 per defecte; només ~14 % van optar per participar). https://www.legalgenealogist.com/2019/05/19/gedmatch-reverses-course/

[9] National Human Genome Research Institute — *GINA: Genetic Information Nondiscrimination Act (2008)* (no cobreix vida, invalidesa ni cures de llarga durada). 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; pujar el teu ADN no fa «públic» el dels teus parents). https://www.sciencedirect.com/science/article/pii/S0267364925000019

Justícia penal: la prova que el tribunal ha de poder creure

«És millor que deu culpables s'escapin que no pas que un innocent pateixi.»

— William Blackstone, Commentaries on the Laws of England, IV, 27 (1769)

El 24 de gener de 2017, l'agent de policia de Baltimore Richard Pinheiro va entrar en un pati ple de brossa, va col·locar una bossa de càpsules dins d'una llauna de sopa, va sortir al carreró i *llavors* va encendre la seva càmera corporal per gravar el «descobriment» de la droga. El que no sabia és que aquell dispositiu conserva automàticament els **trenta segons anteriors a l'activació, sense so**. Aquells trenta segons muts el van delatar: va ser condemnat per fabricar proves, i el cas de drogues es va esfondrar [4]. La mateixa tecnologia pensada per vigilar el ciutadà havia gravat el vigilant.

Aquell cas conté les dues cares d'aquest capítol, diferent del capítol 20 —que tractava l'evidència d'atrocitats davant d'un tribunal internacional. Aquí el terreny és la **justícia penal ordinària**: la càmera corporal d'un agent, l'àudio d'un divorci, el vídeo d'un judici nacional. I planteja la pregunta que avui esquerda els tribunals de tot el món: en una era en què qualsevol so o imatge es pot falsejar de manera convincent, **com pot un tribunal saber quina prova ha de creure?**

El dividend del mentider dins de la sala

L'amenaça té dues direccions. La primera és el fals que enganya: un àudio o vídeo fabricat amb intel·ligència artificial presentat com a autèntic. En un cas de família britànic, una mare va aportar un àudio en què el pare suposadament feia amenaces violentes; els pèrits van demostrar, analitzant les metadades, que havia estat editat després de la trucada per inserir paraules que el pare mai no va dir [9].

La segona direcció és més insidiosa i té nom propi. Els juristes Robert Chesney i Danielle Citron, en el seu article de referència *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* (2019), la van batejar com el «dividend del mentider»: a mesura que tothom assumeix que tot es pot falsejar, alguns eludiran la seva responsabilitat denunciant com a deepfake una gravació autèntica [6].

I ja ha arribat als tribunals. En el litigi per la mort d'un enginyer al volant d'un Tesla, els advocats de l'empresa van arribar a sostenir que els vídeos en què Elon Musk promociona la seguretat del seu sistema «podrien ser *deepfakes*». La jutgessa **Evette Pennypacker** ho va qualificar de «profundament inquietant»: amb aquella lògica, qualsevol figura pública podria dir el que volgués i després negar-ho [1]. I en el judici de Kyle Rittenhouse, la defensa va aconseguir que el jutge dubtés que ampliar un vídeo en una tauleta —una simple interpolació de píxels— l'«alterés amb intel·ligència artificial», i va donar a la fiscalia només vint minuts per portar un enginyer d'Apple; la imatge ampliada no es va mostrar mai al jurat [2]. Quan clonar una veu convincent requereix només uns segons d'àudio i, segons un estudi de 2025, només el 0,1 % de les persones distingeix amb fiabilitat el real del fals, el dubte es converteix en una arma.

Qui controla l'arxiu

Hi ha un tercer problema, més prosaic però igual de corrosiu: **qui custodia la prova**. La càmera corporal es va vendre com una eina de transparència, però sovint s'ha convertit en una eina controlada per la mateixa policia. Una investigació de **ProPublica** va trobar que, de setanta-nou homicidis policials amb càmera als Estats Units, només el 42 % tenia la gravació publicada un any i mig després, i que en aproximadament un de cada cinc casos el departament va dir falsament a l'òrgan de control que la gravació **no existia** [5]. A Anglaterra i Gal·les, una investigació de la BBC va documentar més de cent cinquanta informes de mal ús de càmeres —agents que les apagaven, esborraven o compartien gravacions —, fets que, segons un alt comandament, «van al cor del que soscava la confiança en la policia» [10]. Com resumeix The Sedona Conference, el think tank de dret probatori, en l'era digital la prova no es «guarda», es **custodia amb traçabilitat**: sense una cadena demostrable, la dada més valuosa és impugnable.

La prova d'existència: segellar en el segon de gravació

És aquí on **t2p** ataca el problema en el seu origen exacte. En l'instant de la captura, la càmera corporal o el mòbil del testimoni calcula **al dispositiu** l'empremta SHA-512 del fitxer —que no surt mai; només viatja

l'empremta—, l'ancora a la **blockchain pública** i hi adjunta un **segell de temps RFC 3161** conforme a eIDAS, un **GPS forense** i un contenidor **.asice**. El segell no es posa *després*, a la sala de proves: es posa **en el segon de gravació**, tancant la finestra de manipulació.

L'efecte sobre les dues amenaces és directe. Contra l'edició o l'esborrament posterior —el cas de Baltimore o els cent cinquanta informes de la BBC—, qualsevol tall o «pèrdua» d'un clip segellat fallaria la verificació. I contra el dividend del mentider, davant del «aquest vídeo és un *deepfake*», l'ancoratge independent prova que **aquell fitxer exacte existia intacte abans de tal instant**, desplaçant la càrrega del dubte a qui l'impugna. Tot això encaixa amb el dret existent: la regla federal nord-americana 902(14) ja admet el **hash** com a via d'autoautenticació de còpies digitals, i el reglament europeu eIDAS dona al segell de temps qualificat una **presumpció legal** d'integritat i data. I el contenidor .asice permet que tant la defensa com la fiscalia verifiquin la integritat **sense l'aplicació i sense confiar en t2p**, amb eines obertes: una garantia d'igualtat d'armes, perquè la defensa pot auditar de manera independent la prova de càrrec.

Cal dir el límit amb tota la cruesa, perquè el cas de Baltimore n'és l'exemple demolidor. Una càmera corporal segellada **en el moment** de gravar Pinheiro plantant la droga hauria certificat, amb un segell inalterable, una escena fraudulenta. «Escombraries a l'entrada, escombraries a la cadena»: si l'agent actua de mala fe davant de la càmera, la cadena certifica la mentida amb data certa. El segell prova integritat, instant, lloc i persona, **no la veritat de l'escena**. I hi ha límits específics d'aquest front. Primer, la prova només serveix si el segell s'aplica **en origen**: no rescata les gravacions històriques sense segellar, que avui són el 99,9 % de la prova real als jutjats. Segon, **no obliga la policia a encendre la càmera**: el problema de ProPublica no és la integritat del clip, sinó la seva *inexistència*, i cap segell no crea gravacions que ningú no va fer. Tercer, davant del dividend del mentider, l'àncora només ajuda si la prova **estava** segellada; per a l'oceà de material sense segellar, el dubte segueix intacte, i un sistema que només avali el material segellat podria, perversament, **augmentar** la sospita sobre tota la resta. I quart, l'admissibilitat final la decideix el jutge segons les regles nacionals, no la cadena de blocs: el hash autoautentica el *fitxer*, no la seva rellevància ni la legalitat de la seva obtenció.

La promesa i el perill

La promesa és restaurar la base de fets sense la qual cap judici no és possible. Una prova segellada a l'origen donaria al tribunal una manera de distingir el fitxer íntegre del fabricat, blindaria la cadena de custòdia de la càmera corporal i trencaria el dividend del mentider per al material protegit. El mateix òrgan que escriu les regles probatòries als Estats Units, l'Advisory Committee presidit pel professor Daniel Capra, ja debat noves regles per a la prova generada per màquina, reconeixent que ni les eines ni els jutges saben encara distingir els *deepfakes* amb fiabilitat. El segell d'origen és exactament el reforç d'autenticació que aquest debat busca.

El perill demana els matisos que hem dit, i aquí són crucials. El primer, no confondre integritat amb veritat: una càmera segellada que grava un muntatge certifica el muntatge. El segon, que el segell no obliga a encendre la càmera ni rescata el material antic. I el tercer, el més subtil: si només es confia en el que està segellat, es pot acabar desconfiant injustament de tota la resta. La prova d'existència és un reforç poderós de l'autenticació probatòria, no un detector de mentides ni un substitut del judici humà.

És hora d'actuar

Per als **cossos policials**: segellar cada gravació al segon de la captura i fer obligatòria l'activació de la càmera, perquè la integritat i l'existència del clip no quedin en mans de qui s'investiga. Per als **tribunals i els qui escriuen les regles** (l'Advisory Committee, els legisladors): reconèixer el segell d'origen com a via d'autoautenticació i adaptar les normes a la prova generada per màquina. Per a la **defensa i la fiscalia**: exigir contenidors verificables de forma independent, per garantir la igualtat d'armes. I per als **ciutadans**: una manera de provar que el que van gravar és exactament el que va passar.

Un agent va ser delatat per la seva pròpia càmera, però una càmera segellada hauria pogut certificar igual de bé la seva mentida si l'hagués gravada amb cara de pòquer. Donar a cada prova una empremta segellada en el moment de néixer —sense oblidar mai que el segell no fa veritat l'escena— és, en aquest front del qual depèn la justícia, time2act.

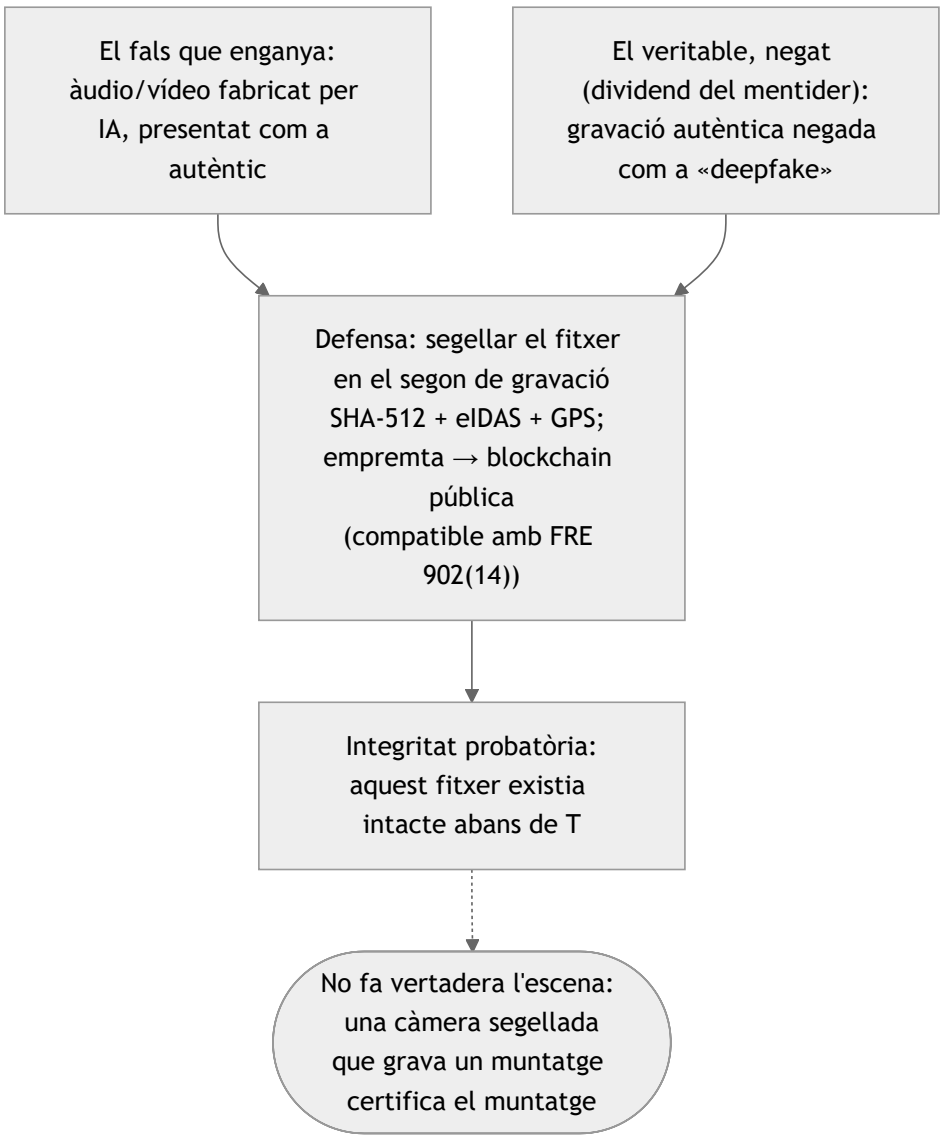


Figura 77.1 — La prova digital pateix dos atacs oposats. A l'esquerra, el fals que enganya: un àudio o vídeo fabricat amb IA presentat com a autèntic (com l'àudio editat d'un cas de família britànic). A la dreta, el dividend del mentider: una gravació autèntica negada com a «deepfake» per eludir la responsabilitat (com en el litigi Huang contra Tesla, on es va al·legar que els vídeos de Musk «podrien ser deepfakes»). La mateixa defensa val per a tots dos: segellar el fitxer en el segon de la gravació amb empremta SHA-512, segell eIDAS i GPS (compatible amb la regla 902(14): el hash autoautentica còpies). Límit: el segell prova integritat i moment, no la veritat de l'escena —una càmera segellada que grava un muntatge certifica el muntatge. Fonts: Chesney i Citron (2019); ProPublica; casos Tesla i Baltimore.

---

[1] Fortune — *Tesla lawyers argue recordings of Musk touting Autopilot could be deepfakes* (Huang contra Tesla; jutgessa 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 càrrega traslladada a la fiscalia; 20 minuts per a un pèrit d'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; jutge 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* (l'agent Pinheiro; el búfer de 30 segons sense so). 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* (només el 42 % de 79 homicidis; «no existeix» fals en 1 de cada 5). https://www.propublica.org/article/how-police-undermined-promise-body-cameras ↩

[6] Robert Chesney i Danielle Keats Citron — *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* (107 California Law Review 1753, 2019; el «dividend del mentider»). 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: proposta de Regla 707 (prova generada per màquina) i 901(c)* (comentari fins al 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 còpies digitals). 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* (àudio editat després de la trucada per inserir amenaces). 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* (Anglaterra i Gal·les; Jim Colwell, NPCC). https://www.lbc.co.uk/article/150-reports-police-officers-misusing-body-cameras-investigation-england-wales-DWzgZZ_2/ ↩

Historials mèdics: qui va tocar el registre, i quan

«Pot semblar un principi estrany enunciar com a primeríssim requisit d'un hospital que no faci cap mal al malalt.»

— Florence Nightingale, Notes on Hospitals (1863)

A Chicago, una mare va demandar el Rush University Medical Center en nom del seu fill, nascut amb una lesió cerebral per falta d'oxigen durant el part. Per provar què havia passat minut a minut a la sala, necessitava una cosa concreta: el **registre d'auditoria** de l'historial electrònic, el rastre que mostra qui va escriure, modificar o esborrar cada anotació i quan. Durant més de tres anys, l'hospital va lliurar un simple registre d'accessos en lloc del rastre complet i va fer afirmacions sobre la seva capacitat de produir-lo que el jutge va considerar **falses**. El 2022, el jutge James O'Hara va imposar una sanció equivalent a una **sentència en rebel·lia**: la culpabilitat quedava fixada, només faltava posar-hi la xifra [1]. La ironia és cruel: el document sobre el qual es litigava era, precisament, el que havia de dir la veritat del que va passar.

Aquell rastre retingut conté la pregunta d'aquest capítol, diferent de la del capítol 18 —que tracta la imatge mèdica i les receptes. Aquí no parlem del *contingut* clínic, sinó de la **governança del registre**: **qui va accedir a un historial, qui el va alterar, quan, i va consentir-ho el pacient?** Perquè un historial electrònic, per molt sofisticat que sembli, és un registre que es pot reescriure, retrodatar i amagar.

El registre que es pot reescriure

La manipulació de l'historial és un frau documentat i tècnicament senzill. Els forenses han trobat casos en què les notes d'un torn es van redactar **després de la mort del pacient i amb data retroactiva**, fetes des d'una estació de treball no clínica hores després de l'aturada cardíaca: el que en paper semblava contemporani, en les metadades era posterior. Per això la normativa de l'agència del medicament nord-americana és taxativa: un canvi en un registre electrònic **no pot ocultar la informació anterior** [3]. A escala més gran, el frau pren la forma del **copiar-enganxar**: l'oficina d'inspecció del sistema de salut nord-americà va trobar que només una quarta part dels hospitals tenia polítiques sobre aquesta funció, i que les estades facturades al nivell de gravetat més alt van créixer gairebé un 20 % en cinc anys, fins a representar **gairebé la meitat de tota la despesa** de Medicare en hospitalitzacions [4][5]. I hi ha el tafaneig: la xafarderia als historials de famosos va costar a l'hospital de la UCLA una multa de **865.500 dòlars** el 2011, i un altre exempleat del mateix centre, **Huping Zhou**, que havia accedit a registres **323 vegades**, va ser **la primera persona empresonada als Estats Units per una violació de la llei de privacitat sanitària** [6][7]. El registre d'auditoria revela tots aquests fraus —però, com va mostrar el cas Prieto, també es pot retenir.

El consentiment com a rebut, no com a casella

Hi ha una segona dimensió, la del **consentiment**. Avui el consentiment del pacient sol ser una casella perduda en un formulari, impossible d'auditar i fàcil de fabricar a posteriori. La iniciativa **Kantara**, en la seva especificació de *rebut de consentiment* —base de la norma internacional ISO 27560—, proposa una idea senzilla i poderosa: que el consentiment es materialitzi en un **rebut llegible per humans i processable per màquines**, com el d'una compra, que registri qui va consentir, per a quina finalitat i sota quina política. Així el consentiment esdevé **auditable i revocable**, no una casella oblidada. I la llei nord-americana ja empeny en aquesta direcció: la Cures Act obliga a donar als pacients accés a la seva informació de salut i prohibeix el «bloqueig d'informació» —exactament el que va fer l'hospital del cas Prieto.

La prova d'existència: segellar l'esdeveniment, no la imatge

És aquí on **t2p** aporta una capa d'integritat al registre i al consentiment. El que se segella **no és la imatge ni la dada clínica** —que queda al servidor de l'hospital—, sinó l'**esdeveniment**. Cada vegada que es crea, modifica o s'esborra una anotació, el dispositiu calcula l'**empremta SHA-512** del parell format pel contingut de l'entrada i les seves metadades d'auditoria —identificador de l'usuari, rol, hora,

tipus d'acció—, i aquesta empremta s'ancora a la **blockchain pública** amb un **segell de temps eIDAS**. Es genera una prova pública i inalterable que *aquella* entrada existia amb *aquell* contingut en *aquest* instant. El mateix s'aplica al **rebut de consentiment** —demostrant quan es va concedir i, sobretot, quan es va **revocar**, impedint el consentiment retroactiu fabricat— i al **rebut d'accés**, que crea un registre de qui ha consultat l'historial i que ja no pot desaparèixer, com en el cas de la UCLA.

L'efecte és directe. La **prova de vida** lliga la firma d'una nota a un clínic real i present, no a una sessió robada; el **GPS forense** corrobora que l'entrada es va fer des d'una ubicació clínica plausible, no des d'una estació remota; el **segell de temps** fixa l'instant de manera independent del rellotge manipulable de l'historial; i el contenidor **.asice** empaqueta l'entrada, el seu rebut de consentiment i la prova d'ancoratge perquè un pèrit els pugui verificar **sense accés al sistema de l'hospital**. La retrodatació, la sobreescriptura i el filtratge selectiu del rastre en un litigi es tornen detectables.

Cal dir el límit amb tota la cruesa, perquè aquí és fonamental. «Escombraries a l'entrada, escombraries a la cadena»: el segellat prova la **integritat temporal i d'autoria** del registre, no la **veritat clínica**. Si un metge escriu en temps real una observació falsa —«pacient estable» quan no ho estava— i la segella a l'instant, t2p certificarà per sempre que aquella mentida va existir en aquell moment i d'aquella mà, i la farà **més** difícil de retractar, no menys. La prova no detecta la negligència ni l'error clínic; només congela el que es va escriure. A més, no substitueix el registre d'auditoria natiu de l'historial: si l'hospital no genera o no segella un esdeveniment, no hi ha res per ancorar, i un accés fora del flux segellat és invisible a la cadena. El rebut de consentiment prova que el pacient va firmar, no que ho entengués ni que el consentiment fos lliure. I el registre de qui mira pot revelar **patrons** sensibles, cosa que exigeix governança. La prova d'existència dona integritat al registre, no veracitat al seu contingut.

La promesa i el perill

La promesa és restaurar la confiança en el document del qual depèn la vida i la justícia. Un historial amb cada esdeveniment segellat en origen faria impossible retrodatar una nota després d'un mal resultat, amagar l'empremta en un litigi com el del cas Prieto, o esborrar les empremtes d'un tafaner. I donaria al pacient un control real sobre el seu consentiment, amb un rebut que demostra què va autoritzar i quan ho va revocar. En un sistema on el registre es pot reescriure, fer l'esdeveniment inalterable és protegir tant el pacient com el clínic honest, que podria demostrar que la seva nota és exactament la que va escriure.

El perill demana els matisos que hem dit. El primer, no confondre integritat amb veritat: una nota falsa segellada continua sent falsa i ara, a més, immutable. El segon, que el segell no substitueix el registre natiu ni rescata el que no es va segellar. I el tercer, la privacitat de la pròpia empremta d'accés, que cal protegir perquè no es converteixi en una eina de vigilància del clínic. La prova d'existència és una capa poderosa de governança del registre, no un certificat de bona pràctica ni un substitut del judici pericial que sap llegir un audit-trail.

És hora d'actuar

Per als **hospitals i els fabricants d'historials** (Epic, Cerner): segellar cada esdeveniment d'escriptura, accés i consentiment en origen, perquè el rastre no es pugui retrodatar ni amagar. Per als **reguladors** (les agències de salut, del medicament, d'interoperabilitat): reconèixer el segell d'origen com a compliment dels controls d'auditoria i d'integritat que la llei ja exigeix. Per als **pacients**: un rebut de consentiment en mans pròpies que demostri què van autoritzar i quan ho van revocar. I per als **tribunals**: tractar el registre d'auditoria segellat com la prova fiable que va faltar en el cas Prieto.

Una mare va lluitar tres anys per un registre que havia de dir la veritat del part del seu fill, i l'hospital el va amagar. Donar a cada esdeveniment d'un historial una prova segellada de qui el va tocar i quan —sense oblidar mai que el segell no fa veritable el que s'hi escriu— és, en aquest front que toca la salut i la justícia, time2act.

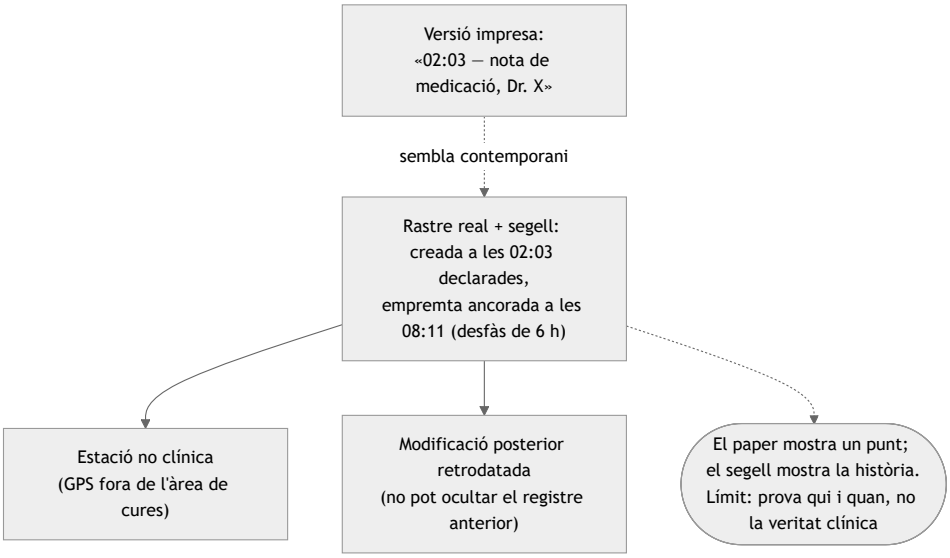


Figura 78.1 — Una nota clínica vista en dos carrils. A dalt, la versió impresa: un sol punt, «02:03 — nota de medicació, Dr. X». A baix, el rastre d'auditoria real amb segell de t2p: l'esdeveniment de creació declarat a les 02:03 però amb l'empremta ancorada a la blockchain pública a les 08:11 —un desfàs de sis hores—, fet des d'una estació no clínica (GPS forense fora de l'àrea de cures), amb una modificació posterior retrodatada que no pot ocultar la informació anterior (21 CFR 11.10(e)). El papel mostra un punt; el segell mostra la història. Límit: el segell prova qui i quan, no la veritat clínica del que s'hi va escriure. Fonts: HIPAA i FDA (controls d'auditoria); cas Prieto contra Rush; anàlisi forense d'historials.

---

[1] Enigma Forensics — *Judge sanctions hospital for not producing complete EMR audit trail* (Prieto contra Rush University Medical Center; jutge 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* (controls d'auditoria obligatoris; integritat de l'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 amb segell de temps; un canvi no pot ocultar el registre 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; només ~25 % amb polítiques de copiar-enganxar). 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; gairebé la meitat de la despesa al nivell màxim de severitat). 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 als historials). 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 accessos; la primera condemna de presó per una violació 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; accés del pacient a la seva informació de salut). 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 i Adam Wright (Applied Clinical Informatics) — *Identifying a Clinical Informatics or EHR Expert Witness* (2023; el log és prova que cal interpretar). https://pmc.ncbi.nlm.nih.gov/articles/PMC10033222/

Models d'IA: amb què es van entrenar, i què executem de debò

«Val més que estiguem ben segurs que el propòsit posat dins la màquina és el propòsit que de debò desitgem.»

— Norbert Wiener, «Some Moral and Technical Consequences of Automation», Science (1960)

El desembre de 2023, un equip de l'**Observatori d'Internet de Stanford** va mirar dins d'una cosa que feia anys que ningú no havia auditat de debò: **LAION-5B**, el conjunt de cinc mil milions de parells d'imatge i text amb què s'havien entrenat Stable Diffusion i bona part de la generació d'imatges per IA. Hi van trobar milers d'enllaços a material d'abús sexual infantil —més de **3.200 casos sospitosos**, una part confirmada per tercers— amagats entre les dades rascades de la web [1]. LAION va retirar el conjunt de la xarxa, i l'informe recomanava **deprecar i discontinuar** els models entrenats amb ell; mesos després en va publicar una versió netejada, Re-LAION-5B, de la qual va eliminar més de dos mil enllaços [1][2]. El problema de fons no era només el contingut: era que **ningú —ni els qui l'havien creat— podia dir amb certesa què hi havia a dins** fins que algú de fora ho va auditar. Un model que ja s'havien descarregat milions de persones s'havia entrenat sobre una pila de dades que resultava ser, en part, il·legal, i no existia cap registre fiable que ho digués.

Aquesta és la pregunta d'aquest capítol, diferent de la del capítol 40 —que tracta els drets de qui crea una obra. Aquí no parlem de l'autoria del contingut, sinó de la **procedència del model mateix**: amb quines dades es va entrenar, qui el va construir, quan, i —no menys important— si els **pesos** que t'has descarregat i executes són exactament els que algú va avaluar. Perquè un model d'IA, per impressionant que sigui, és un artefacte opac: un fitxer de pesos i una targeta de documentació que es poden reescriure, retrodatar i, com veurem, fins i tot infectar.

El model que ningú pot auditar

L'opacitat té tres cares. La primera són les **dades**: els grans models s'entrenen sobre corpus rascats de tot internet, tan enormes que la seva composició només es coneix per aproximació; el cas de LAION va mostrar que ni tan sols els creadors saben del cert què contenen. La segona és la **documentació**: des de 2019, les *model cards* proposades per Mitchell i col·legues estandarditzen com declarar l'ús previst, el rendiment i els límits d'un model [9]; però una targeta de model és un document voluntari que viu en un repositori que el proveïdor controla, i que pot editar —o suavitzar— després d'un incident. I la tercera, la més inquietant, és la **integritat dels pesos**. El 2024, els investigadors de JFrog van trobar **un centenar de models maliciosos** penjats a Hugging Face: aprofitant el format de serialització *pickle* —l'estàndard per empaquetar models—, amagaven codi que s'executava en carregar el fitxer i obria una **porta del darrere** a la màquina de la víctima [3][4]. La conseqüència és demolidora: el model que descarregues pot **no ser** el que el laboratori va avaluar i declarar segur. Entre l'avaluació i la teva GPU hi ha una cadena de custòdia que avui ningú no segella.

La llei demana paper; falta l'àncora

La llei ha començat a respondre. El Reglament europeu d'IA obliga, des del 2 d'agost de 2025, els proveïdors de models de propòsit general a mantenir documentació tècnica —arquitectura, nombre de paràmetres, recursos de còmput, descripció de les dades— i a publicar un «resum prou detallat» del contingut d'entrenament segons una plantilla de l'Oficina d'IA [5][6]. L'incompliment es paga car: fins a 15 milions d'euros o el 3 % de la facturació mundial, i a partir del 2 d'agost de 2026 l'Oficina podrà verificar-ho; des de la mateixa data, l'article 50 exigeix marcar de manera llegible per màquina el contingut generat per IA [5][6]. La indústria ha proposat un AI-BOM, la llista de materials d'un model com la que ja existeix per al programari. L'estàndard CycloneDX hi va afegir el ML-BOM —datasets, models i configuracions amb la seva procedència— (com hem vist) i el projecte AIBOM d'OWASP impulsa la seva estandardització [7][8]. Però aquí xoquem amb el mateix mur: un BOM, com una targeta de model o un resum d'entrenament, és tan fiable com la voluntat de qui el signa; un PDF de compliment és només un PDF i res no impedeix retocar-lo demà.

Per què el manifest sol no salva

Cal dir-ho amb cruesa: publicar un resum d'entrenament o un *hash* dels pesos en un fitxer LLEGEME no demostra res si aquell fitxer es pot canviar sense deixar rastre. Un proveïdor que, després d'un incident com el de LAION, edités discretament la seva targeta de model per treure-hi una font incòmoda, no deixaria cap empremta d'haver-ho fet. Un *hash* de pesos sense una **data certa i independent** no distingeix l'original de la versió retocada a posteriori. I un AI-BOM emmagatzemat al mateix repositori que controla qui l'ha d'explicar és, en una disputa, paper de part. El que falta no és el document: és **un ancoratge inalterable que fixi qui va declarar què, i quan**.

La prova d'existència aplicada

És aquí on **t2p** aporta la capa que falta, i ho fa sobre l'artefacte digital, no sobre una foto del terreny. En publicar un model es calcula l'**empremta SHA-512** del fitxer de pesos i la del **manifest AI-BOM** —el resum de dades d'entrenament, l'informe d'avaluació i de seguretat, les llicències— i ambdues s'ancoren amb un **segell de temps RFC 3161 conforme a eIDAS** a la blockchain pública, dins d'un contenidor **.asice** verificable fora de línia. Això genera una prova pública i inalterable que *aquell* dia el proveïdor va declarar *aquell* resum d'entrenament i *aquell* resultat d'avaluació, i que *aquests* pesos —per la seva empremta— són els avaluats.

L'efecte és directe sobre les tres opacitats. Sobre les **dades**, el resum d'entrenament queda amb data certa: si demà cal deprecar el model com a LAION, no es pot fingir que mai es va declarar el que es va declarar. Sobre la **documentació**, l'edició silenciosa posterior es torna detectable, perquè l'auditor pot confrontar la targeta actual amb la versió segellada el dia zero. I sobre els **pesos**, qualsevol que desplegui el model recalcula l'empremta i la compara amb l'àncora: una substitució a l'estil *nullifAI* **falla la comprovació** abans d'arribar a producció. És, sobre el model, el complement del que proposen els capítols 13 i 15 respecte a la sortida: la marca C2PA i SynthID segellen **el que un model produeix** —Google ja ha marcat amb SynthID més de cent mil milions de continguts [10]—; t2p segella **el que un model és**.

Ara el límit, amb tota la cruesa, perquè aquí és essencial. «Escombraries a l'entrada, escombraries a la cadena»: el segell prova que el proveïdor **es va comprometre** amb un resum d'entrenament determinat i que els pesos coincideixen amb una empremta en un instant; **no prova que el resum sigui veritat** —que les dades fossin realment només les declarades—, ni que el model sigui segur, ni detecta un enverinament hàbil del conjunt. Lliga una afirmació a una data i a un autor; no en verifica el contingut. A Stanford el material il·legal l'han hagut de trobar **humans** auditant; cap segell ho hauria fet pel seu compte. La prova d'existència no substitueix l'auditoria del *dataset*, el *red-teaming* ni la marca d'aigua: els fa **responsables**, perquè impedeix negar després el que es va declarar abans.

La promesa i el perill

La promesa és un ecosistema d'IA on el llinatge és **verificable**: poder demostrar amb quines dades, quina versió i quina avaluació es va construir un model, i que els pesos que corren en producció són els auditats, amb una responsabilitat que sobreviu als incidents. En una indústria on un fitxer de pesos viatja de mà en mà sense cap rebut, fer l'origen inalterable protegeix tant el desplegador honest com el públic.

El perill demana els matisos de sempre. Primer, cal recordar que **el segell no prova la veracitat del resum d'entrenament**; un document fals i segellat continua sent fals, i ara, a més, immutable, i genera una falsa tranquil·litat —«està ancorat, doncs és segur»— que no es correspon amb res. Segon, la **concentració**: si només els grans laboratoris poden segellar i documentar, l'estàndard pot expulsar els models oberts en lloc d'enfortir-los, consolidant un poder de mercat que podria limitar la diversitat i la innovació. Tercer, la tensió entre publicar el resum d'entrenament com a prova de governança i preservar el secret industrial legítim; cal equilibrar la transparència necessària amb la protecció de propietats intel·lectuals i avantatges competitius. La prova d'existència és una capa de governança del model, no un certificat de bondat ni un substitut del judici expert que sap auditar un corpus.

A més, segellar la procedència d'un model no resol la dificultat fonamental de comprendre els criteris de decisió que es generen dins les xarxes neuronals profundes. Com assenyala Cathy O'Neil, aquests sistemes són «opacs i invisibles excepte per als sacerdots del sector: els matemàtics i els enginyers» [11]. Això crea una nova forma de poder concentrat: només qui té accés a l'expertise interna pot desxifrar o manipular les lògiques subjacents, mentre que el públic i fins i tot reguladors es queden amb un segell d'autenticitat

sense saber *per què* el model actua com ho fa. En paral·lel, el marc legal que hauria de frenar aquesta asimetria retrocedeix: com hem vist, la Unió Europea ha ajornat les obligacions per a la IA d'alt risc del 2026 fins al període 2027-2028 [12], i l'estat de Colorado ha suprimit completament la seva llei d'IA, eliminant el deure de no discriminar [12]. Aquest retrocés normatiu afavoreix un entorn on la vigilància esdevé més difícil i el poder dels qui controlen els models s'intensifica sense cap contrapès efectiu.

Un reforç inesperat ve de les mateixes IA públiques, ja que moltes d'elles produeixen registres intrínsecament auditables. L'eina **Policy Synth**, dissenyada per Beth Noveck, genera un registre detallat —cita a cita— de totes les accions dels seus agents, i cada sortida ve acompanyada del seu origen documental [13]. Això significa que, més enllà del segell blockchain que garanteix la immutabilitat, ja existeix una capa de traçabilitat: qualsevol auditor pot seguir el fil de decisions fins a la font original sense dependre d'un únic proveïdor. A escala municipal, ciutats com Helsinki i Amsterdam van publicar els seus primers inventaris algorítmics (2020), exposant les dades d'entrenament i els mecanismes de supervisió humana per a cada sistema [14]. Ancorar aquests logs i inventaris amb una prova d'existència neutral els converteix en **no-repudiables** i verificables per qualsevol actor, eliminant la necessitat de «confiar en la web de l'administració» i afegint un nou nivell de confiança descentralitzada al teixit de governança algorítmica.

És hora d'actuar

Per als **proveïdors de models** (OpenAI, Google, Meta, Mistral, els laboratoris de pes obert): segellar l'AI-BOM en publicar —empremta dels pesos, resum d'entrenament i informe d'avaluació— perquè el llinatge tingui data certa. Per als **desplegadors i les empreses** que integren models: verificar que els pesos que executen coincideixen amb l'empremta segellada abans de desplegar-los i exigir un AI-BOM ancorat al proveïdor com a requisit de compra. Per als **repositoris de models** (Hugging Face): ancorar l'empremta de cada model en pujar-lo, de manera que una substitució maliciosa sigui detectable. I per als **auditors i reguladors** (l'Oficina d'IA): reconèixer l'AI-BOM segellat com a evidència de la documentació que l'article 53 ja exigeix i tractar la data certa com la diferència entre una declaració i una coartada fabricada després.

A Stanford, un grup d'investigadors va haver d'auditar des de fora un model que ja corria a tot el món per descobrir què contenia. Donar a cada model una prova segellada del que s'ha entrenat, qui l'ha fet i quins pesos són els correctes —sense oblidar mai que el segell no fa veritable el que s'hi declara— és, en aquest front on la màquina aprèn de nosaltres, **time2act**.

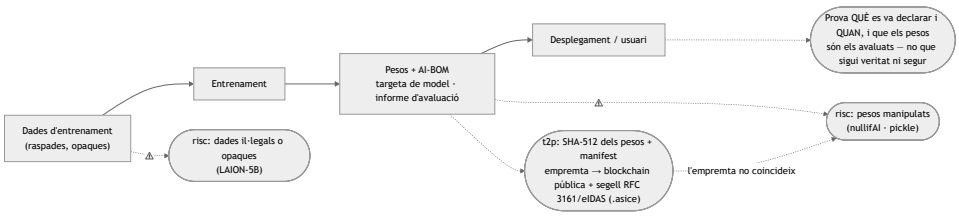


Figura 79.1 — El cicle de vida d'un model en quatre baules: dades d'entrenament → entrenament → pesos + AI-BOM (targeta de model, informe d'avaluació) → desplegament. t2p ancora l'empremta SHA-512 dels pesos i del manifest a la blockchain pública, amb segell RFC 3161/eIDAS complementari (.asice). Dos punts de risc: dades il·legals o opaques a l'origen (LAION-5B) i pesos manipulats entre el laboratori i l'usuari (porta del darrere nullifAI *via* pickle*), que la comprovació d'empremta detecta. Límit: el segell prova què es va declarar i quan, i que els pesos són els avaluats; no prova que la declaració sigui certa ni que el model sigui segur. Fonts: Stanford Internet Observatory (LAION-5B); JFrog (models maliciosos); Reglament europeu d'IA, art. 53 i 50; CycloneDX ML-BOM.*

[1] Stanford Internet Observatory / 404 Media — *Largest Dataset Powering AI Images Removed After Discovery of Child Sexual Abuse Material* (desembre de 2023; 3.226 casos sospitosos a LAION-5B; recomanació de deprecar els models). 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* (agost de 2024; 2.236 enllaços eliminats). https://laion.ai/blog/relaion-5b/ ↩

[3] JFrog Security Research — *Data Scientists Targeted by Malicious Hugging Face ML Models with Silent Backdoor* (2024; tècnica *nullifAI*, abús de *pickle*, porta del darrere). 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* (març 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* (documentació tècnica Annex XI; resum del contingut d'entrenament; sancions de fins a 15 M€ o 3 %). https://artificialintelligenceact.eu/article/53/ ↩

[6] Comissió Europea — *General-Purpose AI Models in the AI Act: Questions & Answers* (plantilla del resum d'entrenament; aplicació des del 2 d'agost de 2025; marcatge de l'art. 50 des del 2 d'agost 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, models i configuracions amb procedència; des de 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: més de 100.000 milions de continguts marcats segons Google I/O 2026 (maig de 2026); credencials de contingut). 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] Consell 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 ↩

Els agents d'IA: el mandat verificable

«Com que ara no tenim cap manera de fer savis els ordinadors, ara no els hauríem d'encarregar tasques que exigeixen saviesa.»

— Joseph Weizenbaum, Computer Power and Human Reason (1976)

Novembre de 2022. Jake Moffatt, un canadenc que acaba de perdre l'àvia, consulta el web d'Air Canada el mateix dia. El chatbot de la companyia li explica, servicial, una política que no existeix: que pot comprar el bitllet a preu complet i demanar després, en 90 dies, la tarifa de dol. Moffatt compra — 1.630,36 dòlars canadencs. Quan reclama, la companyia li respon que la política real no s'aplica a viatges ja fets, i s'hi nega. El febrer de 2024, el tribunal civil de la Colúmbia Britànica condemna Air Canada a pagar-li 812 dòlars: la companyia «no va tenir la cura raonable de garantir que el seu chatbot fos exacte» [1]. I deixa una frase per a la història: «hauria de ser obvi per a Air Canada que és responsable de tota la informació del seu web; tant li fa que vingui d'una pàgina estàtica o d'un chatbot». Pel camí, la companyia havia arribat a al·legar que el chatbot era «una entitat legal separada», responsable dels seus propis actes. El tribunal no s'ho va empassar [1].

Allò era només un chatbot que informava. El que ja és aquí són agents que actuen: compren bitllets, contracten serveis, responen clients, mouen diners. Cada acte d'un agent és un acte jurídic de qui l'ha activat — i cada error, una disputa a tres bandes: l'usuari, que sosté que no va autoritzar allò; la plataforma de l'agent, que assegura que va executar el que li van manar; i el comerç, que va rebre una ordre aparentment vàlida.

Aquest capítol tracta la delegació en màquines que s'equivoquen. Què és el model per dins — les dades, els pesos, l'AI-BOM — es tracta al capítol 79; els registres d'accions dels agents del sector públic, al capítol 107; la identitat de qui contractes en remot, al capítol 91; la suplantació de directius que ordena transferències, al capítol 87. Pregunta clau: quan la compra surt malament, com es prova què vas autoritzar exactament — i què va fer exactament l'agent? Resposta: amb el mandat i el registre d'accions segellats amb **t2p** — el paquet probatori del capítol 13 [3] — en una capa neutral que cap de les tres parts interessades no controla.

La indústria ja construeix el mandat

Llegeix el panorama amb els ulls d'aquest llibre, perquè és revelador [2]. Visa, amb Intelligent Commerce, emet credencials tokenitzades d'abast limitat per a agents: un token per a l'agent de viatges vàlid només per a una aerolínia i una finestra de dates; un token amb límit de 200 dòlars que no pot autoritzar una compra de 500. Mastercard va anunciar l'abril de 2025 Agent Pay: agents verificats que transaccionen amb «Agentic Tokens» que lliguen la credencial de pagament a un agent concret, un àmbit de comerços i una política de consentiment. I Google va publicar el setembre de 2025 el protocol obert AP2, amb més de seixanta socis — Mastercard, American Express, PayPal, Coinbase, Salesforce —, que defineix dues peces amb noms reveladors: l'«Intent Mandate» — què vol l'usuari — i el «Cart Mandate» — què proposa comprar l'agent —, tots dos signats com a credencials verificables [2]. Mentrestant, els agents mateixos ja són productes de consum: Operator d'OpenAI, Project Mariner de Google, Computer Use d'Anthropic, els agents de Microsoft Copilot [2].

Fixa't en el vocabulari: mandats, credencials verificables, abast, consentiment. És el llenguatge del dret civil de tota la vida, reescrit en criptografia. La indústria de pagaments ha entès abans que ningú que el problema dels agents és el mandat.

Però cada solució viu dins del seu ecosistema — la de Visa mira el pagament Visa; la de Google, el seu protocol — i totes miren el moment de pagar. La disputa, en canvi, arriba després i és més ampla: què vas autoritzar, què va veure l'agent, què va fer, en quin ordre. I l'evidència d'això no pot viure a casa de cap de les tres parts interessades — ni al mòbil de l'usuari que reclama, ni als servidors de la plataforma que es defensa, ni als sistemes del comerç que va cobrar. Falta la capa neutral.

La prova d'existència aplicada

Quatre gestos converteixen la delegació en un fet auditable [3].

1. El mandat segellat

Abans d'activar l'agent, l'usuari — o l'empresa — redacta el mandat: pressupost màxim, àmbits permesos, vetos, durada. El document se segella amb t2p: empremta SHA-512 calculada al dispositiu, data certa, ancoratge [3]. No cal que ningú més el vegi: el dia de la disputa, el mandat existia amb aquest contingut exacte abans de la primera acció de l'agent. El «jo no vaig autoritzar això» i el «sí que ho vas autoritzar» deixen de ser un pols de memòries: hi ha un text, amb una data.

2. El registre d'accions ancorat

L'agent genera el seu registre — què ha fet, quan, sobre quins llocs — i aquest registre se segella periòdicament per lots: l'empremta de cada tram, encadenada amb l'anterior [3], com els registres de facturació del capítol 34. La plataforma que ho ofereix de sèrie converteix la caixa negra del seu agent en un historial auditable — i es protegeix a si mateixa: davant del client que nega haver rebut el resum, o del comerç que al·lega una ordre fantasma, el registre ancorat respon.

3. L'instant de l'oferta

Els preus i les condicions canvien per segons; l'agent decideix sobre el que veu ara. La captura certificada del que l'agent tenia davant — la pàgina de l'oferta, amb imatge completa i codi font [3] — congela l'instant de la decisió. Quan el comerç digui «aquest preu mai no va existir», o l'usuari digui «l'oferta prometia una altra cosa», la pantalla d'aquell moment té data certa. És la lliçó d'Air Canada [1], portada al món dels agents: la informació sobre la qual es va actuar, preservada.

4. L'autorització forta

Per sota del llindar que l'usuari hagi fixat al mandat, l'agent va sol; per sobre — la compra gran, el contracte nou, el pagament inusual —, l'acte requereix l'aprovació humana explícita: la signatura amb vídeo-selfie de t2p, amb els seus dos reptes de vida aleatoris i la verificació biomètrica del dispositiu [3]. L'aprovació queda lligada a l'acte concret, amb data certa. Ni l'usuari pot negar el que va aprovar mirant la càmera, ni ningú pot fer passar per aprovat el que mai no es va sotmetre.

Els límits, dits clarament: el segell no fa l'agent més llest — no evita l'al·lucinació ni l'error: els detecta, els data i els fa atribuïbles. La responsabilitat final la reparteixen els contractes i els tribunals — i Air Canada [1] va fixar el principi: qui desplega l'agent respon del que l'agent diu i fa. I no tot ha de ser un agent: hi ha actes — els més personals — que mereixen mans humanes de principi a fi.

La promesa i el perill

La promesa: delegació amb confiança — l'usuari que activa un agent sabent que el mandat i cada acció tenen data certa [3]; disputes que es resolen en minuts comparant mandat, registre i captura, en lloc d'anys de litigi [1]; plataformes que competeixen per auditabilitat; i la infraestructura de mandats que la indústria ja construeix [2], completada amb la capa neutral que cap de les parts no controla.

Els perills, mirats de cara.

El primer és **la vida sencera al registre**. El registre d'accions d'un agent personal és un diari íntim: què compres, què llegeixes, què negocies. Ha de quedar al dispositiu o als sistemes de l'usuari — només empremtes a la cadena [3] —, amb revelació selectiva del tram disputat, mai de la vida sencera.

El segon és **l'agent com a coartada**. «Ho va fer l'agent» no pot esdevenir la versió digital de «no vaig ser jo». El mandat datat delimita responsabilitats, no les esborra: qui activa un agent amb un mandat ampli assumeix el que hi cap dins; qui el desplega comercialment respon davant del client — el principi d'Air Canada [1]. La traça serveix per repartir bé les culpes, no per fer-les desaparèixer.

El tercer és **la cursa d'agents**. El comerç també té els seus agents, i l'asimetria es reprodueix: el gegant amb flota d'agents i registres perfectes contra el consumidor amb un mòbil. La neutralitat de la prova és el mínim; la protecció del més feble, com sempre, és regulatòria.

I el quart és **el tecnosolucionisme agèntic**. Cap segell no fa que delegar sigui sempre bona idea. L'agent és una eina per a tasques delegables; el criteri sobre què es delega — i què no — continua sent la decisió més humana de totes.

És hora d'actuar

Que la delegació tingui memòria.

Per a qui activa agents — persones i empreses: mandat per escrit i segellat abans d'activar [3]; llindars d'aprovació humana per als actes grans; i el registre, exportat i ancorat periòdicament.

Per a les plataformes d'agents: registre d'accions auditable i ancorat de sèrie [2][3] — la vostra defensa en la disputa i el vostre argument de venda; i que el mandat de l'usuari sigui un objecte verificable, no una casella acceptada.

Per als comerços: captureu i ancoreu el que serviu als agents — l'oferta, el preu, les condicions de l'instant [3]; la disputa de demà es guanya amb la pantalla d'avui.

Per a les xarxes de pagament i els protocols: els vostres mandats signats [2] són el fonament; obriu-los a l'ancoratge neutral perquè la prova sobrevisqui a qualsevol de vosaltres.

Per als reguladors i legisladors: el principi d'Air Canada [1] — qui desplega respon — mereix rang de norma; i tot agent que actuï davant de consumidors hauria de tenir mandat datat i registre auditable com a condició d'operació.

Deleguem perquè la vida no ens cap a les mans; que la delegació tingui memòria. Quan el teu agent compri, contracti i respongui per tu, que tu puguis provar què li vas manar — i ell, què va fer. Per una delegació amb data certa, **time2act**.

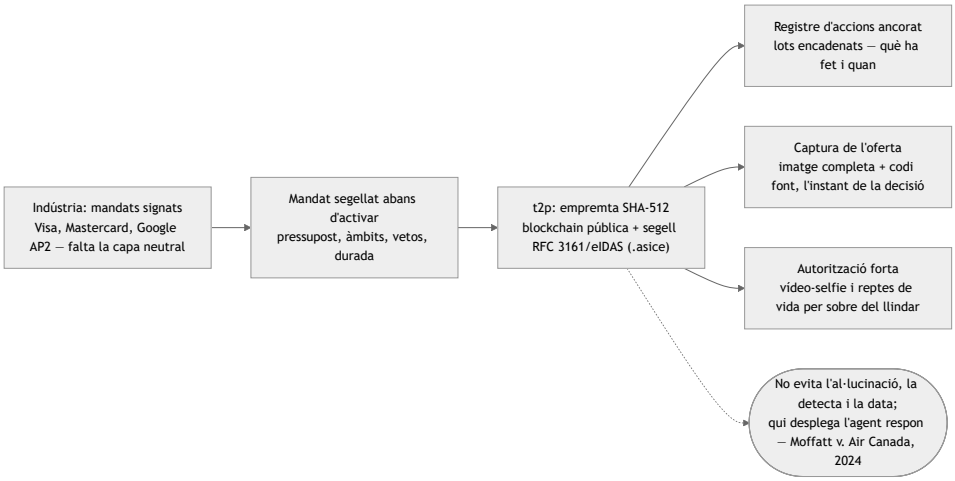


Figura 80.1 — El mandat verificable per a agents d'IA amb prova d'existència (segellat amb t2p — capítol 13): el mandat segellat abans d'activar (pressupost, àmbits, vetos), el registre d'accions ancorat per lots encadenats, la captura certificada de l'oferta que l'agent va veure (imatge + codi font) i l'autorització forta amb vídeo-selfie per sobre del llindar. Context: la indústria ja construeix mandats signats (Visa Intelligent Commerce, Mastercard Agent Pay, Google AP2 — Intent/Cart Mandate com a credencials verificables); la capa que falta és la neutral entre usuari, plataforma i comerç. Precedent: Moffatt v. Air Canada (2024) — qui desplega l'agent respon. Fonts: tribunal de la Colúmbia Britànica; 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, febrer de 2024: el chatbot va inventar una política de tarifa de dol; 812 $ canadencs de compensació sobre 1.630,36 pagats; «Air Canada no va tenir la cura raonable de garantir que el seu chatbot fos exacte»; «és responsable de tota la informació del seu web — tant li fa que vingui d'una pàgina estàtica o d'un chatbot»); Forbes — *What Air Canada Lost In 'Remarkable' Lying AI Chatbot Case* (l'al·legació que el chatbot era «una entitat 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* (credencials tokenitzades d'abast limitat per a agents; servidor MCP; un token de 200 $ no pot autoritzar 500 $); Mastercard — *Agent Pay* (anunciat el 29-4-2025: Agentic Tokens que lliguen credencial, agent, àmbit de comerços i política de consentiment; «Agent Pay for Machines», juny de 2026); Google AP2 (setembre de 2025, 60+ socis: Intent Mandate + Cart Mandate signats com a credencials verificables); Eco/Paz — guies del comerç agèntic 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 producte (certificar qualsevol fitxer — el mandat i els registres, només l'empremta viatja; captura de pàgina web amb imatge completa + codi font; signatura amb vídeo-selfie, dos reptes de vida aleatoris i verificació biomètrica del dispositiu; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; la procedència dels models, al capítol 79; els agents del sector públic, al capítol 107. ↩

La teva cara, la teva veu: drets d'imatge i rèpliques digitals

«El número de sèrie d'un exemplar humà és la cara, aquesta combinació accidental i irrepetible de trets.»

— Milan Kundera, La immortalitat (1990)

L'octubre de 2023, **Tom Hanks** va haver d'avisar els seus seguidors per Instagram d'una cosa estranya: «Hi ha un vídeo per aquí que promociona un pla dental amb una versió d'IA de mi. No hi tinc res a veure» [1]. Mesos després, l'actriu **Scarlett Johansson** explicava que havia rebutjat la petició d'OpenAI de prestar la seva veu a ChatGPT, i que l'empresa havia llançat igualment una veu —«Sky»— que s'hi assemblava tant que una anàlisi forense de la Universitat Estatal d'Arizona la va trobar més semblant a la de Johansson que la del **98 %** de les altres actrius examinades; OpenAI la va retirar després de rebre cartes dels seus advocats [2]. En tots dos casos, la persona va haver de sortir a desmentir-ho **després**, sense cap manera de provar, d'entrada, que mai no havia donat permís. La càrrega requeia sobre la víctima.

Aquesta és la pregunta d'aquest capítol, diferent de la del capítol 40 —l'autoria d'una obra— i de la del capítol 67 —l'actuació en directe i els drets de reproducció. Aquí l'**obra protegida ets tu**: la teva cara, la teva veu, el teu cos. I la pregunta no és qui ho ha fet, sinó **vas consentir-ho, per a quin ús, i es pot demostrar?** Perquè generar una rèplica digital d'algú s'ha tornat trivial, i desmentir-la, no.

Una cara que ja no és teva

El problema té tres formes. La primera són els **anuncis fraudulents**: rostres famosos —Hanks, Johansson— però també persones anònimes— enganxats a productes que mai no han avalat, en una onada d'estafes que es multiplica perquè fabricar-les costa minuts. La segona és la **por dels professionals de la veu i la imatge**: com hem vist, el 2023 els actors de Hollywood van fer vaga durant mesos i una de les seves línies vermelles eren precisament les **rèpliques digitals**; l'acord que va tancar la vaga exigeix consentiment informat per crear o reutilitzar la rèplica d'un intèrpret, amb una «descripció raonablement específica» de l'ús previst, i un consentiment **nou** —i una paga nova— si la rèplica es trasllada a un altre projecte [3]. La tercera és la **resurrecció dels morts**: veus i cares de difunts reanimades per vendre o entretenir sense que ningú pugui dir si la família ho va autoritzar. En les tres, la mateixa asimetria: és fàcil falsificar i difícil desmentir, i qui pateix el dany ha de perseguir cada còpia una per una.

La llei reconeix el dret; falta el rebut

La llei ha reaccionat amb una rapidesa inusual. A Tennessee, l'**ELVIS Act** —*Ensuring Likeness, Voice and Image Security*— va entrar en vigor l'1 de juliol de 2024 i va incorporar la **veu** al dret de publicitat, fins i tot creant responsabilitat per a qui distribueixi una eina d'IA la finalitat principal de la qual sigui imitar la veu o la imatge d'algú [4]. Als Estats Units, la **NO FAKES Act** —que crearia un dret federal sobre la rèplica digital— va superar el 18 de juny de 2026 la Comissió Judicial del Senat per unanimitat, tot i que encara ha de passar el ple del Senat i la Cambra de Representants [5]. I Dinamarca ha fet el pas més radical: el juny de 2025 va presentar una reforma de la seva llei de propietat intel·lectual —encara en tràmit parlamentari, amb entrada en vigor prevista a mitjan 2026— per donar a **cada persona un dret de tipus copyright sobre la seva pròpia cara, cos i veu**, amb dret a exigir la retirada dels *deepfakes* i una compensació, protecció fins a cinquanta anys després de la mort i excepcions per a la paròdia i la sàtira [6]. A Europa, l'article 50 del Reglament d'IA obligarà a **marcar** el contingut generat per IA [veure capítol 79]. Però totes aquestes lleis topen, a l'hora de la veritat, amb una sola pregunta: **aquesta persona va consentir aquest ús, i on és la prova?** Avui el consentiment és un PDF en un calaix —o no és res.

Per què la llei sola no salva

Cal dir-ho amb cruesa: un dret de publicitat val tant com l'evidència que el sosté. Quan apareix un anunci amb la teva cara, has de demostrar que **no** vas consentir —provar un fet negatiu—, i la plataforma ha de decidir en hores si el retira. Un contracte de cessió guardat en un servidor d'un estudi es pot retocar o

retrodatar; un estudi sense escrúpols pot al·legar «ja hi va estar d'acord» i ensenyar un paper. Sense un registre de consentiment **verificable i amb data certa**, cada disputa es converteix en la teva paraula contra la seva, i guanya qui té més advocats. El dret existeix; el que falta és el **rebut inalterable**.

La prova d'existència aplicada

És aquí on **t2p** aporta dues capes complementàries. La primera la controla la **persona**: amb una **prova de vida**, crea un *registre de consentiment de la imatge* que lliga una **referència biomètrica** —l'empremta SHA-512 d'una mostra de rostre o veu, que **no surt del dispositiu**— a una concessió explícita i **acotada**: quins usos autoritza, per a qui i fins quan. Tot plegat se segella amb un **segell de temps RFC 3161/eIDAS** i s'ancora a la **blockchain pública** dins d'un contenidor **.asice**. Una rèplica digital legítima porta llavors un **punter verificable** a un consentiment segellat i vigent; i la **revocació** també queda segellada i datada, de manera que ningú no pot al·legar un permís que ja s'havia retirat. La segona capa la segella l'**estudi o l'anunciant** en el moment de signar: el consentiment informat a l'estil de l'acord dels actors, amb la descripció específica de l'ús i la prova de vida de l'intèrpret, de manera que reutilitzar la rèplica en un altre projecte sense un consentiment nou esdevé **detectable**.

L'efecte és que la càrrega de la prova canvia de bàndol. El cas de Hanks deixa de dependre de la seva paraula: pot mostrar que **mai** va emetre cap concessió segellada per a aquell anunci dental, i l'**absència** d'un permís ancorat es converteix, ella mateixa, en prova de la falta de consentiment. Es combina amb la procedència del capítol 13 i 15: la marca C2PA o SynthID diu «això és sintètic»; el registre de consentiment hi afegeix «i ningú no va autoritzar aquesta cara».

Ara el límit, amb tota la cruesa. «Escombraries a l'entrada, escombraries a la cadena»: el segell prova que el consentiment es va donar —o no—, de qui i quan; **no detecta el *deepfake*** pel seu compte (això depèn de la marca de procedència i dels detectors), **no n'impedeix la creació**, i un consentiment segellat sota pressió continua sent un consentiment viciat, ara a més immutable. Prova l'**acte** de consentir, no la seva **justícia**. El que fa és treure les disputes del terreny de la paraula contra paraula i portar-les al de «ensenya la concessió segellada».

La promesa i el perill

La promesa és un món on la teva cara i la teva veu tornen a ser teves de manera **demostrable**: els intèrprets llicencien les seves rèpliques amb un consentiment datat, acotat i revocable; les plataformes i els tribunals disposen d'un registre per distingir l'ús autoritzat de la violació; i els difunts queden protegits per concessions segellades pels seus hereus. En una època en què qualsevol cara es pot clonar en minuts, fer el consentiment immutable és tornar el control a la persona.

El perill demana matisos. Primer, un consentiment **arrencat per coacció** i segellat no deixa d'ésser injust perquè sigui immutable. Segon, construir un registre de referències biomètriques és sensible: per això la regla d'or —la cara **no surt del dispositiu**, només se'n segella una empremta— ha de substituir qualsevol base central de rostres que seria un somni per a la vigilància. Tercer, cal evitar que els estudis acabin custodiant les fitxes d'imatge de tothom. I quart, no s'ha de confondre l'absència de consentiment amb usos legítims —paròdia, sàtira, crítica, informació— que la normativa ja protegeix. La prova d'existència és una capa de control sobre la pròpia imatge, no un permís automàtic ni un detector de falsedats.

A més a més, delegar la gestió biomètrica a xarxes descentralitzades no elimina el risc que el control efectiu es concentri en mans d'uns pocs actors tècnics. La infraestructura necessària per crear i validar empremtes digitals requereix servidors potents, accés a bases de dades massives i una capa de programari complexa que només un nombre limitat d'empreses pot desenvolupar i mantenir. Com assenyala Marc Goodman, Facebook —i no un programa estatal— és «el magatzem més extens de dades biomètriques que hi ha sobre la Terra, superant de bon tros el de qualsevol govern»[11]. Això mostra com una plataforma privada pot acumular informació biogràfica a escala global, convertint-se en un punt d'entrada privilegiat per a la captura i l'explotació de les empremtes. Per tant, fins i tot amb protocols que garanteixen que la cara no surti del dispositiu, cal establir mecanismes de governança i auditoria independents que impedeixin que aquesta concentració tècnica es tradueixi en un poder real sobre la identitat de les persones.

Com hem vist, l'exemple de **PalmerAI** al caucus demòcrata de Samoa Americana il·lustra com la pregunta ja no és «és real el vídeo?», sinó «què va dir la persona i què diu la rèplica?»[12]. L'avançament

d'un avatar que reproduïa la veu i l'aspecte de Jason Palmer, capaç de guanyar una elecció amb 51-40 punts, posa en relleu un buit: el votant necessita saber si el missatge prové del candidat o d'una entitat digital. Un ancoratge neutral en blockchain pot registrar cada declaració amb una prova d'existència immutable, vinculada al certificat de consentiment original i a la clau privada del titular. Així, qualsevol observador podria traçar l'origen del discurs i validar-lo sense dependre de plataformes centralitzades. No obstant això, el mateix mecanisme pot crear un nou risc: si les claus es comprometen o s'empren per part d'un grup de poder, la cadena certificadora podria ser utilitzada per legitimar rèpliques manipulades, convertint-se en una «capa de confiança» que, mal governada, reforça la concentració de control sobre el discurs polític i social.

És hora d'actuar

Per a les **persones i els intèrprets**: segellar un registre de consentiment de la imatge acotat i revocable, mantenint la referència biomètrica privada al dispositiu. Per als **estudis, anunciants i proveïdors d'eines d'IA**: segellar el consentiment informat en signar, amb l'abast específic de l'ús, i **verificar una concessió vigent** abans de generar cap rèplica. Per a les **plataformes** on corren els anuncis: exigir un punter de consentiment verificable per a qualsevol aval sintètic, i tractar-ne l'absència com a senyal de retirada. I per als **legisladors i tribunals** (ELVIS Act, NO FAKES, Dinamarca, el Reglament europeu): reconèixer el registre de consentiment segellat com a evidència amb data certa del consentiment —o de la seva falta.

Tom Hanks va haver de sortir a dir que la cara que venia plans dentals no era la seva. Donar a cada persona una prova segellada de què autoritza la seva imatge, per a qui i fins quan —sense oblidar mai que el segell prova el consentiment, no la seva justícia— és, en aquest front on ens poden robar la cara, **time2act**.

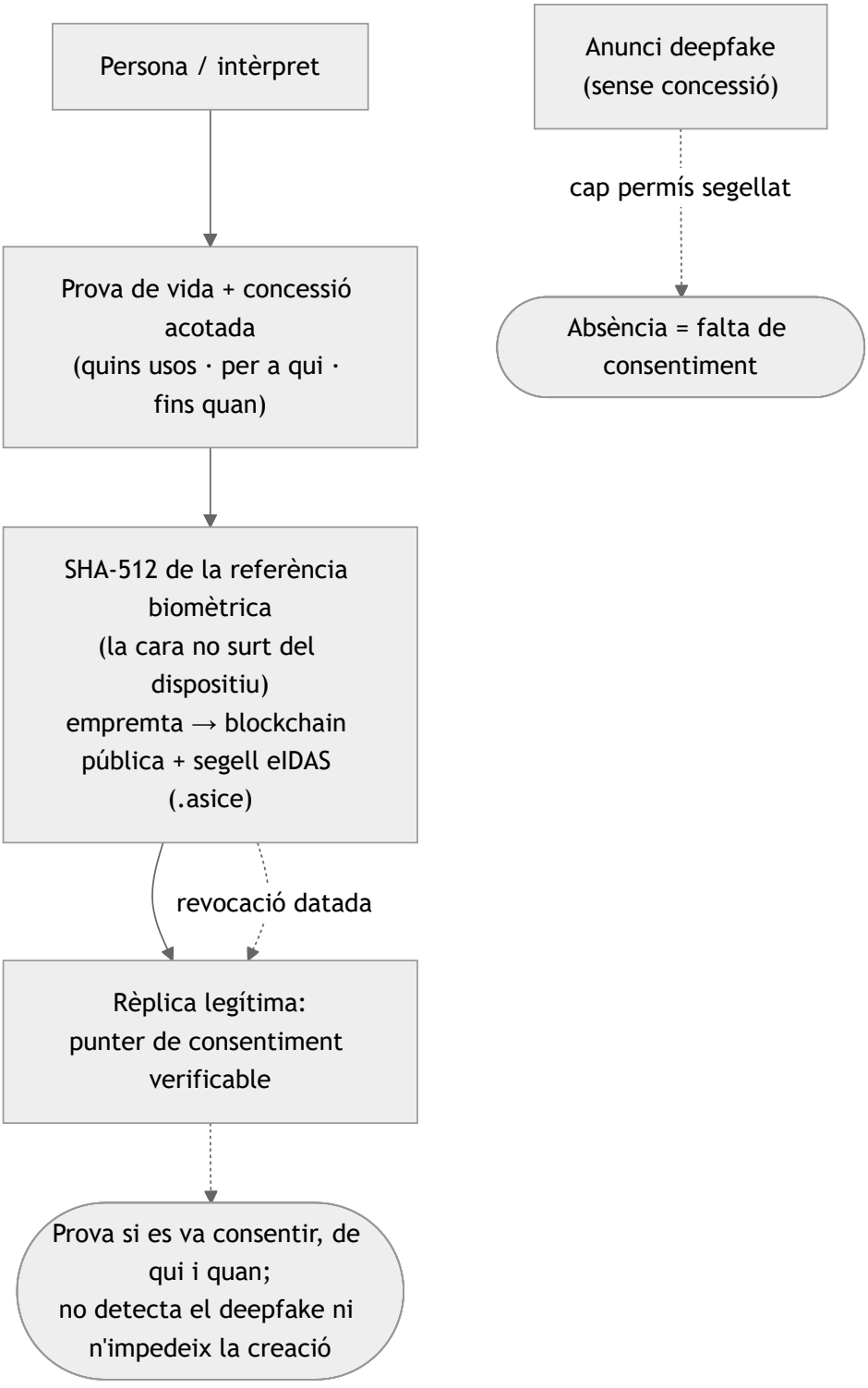


Figura 81.1 — Dues vies. A dalt: la persona crea, amb prova de vida, una concessió de consentiment acotada (quins usos, per a qui, fins quan) lligada a una referència biomètrica (empremta SHA-512; la cara no surt del dispositiu), ancorada a la blockchain pública, amb segell eIDAS complementari (.asice); una rèplica legítima en porta un punter verificable, i la revocació queda datada. A baix: un anunci deepfake sense cap concessió segellada —l'absència mateixa demostra la falta de consentiment. Límit: el segell prova si es va consentir, de qui i quan; no detecta el deepfake ni n'impedeix la creació, i no jutja si el consentiment va ser lliure. Fonts: cas Tom Hanks; cas Johansson–OpenAI; acord 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'* (maig de 2024; anàlisi forense de la Universitat Estatal d'Arizona: més semblant que el 98 % de les actrius). 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* (consentiment informat; descripció específica de l'ús; consentiment nou per a la reutilització). 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 l'1 de juliol de 2024; la veu al dret de publicitat; responsabilitat de les eines d'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)* (dret federal sobre la rèplica digital; versió revisada de 2026, aprovada per la Comissió Judicial del Senat el 18 de juny de 2026). https://www.judiciary.senate.gov/no-fakes-act ↩

[6] World Economic Forum — *Deepfake legislation: Denmark takes action* (presentada el juny de 2025; dret de tipus copyright sobre cara, cos i veu; retirada i compensació; excepcions de paròdia; en tràmit parlamentari, entrada en vigor prevista a mitjan 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'* (maig de 2024). https://variety.com/2024/digital/news/scarlett-johansson-responds-shocked-angered-openai-chatgpt-her-1236011135/

[8] SAG-AFTRA — *Digital Replicas 101* (tipologia i drets de consentiment de l'intèrpret). 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* (marcatge del contingut generat o manipulat per 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 imatge de qui no pot consentir

«No hi ha nens: hi ha persones; però amb una altra escala de conceptes, un altre cabal d'experiència, altres impulsos, un altre joc de sentiments.»

— Janusz Korczak, Quan torni a ser petit (1925)

El primer dia d'escola, amb la motxilla nova i el somriure a mig fer. La festa d'aniversari, els globus, el pastís. La tarda de platja. I el gest automàtic de cada vegada: publicar. Cap malícia — amor, orgull i el costum del segle. La dada que ho emmarca [1]: un infant apareix de mitjana en 1.300 fotografies publicades en línia abans de fer els 13 anys — un àlbum públic que ell no ha triat, indexat, replicable i permanent. I els riscos que el legislador francès va llistar en tramitar la seva llei no són hipotètics: usurpació d'identitat, xantatge, ciberassetjament — i els pitjors [1].

El matís que fa el capítol sencer: això no va de culpar pares. Va d'una pregunta jurídica que ningú no s'havia fet fins fa poc — qui consent la imatge de qui encara no pot consentir, i on queda escrit? Qui pot demostrar que una publicació tenia el permís de tots dos progenitors, o que un s'hi va negar? On és l'autorització que l'escola diu que tenia?

Aquest capítol tracta el consentiment sobre la imatge dels menors — i com acreditar-lo. El dret d'imatge dels adults — l'obra protegida ets tu — és al capítol 81; la difusió d'imatges íntimes, al capítol 83; l'odi i l'assetjament als joves, al capítol 84; la coparentalitat — on el menor mai no és objecte de registre —, al capítol 53; l'escola, al capítol 19. Pregunta clau: com es protegeix el dret d'algú que encara no el pot exercir? Resposta: documentant les decisions dels adults que el custodien — l'autorització, la negativa, la petició de retirada — amb data certa: **t2p**, la mecànica de sempre, la del capítol 13 [3]. Es documenten consentiments; mai el menor — la línia del capítol 53, aquí, és sagrada.

França escriu el que ningú no havia escrit

El 19 de febrer de 2024, el Parlament francès va aprovar — per unanimitat — la Llei 2024-120, que garanteix el respecte del dret a la imatge dels infants [1]. La reforma toca el cor del dret de família: l'article 371-1 del Codi civil diu ara, expressament, que l'autoritat parental inclou la protecció de la vida privada del menor i del seu dret a la imatge; que els pares el protegeixen en comú; i que hi han d'associar l'infant segons la seva edat i maduresa. I la peça més contundent: si la difusió de la imatge del fill pels seus propis pares atempta greument contra la seva dignitat o la seva integritat moral, el jutge pot delegar a un tercer l'exercici del dret d'imatge del menor — retirar-lo als pares [1].

A Espanya, el marc protegeix el menor amb intensitat — la llei orgànica que empara l'honor, la intimitat i la pròpia imatge, la de protecció jurídica del menor, la vigilància del Ministeri Fiscal [2] — i els tribunals ja exigeixen l'acord de tots dos progenitors per publicar imatges dels fills: la negativa d'un hauria d'aturar la difusió [2].

I aquí, el diagnòstic d'aquest llibre: el consens legal existeix; la seva prova, no. Tot l'edifici — el consentiment comú, la negativa d'un progenitor, l'autorització escolar, la petició de retirada — funciona sobre actes que ningú no pot acreditar després: el «jo mai no vaig autoritzar això» del pare separat, el «l'escola tenia permís» que no es troba, el «vaig demanar que ho esborressin fa un any» sense data. Declaracions que pesen poc quan arriba el conflicte — perquè no tenen data ni forma.

La prova d'existència aplicada

Es documenten les decisions dels adults — mai el menor [3].

1. L'autorització que diu què

L'autorització escolar o d'extraescolar — sovint una casella genèrica — convertida en un document precís i segellat: quins usos (la web del centre? xarxes? el grup de famílies?), quins canals, quant de temps; signada amb data certa [3]. L'escola que la té ancorada sap què pot fer; la família sap què ha permès; i el «teníem permís» esdevé un fet consultable, no una discussió d'inici de curs.

2. El desacord que consta

Quan un progenitor no vol que es publiquin imatges del fill — el cas clàssic de la separació —, la seva negativa, comunicada i segellada amb data certa [3]: a l'altre progenitor, a l'escola, al club. Els tribunals ja exigeixen l'acord de tots dos [2]; el que faltava era que la negativa tingués data. La lògica és la del capítol 53 — documentar els acords i desacords dels adults, mai el menor — aplicada a la imatge.

3. La retirada datada

La petició d'esborrar una foto — a l'altre progenitor, a l'avi entusiasta, a la plataforma — enviada i capturada amb data certa; i el silenci o la negativa, també datats [3]. Si el conflicte escala — fins al jutge que la llei francesa ja preveu [1] —, la cronologia sencera existeix: es va demanar tal dia; no es va atendre; això és el que hi havia publicat.

4. L'empremta per al futur

La foto publicada — o l'àlbum sencer — registrada per empremta: la SHA-512 al dispositiu de la família, res del contingut enlloc [3]. Semblaria paradoxal — documentar el que voldríem que no existís —, però és el regal probatori al fill gran: el dia que vulgui exercir els seus drets — retirada, oblit, o simplement saber —, podrà acreditar què es va publicar d'ell i quan, sense dependre de la memòria de ningú ni de la memòria cau de cap cercador. La seva infància digital, auditable per ell.

Els límits, abans que ningú es faci il·lusions: el segell acredita consentiments, negatives i dates — no decideix què és l'interès superior del menor: això ho fan els pares que s'entenen i, quan no, el jutge [1][2]. Res d'això no és una invitació a documentar el nen — la línia del capítol 53 mana: es registren les decisions dels adults. I la millor protecció continua sent la més antiga: publicar menys, pensar abans, i preguntar al fill quan tingui edat de respondre — la llei francesa ho diu amb una paraula preciosa: associar-lo [1].

La promesa i el perill

La promesa: escoles amb autoritzacions precises i consultables [3]; progenitors separats que discuteixen el fons — què convé al fill — i no els fets; peticions de retirada que no es perden en converses; i una generació que, en fer 18 anys, podrà mirar la seva infància digital amb els drets a la mà [1] — perquè algú va tenir la cura de datar-la.

Ara, els perills.

El primer és **l'expedient contra l'exparella**. El desacord documentat pot esdevenir munició del conflicte parental. El contrapès és el del capítol 53: la traça és per protegir el menor, no per guanyar la guerra — el disseny bilateral i l'interès superior del menor com a nord; i els jutges detecten de seguida qui documenta pel fill i qui contra l'altre.

El segon és **la burocratització de la tendresa**. Si publicar la foto de l'aniversari exigeix un tràmit, la vida familiar es fa impossible. La resposta és la proporcionalitat: el consentiment precís és per a les institucions — escoles, clubs, mitjans — i per als desacords; entre adults que s'entenen, n'hi ha prou amb el respecte.

El tercer és **el fals segell de legitimitat**. Una autorització datada no fa bona una publicació que fa mal. El consentiment dels pares té límits — la dignitat del menor els marca, i la llei francesa ho ha escrit [1]: hi ha difusions que cap signatura parental no empara.

I el quart, el més íntim: buscar en una eina l'excusa per no pensar. Cap empremta no substitueix el criteri. La pregunta abans de publicar no és «tinc el permís?», sinó «li agradarà, d'aquí a quinze anys, que això existeixi?». La prova d'existència ordena els consentiments; la prudència els fa innecessaris.

És hora d'actuar

Que cada imatge d'un infant tingui darrere una decisió que es pugui ensenyar.

Per a mares i pares: penseu abans de publicar — i quan el fill tingui edat, pregunteu-li [1]; si hi ha desacord entre vosaltres, que consti amb data [3]: el fill mereix que la seva imatge no sigui camp de batalla.

Per a les escoles, clubs i entitats: autoritzacions precises, segellades i renovades [3] — la casella genèrica de principi de curs no protegeix ni les famílies ni el centre.

Per a les plataformes: peticions de retirada d'imatges de menors amb resposta datada i traçable — el silenci també és una decisió, i hauria de constar.

Per als legisladors: França ha marcat el camí [1] — el dret a la imatge del menor com a deure comú dels pares, amb el jutge com a última garantia; que la transposició d'aquesta idea vingui amb consentiments i negatives acreditables.

Per als fills, quan sigueu grans: la vostra infància digital és vostra; reclameu-la — i que les empremtes datades [3] us estalviïn haver de provar l'evident.

Les 1.300 fotos [1] ja hi són; les següents encara no. Que cada imatge d'un infant tingui darrere un consentiment que es pugui ensenyar — i un adult que s'hagi aturat a pensar. Pels qui encara no poden dir que no, **time2act**.

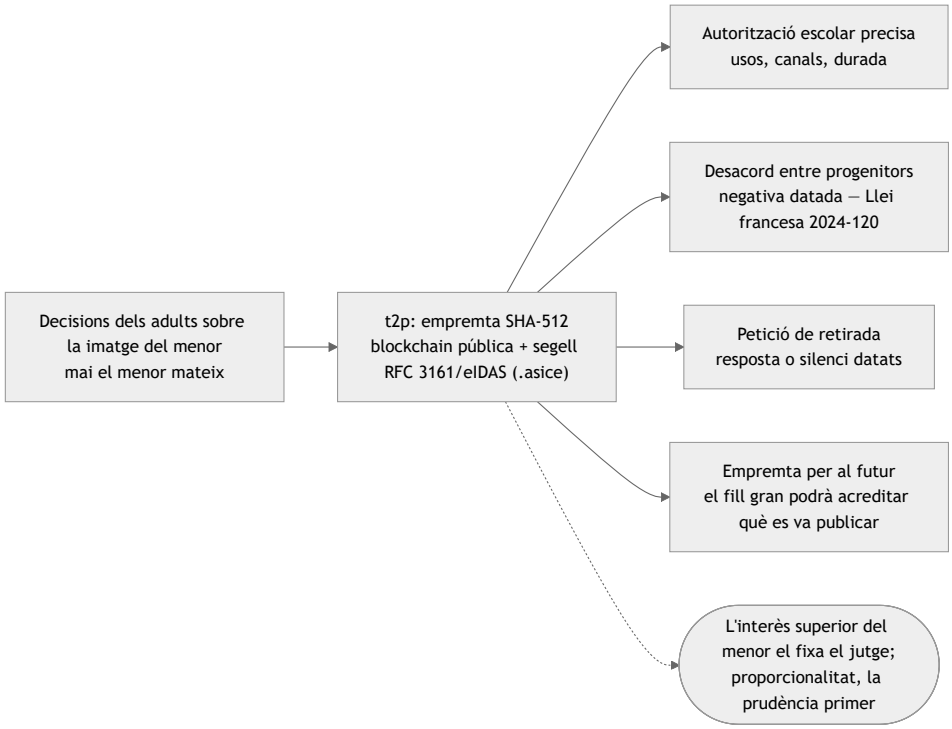


Figura 82.1 — La imatge del menor amb prova d'existència (segellat amb t2p — capítol 13) — es documenten les decisions dels ADULTS, mai el menor: l'autorització escolar precisa i segellada (usos, canals, durada), el desacord entre progenitors datat, la petició de retirada amb resposta o silenci datats, i l'empremta de la publicació per al futur (el fill gran podrà acreditar què es va publicar d'ell, sense que cap contingut viatgi). Context: un infant apareix en ~1.300 fotos en línia abans dels 13 anys; Llei francesa 2024-120 (dret a la imatge dins l'autoritat parental, exercit en comú; delegació judicial en casos greus). Límits: l'interès superior del menor el fixa el jutge; proporcionalitat; la prudència primer. Fonts: Légifrance; DAJ.

---

[1] Légifrance — *Llei núm. 2024-120, de 19 de febrer de 2024, per garantir el respecte del dret a la imatge dels infants* (modificació de l'art. 371-1 del Codi civil: l'autoritat parental inclou la protecció de la vida privada i del dret a la imatge del menor; protecció exercida en comú pels dos progenitors, associant-hi l'infant segons edat i maduresa; delegació judicial de l'exercici del dret d'imatge en cas d'atemptat greu a la dignitat o la integritat moral); DAJ/economie.gouv.fr — *Respect du droit à l'image des enfants: les apports de la loi* (context: un infant apareix de mitjana en 1.300 fotografies en línia abans dels 13 anys; riscos: usurpació, xantatge, ciberassetjament); 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] Marc espanyol (LO 1/1982 sobre l'honor, la intimitat i la pròpia imatge; LO 1/1996 de protecció jurídica del menor; intervenció del Ministeri Fiscal; doctrina judicial que exigeix l'acord de tots dos progenitors per publicar imatges dels fills). Vegeu el capítol 81 per al dret d'imatge general i el capítol 53 per als registres de coparentalitat. ↩

[3] t2p — manual de producte (escàner de documents; captura de pantalla i correu certificades; certificar qualsevol fitxer — només l'empremta viatja, el contingut no surt mai del dispositiu; signatura amb vídeo-selfie; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; la coparentalitat, al capítol 53; la difusió íntima, al capítol 83. ↩

Imatges íntimes no consentides: el dany, la prova i la retirada

«A les noies de tot arreu: soc amb vosaltres. Les nits que us sentiu soles, soc amb vosaltres. Quan la gent dubti de vosaltres o us menystingui, soc amb vosaltres.»

— Chanel Miller, declaració d'impacte de la víctima, cas People v. Turner (2016)

El setembre de 2023, a **Almendralejo**, un poble de l'Extremadura, desenes d'adolescents van descobrir que circulaven per WhatsApp imatges seves despullades que mai no havien existit. Algú havia agafat fotos vestides dels seus comptes d'Instagram i, amb una aplicació d'IA, les havia convertit en nus falsos. Les víctimes tenien entre dotze i catorze anys. «Moltes nenes estaven completament aterrides i tenien atacs d'ansietat tremends perquè ho patien en silenci», va explicar una mare [1]. Un jutjat de menors de Badajoz va condemnar quinze nois —de tretze a quinze anys— per vint delictes de creació de material d'abús infantil i vint més contra la integritat moral de les víctimes [2]. El dany ja estava fet: les imatges eren falses, però la humiliació i la por eren reals.

Aquest capítol tracta una de les cares més cruels de les *deepfakes*, diferent de la del capítol 81 —l'ús comercial de la imatge. Aquí no parlem de diners ni de marca, sinó de **dignitat**. I cal dir una xifra que ho emmarca tot: més del **90 % del contingut *deepfake*** que circula per la xarxa és pornogràfic, i gairebé tot té com a víctima una **dona** [6]. La pregunta d'aquest capítol no és com evitar que existeixi —no es pot del tot—, sinó com donar a la víctima **prova del dany i una retirada demostrable** sense obligar-la a reviure'l.

Un dany fàcil d'infligir, difícil de reparar

El cas d'Almendralejo no és aïllat. Al gener del 2024, imatges sexuals falses de **Taylor Swift** van inundar la xarxa X: una sola publicació es va veure més de **47 milions de vegades** abans que la retiressin, i la plataforma va bloquejar les cerques del seu nom durant dos dies [3]. Si això li passa a una de les dones més poderoses del planeta, imaginem-ne una adolescent anònima. L'asimetria és brutal: fabricar la imatge costa minuts i és gratuïta; retirar-la obliga la víctima a perseguir cada còpia en cada plataforma, demostrar que és ella i sovint **tornar a mirar** allò que la fereix per aportar-ho com a prova.

Ja existeix una defensa que, no per casualitat, fa servir exactament el principi d'aquest llibre. **StopNCII.org** permet a una víctima generar al seu dispositiu una **empremta** (un *hash*) de la imatge íntima; **només l'empremta —mai la imatge— surt del telèfon**, i es comparteix amb Meta, TikTok, Reddit o Google perquè en bloquegin les pujades coincidents. Des de 2021 ha protegit més de **500.000 imatges** i ha impedit més de **10.000 intents** de publicació, amb èxit superior al 90 % [7]. És la prova que es pot defensar la víctima **sense centralitzar** ni una sola imatge.

La llei ja hi és; falta la prova inalterable

La resposta legal ha estat ràpida i contundent. Als Estats Units, la **TAKE IT DOWN Act**, signada el 19 de maig de 2025, criminalitza la publicació d'imatges íntimes no consentides —incloses les *deepfakes*— i obliga les plataformes a retirar-les en un màxim de **48 hores** des de l'avís; des del **19 de maig de 2026** la FTC ja n'aplica el compliment a les plataformes [4]. A Europa, la **Directiva (UE) 2024/1385** sobre la violència contra les dones, en vigor des del juny de 2024 i a transposar abans del juny de 2027, tipifica la producció i difusió no consentida de material íntim manipulat i obliga els estats a oferir **ordres de retirada i preservació ràpida de proves** [5]. La llei, doncs, ja demana dues coses: retirar de pressa i **conservar la prova**. I aquí torna el mur de sempre: una captura de pantalla és manipulable, l'avís a la plataforma pot no deixar rastre datat, i la víctima acaba havent de custodiar ella mateixa el material que la fereix.

Per què la denúncia sola no salva

Cal dir-ho amb cruesa, perquè aquí és especialment delicat. Perquè un tribunal condemni —com a Almendralejo— i perquè una retirada sigui exigible, cal **evidència admissible**: que aquesta imatge existia, on, quan, i que es va demanar retirar-la. Avui aquesta evidència és fràgil: una captura sense segell

no prova la data; demostrar que la plataforma va rebre l'avís i no va actuar en 48 hores depèn de correus i registres que es poden discutir; i conservar la prova significa, massa sovint, que la víctima ha de guardar i tornar a ensenyar la pròpia imatge. Falta una manera de **fixar la prova del dany i de l'avís amb data certa, sense reviure'l ni emmagatzemar-lo**.

La prova d'existència aplicada

És aquí on **t2p** estén la lògica de StopNCII amb la peça que falta. Quan una víctima, una entitat de suport o una plataforma detecta una imatge no consentida, es calcula al dispositiu l'**empremta SHA-512** del contingut i se segella, juntament amb **on i quan** s'ha trobat (l'URL, l'hora) i la **sol·licitud de retirada**, amb l'empremta ancorada a la **blockchain pública** i un **segell de temps RFC 3161/eIDAS** complementari, dins d'un contenidor **.asice**. El que en resulta és una **cadena de custòdia inalterable i datada** —útil per a la fiscalia, com en el cas d'Almendralejo, i per demostrar que la plataforma va ser avisada en tal moment i tenia 48 hores per actuar— **sense que la víctima hagi d'emmagatzemar ni tornar a compartir la imatge**: només se'n segella l'empremta. La data certa demostra que *aquell* contingut existia i va ser marcat com a abús en *aquell* instant, i l'acusat ja no pot al·legar que la prova es va fabricar després.

Hi ha una segona aplicació, per a la cara inversa del problema: la **sextorsió** i la falsa acusació. Quan algú amenaça una víctima amb difondre una imatge que sembla real, la **procedència** —l'absència de cap origen segellat, combinada amb la marca C2PA dels capítols 13 i 15— ajuda a establir que la imatge és **sintètica**, i a treure-li el poder de xantatge.

Ara el límit, amb tota la cruesa, perquè aquí enganyar-se faria mal. «Escombraries a l'entrada, escombraries a la cadena»: el segell **no retira la imatge**, **no n'impedeix la creació**, **no detecta** per si sol que sigui una *deepfake* i no pot fer que allò que s'ha vist deixi de veure's. El que fa és donar **prova del dany i retirada demostrable**, no prevenció. I imposa una línia vermella absoluta: **mai** no pot convertir-se en un registre d'imatges íntimes; només empremtes calculades al dispositiu, com a StopNCII. La protecció real continua sent la suma de l'empremta, la llei i el deure de la plataforma; el segell hi afegeix la prova inalterable.

La promesa i el perill

La promesa és tornar a la víctima una mica de poder: una **prova datada i admissible** del dany i de l'avís, i una retirada **exigible i verificable** a totes les plataformes, sense haver de rendir ni una sola imatge ni reviure-la cada vegada. L'agressor i la plataforma lenta perden la possibilitat de negar-se; la nena d'Almendralejo tindria, demà, una prova que cap advocat podria discutir.

El perill exigeix els matisos més estrictes del llibre. Primer: **res d'imatges centralitzades**; només empremtes al dispositiu. Segon: no convertir el procés de denúncia en una nova font de trauma; l'eina ha d'acompanyar, no obligar a mirar. Tercer: la governança del banc d'empremtes, que ha de ser auditada i a prova d'abús. I quart: recordar sempre que el segell demostra **l'acte de marcar** un contingut com a no consentit, amb data i autor; la determinació de qui el va crear correspon a la investigació. La prova d'existència és una eina de dignitat i de justícia, no un escut tecnològic que esborri el dany.

A més a més, l'immutabilitat inherent als registres basats en blockchain pot convertir-se en una cadena invisible de persecució per a les víctimes que busquen recuperar la vida després del trauma. Un cop gravada una empremta d'una imatge no consentida, aquesta queda inscrita per sempre al llibre públic de proves; el fet que no es pugui eliminar també implica que no hi ha cap mecanisme natural per retirar-la quan les circumstàncies canvien o quan la víctima decideix deixar enrere aquell capítol. Com avisa Edward Snowden, l'existència d'un «passat del qual em penedia del tot, però que tot just recordava» pot quedar «tan inextricablement i tecnològicament lligat» a la identitat de la persona afectada, augmentant el risc de revictimització a llarg termini [11]. Per això, qualsevol arquitectura de segell digital ha d'incloure una capa de caducitat o revocabilitat controlada per una autoritat independent, que permeti esborrar o invalidar l'empremta quan la prova ja no sigui necessària o resulti contraproduent. Aquesta salvaguarda equilibraria la necessitat de certitud legal amb el dret a l'oblit i a la rehabilitació personal.

Com hem vist, la magnitud del problema ja supera el terreny de l'empresa i arriba a les alçades de la política: l'American Sunlight Project va constatar que, al desembre de 2024, prop d'un de cada sis congressistes nord-americans són víctimes d'imatges íntimes no consentides generades per IA, una xifra que revela un patró sistemàtic d'abús i vulnerabilitat a escala institucional [12]. Aquesta realitat obliga les

plataformes a adoptar mecanismes «Take It Down» capaços de respondre en temps real, però sense una prova d'existència ancorada a la blockchain la retirada es queda a l'aire: no hi ha cap registre immutable que demostri que la denúncia s'ha fet i que el contingut ha estat eliminat. L'ancoratge neutral de l'evidència, independent del creador i dels tercers, converteix cada sol·licitud d'eliminació en una pista verificable per al tribunal, evitant que les víctimes hagin d'assumir la càrrega de demostrar el dany i garantint que les autoritats puguin actuar amb la certesa legal necessària.

És hora d'actuar

Per a les víctimes i les entitats de suport (StopNCII, línies d'ajuda): segellar l'empremta i les circumstàncies del dany com a prova, sense emmagatzemar la imatge. Per a les plataformes: conservar el banc d'empremtes i emetre rebuts segellats per cada avís i retirada, demostrant el compliment de les 48 hores. Per a la policia i els tribunals: tractar l'empremta segellada amb segell de temps com a cadena de custòdia, com es va fer en el cas d'Almendralejo. Per als legisladors (TAKE IT DOWN Act, Directiva 2024/1385): reconèixer la prova segellada com a evidència vàlida i garantir-ne la preservació ràpida. I per als proveïdors d'aplicacions d'IA que «despullen» fotos: assumir la responsabilitat de l'eina, tal com ja exigeixen les noves lleis sobre imatge.

A Almendralejo unes nenes van patir en silenci un dany fet amb un clic. Donar a cada víctima una prova segellada del dany i una retirada que es pugui exigir —sense centralitzar mai la seva imatge ni obligar-la a reviure-la— és, en aquest front que toca la dignitat més íntima, time2act.

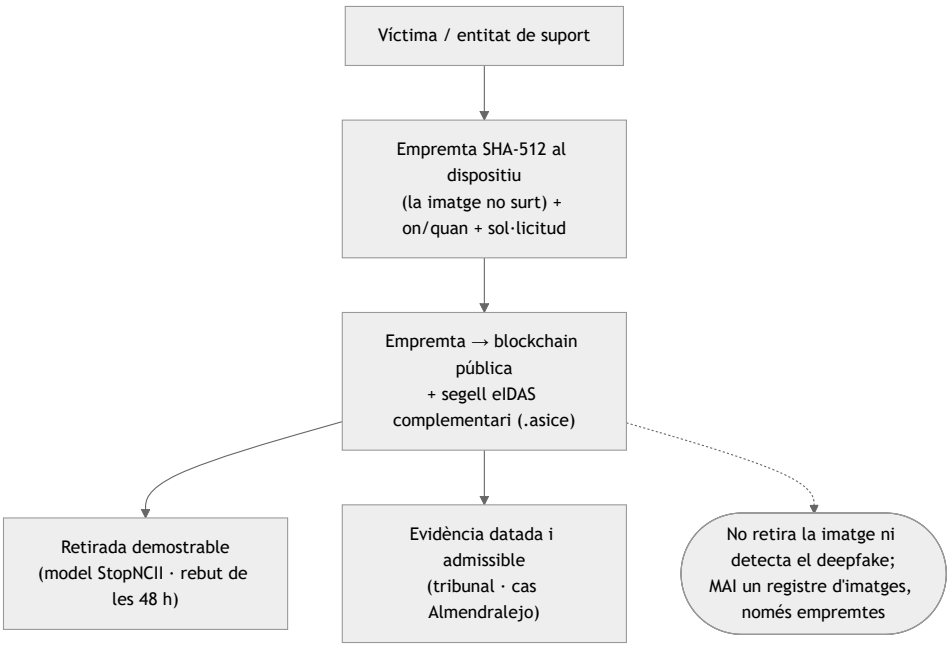


Figura 83.1 — La víctima o l'entitat de suport calcula al dispositiu l'empremta SHA-512 del contingut (la imatge no surt del telèfon) i hi afegeix on i quan s'ha trobat; l'empremta del conjunt s'ancora a la blockchain pública, amb segell eIDAS complementari (.asice). Dos resultats: a l'esquerra, la retirada demostrable a totes les plataformes (model StopNCII, amb rebut segellat de les 48 hores); a la dreta, evidència datada i admissible per al tribunal (com a Almendralejo). Límit: el segell no retira la imatge, no impedeix crear-la ni detecta el deepfake; mai un registre d'imatges, només empremtes. Fonts: cas Almendralejo; cas 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* (setembre de 2023; testimoni d'una mare; víctimes de 12-14 anys). 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* (juliol de 2024; 15 menors condemnats; 20 delictes de material d'abús infantil i 20 contra la integritat moral). https://www.scottishlegal.com/articles/spain-court-punishes-schoolboys-for-spreading-ai-deepfakes-of-girls ↩

[3] Wikipedia — *Taylor Swift deepfake pornography controversy* (gener de 2024; una publicació vista més de 47 milions de vegades; X bloqueja les cerques del seu nom). https://en.wikipedia.org/wiki/Taylor_Swift_deepfake_pornography_controversy

↩

[4] Congress.gov / The White House — *TAKE IT DOWN Act* (S.146; signada el 19 de maig de 2025; retirada en 48 h; compliment a plataformes aplicat per la FTC des del 19 de maig de 2026; primera condemna penal l'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 juny de 2024; tipifica el material íntim manipulat; ordres de retirada i preservació de proves). 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; més del 90 % del contingut deepfake és pornogràfic, gairebé tot contra dones). 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* (empremta generada al dispositiu; la imatge no surt mai; més de 500.000 imatges protegides; socis 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* (anàlisi del mecanisme d'avís i retirada). https://www.skadden.com/insights/publications/2025/06/take-it-down-act

[9] RAINN — *TAKE IT DOWN Act* (perspectiva de les víctimes de violència sexual). https://rainn.org/federal-legislation/take-it-down-act/

[10] EU Artificial Intelligence Act — *Article 50: transparency obligations* (marcatge del contingut generat o manipulat per 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 ↩

L'odi a les xarxes: el dany, la prova i la dignitat

«Si poses la vergonya en una placa de Petri, li calen tres coses per créixer exponencialment: secretisme, silenci i judici. Si la ruixes amb empatia, no pot sobreviure.»

— Brené Brown, «Listening to Shame», TED (2012)

El 2013, a Novara, Itàlia, Carolina Picchio, una adolescent de 14 anys, va veure com un vídeo seu —aparentment beguda en una festa— s'escampava per Facebook. El clip va desencadenar una onada d'insults que va omplir la seva safata d'entrada amb uns 2.600 missatges de burla, amenaces i difamació, enviats pel seu ex-xicot i el grup d'amics que el secundava. La pressió psicològica va ser tan intensa que Carolina es va llançar per la finestra de casa seva. El cas es va convertir en l'impuls legislatiu de la Llei 71/2017, la primera norma europea específica contra el ciberassetjament, promoguda per la senadora Elena Ferrara i dedicada a la víctima [1]. Aquest episodi mostra com les paraules digitals, encara que es puguin suprimir o editar en un instant, deixen una empremta real i devastadora en la vida d'un jove.

Aquest capítol se centra exclusivament en l'odi, l'assetjament i la humiliació a les xarxes socials —no en el sexe ni en la difusió de contingut íntim (capítols 83 i 81)—; el marc general de la crisi de la veritat es troba al capítol 10, mentre que els eixams de bots i la prova de personalitat cívica s'expliquen al capítol 108. La pregunta clau és: com podem oferir a les víctimes —sovint menors— una **prova** tangible del dany i una retirada demostrable sense obligar-les a custodiar el contingut que les ha ferides? La resposta es troba en **t2p**, la prova d'existència basada en blockchain que segella al dispositiu l'empremta SHA-512 del contingut d'odi, juntament amb l'URL i la marca horària de detecció, i registra la sol·licitud de retirada. Aquesta cadena de custòdia datada és inalterable i admissible en un tribunal, tot sense emmagatzemar ni reexposar el material ofensiu [15]. La tecnologia aporta la peça que falta: una prova fiable del dany que no depèn de plataformes centralitzades i que protegeix la dignitat de la víctima mentre manté la neutralitat total.

Un dany fàcil d'infligir, difícil de reparar

L'odi a les xarxes es propaga amb la mateixa facilitat que un missatge de text: uns quants clics i una connexió a Internet són suficients per crear una explosió d'insults, rumors o amenaces. En canvi, el procés de reparació és una marxa enrere interminable. Cada còpia del contingut ofensiu es replica en milers de dispositius, s'emmagatzema en servidors que sovint no ofereixen cap rastre d'origen i, fins i tot quan la víctima aconsegueix fer desaparèixer el post original, les empremtes digitals persisteixen en memòries col·lectives i algoritmes que recomanen contingut similar. La càrrega recau totalment sobre qui ha patit l'agressió: cal localitzar cada fragment, demostrar que és una extensió del dany i, sovint, tornar a mirar el material per identificar-se com a objecte de l'odi, un procés que reobre les ferides psicològiques i consumeix recursos econòmics i temporals.

Aquesta asimetria es fa especialment evident entre els joves. Un estudi del Pew Research Center mostra que el 46 % dels adolescents nord-americans (13-17 anys) ha patit almenys una de sis formes de ciberassetjament, amb un 32 % d'insults i un 10 % d'amenaces físiques [2]. L'Organització Mundial de la Salut, a través del projecte HBSC, confirma aquesta tendència a Europa: el 16 % (aproximadament un de cada sis) dels joves d'11, 13 i 15 anys ha estat víctima de ciberassetjament, i la incidència ha augmentat entre 2018 i 2022 [3]. A Espanya, l'informe conjunt de les fundacions ANAR i Mutua Madrileña indica que el 12,3 % de l'alumnat declara haver experimentat assetjament o ciberassetjament, una xifra superior al 9,4 % de l'any anterior [4]. D'aquests casos, el 91,7 % dels assetjadors són companys del mateix centre educatiu i un 14,2 % ja fan servir intel·ligència artificial per crear vídeos falsos o suplantacions d'identitat. L'impacte es tradueix en una realitat palpable: l'ADL informa que el 50 % dels adolescents han patit assetjament en línia durant els últims dotze mesos, i un 36 % afirma que aquesta experiència ha desembocat en assetjament presencial [5].

Aquests números no són meres estadístiques; són testimonis d'una crisi de confiança que s'estén més enllà del ciberespai. Quan la violència verbal es converteix en una forma de control social, el benestar mental dels joves queda compromès i les seves oportunitats educatives i professionals es veuen erosionades. La magnitud del problema és evident: no es tracta d'un fenomen marginal o puntual, sinó d'una amenaça ambiental que afecta la salut col·lectiva i el teixit social. Cada vegada que una víctima ha de perseguir un rastre digital per demostrar el seu dany, la societat renuncia a la seva pròpia responsabilitat de protegir els més vulnerables i perpetua un cicle de silenci i impunitat. La solució no pot limitar-se a sancionar

l'agressor; cal una prova fiable del dany que sigui independent de les plataformes, neutral i admissible en tribunals —exactament el que ofereix t2p.

La ferida invisible i el debat honest

El 30 de setembre del 2022, el dictamen forense d'Andrew Walker va trencar un silenci que semblava inexpugnable: la mort de Molly Russell, una adolescent britànica de 14 anys, es vinculava directament als efectes nocius del contingut en línia. Dels 16.300 missatges que la jove havia desat a Instagram durant els sis mesos previs al seu suïcidi, 2.100 mostraven temàtiques d'autolesió, depressió i incitacions a l'autodestrucció [6]. Aquest primer dictamen mundial va demostrar que no es tractava d'una simple coincidència tràgica, sinó d'un contingut que havia erosionat la salut mental de Molly fins al punt letal.

El debat acadèmic actual gira entorn de dues perspectives oposades. Jonathan Haidt sosté que la proliferació massiva de telèfons mòbils i plataformes digitals ha provocat un «gran recablejat» del cervell adolescent, alimentant una epidèmia de salut mental entre les generacions més joves [7]. En contraposició, Candice Odgers refuta aquesta correlació directa i argumenta que no hi ha evidència empírica que demostri que les xarxes «recablegin» el cervell ni que siguin la causa única dels trastorns observats; assenyala, en canvi, factors socials, econòmics i familiars com a contributors complexos [7].

L'odi en línia es manifesta com una ferida invisible que, encara que efímera o manipulada digitalment, deixa cicatrius profundes. Les directrius del DSA (2025) imposen verificació d'edat i persegueixen el contingut nociu, mentre l'avantprojecte de llei orgànica espanyol (2024) crea l'allunyament en línia com a agreujant [10][11]. Tanmateix, aquestes normes depenen de proves fiables del dany: sense una evidència immutable, els jutges disposen només d'una prova fràgil.

Aquí t2p aporta la peça que falta: una prova immutable del dany —segellada al dispositiu i ancorada a la blockchain pública dins d'un contenidor .asice [15]— que permet a les autoritats actuar amb certesa i restaurar, encara que parcialment, la dignitat de les persones joves víctimes d'odi digital.

Odi que ningú va escriure: deepfakes i eixams

Al gener del 2024, a la Pikesville High School (Maryland), un senzill clip d'àudio es va convertir en l'arma més corrosiva d'un odi sintètic. Dazhon Darien, director esportiu del centre, va utilitzar una eina d'intel·ligència artificial per crear un deepfake sonor que feia sonar el director Eric Eiswert pronunciant frases racistes i antisemites. L'àudio, difós a les xarxes socials en qüestió de minuts, va desencadenar crítiques i amenaces contra el director i el va convertir en objecte de difamació i represàlia. La policia va identificar el contingut com a fals i va detenir Darien a l'abril del 2024, però no es va poder revertir el dany immediat: els comentaris i les captures de pantalla ja havien circulat, alimentant una narrativa d'odi que ningú no havia escrit [8]. El cas mostra com la tecnologia de síntesi pot fabricar «paraules que ningú no ha dit mai» i convertir l'odi en un producte manipulable, totalment desconnectat de la persona suplantada.

L'altra cara de l'eina és l'ampliació massiva d'un discurs d'odi ja existent. Un estudi publicat a *PNAS* el 2025, centrat en la plataforma X sota la direcció de Musk, va revelar que la taxa setmanal de contingut odiós havia pujat aproximadament un 50 % després de l'adquisició, i que els «m'agrada» associats a aquest tipus de publicació s'havien incrementat un 70 % [9]. No es tracta sempre d'una comunitat real: sovint el que sembla una multitud és la maniobra d'un únic troll o d'un grup coordinat de comptes falsos, capaços de multiplicar la visibilitat del missatge odiós amb poques interaccions. Aquesta dinàmica d'autenticitat feble alimenta la crisi de confiança descrita al capítol 108, on la prova de personalitat cívica intenta desvetllar qui hi ha realment darrere d'un perfil digital.

En ambdós escenaris, el dany és tangible i real, encara que el contingut sigui efímer o manipulable. Les lleis actuals —com l'art. 510 del Codi Penal espanyol o l'Online Safety Act del Regne Unit— castiguen la incitació a l'odi i l'assetjament, però depenen d'una prova robusta que sovint manca: captures de pantalla modificables, avisos sense rastre horari i contingut que l'agressor pot esborrar. Aquí entra *t2p*, aplicant la recepta forense del capítol 13/15: es calcula al dispositiu una empremta SHA-512 del contingut odiós, juntament amb l'URL i l'hora exactes on s'ha trobat, i s'ancora l'empremta a la blockchain pública amb un segell de temps RFC 3161/eIDAS complementari, dins d'un contenidor .asice. El resultat és una cadena de custòdia immutable i admissible. Aquesta prova no elimina el post ni impedeix la creació d'odi, ni tampoc el detecta; però ofereix una evidència verificable que les autoritats poden fer servir per aplicar la llei sense dependre d'una captura manipulable.

La llei ja hi és; falta la prova inalterable

Des que la Unió Europea va publicar les directrius del DSA sobre protecció de menors (14 de juliol de 2025) [10], els estats membres han d'impulsar mesures concretes contra el ciberassetjament i el grooming. A Espanya, l'avantprojecte aprovat el 4 de juny de 2024 [11] introdueix l'anomenat «allunyament en línia» i reforça el marc penal existent: l'article 510 del Codi Penal castiga l'odi amb presó d'1 a 4 anys i multes, i l'article 172 ter tipifica l'assetjament reiterat amb penes d'entre tres mesos i dos anys [12]. Al Regne Unit, l'Online Safety Act del 2023, en vigor des del 25 de juliol de 2025, obliga les plataformes a protegir els menors contra el bullying i el contingut d'odi, establint multes que poden arribar al 10 % de la facturació mundial [13]. Austràlia ha anat un pas més enllà amb l'Online Safety Amendment (Social Media Minimum Age) Act del 2024, que prohibeix l'accés a les xarxes socials a qualsevol menor de 16 anys a partir del 10 de desembre de 2025, amb sancions d'aproximadament 50 milions de dòlars australians per a les empreses infractores [14].

Totes aquestes regulacions convergeixen en un requisit fonamental: la necessitat de **provar** què ha succeït, quan ha passat i quina sol·licitud de retirada s'ha formulat. A la pràctica, aquest requeriment es topa amb el mateix mur que ha dificultat la defensa de les víctimes durant anys. Una captura de pantalla, per molt detallada que sigui, no garanteix la data exacta; les metadades poden ser manipulades o eliminades. Un avís enviat a la plataforma sovint desapareix sense deixar cap rastre horari verificable, i el contingut ofensiu es pot esborrar abans que les autoritats en puguin recollir proves sòlides.

Aquesta fragilitat de la prova no és només una qüestió tècnica, sinó un obstacle legal que impedeix l'aplicació efectiva de les lleis: **la manca d'evidència fiable allibera els agressors**, perpetua el silenci de les víctimes i manté viu el cicle d'odi i assetjament en línia.

Com hem vist, **t2p** calcula l'empremta SHA-512 del contingut d'odi directament al dispositiu de la víctima, sense que el material surti mai del telèfon. A aquesta empremta s'associa la informació d'**on** (URL o identificador) i **quan** (marca horària exacta), juntament amb la sol·licitud formal de retirada; el segell de temps, basat en el protocol RFC 3161/eIDAS i ancorat a la blockchain pública, crea una cadena de custòdia datada i verificable dins d'un contenidor .asice [15]. Aquest procés produeix una prova **neutral**, independent de qualsevol creador o intermediari, que es pot presentar davant els tribunals com a evidència admissible.

La prova d'existència aplicada

A les aules de Barcelona, una professora de secundària rep un correu electrònic amb un enllaç a la captura d'un xat on un grup d'alumnes ha enviat missatges d'odi i falses acusacions contra una companya de 14 anys. El contingut ja no està disponible: el telèfon del remitent només mostra la notificació «missatge eliminat». Sense proves tangibles, l'escola queda atrapada entre la necessitat d'actuar i la impossibilitat de demostrar que l'assetjament reiterat (art. 172 ter) s'ha produït realment. És aquí on **t2p** entra en joc: calcula al dispositiu una empremta SHA-512 del missatge, hi afegeix l'enllaç i la marca horària de detecció, i n'ancora l'empremta a la blockchain pública amb un segell de temps complementari —com hem vist—, dins d'un contenidor .asice. El resultat és una cadena de custòdia inalterable que es pot presentar com a prova admissible tant en l'expedient escolar com davant del jutge.

1. L'expedient escolar

Segons l'informe de la Fundació ANAR i Mutua Madrileña, aquest percentatge elevat de ciberassetjadors que són companys del mateix centre ja s'ha assenyalat [4]. Aquestes dinàmiques sovint es tradueixen en un «no es fa res», deixant les víctimes sense recurs. Amb **t2p**, l'alumna pot aportar una prova digital que trenca aquest silenci: l'empremta demostra que el missatge existia, quan i on es va publicar, i que se'n va sol·licitar la retirada. L'escola, obligada per les directrius del DSA a protegir els menors [10], pot actuar immediatament, obrir una investigació formal i imposar mesures disciplinàries contra l'agressor, sense necessitat de conservar el contingut complet.

2. La denúncia penal

L'article 510 del Codi Penal espanyol castiga la incitació pública a l'odi amb presó de fins a quatre anys i multes [12]. Per demostrar que una sèrie de publicacions constitueixen un assetjament «insistent i reiterat» (art. 172 ter), cal provar la continuïtat temporal i la intenció danyosa. La cadena de custòdia generada per **t2p** ofereix exactament això: cada empremta inclou l'hora i el lloc, i crea un registre

cronològic que es pot presentar com a prova directa del caràcter repetitiu de l'odi. Així, la víctima no ha d'emmagatzemar ni reexposar els missatges ofensius; només presenta l'empremta, que és immutable i admissible.

3. Notice-and-action per a les plataformes

El DSA europeu i l'Online Safety Act del Regne Unit imposen a les xarxes socials l'obligació de retirar el contingut il·legal en un termini raonable [10][13]. Un rebut segellat generat en el moment de la denúncia funciona com a prova que la plataforma ha estat notificada i quan. Això impedeix el «memory-holing»: encara que l'agressor esborri el post, l'empremta i la data demostren inequívocament que el contingut va existir i que es va complir la resposta requerida.

Casos complementaris

En casos com el de Pikesville, on un àudio sintètic va difamar el director d'un centre [8], la procedència —la marca C2PA i el requisit d'etiquetatge de l'AI Act [16]— és el complement que ajuda a establir que un contingut és sintètic, i t2p hi afegeix la prova neutral i datada del dany. A més, la prova de personalitat al dispositiu, com hem vist al capítol 108, permet verificar «una persona, una veu» sense recórrer a la desanonimització biomètrica, i preserva la llibertat d'expressió i la privacitat.

En resum, **t2p** no elimina l'odi ni impedeix que es generin nous missatges nocius; tampoc crea un registre centralitzat del contingut abusiu. La seva força rau a proporcionar una empremta immutable al dispositiu de la víctima, que demostra l'existència i la data del dany sense exposar el contingut mateix [17]. Aquesta és la peça clau que transforma les obligacions legals en accions viables, i defensa la dignitat digital dels joves davant l'odi en línia.

La promesa i el perill

En un món on cada comentari, meme o vídeo es pot capturar, replicar i difondre en segons, la víctima d'odi digital sovint es troba sense una prova sòlida del dany que ha patit. La promesa de **t2p** és tornar poder a aquesta persona: generar, al propi dispositiu, una empremta SHA-512 del contingut ofensiu, afegir-hi l'URL i l'hora exacta, i registrar alhora la sol·licitud de retirada. Aquest segell de temps, conforme a les especificacions que ja hem citat i ancorat a la blockchain pública dins d'un contenidor .asice, crea una cadena de custòdia immutable i datada que es pot presentar davant els tribunals com a prova admissible, sense necessitat d'emmagatzemar ni reexposar el contingut. Així, la víctima disposa d'una evidència verificable del dany i de l'avís legal, capaç de fer complir les obligacions establertes contra el ciberassetjament i els articles 510 i 172 ter del Codi Penal espanyol [12].

Tanmateix, aquesta tecnologia comporta una sèrie de perills que cal reconèixer amb la mateixa claredat amb què es presenta la promesa. Primer, **no crea cap registre centralitzat** del contingut abusiu: totes les empremtes es generen i es conserven únicament al dispositiu de la víctima, tal com fa el model de StopNCII.org [17]. Això evita que una base de dades global d'abusos es converteixi en un instrument de vigilància massiva.

En segon lloc, **mai no pot servir per desanonimitzar ni vigilar** els usuaris. El segell demostra l'existència d'un dany patit per una persona, però no revela qui és exactament; convertir-lo en una eina per identificar qualsevol veu aniria contra la llibertat d'expressió i amenaçaria la sàtira, el whistleblowing i altres formes legítimes de dissentiment (vegeu el capítol 62). Desanonimitzar el discurs podria glaçar el debat públic i protegir només els poderosos; per això el valor de la prova és, precisament, la seva neutralitat.

Un tercer perill és la **necessitat d'una caducitat o revocabilitat** de l'empremta. La immutabilitat que garanteix la validesa judicial també pot convertir-se en un registre perpetu de la victimització, vulnerant el dret a l'oblit i perpetuant el dany psicològic. Per això qualsevol implementació ha de permetre esborrar o invalidar les empremtes quan la víctima ho demani.

Finalment, cal recordar que **el segell és infraestructura de prova, no cura**. L'arrel del problema rau en els models de negoci basats en l'atenció que premien la indignació, com mostra, com hem vist, el discurs d'odi a X després del canvi de propietat [9]. Sense canvis estructurals en aquestes plataformes —i sense un debat honest sobre la verificació d'edat, que protegeix els menors però també pot vigilar-los [10] [14]— cap eina tècnica no serà més que un pedaç. La promesa de **t2p** és poderosa; el perill és confiar que la

tecnologia pugui substituir les reformes legals i socials necessàries per garantir dignitat i seguretat als joves en línia. El segell és una eina de dignitat i de justícia, no un escut tecnològic que esborri el dany.

És hora d'actuar

La violència digital no és una ombra efímera: deixa cicatrius reals en joves que viuen l'adolescència entre pantalles i notificacions. El 46 % dels adolescents nord-americans ha patit alguna forma de ciberassetjament [2] i la meitat ho ha sofert durant l'últim any [5]; a Europa, un de cada sis joves (16 %) ja n'ha experimentat una, amb una tendència a l'alça des del 2018 [3]. Les lleis com la Llei 71/2017, nascuda del cas de Carolina Picchio, han establert penes clares contra el ciberassetjament i l'odi en línia, però el problema persisteix perquè la prova del dany continua sent feble: captures manipulables, avisos sense marca temporal i contingut que l'agressor esborra abans de ser documentat.

Per a les víctimes i famílies: el primer pas és segellar al dispositiu una empremta SHA-512 del contingut ofensiu, juntament amb l'URL i l'hora exacta de detecció. Aquesta empremta es combina amb una sol·licitud formal de retirada i es registra en un contenidor .asice, amb l'empremta ancorada a la blockchain pública i un segell de temps RFC 3161/eIDAS complementari [15]. Així, la víctima conserva una prova inalterable del dany sense haver de guardar el contingut ofensiu i evita reviure'l cada vegada.

Per als centres educatius: les escoles han de tractar l'empremta segellada com un document de l'expedient. Cada cas registrat pot ser revisat per equips multidisciplinaris (psicòlegs, treballadors socials i juristes) que, sobre una cadena de custòdia verificable, poden aplicar mesures ràpides i legalment sòlides: suport psicològic, sancions o mediació.

Per a les plataformes: el DSA europeu i l'Online Safety Act del Regne Unit imposen obligacions clares; cada avís ha de generar un rebut segellat, amb data i hora, que es lliuri al denunciant i s'arxivi com a empremta només al dispositiu. Aquest mecanisme compleix les directrius del DSA sobre la protecció dels menors [10] i evita crear bases de dades centralitzades que vulnerin la privacitat.

Per a la policia i els tribunals: l'empremta datada s'ha d'acceptar com a prova admissible per als articles 510 i 172 ter del Codi Penal espanyol, ja que constitueix una cadena de custòdia inalterable que demostra la presència i el contingut del discurs d'odi en el moment exacte. Els jutges poden fer servir aquesta evidència per emetre ordres de retirada i imposar sancions sense dependre de proves que es puguin esborrar o alterar.

Per als legisladors: cal reconèixer legalment la prova segellada com a forma legítima d'evidència, amb una disposició que en garanteixi la preservació i, alhora, el dret a l'oblit, de manera que el dany no es perpetuï però la responsabilitat sigui rastrejable.

Com recorda el cas de Carolina Picchio [1], la Llei 71/2017 va néixer per donar veu a xicots com ella; ara podem oferir a cada jove una prova segellada del dany i una retirada exigible —sense centralitzar mai el contingut ni obligar-la a reviure'l—. En aquest front que toca la dignitat, **time2act**.

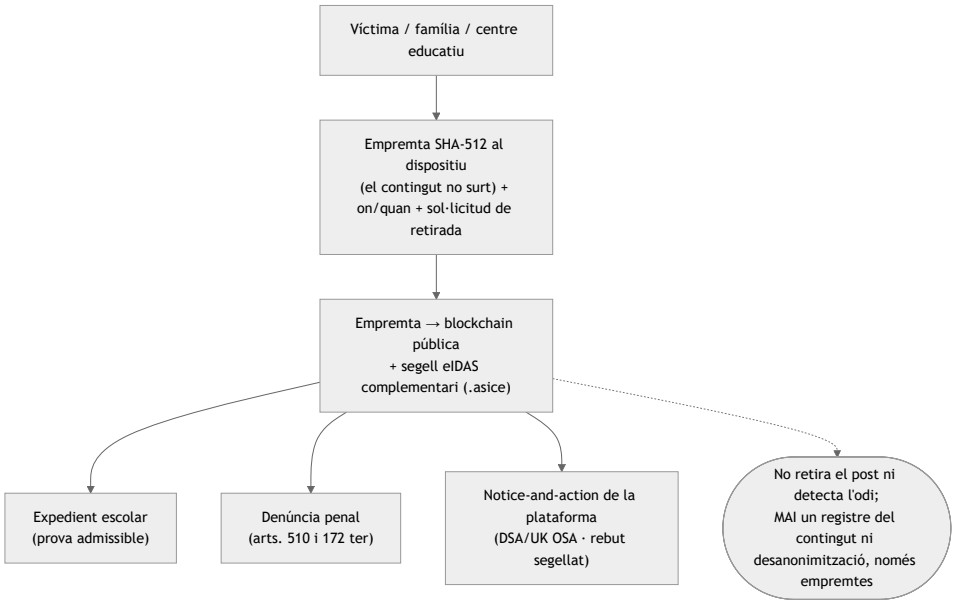


Figura 84.1 — La víctima, la família o el centre educatiu calcula al dispositiu l'empremta SHA-512 del contingut d'odi (el contingut no surt del telèfon) i hi afegeix on i quan s'ha trobat i la sol·licitud de retirada; l'empremta del conjunt s'ancora a la blockchain pública, amb segell eIDAS complementari (.asice). Tres sortides: l'expedient escolar, la denúncia penal (arts. 510 i 172 ter) i el notice-and-action de la plataforma (DSA/UK OSA), amb rebut segellat. Límit: el segell no retira el post, no impedeix crear odi ni el detecta; mai un registre del contingut ni una eina de desanonimització, només empremtes al dispositiu. Fonts: cas Picchio; Molly Russell; ANAR; StopNCII.

---

[1] The Local (Itàlia) — *Italy unanimously passes anti-cyberbullying law* (maig 2017; Llei 71/2017; Carolina Picchio, 14 anys, 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 desembre de 2022; 46 %; insults 32 %, rumors 22 %, amenaces 10 %). https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/ ↩

[3] OMS-Europa i estudi HBSC — *One in six school-aged children experiences cyberbullying* (27 de març de 2024; 16 %; 44 països; ≈280.000 joves). https://www.who.int/europe/news/item/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study ↩

[4] Fundació ANAR i Fundació Mutua Madrileña — *VIII Informe de Prevenció de l'Assetjament Escolar* (2025; 12,3 % vs 9,4 %; 14,2 % amb IA; 91,7 % del mateix centre; 17.562 alumnes). 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* (juny de 2024; adolescents 50 %; 36 % salt al món físic). https://www.adl.org/resources/report/online-hate-and-harassment-american-experience-2024 ↩

[6] CBS News / ITV News — *Molly Russell inquest* (30 de setembre 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, març de 2024; rèplica 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; gener-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 % odi; +70 % «m'agrada»; activitat coordinada sense reduir). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11819532/ ↩

[10] Comissió Europea — *Guidelines on the protection of minors under the Digital Services Act* (14 de juliol de 2025; ciberassetjament, verificació d'edat; riscos sistèmics = discurs d'odi il·legal). https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors ↩

[11] La Moncloa — *Avantprojecte de Llei Orgànica per a la protecció de les persones menors d'edat als entorns digitals* (Consell de Ministres, 4 de juny de 2024; «allunyament en línia»; verificació d'edat). https://www.lamoncloa.gob.es/consejodeministros/resumenes/Paginas/2024/040624-rueda-de-prensa-ministros.aspx ↩

[12] Codi Penal (Espanya) — arts. 510 (delicte d'odi; presó 1-4 anys) i 172 ter (assetjament/stalking; agreujat per l'edat 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* (deures en vigor el 25 de juliol de 2025; bullying i contingut d'odi; multes fins al 10 % de la facturació mundial). https://www.gov.uk/government/collections/online-safety-act ↩

[14] eSafety Commissioner (Austràlia) — *Social media age restrictions* (Act 2024; menors de 16 des del 10 de desembre de 2025; primer país). https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions ↩

[15] t2p — manual de producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice). Vegeu els capítols 13 i 15. ↩

[16] EU Artificial Intelligence Act — *Article 50: transparency obligations* (marcatge del contingut generat o manipulat per IA). https://artificialintelligenceact.eu/article/50/ ↩

[17] StopNCII.org — *How StopNCII.org works* (empremta generada al dispositiu; el contingut no surt mai; model de només-empremtes). https://stopncii.org/how-it-works/ ↩

Gent gran: la veu clonada i l'abús invisible

«Els vells, són homes? Veient com els tracta la nostra societat, és lícit dubtar-ne.»

— Simone de Beauvoir, La vellesa (1970)

Un vespre qualsevol, en un pis qualsevol, el mòbil d'una mare gran s'il·lumina: «Hola mamà, se m'ha trencat el mòbil, aquest és el meu nou número. Escriu-me per WhatsApp quan puguis.» El text, senzill i urgent, és l'esquer d'una de les estafes més esteses a Espanya. L'estafador ha tret el nom i la relació familiar de xarxes socials o de bases de dades filtrades i ha fabricat una urgència creïble — la variant recent diu «se m'ha mullat el mòbil» —; l'INCIBE recomana verificar sempre per una altra via, i la Policia Nacional n'ha alertat repetidament [1]. I això és només la versió escrita. Amb la intel·ligència artificial actual, la trucada següent pot portar la veu clonada del fill de debò, fabricada a partir d'uns segons d'àudio trets d'un vídeo públic (vegeu el capítol 68) [3].

Les xifres del termòmetre nord-americà donen l'escala del que s'acosta. Segons l'FBI, el 2024 els majors de 60 anys van perdre prop de 4.900 milions de dòlars en ciberdelictes, un 43 % més que l'any anterior; el 2025, les denúncies van pujar a 201.266 i les pèrdues a 7.750 milions (+59 %), amb més de 3.100 denúncies de sèniors que mencionaven la IA — més de 352 milions perduts — i més de 5 milions de dòlars en estafes d'angoixa amb veu clonada [2].

Aquest llibre ha dedicat un capítol al dany digital sobre els joves (capítol 84); aquest n'és el mirall per a la gent gran. La tecnologia de la veu clonada s'explica al capítol 68; el testament i l'herència, al capítol 52; la fe de vida, al capítol 64; el frau financer corporatiu, al capítol 16. La pregunta clau: com protegim els nostres grans — de l'estafa, de l'abús i de la pressió — sense convertir-los en menors d'edat vigilats? La resposta és donar-los, a ells i a les seves famílies, evidència verificable amb **t2p** — l'empremta SHA-512 al dispositiu, l'ancoratge de l'empremta a la blockchain pública i el segell de temps RFC 3161/eIDAS complementari [11] —, sota un principi irrenunciable que la llei espanyola ja ha fet seu: suport, no substitució (Llei 8/2021 [10]).

L'estafa que truca a casa

La suplantació familiar ha fet el salt del text a la veu. L'FBI va alertar el desembre de 2024 que la IA generativa s'usa per clonar veus de familiars en les anomenades estafes «de l'avi» o d'angoixa: la trucada que plora i demana diners urgents ja no necessita cap actor — n'hi ha prou amb uns segons d'àudio del net o del fill trets d'un vídeo penjat a qualsevol xarxa [3]. El 2025, les pèrdues declarades per aquestes estafes d'angoixa amb veu clonada van superar els 5 milions de dòlars, dins d'un total de més de 352 milions perduts pels sèniors en fraus amb menció d'IA [2]. Cada trucada és una invasió de la intimitat més profunda: el so d'una veu estimada, girat contra qui més se l'estima.

L'estafa romàntica completa el quadre. La FTC nord-americana va rebre prop de 60.000 denúncies el 2024, amb pèrdues de 1.200 milions de dòlars; i és la franja de 65 a 74 anys la que pateix les pèrdues més altes — més estalvis acumulats, menys familiaritat amb les tàctiques digitals [4]. A Espanya la modalitat és plenament activa, amb detencions anunciades pel Ministeri de l'Interior [6], i ha arribat a l'extrem més fosc: el crim de Morata de Tajuña, l'any 2023 — tres germans grans assassinats després d'haver estat víctimes d'una estafa de l'amor de fins a 263.000 euros [5].

El patró comú de totes aquestes modalitats és doble. Primer, l'estafador explota la millor virtut de la víctima: la confiança en la família i en l'afecte. Segon, compta amb la millor aliada possible: la vergonya de denunciar. Quan la víctima calla, no hi ha prova, no hi ha estadística i no hi ha escarment. I encara hi ha un tercer front, el més incòmode de tots: quan el perill no ve de fora, sinó de dins — de qui cuida, o de qui espera l'herència —, la prova es fa gairebé impossible. Els dos apartats següents hi entren de dret.

L'abús que no es veu

El gener de 2022, el periodista Victor Castanet va publicar a França *Les Fossoyeurs* («Els enterradors»), una investigació sobre Orpea, un dels grans grups europeus de residències, amb uns 260.000 residents: racionament de menjar i de productes d'higiene per retallar costos en un grup subvencionat amb diner públic, i desatenció mèdica. La fiscalia francesa va obrir investigacions penals per indicis de maltractament, malversació de fons públics i infraccions laborals, amb desenes de denúncies de famílies —

algunes per homicidi involuntari —; el Govern francès va anunciar una àmplia operació de control de les residències del grup, i l'Estat hi va acabar injectant 605 milions d'euros a canvi d'una participació majoritària [7]. La lliçó és estructural: l'abús en la cura passa darrere de portes tancades, s'esborra en la rutina, i la paraula d'una persona amb demència no pesa com a prova. Sense evidència, ni les famílies ni els inspectors no poden distingir la residència exemplar de la que raciona bolquers.

Espanya ofereix el contrapunt en petit format, i amb sortida. En una residència d'El Escorial, les filles d'una interna amb demència — informades que la seva mare podia estar sent maltractada — hi van instal·lar una càmera oculta. La treballadora va ser condemnada, amb una multa de 480 euros i una indemnització de 3.000 confirmades per l'Audiència Provincial de Madrid, i la càmera va ser avalada com a prova vàlida [8]. Ho fa possible la doctrina del Tribunal Suprem: amb sospita prèvia i fundada d'un delicte greu, una càmera temporal i enfocada al lloc concret supera el triple judici de proporcionalitat — idoneïtat, necessitat i proporcionalitat estricta — i val en el procés penal, encara que administrativament pugui suposar una infracció de protecció de dades [9]. El matís és essencial: no és barra lliure per espiar cuidadors; és una excepció rigorosa per a la sospita fundada.

I tanmateix, queda un buit: la gravació casolana, sense data certa ni integritat acreditada, continua sent el flanc feble de qualsevol procediment — «quan es va gravar això? qui ens diu que no s'ha editat?». És exactament el buit que la prova d'existència tanca, com veurem tot seguit.

L'última voluntat sota pressió

El capítol 52 va tractar el testament falsificat: la signatura falsa, el document alterat. Aquí el problema és més subtil i més freqüent: el testament autèntic d'una voluntat pressionada. El familiar que aïlla, el «cuidador» que suggereix, la visita al notari arrencada en un mal dia. Cap falsificació enlloc — i tanmateix, cap voluntat lliure.

El marc legal espanyol va fer un tomb de paradigma amb la Llei 8/2021, de 2 de juny: de la substitució al suport [10]. La persona gran o amb discapacitat pot testar si en aquell moment té aptitud per comprendre i expressar la seva voluntat; pot ordenar davant notari mesures voluntàries — poders preventius, autocuratela, voluntats anticipades —; qui li presta suport ha de retre comptes; i la curatela esdevé excepcional. És una arquitectura de dignitat: decideix la persona, no la família.

Però la disputa arriba anys després, sovint quan la persona ja no hi és. Hi havia aptitud? Hi havia pressió? El notari dona fe de l'acte — d'aquell moment, davant seu —, però els mesos d'aïllament o d'influència prèvia no els veu ningú. La prova d'existència aporta el que faltava: profunditat temporal. Les converses pròpies segellades — la persona gran que documenta, al seu propi dispositiu, les pressions que rep —; la decisió expressada i datada quan encara és serena; la rendició de comptes de qui presta suport, ancorada perquè ningú no la pugui reescriure [11]. La voluntat deixa de ser una foto d'un instant per esdevenir una línia coherent en el temps — molt més difícil de capturar, i molt més difícil de discutir.

La prova d'existència aplicada

La mateixa tecnologia que clona la veu d'un fill pot certificar la veu del fill de debò.

1. El fill de debò

Contra la trucada clonada, la verificació familiar. La família acorda una paraula de seguretat i un protocol: davant de qualsevol urgència amb diners, es penja i es retruca al número de sempre [1]. I el fill de debò pot enviar una prova de vida segellada: un àudio o vídeo curt responent el repte acordat, amb l'empremta SHA-512 calculada al dispositiu i el segell de temps del minut exacte [11]. La veu clonada pot imitar el timbre, però no pot respondre el repte ni fabricar un segell criptogràfic del present — és el mateix principi de repte i frescor de la fe de vida del capítol 64, portat a l'escala de la família (l'autenticació de la xarxa telefònica es tracta al capítol 68). La regla de la casa esdevé simple: qui truca demanant diners i no pot segellar la resposta, menteix — per defecte.

2. La família que vigila amb respecte

Dins dels límits estrictes de la doctrina del Suprem — sospita fundada, càmera temporal i enfocada [9] —, la gravació que una família es veu obligada a fer val molt més si neix segellada: cada segment amb empremta i hora ancorades [11], una cadena de custòdia impecable des del primer minut, immune al «això

està editat». En un cas com el d'El Escorial [8], aquest blindatge hauria estalviat qualsevol discussió sobre l'autenticitat de les imatges. I la simetria que ho fa just: les residències també hi guanyen. Registres de cura ancorats — medicació, higiene, torns, visites — protegeixen el professional diligent de l'acusació injusta i fan detectable el racionament sistèmic que va destapar el cas Orpea [7] abans que esdevingui escàndol. La prova no té bàndol: empara la interna, la família i el bon cuidador.

3. La voluntat acreditada

Una persona gran que vol blindar la seva última voluntat — no contra la família, sinó contra el dubte — pot acompanyar les mesures de la Llei 8/2021 [10] amb evidència ancorada: el vídeo del moment de la decisió, amb data certa; les converses on expressa aquesta voluntat al llarg de mesos, empremtades al seu propi dispositiu; la rendició de comptes de qui li presta suport, ancorada [11]. Si mai algú al·lega captació — o si la captació existeix de debò —, hi haurà cronologia verificable en lloc de records interessats. No substitueix el notari: el complementa amb el que cap acta no pot contenir — la consistència d'una voluntat en el temps.

4. El cor verificat

Contra l'estafa romàntica, la prova d'existència talla en les dues direccions. Qui es relaciona en línia pot demanar al pretendent proves de vida segellades — qui no pot acreditar ni un minut verificable de la seva existència real, sospita per defecte [11]. I la víctima que comença a dubtar pot segellar les converses i els justificants de pagament al seu dispositiu — sense vergonya, sense haver-ho d'explicar encara a ningú —, de manera que, si un dia denuncia [6], porti una cronologia completa i no un grapat de captures. Les xifres [4] i el record de Morata de Tajuña [5] diuen prou clar què hi ha en joc.

Cal dir també què no fa el segell: no detecta la mentida ni l'amor fingit; no substitueix la trucada de cada diumenge, ni la companyia, ni el finançament digne de les cures — el cas Orpea és un model de negoci, no una fallada criptogràfica [7]. La prova d'existència dona a la gent gran i a les seves famílies allò que la vergonya i la porta tancada els prenien: la possibilitat de provar-ho.

La promesa i el perill

La promesa és un país on la trucada del fals fill topa amb una pregunta que no pot respondre [11], on l'abús en la cura deixa de ser paraula contra silenci [8], i on l'última voluntat arriba als tribunals acreditada en el temps i no reconstruïda de memòria [10]. Però aquest capítol toca persones en situació vulnerable, i els perills demanen la màxima franquesa.

El primer és **la vigilància paternalista**. Protegir no pot voler dir vigilar. Si la família converteix el mòbil de l'àvia en un dispositiu monitorat, haurem substituït l'estafador per la tutela — exactament el que la Llei 8/2021 va voler desterrar [10]. La regla de disseny: les eines les controla la persona gran — el seu dispositiu, les seves empremtes, la seva decisió de revelar. El suport es presta amb ella, mai sobre ella.

El segon és **la càmera com a norma**. La doctrina del Suprem empara una excepció — sospita fundada, temporal, enfocada [9] —, no la videovigilància permanent dels cuidadors, que vulneraria els seus drets i convertiria la desconfiança en estàndard de la cura. El segell fa sòlida la prova lícita; no fa lícita la captació que no ho era.

El tercer és **el registre que no ha d'existir**. La verificació familiar funciona amb reptes i empremtes al dispositiu de cadascú; un repositori central de veus «autèntiques» seria alhora un botí per als clonadors i una infraestructura de vigilància massiva. Només empremtes, revocables, sense biometria centralitzada i sense desanonimització [11].

El quart perill no és cap estafa: és posar tecnologia on falta companyia. Cap segell no cura la soledat — que és la porta d'entrada de l'estafa romàntica [4] i de la captació de la voluntat. La prevenció real és companyia, atenció i cures ben finançades; la criptografia només garanteix que, quan calgui provar, es pugui. Si la tecnologia serveix d'excusa per trucar menys a casa, haurem perdut molt més del que cap estafador podia endur-se.

És hora d'actuar

La generació que ens va ensenyar a donar la paraula mereix eines per poder demostrar-la.

Per a les famílies: acordeu una paraula de seguretat i el protocol de retrucada [1]; davant de qualsevol urgència amb diners, verificació segellada abans que transferència [11]; i parleu-ne obertament a casa — la vergonya és l'arma de l'estafador.

Per a la gent gran: el teu mòbil pot ser la teva memòria certificada. Segella les converses que et pressionen, els acords que et prometen i la teva voluntat quan la tinguis clara [10][11]; revelar-ho — o no — serà sempre decisió teva.

Per a residències i cuidadors: ancoreu els registres de cura — medicació, higiene, torns, visites —: protegeixen el professional honest i fan visible el racionament abans que esdevingui escàndol [7].

Per a notaris i juristes: combineu la fe pública amb la profunditat temporal — les mesures de la Llei 8/2021 acompanyades de cronologies segellades de la voluntat [10][11].

Per a bancs i plataformes: davant de transferències inusuals de clients grans, oferiu — mai imposeu — la pausa de verificació: un repte de prova de vida al presumpte familiar abans d'executar el pagament [3] [11].

Per als legisladors: reconeixeu la prova segellada en captura en els procediments d'abús i de captació de la voluntat; i finançeu la inspecció de residències — cap cadena de blocs no substitueix un inspector [7].

El pròxim «hola mamà» pot portar la veu exacta del teu fill. Que la resposta de casa teva sigui una pregunta que només el teu fill pot respondre — i un segell que cap màquina no pot falsificar. Pels qui ens van donar la paraula, **time2act**.

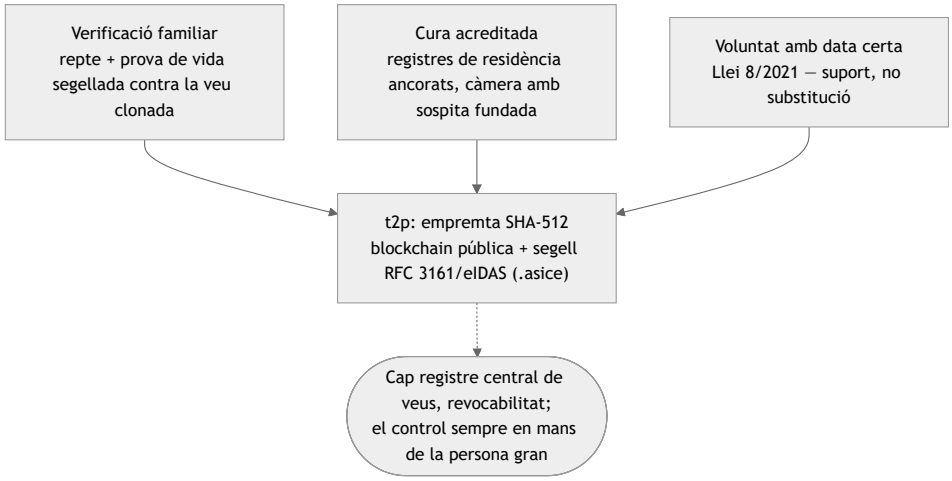


Figura 85.1 — Tres escuts per a la gent gran amb una sola lògica (empremta SHA-512 al dispositiu, segell de temps RFC 3161/eIDAS, ancoratge a la blockchain pública, .asice): la verificació familiar contra la veu clonada (repte + prova de vida segellada), la cura acreditada (registres de residència ancorats; càmera només dins de la doctrina de proporcionalitat del TS) i la voluntat amb data certa (Llei 8/2021: suport, no substitució). Límits: cap registre central de veus, revocabilitat, i el control sempre en mans de la persona gran. Fonts: INCIBE; FBI/IC3; elDiario.es (El Escorial); Llei 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 maig de 2025; mecànica del «hola mamà», variants, recomanacions de verificació); Policia Nacional (alerta) — OKDiario; València News — *Així funciona l'estafa del «fill en apuros» per SMS i 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 $7.75B to cybercrime in 2025 — a 59% jump* (201.266 denúncies de majors de 60; 4.900 M$ el 2024, +43 %; >3.100 denúncies sènior amb IA i >352 M$; >5 M$ en estafes d'angoixa amb veu clonada); PPC Land — *AI-linked fraud costs Americans $893 million* (22.364 denúncies d'IA el 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 desembre de 2024; clonació de veu en estafes d'angoixa i suplantació de familiars). https://www.ic3.gov/PSA/2024/PSA241203 ↩

[4] Factchequeado — *Qué son las estafas de romance y cómo identificarlas* (FTC: ≈60.000 denúncies i 1.200 M$ el 2024; la franja 65-74 amb les pèrdues més altes); 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* (crim de Morata de Tajuña, 2023: tres germans grans assassinats; estafa de fins a 263.000 €). https://es.wikipedia.org/wiki/Estafa_rom%C3%A1ntica ↩

[6] Ministeri de l'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 febrer de 2022; «Les Fossoyeurs» de Victor Castanet; Orpea ≈260.000 residents; racionament; investigacions penals per maltractament, malversació i infraccions laborals; denúncies per homicidi involuntari); infoLibre — *El último escándalo de Orpea* (injecció estatal de 605 M€ per una participació majoritària). 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 € i indemnització de 3.000 € confirmades per l'Audiència Provincial de Madrid; càmera de les filles avalada com a prova). 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?* (sospita fundada de delicte greu; càmera temporal i enfocada; triple judici de proporcionalitat). 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 — *Llei 8/2021, de 2 de juny, per la qual es reforma la legislació civil i processal per al suport a les persones amb discapacitat en l'exercici de la seva capacitat jurídica* (suport, no substitució; mesures voluntàries davant notari; aptitud per testar; rendició de comptes; 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 producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; prova de vida amb repte; contingut mai fora del dispositiu; revelació voluntària). Vegeu els capítols 13, 15 i 64. ↩

Comunicacions oficials: qui certifica que el cap d'Estat ha dit això?

«Les paraules van haver de canviar el seu significat ordinari i prendre el que ara se'ls donava.»

— Tucídides, Història de la guerra del Peloponnès, III, 82 (trad. Crawley)

A mitjan juny del 2025, algú va crear un compte de Signal amb el nom visible «marco.rubio@state.gov». Amb una veu clonada per IA i imitant l'estil d'escriptura del secretari d'Estat dels EUA, **Marco Rubio**, l'impostor va contactar almenys **tres ministres d'exteriors estrangers, un senador dels EUA i un governador**: va deixar missatges de veu a Signal a dos dels contactats i, en un cas, va enviar un missatge de text convidant l'interlocutor a passar a la mateixa aplicació. Un cable del Departament d'Estat del **3 de juliol de 2025** va alertar-ne els empleats: l'objectiu probable era accedir a informació o a comptes, i l'autor no s'ha identificat [3]. No calia piratejar cap sistema; n'hi va haver prou amb una veu i un nom en una aplicació de missatgeria per fer passar per bona la paraula de la diplomàcia nord-americana.

El precedent canònic es remunta al **16 de març de 2022**, quan uns atacants van piratejar el canal ucraïnès **Ukraine 24** i hi van difondre un deepfake del president **Volodímir Zelenski** que semblava ordenar als soldats deposar les armes, mentre el teletip piratejat afirmava que havia fugit de Kíiv; Zelenski el va desmentir en hores amb un selfie real des del centre de Kíiv («provocació infantil») [1] —és el cas que hem analitzat al capítol 20. La pregunta que tots dos episodis deixen oberta vertebra aquest capítol: quan un missatge oficial es pot falsificar i empènyer per un canal de confiança —o per un de personal, com Signal—, com pot el públic confirmar de manera ràpida i independent què ha dit de debò el seu govern?

Aquest capítol és diferent del capítol 48 —la integritat electoral, on el blanc és la campanya, el candidat i el vot— i del capítol 20 —la defensa i els drets humans, on parlem de comandament al camp de batalla i prova de crims de guerra. Aquí el subjecte és l'**autenticitat de les comunicacions oficials de crisi i de les declaracions que mouen mercats**: el que diu un Estat o una institució en el moment que més importa. La pregunta no és si una falsedat es pot crear —es pot—, sinó com una autoritat pot publicar la seva paraula de manera que qualsevol periodista o ciutadà la pugui **verificar en segons** com a genuïna, i com una falsificació es pot **desmentir contra l'original** abans que el pànic faci la seva feina. És la tesi d'aquest llibre aplicada al moment més fràgil de tots: l'emergència.

Quan el canal de confiança es torna l'arma

El cas d'Ukraine 24 no és anecdòtic: com hem vist, és el patró. El **22 de maig del 2023**, una imatge generada per IA d'una explosió prop del **Pentàgon**, difosa per un compte fals que es feia passar per «Bloomberg» i amplificada per la russa RT, va fer caure breument l'**S&P 500 al voltant d'un 0,3 %** (uns 30 punts) i el Dow uns 80 punts entre les 10:06 i les 10:10 del matí, recuperant-se a les 10:13; Bloomberg ho va descriure com «possiblement el primer cop que una imatge generada per IA mou el mercat» [2]. La falsedat va viure quatre minuts i va moure milers de milions: no calia que fos bona, només que arribés per un canal que semblava de confiança.

L'**abril del 2025**, la **Channel 14** d'Israel va emetre en directe, sense verificar-lo, un deepfake d'origen iranià de l'ex-ministre de Defensa **Yoav Gallant** afirmant falsament que els EUA no podien derrotar els hutis; el presentador el va tallar a mig («atureu el vídeo... això és fals») i la cadena es va disculpar [4].

Del frau financer al pànic de masses

La branca preferida dels estafadors són les figures que encarnen la confiança institucional. El febrer de 2024, Mugur Isărescu, el governador del banc central més longeu del món, va aparèixer en un deepfake que promocionava inversions fraudulentes —part d'una onada que ha colpejat els caps de banc central: el luxemburguès Gaston Reinesch, el governador del Reserve Bank de l'Índia i, el juny de 2026, una falsificació del governador del Banc d'Anglaterra, Andrew Bailey [5]. Si es pot fabricar la cara que diu «el vostre diner és segur», el frau no només roba estalvis: erosiona el fonament de tot el sistema.

L'altra cara és el pànic. Com hem vist el **13 de gener de 2018**, una alerta oficial a Hawaii —no un deepfake, sinó un error humà genuí— va anunciar «AMENAÇA DE MÍSSIL BALÍSTIC ENTRANT A HAWAII. BUSQUEU REFUGI IMMEDIAT. AIXÒ NO ÉS UN SIMULACRE», i la correcció es va retardar **38 minuts** [6]; una situació que hauria pogut generar un pànic de masses i decisions irreversibles si

hagués estat falsificada. El **16 de maig de 2026**, la policia de Singapur va revelar una videotrucada de Zoom amb deepfakes d'alts càrrecs, inclòs el primer ministre Lawrence Wong, que va suposar una pèrdua mínima de **4,9 milions de dòlars singapuresos** (3,8 milions de dòlars dels EUA); Wong ja havia advertit al març del 2025 l'ús indegut de la seva imatge per a estafes [8].

El marc: autenticar a l'emissió, però no a la distribució

Els reguladors i les agències de seguretat ja han actuat, sobretot pel costat de l'emissió. Com hem vist, el Reglament europeu d'IA, article 50 (Reglament 2024/1689), obliga els desplegadors —incloses les autoritats públiques en assumptes d'interès públic— a revelar el contingut deepfake (definit a l'art. 3.60) a partir del 2 d'agost de 2026, amb sancions de fins a 15 milions d'euros o el 3 % de la facturació mundial [7]. Als EUA, el sistema d'alertes IPAWS de FEMA ja signa digitalment cada alerta oficial (EAS/WEA, missatges CAP) i l'autentica via IPAWS-OPEN per evitar la suplantació, amb certificats que es renoven cada tres anys: la línia base d'autenticació a l'emissió. Un full informatiu de ciberseguretat de la NSA/CISA i els seus socis dels Five Eyes (29 de gener de 2025) recomana les Content Credentials C2PA i la procedència duradora per als mitjans governamentals i d'infraestructura crítica, en línia amb l'eIDAS i els segells qualificats.

El forat, però, és evident: tota aquesta arquitectura protegeix el moment en què l'autoritat emet. No protegeix el moment en què el missatge es distribueix i es reemet —el teletip d'Ukraine 24, la reemissió no verificada de Channel 14, la imatge falsa de «Bloomberg». És en aquest tram on el públic queda sense defensa.

Per què la signatura a l'emissió sola no salva

Cal dir-ho amb cruesa. Que IPAWS signi una alerta o que un comunicat porti un segell qualificat eIDAS resol l'autenticitat a l'origen, però no arriba al ciutadà que rep el missatge reenviat per WhatsApp, vist en una notícia televisiva estrangera o llegit en un teletip piratejat. La signatura viu en un sistema tancat; el periodista que ha de decidir en dos minuts si emet o no un clip no té cap botó universal per comprovar-la.

Pitjor, cap d'aquests controls existeix al lloc on va passar el dany. Ukraine 24 no va fallar en l'emissió de Zelenski —va fallar perquè algú altre va empènyer una falsedat per un canal que el públic creia seu. La signatura a l'origen només certifica el que l'autoritat va emetre, no desmenteix el que un atacant ha distribuït. Falta una comprovació pública, neutral respecte del proveïdor i fora de línia, al costat de la distribució, que qualsevol pugui fer en segons sense demanar permís a ningú.

La prova d'existència aplicada

És aquí on **t2p** aporta la peça que faltava sobre l'artefacte oficial mateix. L'objecte segellat és la **declaració oficial autoritzada en el moment d'emissió**: el vídeo o àudio de l'oficina de premsa, el comunicat PDF signat, la decisió del banc central o la càrrega útil de l'alerta d'emergència, abans que surti de l'òrgan emissor. A l'oficina de premsa o al centre d'operacions, l'aplicació de captura calcula en el dispositiu l'**empremta SHA-512** —el fitxer no surt mai—, obté un **segell de temps RFC 3161/eIDAS** i ancora l'empremta a la blockchain pública, produint un contenidor **.asice** verificable fora de línia. Per a declaracions en directe del principal —un cap d'Estat gravant un desmentiment, un ministre a l'atril—, una **prova de vida** i el **GPS forense** lliguen l'acte a aquella persona, aquell lloc i aquell minut. L'autoritat publica llavors el **handle de verificació** (un QR o URL al canal oficial) perquè qualsevol confirmi en segons que *aquest* fitxer exacte ve de la font genuïna, a l'hora declarada, bit a bit inalterat.

Així, un teletip piratejat, una reemissió no verificada o un clip falsificat es poden **desmentir contra l'original segellat** en minuts —com el selfie de Zelenski, però criptogràficament demostrable. Complementa, no substitueix, els controls a l'emissió: les signatures IPAWS, la procedència C2PA/Content Credentials (com hem vist al capítol 13 i 15), els segells qualificats eIDAS i les eines de detecció.

El segell prova **l'origen, l'hora, l'autor i la integritat** de l'artefacte oficial —no que el seu contingut sigui veritat, legal o d'interès públic. Si un càrrec autoritzat emet una declaració falsa, presa del pànic o inconstitucional —o comet un error honest com l'alerta de Hawaii del 2018—, un segell vàlid demostrarà que el missatge equivocat va venir realment del despatx correcte. No atura un deepfake que no es compara amb l'original, ni impedeix que el públic ignori el handle de verificació; tampoc substitueix la verificació editorial, la credibilitat institucional o les capes existents de C2PA/SynthID, signatura IPAWS i detecció.

La promesa i el perill

La promesa és tancar el forat de la distribució: tornar a l'autoritat —i al públic— una manera **ràpida, pública i independent** de separar la paraula oficial autèntica de la falsificació, en el moment de crisi en què cada minut compta. El selfie de Zelenski va funcionar perquè ell és Zelenski i el podíem creure; un handle de verificació segellat funcionaria per a qualsevol funcionari, sense dependre de la fama ni de la improvisació, i amb prova matemàtica en comptes de confiança cega.

El perill demana matisos. El primer: la **falsa seguretat** —«està segellat, doncs és cert»—, quan el segell només garanteix l'origen, no la veritat ni la legalitat del contingut. El segon: si els sistemes emissors es pirategen perquè signin una càrrega maliciosa, el segell **autenticaria la mentida** amb tota la solemnitat; la seguretat de l'emissor és condició prèvia, no conseqüència. I el tercer: el **dividend del mentider** s'agreuja si el públic aprèn que «sense segell» equival a «fals», perquè llavors qualsevol declaració incòmoda no segellada es pot descartar com a falsa. La prova d'existència és una capa de verificació pública, no un certificat de veracitat ni un substitut del criteri.

A més, el disseny descentralitzat del protocol pot ser una façana que amaga una concentració de poder real: qui defineix les regles d'actualització i quins nodes tenen l'autoritat per signar-les? Si la comunitat es limita a votar sobre propostes presentades per un petit grup d'experts o per entitats corporatives, el consens aparent es converteix en una decisió imposada des de dins. En aquest escenari, el control del codi —i, per tant, del mecanisme de segellat— passa a mans d'una elite que pot ajustar les condicions d'emissió per afavorir interessos particulars, com ara suprimir declaracions incòmodes o introduir filtres ocults. Com avisa Marc Goodman, «qui controli el codi controlarà el món, per a bé i per a mal»[12]; la vulnerabilitat no resideix només en la tecnologia, sinó en qui té la clau d'actualització i quina transparència ofereixen les seves decisions. Per tant, la promesa de confiança pública es veu amenaçada si la governança del protocol es manté opaca o centralitzada sota una capa de descentralització aparent.

És hora d'actuar

Per a les **oficines de premsa i els gabinets de govern**: segellar cada comunicat, vídeo i àudio oficial en el moment d'emissió i publicar-ne el handle de verificació al canal oficial. Per a les **autoritats d'emergència** (FEMA i les seves homòlogues): estendre la signatura tipus IPAWS amb un segell públic i verificable fora de línia que el ciutadà pugui comprovar sense accés al sistema tancat. Per a les **redaccions i les agències de notícies**: exigir i comprovar el handle de verificació abans de reemetre un clip oficial —el reflex que va faltar a Channel 14. Per als **bancs centrals i les institucions financeres**: segellar tota declaració que mogui mercats, perquè un deepfake d'Isărescu o de Bailey es pugui falsificar en segons. I per als **reguladors** (l'Oficina d'IA, sota l'article 50): reconèixer el handle segellat com a mitjà de compliment de la transparència i com a evidència admissible del que va dir l'autoritat i quan.

A Kíiv, un president es va haver de gravar un selfie per demostrar que continuava al seu lloc. Donar a cada autoritat —i a cada ciutadà— una manera de provar criptogràficament què es va dir oficialment, sense dependre de la fama ni de la sort, i sense oblidar mai que el segell no fa veritat el que s'hi declara, és, en aquest front on la paraula oficial és l'última línia de defensa, time2act.

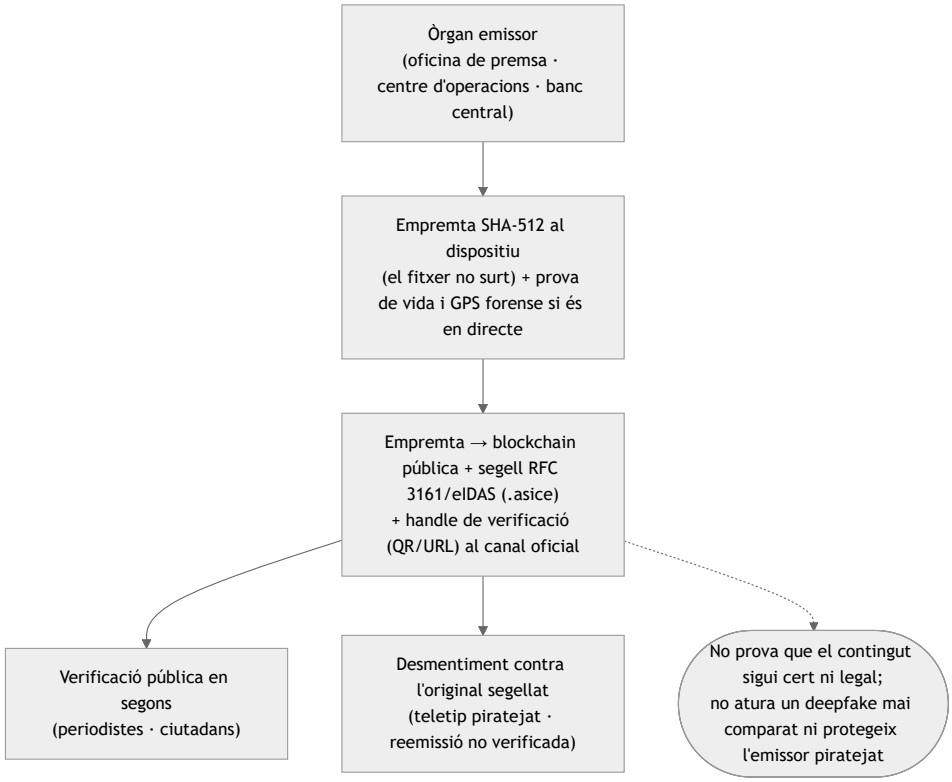


Figura 86.1 — L'òrgan emissor (oficina de premsa, centre d'operacions, banc central) calcula al dispositiu l'empremta SHA-512 de la declaració oficial —vídeo, comunicat, decisió o alerta— sense que el fitxer surti; per a declaracions en directe del principal hi afegeix prova de vida i GPS forense. L'empremta del conjunt s'ancora a la blockchain pública, amb segell RFC 3161/eIDAS complementari (.asice), i se'n publica el handle de verificació (QR/URL) al canal oficial. Dos resultats: a l'esquerra, verificació pública en segons per part de periodistes i ciutadans; a la dreta, el desmentiment d'una falsificació (teletip piratejat, reemissió no verificada) contra l'original segellat. Límit: el segell prova origen, hora, autor i integritat, no que el contingut sigui cert, legal ni assenyat; no atura un deepfake mai comparat ni protegeix l'emissor de ser piratejat. Fonts: cas Ukraine 24/Zelenski; imatge falsa del Pentàgon; cas Rubio; cas Channel 14/Gallant; alerta de Hawaii de 2018; article 50 del Reglament d'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 març de 2022; pirateig del teletip i el web d'Ukraine 24; deepfake de rendició; desmentit amb selfie de «provocació 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 maig de 2023; compte fals de «Bloomberg», amplificació de RT, caiguda breu del mercat). 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* (juliol de 2025; veu clonada del secretari d'Estat a Signal; cable del Departament d'Estat del 3 de juliol). 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; reemissió no verificada de Channel 14 d'un deepfake de Yoav Gallant; tall en directe i 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* (febrer de 2024; deepfake d'inversions fraudulentes; patró en diversos bancs centrals). https://www.romania-insider.com/bnr-mugur-isarescu-deepfake-february-2024 ↩

[6] Wikipedia — *2018 Hawaii false missile alert* (13 de gener de 2018; falsa alerta WEA de míssil balístic; correcció de 38 minuts; error genuí). https://en.wikipedia.org/wiki/2018_Hawaii_false_missile_alert ↩

[7] EU Artificial Intelligence Act — *Article 50: Transparency Obligations* (revelació de deepfakes, incloses autoritats públiques; aplicable des del 2 d'agost de 2026; definició a l'art. 3.60; sancions de fins a 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 gener de 2025; guia Five Eyes que avala les Content Credentials C2PA per a mitjans governamentals i d'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)* (alertes oficials signades digitalment per l'autoritat emissora i autenticades per IPAWS-OPEN; línia base d'autenticació a l'emissió). 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 maig de 2026; deepfake del PM Lawrence Wong, el president Tharman i representants de la MAS; pèrdua de 4,9 M$ SGD per 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* (setembre de 2025; alertes oficials falses, el «dividend del mentider» i l'autenticació de les comunicacions d'emergència). 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 el director financer: qui ha autoritzat de debò aquest pagament?

«És de prudència no fiar-se mai del tot d'aquells que ens han enganyat una vegada.»

— René Descartes, Meditacions metafísiques, I (1641)

El gener de 2024, a l'oficina de Hong Kong de l'empresa britànica d'enginyeria i disseny **Arup**, un empleat del departament financer va rebre la instrucció de transferir uns **200 milions de dòlars de Hong Kong** —al voltant de **25,6 milions de dòlars** dels Estats Units. Al principi va sospitar: el correu que originava l'ordre li semblava una estafa de *phishing*. Però el van convidar a una **videoconferència** on hi havia el director financer del grup, amb seu al Regne Unit, i diversos col·legues més; tots tenien la cara i la veu exactes de qui deien ser. Tranquil·litzat per allò que veia i sentia, l'empleat va executar **15 transferències** a cinc comptes bancaris de Hong Kong al llarg d'una setmana. Tots els participants de la trucada, tret d'ell, eren *deepfakes* generats per IA. El director global de sistemes d'informació d'Arup, Rob Greig, ho va confirmar mesos després: «podem confirmar que es van fer servir veus i imatges falses», i que cap sistema intern no havia estat compromès —el frau va funcionar **purament suplantant una autorització** [1]. El 2025 no s'havia detingut ningú ni s'havien recuperat els fons.

Aquest capítol tracta una cara molt concreta del frau, diferent de la del capítol 16 —que cobreix el paisatge ampli del crim financer i el compliment normatiu. Aquí no parlem de la detecció genèrica del frau, sinó d'un acte únic i puntual: **l'autorització d'un pagament o una instrucció executiva**. La pregunta no és si la cara de la pantalla és real —ja hem vist que és impossible de garantir—, sinó com demostrar que **una directiva prové de debò del directiu**. La tesi del llibre s'hi aplica directament: en comptes de perseguir la falsedat, segellem la veritat a l'origen.

Un frau que no necessita trencar res

El que fa esgarrifar del cas Arup és que no es va vulnerar cap sistema: no hi va haver intrusió, ni programari maliciós, ni contrasenyes robades. El frau va explotar l'única cosa que cap *firewall* protegeix: la **confiança humana en una cara i una veu conegudes**. Greig va ser explícit que els sistemes interns no es van tocar; la debilitat era de procés, no tècnica, perquè la companyia no podia distingir una autorització genuïna del director financer d'una de fabricada, ja que l'autorització mateixa mai no s'havia segellat.

Com hem vist al març de 2025, un director financer d'una multinacional a **Singapur** va autoritzar un pagament de **499.000 dòlars** durant una trucada de Zoom on el director executiu i altres directius eren tots *deepfakes* generats per IA; cap participant no era real [7]. El **juliol de 2024**, un directiu de **Ferrari** va desbaratar una clonació de veu del conseller delegat, Benedetto Vigna —empesa per un número de WhatsApp desconegut per signar amb urgència un acord de confidencialitat sobre una adquisició secreta— amb una pregunta que només el Vigna real podia respondre: el títol d'un llibre que havia recomanat feia poc. La trucada es va tallar de cop [5]. I el **maig de 2024**, uns estafadors van suplantar el conseller delegat de **WPP**, Mark Read, amb un compte fals de WhatsApp, una reunió de Microsoft Teams, una veu clonada i imatges de YouTube; l'intent va fracassar sense pèrdues, i Read va advertir el personal que «tots hem d'estar amatents a les tècniques que van més enllà dels correus per aprofitar reunions virtuals, IA i *deepfakes*» [6]. La diferència entre Arup i Ferrari va ser, literalment, una pregunta a contracorrent.

L'escala del problema, en xifres

La suplantació de directius no és una anècdota: és una indústria en creixement. El **compromís del correu corporatiu** (BEC) continua sent una de les categories més costoses que rastreja el centre de denúncies de l'FBI (IC3): al voltant de **3.000 milions de dòlars** en pèrdues declarades, i gairebé **8.500 milions** perduts per BEC en els tres últims anys [8]. I la IA generativa hi posa benzina. El **Center for Financial Services de Deloitte** projecta que les pèrdues per frau habilitat per IA generativa als Estats Units podrien arribar als **40.000 milions de dòlars el 2027**, des dels 12.300 milions del 2023 —un creixement anual compost del **32 %**—, amb el frau per correu i BEC arribant potencialment als **11.500 milions** en l'escenari més agressiu [2]. El cas Arup, amb els seus **25,6 milions**, és per ara un dels fraus de pagament habilitats per *deepfake* més grans documentats, però la tendència indica que deixarà de ser excepcional.

El que diuen els reguladors

Les autoritats ja han pres nota. El **13 de novembre de 2024**, la unitat d'intel·ligència financera del Tresor nord-americà, **FinCEN**, va emetre l'alerta **FIN-2024-Alert004**, advertint que els criminals fan servir mitjans *deepfake* generats per IA —documents d'identitat fraudulents, àudio i vídeo— per burlar els controls de verificació d'identitat i autenticació de les entitats financeres; recomana **comprovacions en viu** i **autenticació multifactor resistent al *phishing*** [3]. El **15 de maig de 2025**, l'IC3 de l'FBI va publicar l'avís **PSA250515**, alertant que actors maliciosos envien missatges de veu i text generats per IA suplantant alts càrrecs, i aconsella confirmar la identitat **per canals prèviament verificats** i usar **frases de verificació pactades**, perquè el contingut generat per IA «ha avançat fins al punt que sovint és difícil d'identificar» [4].

El marc legal europeu aporta la peça clau: el **Reglament eIDAS (UE) núm. 910/2014**, articles 41 i 42, reconeix un **segell de temps electrònic qualificat** amb presumpció d'exactitud i integritat que no pot ser denegat com a prova en cap estat membre; és la columna vertebral per segellar un artefacte d'autorització. Al Regne Unit, la **Solicitors Regulation Authority** va actualitzar el 5 de març de 2024 la seva avaluació de riscos de blanqueig assenyalant els *deepfakes* com a risc emergent per a les instruccions de pagament i les comunicacions urgents amb clients. Els règims d'APP al Regne Unit i a la UE ja tracten aquests pagaments fraudulents com una categoria pròpia que exigeix reforçar els controls d'autorització.

Per què l'alerta sola no salva

Cal dir-ho amb cruesa. Les recomanacions de FinCEN i de l'FBI són sensates —verificació en viu, devolució de trucada per un canal conegut, frases pactades—, però totes depenen que **algú, sota pressió, recordi i apliqui un procediment** en el moment exacte en què un directiu aparentment furiós exigeix un pagament urgent. L'empleat d'Arup tenia bon olfacte: va sospitar del correu. El que el va vèncer va ser la **prova social** d'una sala plena de cares conegudes. Una política de devolució de trucada no serveix de res si la víctima creu que ja està parlant amb el cap. Una frase de verificació pactada protegeix si la recordes i si l'altre també l'hauria de saber; el directiu de Ferrari se'n va sortir per instint, no per procediment. El problema de fons és que avui l'autorització és un **judici subjectiu** —«això sembla el cap»— en comptes d'una **comprovació objectiva**. Mentre la pregunta sigui «em sembla real?», els *deepfakes* sempre acabaran guanyant, perquè cada any semblen més reals.

La prova d'existència aplicada

És aquí on **t2p** inverteix el model de confiança. L'artefacte que cal protegir no són els fons: és la **directiva d'autorització mateixa** —la instrucció executiva. En comptes que l'equip financer intenti (i fracassi) detectar si la cara de la trucada és real, el **directiu genuí segella proactivament cada directiva que autoritza**. Quan s'emet una ordre de pagament o de transferència, el directiu la captura al seu dispositiu: un text d'instrucció signat, l'aprovació d'una factura en PDF o una breu autorització en vídeo o veu amb **prova de vida** i **GPS forense** que confirmen una persona viva en un lloc conegut. El dispositiu calcula localment l'**empremta SHA-512** —la instrucció no surt mai del dispositiu—, obté un **segell de temps RFC 3161 conforme a eIDAS**, ancorant l'empremta a la blockchain pública i generant un contenidor **.asice** verificable fora de línia.

A partir d'aquí, la tresoreria no mou ni un euro si la instrucció no arriba amb un segell vàlid, datat i lligat al directiu, que es verifica contra l'àncora pública. La pregunta «el cap ho ha aprovat de debò?», deixa de ser un judici subjectiu i passa a ser una comprovació criptogràfica; un director financer deepfake en una trucada de Zoom simplement no pot produir el segell criptogràfic previ del directiu real, de manera que una instrucció «urgent» sense segell és, per disseny, una bandera vermella. Això ataca el mode de fallada d'Arup, on una videoconferència convincent va substituir una autorització verificable. La capa complementa, mai no substitueix, els controls existents: conviu amb la devolució de trucada per canal extern, la doble signatura o «quatre ulls», el cribratge de pagaments i la capa de procedència C2PA/SynthID, com hem vist a les seccions 13 i 15.

El segell demostra que una directiva concreta la va emetre un titular de clau concret en un instant determinat i que no s'ha alterat —prova l'acte d'autoritzar, no que l'autorització sigui legítima o lliure de frau. Si el directiu és coaccionat, subornat o enganyat fins a segellar un pagament fraudulent, o li roben el dispositiu o la clau de signatura, el segell certificarà una mala instrucció; no verifica que el beneficiari sigui

legítim, ni que la factura sigui real, ni impedeix el blanqueig de fons. Tampoc atura un insider amb clau legítima ni detecta un deepfake en una trucada sense segell—només fa sospitosa l'absència del segell. La verificació dels humans de la trucada mateixa — el handshake de vida de cada participant, abans d'obrir els micròfons — es tracta al capítol 88. La recuperació de fons ja transferits depèn d'una política «sense segell, no hi ha pagament», i la capa reforça les devolucions de trucada, el doble control i el judici humà sense substituir l'auditoria, la segregació de funcions ni un responsable financer escèptic.

La promesa i el perill

La promesa és convertir l'autorització en una cosa **verificable** en comptes de creïble: passar de «em sembla el cap» a «el segell quadra». Una tresoreria amb una regla de «sense segell, no hi ha pagament» fa que el directiu *deepfake* més perfecte del món sigui inútil, perquè li falta l'única cosa que no pot fabricar — la clau privada del directiu real. L'empleat d'Arup, demà, no hauria de decidir si una cara és real; només hauria de comprovar un segell.

El perill demana els matisos de sempre. El primer: la **seguretat de la clau**. Si el segell esdevé l'única porta, la clau de signatura del directiu es converteix en l'objectiu —cal protegir-la amb maquinari, biometria i recuperació robusta, o el lladre canvia de cara per clau. El segon: la **falsa tranquil·litat**. «Està segellat, doncs és bo» és un error perillós; el segell certifica l'origen, no la bondat de la instrucció, i un directiu coaccionat segella igual. El tercer: la **concentració i l'exclusió**, que la regla no deixi fora els proveïdors o socis petits sense capacitat de segellar, ni esdevingui una barrera que afavoreixi només els grans. La prova d'existència és una capa de governança del pagament, no un certificat que el pagament sigui savi.

És hora d'actuar

Per als directius i conselleries delegades (Vigna, Read, directors financers): adoptar el costum de segellar cada autorització de pagament al dispositiu en el moment d'emetre-la, perquè la tresoreria pugui exigir-ne la prova. Per als departaments de tresoreria i finances: imposar la regla «sense segell, no hi ha pagament» i combinar-la amb la devolució de trucada i el doble control; un segell vàlid haurà de ser condició necessària, no suficient. Per als bancs i proveïdors de pagaments: oferir la verificació del segell com a part del cribratge de transferències, sobretot en pagaments grans i urgents a comptes nous. Per als reguladors (FinCEN, FBI/IC3, SRA, règims APP): reconèixer la directiva segellada amb segell de temps eIDAS com a control vàlid d'autorització i com a evidència en les investigacions de frau. I per als proveïdors de programari financer i ERP: integrar el segell i la verificació en els fluxos d'aprovació, perquè «sense segell, no hi ha pagament» sigui el camí per defecte, no una excepció heroica.

A Hong Kong, un empleat amb bon olfacte va ser vençut per una sala plena de cares que no existien. Donar a cada autorització una prova segellada que cap deepfake pot fabricar — sense oblidar mai que el segell prova l'acte, no la bondat de la instrucció — és, en aquest front on un clic mou milions, time2act.

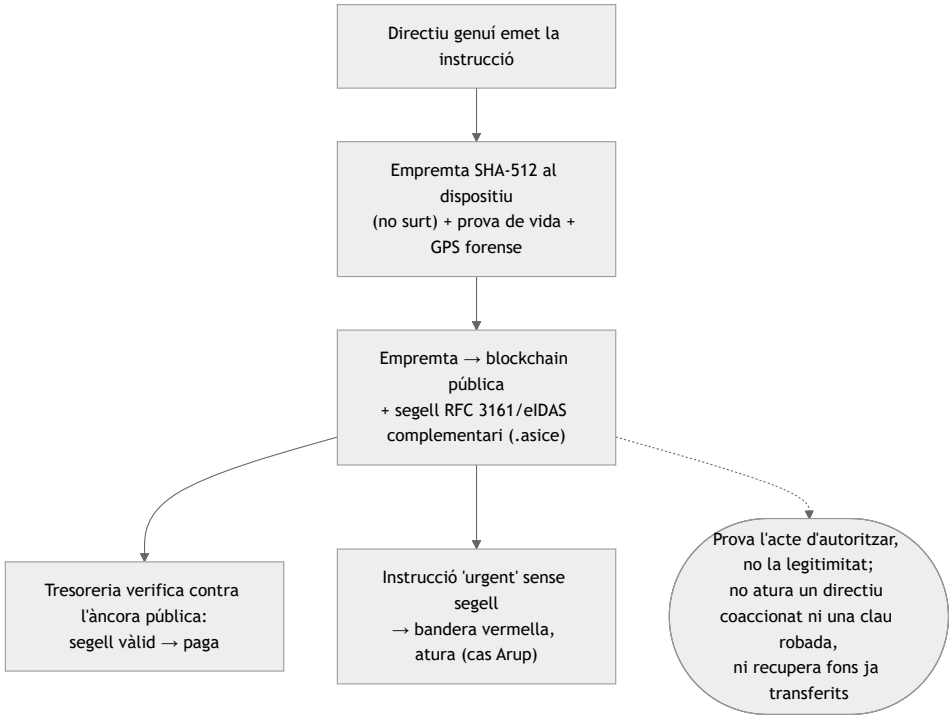


Figura 87.1 — El directiu genuí captura la instrucció de pagament al dispositiu (text signat, factura en PDF o vídeo amb prova de vida i GPS forense), en calcula l'empremta SHA-512 sense que surti del dispositiu, i l'ancora a la blockchain pública, amb un segell de temps RFC 3161/eIDAS complementari (.asice). La tresoreria verifica el segell contra l'àncora pública: si quadra, paga; si falta, atura —la instrucció «urgent» sense segell és, per disseny, una bandera vermella (mode de fallada d'Arup). Límit: el segell prova l'acte d'autoritzar, no que la instrucció sigui legítima; no atura un directiu coaccionat ni una clau robada, ni recupera fons ja transferits. Fonts: cas 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 confirmat com a víctima; HK$200M/US$25,6M; 15 transferències; declaració 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* (projecció: 40.000 M$ de frau per IA generativa el 2027 des de 12.300 M$ el 2023; 32 % de creixement anual; ~11.500 M$ de frau per correu/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 novembre de 2024; recomana verificació en viu i MFA resistent 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 maig de 2025; veu/text generats per IA; verificació fora de banda i frases pactades). 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* (juliol de 2024; clonació de veu desbaratada amb 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* (maig de 2024; WhatsApp fals, Teams, veu clonada i imatges de YouTube; intent fracassat; advertència 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* (març de 2025; un director financer autoritza 499.000 $ en una trucada de Zoom amb tots els participants deepfake). https://www.tookitaki.com/blog/deepfake-ceo-scam-singapore-2025 ↩

[8] Nacha — *FBI's IC3 Finds Almost $8.5 Billion Lost to Business Email Compromise in Last Three Years* (~3.000 M$/any; ~8.500 M$ en tres anys; base del frau de pagament). 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* (anàlisi tècnica del patró d'atac amb videotrucada multiparticipant emprat contra Arup). https://www.trendmicro.com/en_us/research/24/b/deepfake-video-calls.html

[10] EUR-Lex — *Reglament (UE) núm. 910/2014 (eIDAS), articles 41-42* (efecte jurídic dels segells de temps electrònics: presumpció d'exactitud de la data i l'hora i admissibilitat com a prova; base legal de l'artefacte d'autorització segellat). https://eur-lex.europa.eu/eli/reg/2014/910/oj

[11] World Economic Forum — *Cybercrime: Lessons learned from a $25m deepfake attack* (febrer de 2025; anàlisi del cas Arup i de les fallades de control; argument de la verificació fora de banda). https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/

La identitat en directe: qui hi ha de debò a l'altra banda de la pantalla?

«Quan un individu fa un paper, demana implícitament als seus observadors que es prenguin seriosament la impressió que es fomenta davant d'ells.»

— Erving Goffman, La presentació de la persona en la vida quotidiana (1959)

El muntatge que WIRED va documentar el 2024 és d'una senzillesa esgarrifosa: dos mòbils fixats en suports i un anell de llum. Amb el primer, l'estafador fa la videotrucada — sovint per Zoom. La càmera del darrere d'aquest mòbil no l'enfoca a ell: enfoca la pantalla del segon, que executa una aplicació de face-swap apuntant a la seva cara. El que veu la víctima és una cara que parpelleja, somriu i respon en temps real — i que no existeix. Les «relacions» s'allarguen setmanes o mesos, videotrucades incloses, fins que arriba la petició de diners. Són els «Yahoo Boys», la confraria d'estafadors romàntics que opera sobretot des de Nigèria — i són tan descarats que presumeixen dels muntatges en grups de Telegram, amb vídeos i tot, de vegades per vendre'ls a altres estafadors [1]. L'experta en enginyeria social Rachel Tobac ho resumia: aquestes aplicacions han millorat dramàticament en un any — el to de pell, el cabell, el color d'ulls [1].

I no és una anècdota artesanal: és una indústria. iProov, una empresa que verifica identitats remotes per a banca i governs, va documentar el 2024 un augment del 2.665 % dels atacs amb càmera virtual nativa — programari que injecta vídeo sintètic com si vingués de la càmera del dispositiu, convertit ja en el principal vector d'atac —, un 300 % més d'atacs de face-swap dirigits precisament contra sistemes amb detecció de vida, i prop de 24.000 usuaris venent tecnologia d'atac com a servei; el seu catàleg d'amenaces compta 127 eines de face-swap i 91 càmeres virtuals [2]. I el vector nou és encara més barat: convertir una sola foto en vídeo animat, en dos passos [2].

Durant un segle, veure algú moure's i respondre en directe va ser la prova informal definitiva que era real i era ell. Aquesta prova ha mort, i amb ella la confiança de dos moments quotidians: quan algú entra — l'alta en una plataforma — i quan algú es presenta — la videotrucada, l'entrevista, la primera cita. Aquest capítol tracta de recuperar-los. La instrucció del directiu i la seva trucada plena de deepfakes es tracta al capítol 87; la identitat de qui contractes en remot, al capítol 91; el KYC bancari i el crim financer, al capítol 16; la persona única del vot i la participació, al capítol 108; l'aprovació per sobre de llindar, al capítol 80; la veu clonada al telèfon, al capítol 68. La pregunta clau d'aquest: com pot una persona demostrar que és real, present i que és ella, en el moment exacte que importa — i com pot l'altra banda comprovar-ho sense haver de creure ningú? La resposta: amb la signatura amb vídeo-selfie de **t2p** — reptes de vida aleatoris, verificació biomètrica del dispositiu, empremta SHA-512, segell de temps RFC 3161/eIDAS, àncora a la blockchain pública i un certificat que qualsevol pot verificar [8].

El directe ja no és una prova

Tres fronts, una mateixa fallada: la confiança en el moviment d'una cara. El front sentimental ja l'hem vist [1]. Al front laboral, l'FBI alertava el juny de 2022 — abans de l'esclat de la IA generativa actual — d'un augment de denúncies per l'ús de deepfakes i dades personals robades per aconseguir feines remotes: llocs de TI, programació, bases de dades i programari, alguns amb accés a dades de clients, informació financera i sistemes corporatius [4]. Els senyals que llavors delataven l'engany — llavis que no quadren amb el so, una tos que no es veu — eren ja subtils; cada generació d'eines els esborra una mica més [4][2]. I el front executiu té capítol propi: la sala de Hong Kong on totes les cares eren falses i es van autoritzar 25,6 milions de dòlars, al capítol 87.

El paper tampoc no salva. OnlyFake, el servei clandestí destapat el febrer de 2024, generava carnets i passaports falsos «amb xarxes neuronals» per 15 dòlars — Estats Units, Itàlia, Xina, Rússia, Argentina, Txèquia, Canadà —; els periodistes de 404 Media van superar amb un d'aquests carnets el control KYC de l'exchange OKX, que usa un verificador extern professional [5]. El document sol està mort; la selfie sola, ferida de mort [2].

La mateixa indústria ho admet. Gartner preveia que el 2026 el 30 % de les empreses ja no considerarien fiables les solucions de verificació d'identitat i autenticació per si soles, per culpa dels deepfakes contra la biometria facial [3]. Els atacs d'injecció — el vídeo sintètic servit directament al flux de la càmera — van créixer un 200 % el 2023, i els estàndards de detecció d'atacs de presentació, pensats per a la màscara i la

foto impresa, no cobreixen la injecció digital [3]. Traducció: el sector que viu de verificar cares reconeix que li han canviat el tauler.

La resposta instintiva és una cursa de detectors: endevinar si la cara és falsa. El llibre ja ha mostrat on porta: el detector s'equivoca en els dos sentits i el mentider en cobra el dividend (capítol 15). La sortida és una altra: deixar de preguntar «és falsa, aquesta cara?» i començar a exigir «acredita que ets un humà viu, present i disposat a signar-ho — ara». No detectar l'impostor: fer que acreditar-se sigui trivial per a l'humà real i car per a l'impostor. I que la prova la pugui comprovar qualsevol, sense confiar en cap proveïdor.

Acreditar-se en lloc de detectar: què fa exactament el vídeo-selfie

El gest, pas a pas. La signatura amb vídeo-selfie és la signatura més forta de t2p. La persona obre el document — un PDF: un formulari d'alta, el full d'una reunió, una declaració — i comença: la càmera frontal grava un vídeo breu mentre l'app li planteja reptes de vida aleatoris — parpelleja amb naturalitat, i dos més entre girar el cap, somriure o inclinar-lo — que cal completar en menys de 60 segons; el dispositiu exigeix la verificació biomètrica — l'empremta dactilar, o el PIN com a alternativa — i, superat tot, la persona dibuixa la seva signatura manuscrita a la pantalla. En certificar, l'app genera dues transaccions a la blockchain pública — una per la signatura, una pel vídeo — i un certificat dedicat: un PDF d'una pàgina amb el document, la signatura, l'evidència en vídeo i les dues transaccions [8]. Només es pot veure una persona a l'enquadrament; si algú abandona o s'esgota el temps, no queda res.

Què conté la prova. El certificat porta l'empremta SHA-512 del fitxer — calculada al dispositiu —, el segell de temps RFC 3161 conforme a eIDAS, l'àncora a la blockchain pública, un codi QR i una verificació de seguretat forense: GPS contra simulació, coherència temporal, integritat del dispositiu i attestation de maquinari [8]. Aquest últim detall importa més del que sembla: una càmera virtual que injecta vídeo sintètic necessita normalment un dispositiu trucat, i el certificat en deixa constància. El paquet d'evidència .asice — estàndard ETSI — es verifica completament fora de línia, amb eines obertes, sense l'app i sense confiar en el fabricant [8]. I la privadesa per disseny: el vídeo no surt del mòbil — a la cadena només hi viatja l'empremta [8]; compartir l'evidència és sempre una decisió de qui signa.

Què prova i què no prova. El vídeo-selfie segellat acredita que una persona real i present va executar aquell acte de signatura en aquell instant — un humà viu responent reptes imprevisibles, no un vídeo enllaunat. El que no fa és dir el nom civil de ningú: la «identitat verificada» que mostra l'app és la del compte i la biometria del dispositiu, no la d'un registre civil. Qui és la cara del vídeo ho estableix el receptor — comparant-la amb la persona que coneix, amb la de la pantalla, amb la del selfie fundacional del compte — o bé la capa institucional que arriba: la cartera d'identitat europea, que cada estat membre ha d'oferir el desembre de 2026 [7]. La divisió del treball és neta: t2p posa l'artefacte d'evidència; el receptor o la institució, el nom. La identitat civil com a infraestructura — el qui ets davant l'Estat, amb les seves promeses i els seus perills — és la matèria del capítol 47.

La frescor. Un vídeo-selfie de fa un mes no acredita res sobre avui. Per això el document signat és el repte: si conté el context d'ara — la reunió de tal dia, l'alta amb tal nom d'usuari, una frase triada fa un minut —, la prova no es pot reciclar (no-abans), i l'àncora posa el sostre per l'altra banda (no-després). És el sandvitx temporal que el llibre ja coneix del compromís i revelació (capítols 45 i 46), aplicat a la persona.

La prova d'existència aplicada

Tres moments, tres variants del mateix gest.

1. El handshake de la reunió

Abans de la videotrucada que importa — el tancament, la due diligence, l'entrevista final, el consell —, l'amfitrió redacta el full de la reunió: un PDF d'una pàgina amb la data, l'hora, els participants i una frase de context acabada de triar. Cada participant el signa amb el seu vídeo-selfie al seu dispositiu i deixa el certificat al xat de la reunió [8]. Un minut abans d'obrir micròfons, cadascú té dels altres: un vídeo amb reptes de vida superats fa un moment, una signatura manuscrita, una data certa posterior a la convocatòria — i una cara nítida per comparar amb la finestreta de la trucada. El face-swap en directe pot imitar una cara dins de Zoom [1][2]; el que no pot fer amb la mateixa facilitat és produir el certificat d'aquesta signatura: caldria superar reptes aleatoris amb la cara suplantada davant de la càmera nativa d'un dispositiu la integritat del qual queda avaluada al certificat [8]. I si el dubte persisteix, la pregunta a

contracorrent — el títol del llibre que li vas recomanar fa una setmana — continua sent gratuïta i letal (capítol 87). El handshake acredita els humans de la sala; la instrucció que en surti, si mou diners, demana a més el seu propi segell — la regla «sense segell, no hi ha pagament» del capítol 87.

2. L'alta com a humà

El registre en una plataforma — el marketplace, la xarxa social, l'app de cites — és l'altre moment. El formulari d'alta com a document-repte: la persona el signa amb vídeo-selfie i la plataforma rep un artefacte verificable — una persona real i present s'ha donat d'alta avui, amb aquest nom d'usuari — sense quedar-se cap biometria: el vídeo el conserva l'usuari, i a la cadena només hi ha empremtes [8]. És la versió practicable d'allò que la recerca acadèmica reclama amb el nom de «credencials de personalitat»: demostrar que ets una persona real — no una IA — sense revelar cap dada personal; la proposta que investigadors del MIT, d'OpenAI i de Microsoft van publicar el 2024, amb emissió presencial o institucional i verificació criptogràfica [6]. Pseudònim-però-humà: el compte pot dir-se com vulgui; el que no pot és ser un guió que n'obre deu mil. Per als serveis que exigeixen el nom legal — el banc, l'edat —, la cartera europea que arriba el desembre de 2026 posa la identitat civil [7]. I el contramodel també té nom: escanejar iris a canvi de criptomonedes i concentrar la biometria de mig planeta en una sola base de dades — el llibre ja n'ha parlat (capítol 108). Aquí és al revés: la biometria es queda al dispositiu de cadascú.

3. La represa: qui torna, i qui truca de nou

La identitat en directe no és només el primer dia. El compte que torna per a una operació sensible — canviar el correu de recuperació, buidar la cartera, vendre el que té — pot re-acreditar-se amb un vídeo-selfie nou sobre el document de l'operació: el receptor compara la cara d'avui amb la del selfie fundacional del compte — la continuïtat és una cadena de vídeos datats, i la comparació la fa qui verifica, mai l'app [8]. El «mare, soc jo, m'ha canviat el número» que demana diners es respon amb el gest del capítol 85: un repte de vida abans de moure un euro. I la primera videocita després de setmanes de xat — el territori exacte dels Yahoo Boys [1] — admet el mateix ritual que una reunió de consell: un handshake d'un minut. Qui t'estima, el farà somrient — literalment: somriure és un dels reptes [8]; qui no existeix, no el pot fer.

El límit, dit clarament: el segell no reconeix cares ni posa noms — la comparació és del receptor, humana o pericial; no és un detector de deepfakes — és una càrrega de la prova invertida; no substitueix el KYC on la llei l'exigeix — el complementa amb un artefacte que el client controla; i no tot demana handshake: la trucada de cada dia amb qui coneixes de tota la vida no és una due diligence. El criteri de sempre: com més alt el risc, més fort el gest — el llindar del capítol 80.

La promesa i el perill

La promesa: reunions on cada cadira ve acreditada per un certificat que qualsevol participant pot verificar sense confiar en ningú [8]; altes on crear deu mil comptes falsos deixa de ser gratis, perquè cada alta exigeix un humà viu responent reptes davant d'una càmera; estafadors que, per intentar-ho, han de deixar un artefacte datat, signat i lligat a un compte — evidència que treballa per a la víctima des del minut zero; i la infraestructura institucional que arriba — la cartera europea [7] — completada per una capa d'evidència neutral que no custodia cap govern ni cap plataforma.

El liveness també és atacable — honestedat abans que màrqueting: iProov documenta face-swaps dirigits precisament contra sistemes amb detecció de vida [2], i el manual de t2p no promet cap escut anti-deepfake [8]. Els reptes gestuals no són una muralla: són un llistó — més alt en una app nativa, amb la integritat del dispositiu i l'attestation de maquinari al certificat [8], que en una webcam qualsevol —, però cap llistó no és infinit. La resposta és la de tot el llibre: capes — el certificat, la comparació humana de cares, la pregunta a contracorrent (capítol 87), el canal alternatiu — i el cost asimètric: qui salta el llistó deixa una prova datada i signada del seu propi frau. El deepfake que signa queda notariat.

La fricció — dos crèdits i un minut per persona no és per a cada trucada ni per a cada alta. És per als moments que ho valen: l'import alt, el primer contacte, l'operació irreversible. El llindar el posa cadascú — i el capítol 80 ja ha mostrat com.

La biometria com a peatge — la línia ètica del llibre no es mou: la prova de vida és una opció de qui vol acreditar-se, mai un peatge universal. El vídeo resta al dispositiu; a la cadena, només empremtes [8]; hi ha d'haver alternatives per a qui no pot o no vol — el PIN ja ho és dins del gest [8] —, i l'anonimat continua sent legítim i vital allà on ensenyar la cara mata (capítol 113).

L'exclusió — qui no té mòbil amb biometria, qui no pot pagar crèdits, qui té setanta-vuit anys i tremola davant d'un repte cronometrat: si l'acreditació en directe esdevé condició d'accés, hem construït una porta nova per deixar gent fora. Tota plataforma que l'adopti necessita un camí presencial o assistit equivalent — i que no sigui un camí de segona.

El registre que persegueix — un món on cada alta i cada reunió deixen àncora és també un món correlacionable: qui es va acreditar, quan, per parlar amb qui. Les àncores no han de ser enllaçables entre si, la revelació ha de ser selectiva — el tram disputat, mai la vida sencera — i el control de cada camp, de qui signa (capítol 112).

És hora d'actuar

Que «soc real i soc jo» torni a poder-se demostrar.

Per a les plataformes de reunions i videotrucades: doneu al handshake un lloc natiu — una sala d'espera on adjuntar i comprovar els certificats abans d'obrir micròfons; que «tots els participants acreditats» es vegi com es veu el cadenat del navegador. La detecció pot ajudar; l'acreditació decideix.

Per a les plataformes de consum — xarxes, marketplaces, apps de cites: oferiu l'alta com a humà — verificar l'artefacte del vídeo-selfie sense custodiar cap biometria [8][6] — i senyalitzeu els comptes que l'han superada; sense convertir-la en obligació ni penalitzar l'anonimat legítim.

Per a les empreses: política de handshake per a les videotrucades per sobre de llindar — la contractació remota, el proveïdor nou, l'operació gran — encaixada amb la regla del capítol 87: el handshake acredita els humans de la reunió; el segell de la instrucció, l'autorització que en surt. Dues capes, dues preguntes diferents.

Per als ciutadans: abans d'enviar diners a algú que només has vist per pantalla — la videocita que es torna urgent, el «fill» amb número nou, el reclutador de la feina perfecta —, demana un minut de handshake amb reptes de vida [8]. Qui és real, el passa somrient; qui s'hi nega o s'hi enfada, ja t'ha respost.

Per als reguladors i els estàndards: la cartera europea ha d'arribar a l'hora [7] i conviure amb l'evidència d'humanitat de capes neutrals que el ciutadà controla; i els estàndards de prova de vida han de cobrir l'atac d'injecció, no només la màscara i la foto [3] — el forat és allà.

La pantalla ens va ensenyar a veure'ns de lluny; els deepfakes ens han pres el dret de creure el que hi veiem. Es pot recuperar: no endevinant qui és fals, sinó donant a cada humà la manera de provar que és real — aquí, ara, signant això. Que cada «soc jo» — a l'alta, a la sala de reunions, a la nit que algú que estimes et demana ajuda — pugui portar la seva prova. Per mirar la pantalla i saber qui hi ha, **time2act**.

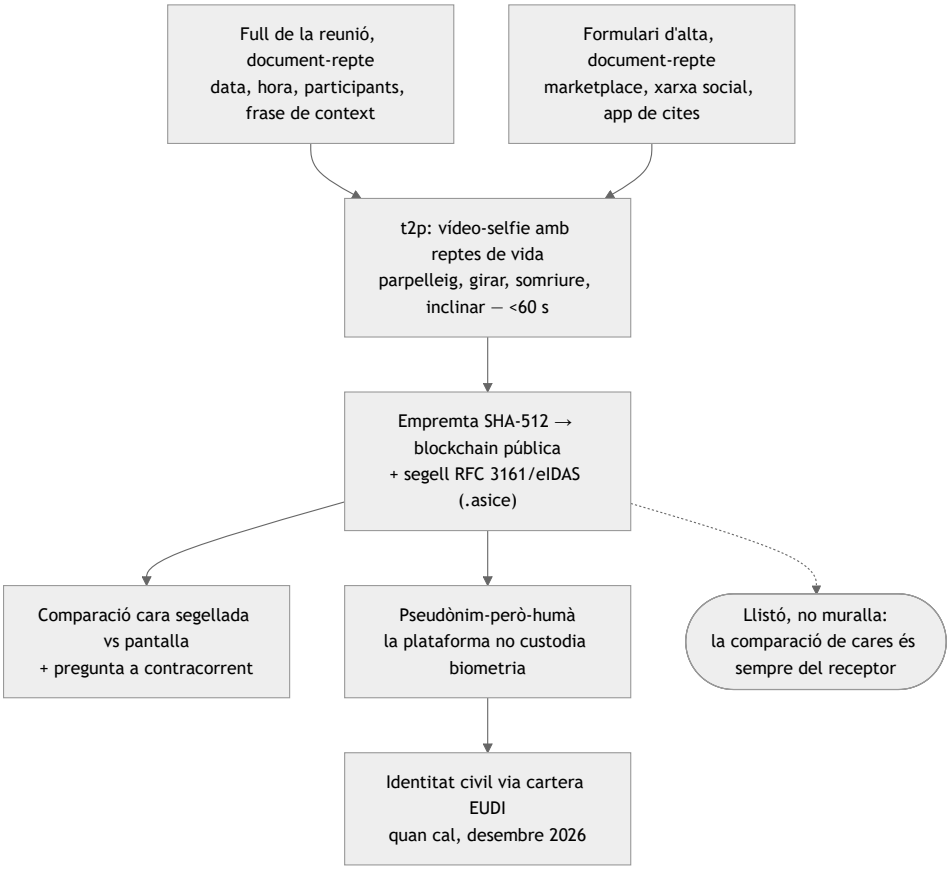


Figura 88.1 — La identitat en directe amb prova d'existència (t2p: vídeo-selfie amb reptes de vida aleatoris — parpellejar, girar, somriure, inclinar — en <60 s, biometria o PIN del dispositiu, empremta SHA-512, segell RFC 3161/eIDAS, àncora a la blockchain pública, certificat amb l'evidència en vídeo i attestation de maquinari, paquet .asice verificable fora de línia): a l'esquerra, el handshake de la reunió (full de la reunió com a document-repte signat per cada participant abans d'obrir micròfons; comparació de la cara segellada amb la de pantalla; la pregunta a contracorrent com a capa extra); a la dreta, l'alta com a humà (el formulari d'alta signat amb vídeo-selfie: pseudònim-però-humà, la plataforma verifica sense custodiar biometria; identitat civil via cartera EUDI quan cal). Context: face-swap en temps real comercialitzat (Yahoo Boys), +2.665 % d'atacs de càmera virtual nativa i +300 % de face swaps contra sistemes amb liveness (iProov 2025), 30 % de desconfiança empresarial prevista (Gartner). Límits: els reptes gestuals són un llistó, no una muralla — capes i cost asimètric (el frau que signa queda notariat); la comparació de cares és del receptor, mai de l'app. Fonts: WIRED/9to5Mac; iProov; Gartner; FBI IC3; Decrypt; arXiv/MIT; CE (EUDI).

---

[1] 9to5Mac (sobre el reportatge de WIRED) — *Latest romance scam tactic uses two phones with face-swap app* (abr-2024: els «Yahoo Boys» i el face-swap en temps real dins de videotrucades — dos mòbils en suports i anell de llum, o portàtil amb webcam; presumeixen dels muntatges a Telegram i els venen; Rachel Tobac: les apps han millorat dramàticament en un any). https://9to5mac.com/2024/04/18/romance-scam-face-swap/ ↩

[2] iProov — *Threat Intelligence Report 2025: Remote Identity Under Attack* (atacs de càmera virtual nativa +2.665 %; face swaps +300 % respecte del 2023, dirigits contra sistemes amb protocols de detecció de vida; ~24.000 usuaris venent tecnologies d'atac com a servei; la conversió d'imatge a vídeo com a vector nou; 127 eines de face-swap, 91 càmeres virtuals i 10 emuladors catalogats). 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 (via FutureCIO) — *Deepfakes to render identity verification and authentication solutions inefficient* (predicció de feb-2024: el 2026, el 30 % de les empreses ja no consideraran fiables aïlladament les solucions de verificació d'identitat i autenticació, pels deepfakes contra la biometria facial; atacs d'injecció +200 % el 2023; els estàndards de detecció d'atacs de presentació no cobreixen la injecció digital; Akif Khan: combinar PAD, IAD i inspecció d'imatge). 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 i dades personals robades per optar a feines remotes de TI, programació, bases de dades i programari — algunes amb accés a dades de clients i sistemes corporatius; senyals: llavis i so desincronitzats, tos o esternuts que no quadren amb la imatge). https://www.ic3.gov/PSA/2022/psa220628 ↩

[5] Decrypt — *People Are Using Basic AI to Bypass KYC — But Should You?* (feb-2024: OnlyFake, carnets i passaports falsos generats «amb xarxes neuronals» per 15 $ — EUA, Itàlia, Xina, Rússia, Argentina, Txèquia, Canadà —; 404 Media va superar-hi el KYC de l'exchange OKX, que usa el verificador extern Jumio; usuaris els feien servir per obrir comptes bancaris i desbloquejar comptes 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 autors, amb investigadors del MIT, d'OpenAI i de Microsoft: credencials digitals per demostrar que ets una persona real — no una IA — sense revelar cap dada personal; emissió presencial o institucional; verificació criptogràfica; «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] Comissió Europea / Corbado — el Reglament (UE) 2024/1183 d'identitat digital europea: els estats membres han d'oferir una cartera EUDI a ciutadans, residents i empreses (termini: desembre de 2026); menys d'un terç dels estats compleixen avui el llistó de preparació (observatori 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 producte (signatura amb vídeo-selfie: «la signatura més forta de l'app» — la càmera frontal grava mentre signes, parpelleig i dos reptes de vida aleatoris (girar el cap, somriure, inclinar-lo) en menys de 60 segons, verificació biomètrica del dispositiu obligatòria amb PIN com a alternativa, signatura manuscrita, 2 crèdits i dues transaccions; certificat dedicat amb el document, la signatura, l'evidència en vídeo i les dues transaccions; només una persona a l'enquadrament; certificat amb SHA-512, segell RFC 3161/eIDAS, àncora a la blockchain pública, QR i verificació forense amb integritat del dispositiu i attestation de maquinari; paquet .asice ETSI verificable fora de línia sense confiar en el fabricant; els fitxers romanen al dispositiu — només l'empremta viatja; la prova de vida confirma «una persona real i present» en signar). Vegeu els capítols 13 i 15; la suplantació de directius i la regla «sense segell, no hi ha pagament», al capítol 87; qui contractes en remot, al capítol 91; el compromís i revelació, als capítols 45 i 46; la persona única de la participació, al capítol 108. ↩

Informació que mou mercats: qui ho ha dit, i quan ho va dir

«El Rumor: cap altre mal no és més veloç; es nodreix del moviment i, tot anant, guanya forces.»

— Virgili, Eneida, IV, 174-175

El 10 de novembre de 2022, a la 1:36 de la tarda, un impostor amb el segell de «verificat» de Twitter Blue de **8 dòlars** (@EliLillyandCo, amb el logotip de Lilly) va publicar: «Estem encantats d'anunciar que la insulina ara és gratuïta». L'acció real d'**Eli Lilly** va caure d'uns 368 a uns 346 dòlars en vint minuts, esborrant momentàniament uns **15.000 milions de dòlars** de valor i forçant la companyia a demanar disculpes i a remetre els inversors al seu compte autèntic, @LillyPad [1]. Sis mesos després, la mateixa mecànica va trobar un blanc més gran: el 22 de maig de 2023, la imatge generada per IA d'una explosió vora el **Pentàgon** —el cas que obria el capítol 17—, amplificada per comptes amb el segell de «verificat» que es feien passar per «Bloomberg News» (@BloombergFeed) i pel compte estatal rus RT, va fer caure l'S&P 500 al voltant d'un 0,26-0,3 % fins al mínim de la sessió —el Dow va perdre uns vuitanta punts entre les 10:06 i les 10:10— abans de recuperar-se del tot en pocs minuts, quan el cos de bombers del comtat d'Arlington i el Pentàgon van confirmar que no hi havia hagut cap explosió [2]. Va ser, segons la mateixa Bloomberg, possiblement el primer cop que una imatge d'IA movia el mercat.

Aquest capítol no parla dels comptes anuals ni de l'auditoria —que ja són el terreny del capítol 55— ni del frau publicitari del capítol 56. Aquí l'artefacte no és un balanç retrospectiu, sinó una **única revelació en directe**, una notícia o un rumor que es publica i mou el preu d'un valor en qüestió de segons. La pregunta és senzilla i brutal: en un mercat on els algorismes reaccionen a un titular en mil·lisegons, **com pot saber el mercat, a l'instant, si una «notícia» ve realment de l'emissor que diu ser-ne l'origen?** I la tesi del llibre hi encaixa directament: davant la falsificació, la prova d'existència no jutja la veritat, però fixa **qui** ho va dir i **quan**.

Una mentida més ràpida que qualsevol desmentiment

El cas de Lilly i el del Pentàgon comparteixen una arrel amb un precedent més antic i brutal. El 23 d'abril de 2013 —el «Hack Crash»— un compte piratejat de l'agència Associated Press va publicar que hi havia hagut explosions a la Casa Blanca i que el president Obama havia resultat ferit. El Dow va caure 143,5 punts i es van esborrar més de **136.000 milions de dòlars** del valor de l'S&P 500 en pocs segons, abans de corregir-se [3]. La lliçó és que els **operadors algorísmics i d'alta freqüència** llegeixen el text de les xarxes socials i hi reaccionen en mil·lisegons: molt abans que cap humà —i no diguem cap empresa— pugui desmentir-ho. L'asimetria és total; publicar una falsa revelació costa segons, mentre corregir-la depèn d'una autoritat o de la mateixa companyia que el verifiqui i el desmenteixi per un canal reconegut pel mercat.

No sempre es tracta d'una broma que es desfà en minuts. El 2025, en l'esquema d'Ostin Technology (NASDAQ: OST), vídeos *deepfake* de l'estrateg de Goldman Sachs David Kostin, d'Elon Musk i de Mark Zuckerberg, combinats amb identitats robades d'assessors registrats a la FINRA, van inflar la cotització un **1.175 %** —de 0,78 a 9,40 dòlars entre mitjan abril i finals de juny— abans d'un esfondrament del **94 % en un sol dia**. El Departament de Justícia dels EUA va presentar càrrecs per frau de valors, frau electrònic i conspiració el setembre de 2025; l'esquema hauria evaporat més de **950 milions de dòlars** [4]. Aquí el *deepfake* ja no és un titular fugaç, sinó el motor d'un *pump-and-dump* complet.

El rumor com a arma, i el frau dels canals legítims

El problema no és només la suplantació d'emissors cotitzats. És també la suplantació de qui dona **consells**. La Borsa de Bombai (**BSE**) ha hagut d'emetre avisos repetits —el 12 de gener de 2026, de nou el 8 de març, i un quart incident cap a l'abril— per vídeos *deepfake* del seu conseller delegat, **Sundararaman Ramamurthy**, donant suposats consells de borsa i prometent «beneficis extraordinaris». La borsa ha hagut d'aclarir que ni ell ni cap directiu de la BSE fa recomanacions ni gestiona grups de WhatsApp o Telegram, i ha promès accions legals [5].

I encara hi ha un tercer vector, el més inquietant per a un editor: els **canals legítims** també es poden enverinar. Un comunicat de premsa fals distribuït a través de **GlobeNewswire** va afirmar que Walmart

acceptaria la criptomoneda **Litecoin**; el preu de Litecoin va pujar més d'un **30 %** abans que Walmart ho desmentís [7]. Si fins i tot els teletips regulats —els que el mercat tracta com a autoritzats— poden vehicular una revelació falsificada, la pregunta de l'origen autèntic deixa de ser teòrica.

Què diu la llei sobre qui dissemina

El dret ja persegueix aquesta conducta, però des de l'altra punta. A Europa, el Reglament d'abús de mercat (MAR) (Reglament UE núm. 596/2014, article 12) inclou expressament dins la «manipulació de mercat» la difusió d'informació a través dels mitjans de comunicació —inclòs internet— que doni o pugui donar senyals falsos o enganyosos sobre l'oferta, la demanda o el preu d'un instrument financer, incloent-hi rumors, quan qui la difon sabia o hauria d'haver sabut que era falsa. L'article 17 del mateix MAR obliga les emissores a comunicar la informació privilegiada al públic **com més aviat millor** i per canals oficials; les esmenes de la Listing Act, aplicables des del 5 de juny del 2026, n'ajusten el règim de retard.

Als Estats Units, la Regla 10b-5 i la Secció 9(a)(2) de la Securities Exchange Act, que aplica la SEC, abasten les falses declaracions i els esquemes que mouen preus, amb càrrecs paral·lels del DOJ per frau de valors i conspiració —com en el cas Ostin. La Reg FD i el Formulari 8-K defineixen els canals legítims de la revelació corporativa: EDGAR més els teletips reconeguts (Dow Jones, Bloomberg, Business Wire, PR Newswire). En un avís conjunt del 25 de gener del 2024, la SEC, la FINRA i la NASAA adverteixen que els defraudadors poden fer servir vídeos *deepfake* per imitar el conseller delegat d'una empresa anunciant notícies falses amb la intenció de manipular el preu d'una acció [6]. Com hem vist, l'arsenal sancionador és contundent: en l'exercici 2025, la SEC va obrir 456 accions i va ordenar 17.900 milions de dòlars en sancions per manipulació de mercat i frau de revelació [8].

Per què la llei sola no salva

Cal dir-ho amb cruesa: el MAR i la Regla 10b-5 castiguen **després**, quan el mal ja s'ha fet i el preu ja s'ha mogut. Persegueixen qui difon la mentida, però no donen al mercat cap manera de saber, **en el segon en què apareix el titular**, si ve de debò de Lilly o d'un impostor de 8 dòlars. El canal legítim —EDGAR, el 8-K, el teletip regulat— és exactament el que la suplantació explota: ningú no pot comprovar, a l'instant i en línia, que aquesta piulada o aquest comunicat tinguin l'origen que diuen. La falla és d'**origen autèntic verificable**, i cap quantia de sancions a posteriori la tanca. Mentre el mercat no pugui distingir el genuí del fals en mil·lisegons, l'algorisme reaccionarà primer i preguntarà després.

La prova d'existència aplicada

És aquí on **t2p** aporta la peça que falta, no com a oracle de veritat, sinó com a **referència criptogràfica de l'article genuí**. Quan l'equip de relacions amb inversors d'un emissor —o el seu agent de presentació, o el teletip— publica un element sensible al preu (un formulari 8-K, un anunci d'informació privilegiada sota l'article 17 del MAR, una declaració del conseller delegat, un resultat trimestral, una publicació oficial a les xarxes o un vídeo), l'artefacte se segella **al dispositiu**: es calcula localment l'**empremta SHA-512** —el fitxer no surt mai—, s'embolcalla en un **segell de temps RFC 3161 conforme a eIDAS**, s'ancora a la blockchain pública i s'emet com a contenidor **.asice** verificable fora de línia. Quan un directiu apareix filmant la declaració, s'hi afegeix el **GPS forense** i una **prova de vida**. L'emissor publica l'empremta de verificació al costat del seu compte oficial i de la seva pàgina de relacions amb inversors, de manera que qualsevol periodista, borsa, regulador, *bróker* o canal algorísmic de notícies pot confirmar en mil·lisegons si una piulada, captura o comunicat «d'última hora» ve realment de la companyia —o és l'impostor: la falsa piulada de @EliLillyandCo, el fals compte de Bloomberg del Pentàgon, el vídeo *deepfake* del conseller de la BSE, les identitats robades d'Ostin. No substitueix res: s'asseu **a sota** de l'EDGAR/8-K, la Reg FD, el MAR i els teletips regulats com a **capa d'autenticitat**, i es complementa amb la procedència de contingut C2PA/SynthID dels capítols 13 i 15 —el segell prova «això ve de l'emissor», la procedència marca «això és generat per IA», i el regulador continua jutjant l'abús.

Ara el límit, amb tota la cruesa. «Escombraries a l'entrada, escombraries a la cadena»: el segell prova que un fitxer concret va ser emès per una font autenticada en un instant amb la integritat intacta; **no prova que la revelació segellada sigui veritat**, completa, legal o no manipulativa. Una empresa pot segellar a la perfecció un comunicat que sigui ell mateix una mentida —un comunicat de *pump-and-dump* segellat per la societat pantalla dels mateixos defraudadors és autèntic-però-fals—, i el segell no atura un emissor que vol enganyar ni atrapa la revelació enganyosa per omissió: això continua sent feina de la SEC, l'ESMA,

la FINRA, la vigilància de les borses i els auditors. Tampoc no fa «fallar» un rumor no segellat: només permet que els verificadors confirmin que el genuí no hi coincideix —i això depèn que els emissors segellin de debò les seves revelacions reals i que el mercat les comprovi. No demostra per si sol que un vídeo sigui real i no IA (això és C2PA/SynthID i la detecció), no avalua la materialitat ni la intenció d'ús d'informació privilegiada, i no impedeix la reacció algorísmica en mil·lisegons abans que la verificació pugui produir-se. És una capa d'autenticitat i de data certa, no un oracle de veritat.

La promesa i el perill

La promesa és oferir al mercat un **patró de referència genuí** contra el qual contrastar qualsevol còpia viral: si Lilly hagués pogut publicar l'empremta del seu comunicat real, qualsevol verificador hauria vist en un segon que la piulada de l'impostor no hi coincidís. L'emissor honest recupera el control del seu propi origen; el periodista, el *bróker* i el canal de notícies guanyen una comprovació instantània abans d'amplificar.

El perill demana els matisos de sempre. El primer, la **falsa seguretat**: «està segellat, doncs és cert» és precisament la confusió entre integritat i veritat que un *pump-and-dump* segellat explotaria. El segon, la **cobertura desigual**: si només els grans emissors segellen, l'absència de segell en una empresa petita i honesta es podria llegir, injustament, com a sospita. I el tercer, la **velocitat**: mentre la verificació no estigui integrada de manera nativa als canals de notícies algorísmics, el segell arribarà tard per a la primera onada de mil·lisegons. La prova d'existència és una capa d'autenticitat, no un substitut del judici humà ni regulador.

A més, el fet que el segell de prova d'existència es converteixi en una font de dades massives per a models predictius genera un risc de **poder sobre la conducta col·lectiva**. Cada vegada que una entitat pot anticipar quins continguts seran considerats autèntics o falsos, adquireix la capacitat d'influir —o fins i tot de modelar— les decisions dels usuaris abans que aquests actuïn. Com avisa Carissa Véliz, «tot intent de predir el comportament humà és també un intent de controlar-lo, cosa que, en el seu extrem, condueix a l'autoritarisme»[11]. Si els algoritmes que processen les empremtes es concentren en mans d'unes poques corporacions o governs, la informació sobre quins missatges són «verificats» pot ser utilitzada per restringir la llibertat d'expressió i imposar narratives oficials. Per això, el disseny del registre ha de garantir una arquitectura descentralitzada i transparent, amb mecanismes de governança que impedeixin l'acumulació de poder predictiu en cap entitat única, assegurant que la capa d'autenticitat continuï servint a la confiança col·lectiva i no a la vigilància autoritària.

És hora d'actuar

Per als **emissors i els seus equips de relacions amb inversors** (com Lilly després del seu propi cas): segellar cada revelació sensible al preu en el moment d'emetre-la i publicar-ne l'empremta al costat del compte oficial. Per a les **borses i els reguladors** (SEC, ESMA, FINRA, BSE, SEBI): reconèixer l'origen segellat com a senyal de verificació i integrar-ne la comprovació a la vigilància de mercat. Per als **teletips regulats** (Business Wire, PR Newswire, GlobeNewswire): segellar a l'origen cada comunicat per tancar la bretxa que va permetre el frau Walmart-Litecoin. Per als **mitjans i els canals algorísmics de notícies** (Bloomberg, Dow Jones, agregadors): comprovar l'empremta abans d'amplificar un titular «d'última hora». I per als **bròkers i les plataformes** (X i la resta de xarxes on neix el rumor): exposar l'estat de verificació al costat del contingut financer, perquè el segell blau de 8 dòlars no torni a confondre's amb una font autoritzada.

Com hem vist el 22 de maig, una imatge que no mostrava res real va moure l'S&P 500 abans que ningú pogués desmentir-la. Oferir al mercat una manera de comprovar, en el mateix segon, qui ho ha dit i quan ho ha dit —sense pretendre mai que el segell digui si és veritat— és, en aquest front on els mil·lisegons valen milions, **time2act**.

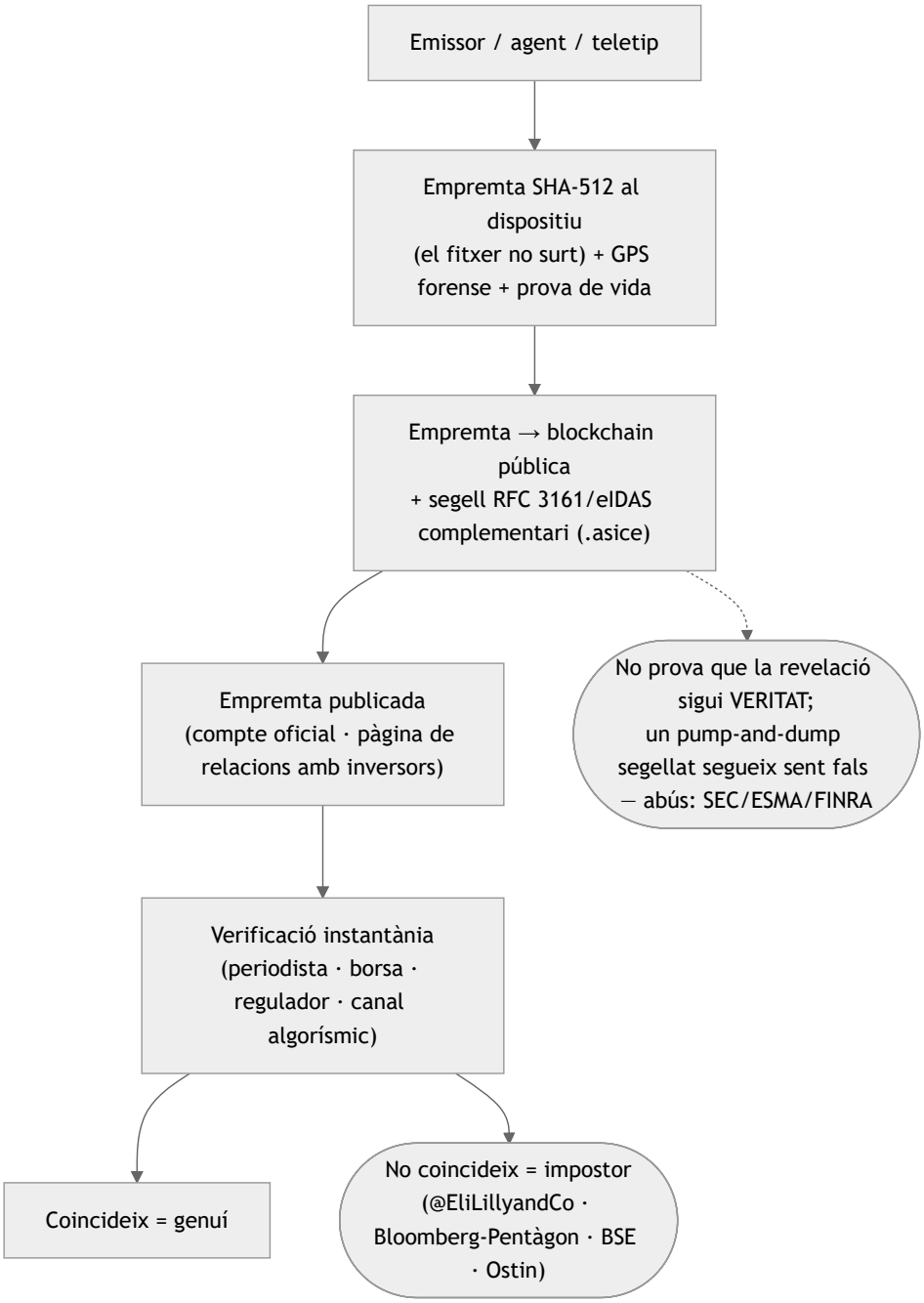


Figura 89.1 — L'emissor (o el seu agent o teletip) segella la revelació sensible al preu en el moment d'emetre-la: empremta SHA-512 al dispositiu → blockchain pública, amb segell de temps RFC 3161/eIDAS complementari (.asice), amb GPS forense i prova de vida si hi ha un directiu filmant. L'empremta es publica al costat del compte oficial; qualsevol periodista, borsa, regulador o canal algorísmic confirma en mil·lisegons si una piulada o comunicat «d'última hora» coincideix amb el genuí (Lilly, Pentàgon-Bloomberg, BSE, Ostin) o és l'impostor. Límit: el segell prova qui ho va emetre i quan, no que la revelació sigui veritat; un comunicat de pump-and-dump segellat continua sent fals, i la manipulació continua sent feina de la SEC/ESMA/FINRA i les borses. Fonts: cas Eli Lilly; imatge falsa del Pentàgon; Hack Crash de 2013; cas Ostin Technology; avís 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; caiguda de ~368 a ~346 $; ~15.000 M$ esborrats; disculpa de l'empresa i compte @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 maig 2023; difosa per comptes verificats inclòs un fals Bloomberg; breu caiguda de l'S&P 500; desmentida pels bombers d'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; piulada piratejada d'AP; Dow −143,5 punts; >136.000 M$ esborrats en segons; reacció algorísmica i d'alta freqüència). 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; identitats robades d'assessors FINRA; inflació del 1.175 %; caiguda del 94 % en un dia; acusació del DOJ el set. 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 conseller delegat Sundararaman Ramamurthy; incidents recurrents gener-abril; promesa d'accions legals). 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 gen. 2024; avís explícit sobre vídeos *deepfake* de consellers delegats per «manipular el preu d'una acció»). https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/artificial-intelligence-fraud ↩

[7] PRNEWS — *Hoax Releases Hit Newswire Services* (comunicat fals Walmart-Litecoin via GlobeNewswire; Litecoin +30 %; angle d'autenticació dels teletips). https://www.prnewsonline.com/hoax-releases-hit-newswire-services/ ↩

[8] Sidley Austin — *SEC Enforcement FY2025 Results Signal Shift in Priorities* (456 accions; 17.900 M$ ordenats; ajustat 1.400 M$ + 1.300 M$; prioritat a la manipulació de mercat i el frau de revelació). 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* (difusió d'informació falsa o enganyosa i de rumors a través dels mitjans i internet com a manipulació de mercat). https://lexparency.org/eu/32014R0596/ART_12/

[10] FINRA — *Artificial Intelligence (AI) and Investment Fraud* (versió de la FINRA de l'avís; llenguatge sobre vídeos *deepfake* de consellers delegats i notícies falses per moure el preu d'una acció). https://www.finra.org/investors/insights/artificial-intelligence-and-investment-fraud

[11] Carissa Véliz — *Prophecy: Prediction, Power, and the Fight for the Future* (2025). ↩

Titularitat real: qui és la persona de carn i ossos darrere de l'empresa

«El respecte va lligat als noms. L'anonimat i el respecte s'exclouen mútuament.»

— Byung-Chul Han, In the Swarm (2017)

El 3 d'octubre de 2021, el **Consorci Internacional de Periodistes d'Investigació** (ICIJ) va publicar els **Papers de Pandora**: una filtració de **11,9 milions de documents** —2,94 terabytes— procedents de **catorze** despatxos de serveis *offshore*. A dins hi havia els veritables amos de més de **30.000 societats** i més de **29.000 titulars reals** ocults darrere de cadenes de societats pantalla, fideïcomisos i fundacions repartides per més de dos-cents països. Els fitxers van assenyalar **35 caps d'estat i de govern** en actiu o passats i més de **330 polítics**, entre ells el rei Abdal·là II de Jordània, l'aleshores primer ministre txec Andrej Babiš i els presidents de Kenya, l'Equador i el Gabon, a més de més de **130 milmilionaris** —46 d'ells oligarques russos [1]. Arribava cinc anys després dels **Papers de Panamà** de l'abril de 2016 —11,5 milions de documents d'un sol despatx, Mossack Fonseca, que va tancar el 2018 [2]— i identificava aproximadament el doble de titulars reals. El fil comú: l'amo que figurava al paper, un administrador fiduciari o una capa de societats anònimes, gairebé mai era el titular real últim, i cap registre de l'època podia provar **qui** era aquesta persona, **en quin moment** havia pres el control, ni si la declaració de propietat era **autèntica**.

Aquest capítol no tracta el contracte públic del capítol 43 —licitacions i adjudicacions— ni la factura del capítol 54 —el frau documental en el comerç—, sinó allò que hi ha **aigües amunt** de qualsevol operació: provar el **titular real últim** que hi ha darrere de la persona jurídica, sigui el que sigui que aquesta empresa compri, vengui o financi després. La pregunta és quirúrgica: com fixem **qui** declara ser l'amo, **què** declara i **quan**, de manera que la declaració no es pugui retrodatar ni manipular en silenci? És la tesi del llibre aplicada al cor de l'opacitat societària: la prova d'existència no descobreix el secret, però impedeix negar després el que es va declarar abans.

Una arquitectura de secret que sobreviu a totes les filtracions

Els Papers de Pandora no van ser una anomalia, sinó una confirmació. Cap d'aquelles societats era il·legal en si mateixa; el que les feia perilloses era que ningú no podia provar **qui** s'amagava darrere. Deu anys després dels Papers de Panamà, el balanç és alliçonador: les investigacions fiscals havien recuperat uns **1.360 milions de dòlars** i havien desencadenat reformes profundes —la Corporate Transparency Act nord-americana, els registres de titularitat real de la UE, el Registre d'Entitats Estrangeres del Regne Unit —, i tot i així Transparency International conclou amb cruesa que «**l'arquitectura fonamental del secret *offshore* roman intacta**» [3]. La raó és estructural: cada reforma ha demanat **declarar** qui és l'amo, però gairebé cap ha pogut **verificar-ho** ni **datar-ho** de manera inalterable.

El frau no és, doncs, només l'omissió: és la **declaració falsa**. Un cleptòcrata posa un testaferro al capdavant, interposa un fideïcomís a una jurisdicció opaca, i el registre nacional recull obedientment un nom que no és el seu. Quan finalment salta una filtració —Panamà, Paradís, Pandora—, el dany ja fa anys que corre, i la pregunta judicial sempre és la mateixa: aquesta declaració, era així el dia que es va presentar, o s'ha retocat després? Sense una àncora temporal independent, la resposta depèn d'un registre que el mateix declarant, o un funcionari complaent, pot haver modificat.

Registres que es declaren sols i no es comproven

El problema tècnic té un nom: **autodeclaració sense verificació**. Open Ownership, l'autoritat de referència en dades de titularitat real, és contundent: la majoria de registres es basen en dades que el mateix obligat declara, i **sense verificació** —comprovacions de conformitat, contrastos creuats i revisió de l'evidència de suport— els registres permeten introduir informació falsa i estructures de testaferro que oculten el control real [11]. Un camp de base de dades, mutable i sense segell, no és una prova; és una afirmació.

Les xifres del desplegament ho il·lustren. La **Corporate Transparency Act** nord-americana estimava de partida unes **32 milions** de societats obligades a informar, més uns 5 milions de noves cada any; el novembre de 2024 només se n'havien presentat 6,5 milions [5]. I el març de 2025 una norma provisional

de la **FinCEN** va capgirar tot el règim: va exonerar **totes** les societats domèstiques nord-americanes i les persones nord-americanes, i va reduir la població coberta d'uns 32 milions a **menys de 12.000** entitats —les estrangeres [4]. El registre més ambiciós del món, abans de consolidar-se, va quedar pràcticament buit. A Europa, mentrestant, la sentència del **Tribunal de Justícia de la UE** del 22 de novembre de 2022 va invalidar l'accés públic general als registres de titularitat real per ser una «**ingerència greu**» en els drets a la vida privada i a la protecció de dades (articles 7 i 8 de la Carta): l'accés queda limitat ara a autoritats, subjectes obligats i qui acrediti un interès legítim [6]. El resultat és un mosaic on les dades existeixen, però la seva **fiabilitat** i la seva **accessibilitat** continuen en disputa.

Una marea regulatòria que demana exactitud

La resposta normativa de 2024-2027 és la més ambiciosa de la història en aquest front. A Europa, el **Reglament (UE) 2024/1624** —el codi únic antiblanqueig (AMLR)— s'aplicarà directament als 27 estats des del **10 de juliol de 2027**, i la nova **Autoritat de Lluita contra el Blanqueig (AMLA)**, amb seu a Frankfurt, és operativa des de l'**1 de juliol de 2025**; el seu mandat inclou registres de titularitat real **interoperables** a escala de la UE [7]. Al Regne Unit, l'**Economic Crime and Corporate Transparency Act 2023** ha començat a desplegar des del **18 de novembre de 2025** la **verificació d'identitat obligatòria** per a administradors i persones amb control significatiu; només entre el març de 2024 i el març de 2025, Companies House va retirar informació falsa o enganyosa que afectava **100.400 societats** i va rebutjar més de **10.200 sol·licituds sospitoses** [8]. Als Estats Units, el **16 de desembre de 2025** l'**Onzè Circuit**, a *National Small Business United v. Treasury*, va esdevenir el tribunal nord-americà de més rang en confirmar la constitucionalitat de la CTA, tot i que la norma de març limita el seu abast pràctic [9]. I per damunt de tot, la **Recomanació 24** del **GAFI**, revisada al març de 2022, exigeix a cada país garantir que les autoritats competents disposin d'informació de titularitat real **adequada, exacta i actualitzada** mitjançant un enfocament multidimensional, inclòs un registre o mecanisme equivalent [10]. Tota aquesta arquitectura demana una cosa que els documents en paper no donen per si sols: **exactitud verificable i datada**.

Per què el registre sol no salva

Cal dir-ho sense embuts: un registre de titularitat real, per molt obligatori que sigui, **és tan fiable com la voluntat de qui l'omple i la capacitat de qui el comprova**. Una entrada de base de dades es pot editar; una declaració presentada avui es pot retrodatar demà sense deixar rastre; i un funcionari pot acceptar un nom que sap fals. El cas de la FinCEN ho demostra a la inversa: un règim sencer es pot buidar amb una norma administrativa, i les dades que quedaven deixen de ser comparables amb les d'ahir. Un PDF de declaració de titularitat és un PDF. El que falta no és el formulari ni la llei que l'exigeix —tots dos ja existeixen—, sinó una **àncora inalterable que fixi qui va declarar què, i en quin instant exacte**, de manera que ni el declarant ni el custodi del registre puguin alterar-ho a posteriori sense que es noti.

La prova d'existència aplicada

És aquí on **t2p** aporta la capa que falta, i ho fa sobre l'artefacte de la declaració, no sobre l'estructura societària que mai veurà. Quan un titular real, un administrador o un proveïdor de serveis societaris presenta o actualitza una declaració de titularitat real, el segell lliga **aquella declaració concreta i la seva evidència** a un punt fix en el temps i en la identitat. En presentar-la, el document de declaració més la prova subjacent —l'extracte del registre d'accionistes, l'escriptura del fideïcomís, la divulgació de l'acord de testaferro, la pàgina del passaport o del DNI, i una **prova de vida** del declarant capturada al terreny— es calcula amb una **empremta SHA-512 al dispositiu** del declarant; l'empremta rep un **segell de temps RFC 3161 conforme a eIDAS** i s'ancora a la blockchain pública, produint un contenidor **.asice** verificable fora de línia. Quan una persona real afirma el control —l'humà de carn i ossos darrere de la societat pantalla—, la captura de camp afegeix **GPS forense** i prova de vida, que demostren que un humà viu, no una *deepfake* ni una foto reciclada, va fer l'atestació en aquell lloc i en aquell moment.

Això complementa els registres i els règims de verificació —la BOI de la FinCEN, els registres interoperables de l'AMLR/AMLA, la verificació d'identitat de Companies House, la R.24 del GAFI— sense substituir-los: el registre continua custodiant i divulgant les dades, i el guardià continua filtrant-les, però ara cada declaració porta un rebut a prova de manipulació i comprovable de manera independent que

indica qui va declarar què, quan, i que la declaració i la seva evidència no s'han alterat des d'aleshores. Això converteix una entrada de base de dades autodeclarada i mutable en una atestació segellada i a prova de tribunal, i fa detectable la retrodatació silenciosa o la manipulació posterior d'un registre de propietat. És el complement, sobre l'acte de declarar, del que els capítols 13 i 15 proposen sobre la procedència del contingut amb C2PA: allà se segella el que es produeix; aquí, qui declara ser l'amo.

Ara el límit, amb tota la cruesa, perquè aquí enganyar-se faria mal. «Escombraries a l'entrada, escombraries a la cadena»: el segell prova l'acte de declarar, qui el va fer, quan, i que la declaració i l'evidència adjunta són inalterades; **no prova que la persona declarada sigui el titular real últim**. Un cleptòcrata pot plantar-se davant la càmera, superar la prova de vida i segellar una atestació perjura que nomena un testaferro, o ometre completament el fideïcomís ocult, i el segell datarà fidelment la mentida. No pot travessar una cadena de societats estrangeres que no veu mai, ni detecta un acord de testaferro, ni sap si un registre d'accionistes notariat ja és fals a l'origen. No verifica els documents d'identitat contra les autoritats emissores, no avalua si l'estructura serveix per blanquejar o evadir sancions, i no protegeix el registre central d'una bretxa posterior —com va mostrar la intrusió de pirates estatals al Tresor i a la FinCEN al desembre. El segell és una capa d'integritat i procedència per a cada declaració; la veritat substantiva de la propietat depèn encara de la verificació del registre, la diligència del guardià, el periodisme d'investigació, l'intercanvi transfronterer de dades i el judici humà, cap dels quals substitueix.

La promesa i el perill

La promesa és tornar als registres allò que avui falta: que cada declaració de titularitat sigui **datada, atribuïble i a prova de tribunal**. Quan torni a saltar una filtració com Pandora, ja no es podrà fingir que mai es va declarar el que es va declarar; el periodista, el fiscal i l'autoritat tindran un rebut inalterable de qui va dir què i quan. En un món on un nom al paper viatja sense cap garantia, fer l'origen de la declaració inalterable protegeix tant l'investigador honest com el ciutadà.

El perill demana els matisos de sempre. Primer, no confondre **integritat amb veritat**: una declaració falsa i segellada continua sent falsa, i ara, a més, immutable; el segell podria donar una falsa tranquil·litat —«està ancorat, doncs és cert»— que no es correspon amb res. Segon, la **privacitat**: després de la sentència del TJUE, segellar declaracions no pot convertir-se en una excusa per exposar dades personals més enllà de l'interès legítim; l'empremta s'ancora, no les dades. Tercer, la **concentració**: si només els grans proveïdors de serveis societaris poden segellar amb solvència, l'estàndard podria expulsar les jurisdiccions i els actors petits en lloc d'enfortir-los. La prova d'existència és una capa de governança de la declaració, no un certificat de propietat veritable ni un substitut de la diligència que sap auditar una estructura.

A més, cal reconèixer que la mateixa infraestructura immutable pot esdevenir una arma de **lock-in** corporatiu si no s'instauren mecanismes d'obertura i interoperabilitat. Quan les grans plataformes controlen els protocols de segellatge, qualsevol canvi o migració a un entorn competidor requereix reescriure tot l'historial —un cost prohibitiu que consolida la seva dominància. Carissa Véliz avisa que «els gegants tecnològics d'avui poden aconseguir blindar (lock-in) la seva posició»[12], i aquest escenari es materialitza quan les autoritats reguladores no imposen normes de portabilitat o formats oberts. El risc queda agreujat pel precedent del 2025, com hem vist, en què FinCEN va eximir les empreses estatunidenques de declarar la titularitat real, buidant el registre i deixant l'estructura de confiança a mans d'un nombre reduït d'entitats privades[13]. Sense garanties explícites contra aquest encadenament, la transparència registral podria retrocedir, convertint-se en una capa que reforça la concentració en lloc d'alçar els actors més petits.

És hora d'actuar

Per als registres mercantils i les autoritats (FinCEN, AMLA, Companies House): exigir que cada declaració de titularitat real arribi amb una empremta segellada i datada, perquè la retrodatació i la manipulació silenciosa siguin detectables. Per als proveïdors de serveis societaris i els subjectes obligats (despatxos, notaris, bancs): segellar la declaració i la seva evidència de suport en el moment de presentar-la, no després, i conservar el contenidor .asice com a part de la diligència deguda. Per als legisladors i el GAFI: reconèixer la declaració segellada com a prova de l'exactitud i l'actualització que la Recomanació 24 ja exigeix, i tractar la data certa com la diferència entre una declaració i una coartada fabricada posteriorment. Per als periodistes d'investigació i la societat civil (ICIJ, Open Ownership, Transparency

International): poder confrontar la declaració actual amb la versió segellada el dia zero, perquè l'edició silenciosa deixi de ser invisible. I per als declarants honestos: assumir la prova de vida i el GPS forense com a elements que els distingeixen del testaferro que es nega a posar la cara.

Com hem vist el 2021, onze milions de documents van revelar el que cap registre podia provar: qui hi havia, de debò, darrere de trenta mil empreses. Donar a cada declaració de titularitat un rebut segellat de qui la va fer, què va dir i quan —sense oblidar mai que el segell no fa veritable el que s'hi declara— és, en aquest front on s'amaga la propietat del món, time2act.

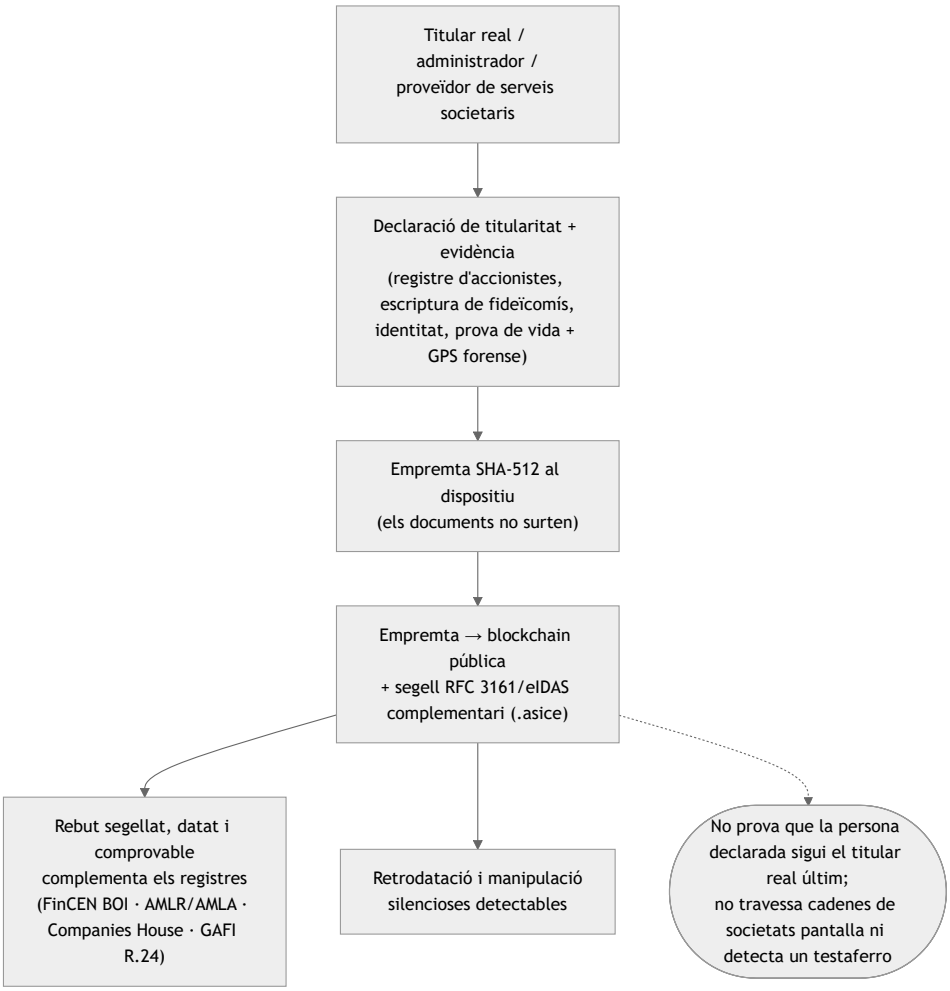


Figura 90.1 — El titular real, l'administrador o el proveïdor de serveis societaris presenta la declaració i la seva evidència (registre d'accionistes, escriptura de fideïcomís, identitat, prova de vida amb GPS forense al terreny); es calcula l'empremta SHA-512 al dispositiu —els documents no surten— i s'ancora l'empremta a la blockchain pública, amb segell RFC 3161/eIDAS complementari (.asice). El rebut complementa els registres (FinCEN BOI · AMLR/AMLA · Companies House · GAFI R.24): prova qui va declarar què i quan, i fa detectable la retrodatació. Límit: el segell no prova que la persona declarada sigui el titular real últim; no travessa cadenes de societats pantalla ni detecta un testaferro. Fonts: Papers de Pandora (ICIJ); Papers de Panamà; Transparency International; FinCEN; CJUE C-37/20 i C-601/20; GAFI R.24; Open Ownership.

---

[1] ICIJ — *About the Pandora Papers investigation* (3 d'octubre de 2021; 11,9 milions de documents, 2,94 TB, 14 proveïdors, 29.000+ titulars reals, 35 líders i 330+ polítics). https://www.icij.org/investigations/pandora-papers/about-pandora-papers-investigation/ ↩

[2] Wikipedia — *Panama Papers* (3 d'abril de 2016; 11,5 milions de documents de Mossack Fonseca, 214.488 entitats, 150 investigacions a 79 països, tancament el 2018). https://en.wikipedia.org/wiki/Panama_Papers ↩

[3] Transparency International — *Panama Papers: 10 years on* (~1.360 M USD recuperats; reformes CTA, registres UE, ROE; «l'arquitectura del secret offshore roman 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 març de 2025; exoneració de societats domèstiques; població coberta < 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* (estimació original de 32 M de societats obligades; 6,5 M presentades el novembre 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* (sentència del TJUE de 22 de novembre de 2022; invalidació de l'accés públic; marc d'interès legítim). 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 Frankfurt operativa des de l'1 de juliol de 2025; AMLR (UE) 2024/1624 aplicable el 10 de juliol de 2027; registres 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; verificació d'identitat d'administradors i PSC; 100.400 societats afectades, 10.200+ sol·licituds rebutjades). 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 desembre de 2025; tribunal de més rang a confirmar la constitucionalitat de la CTA). https://us.transparency.org/news/unanimous-eleventh-circuit-decision-upholds-the-corporate-transparency-act/ ↩

[10] FATF — *Beneficial Ownership* (Recomanació 24 revisada el 2022 i guia de 2023; informació adequada, exacta i actualitzada; enfocament multidimensional). https://www.fatf-gafi.org/en/topics/beneficial-ownership.html ↩

[11] Open Ownership — *Verification of beneficial ownership data: Overview* (les dades autodeclarades necessiten verificació: conformitat, contrastos creuats, evidència de suport). 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 ↩

Identitat laboral: qui contractem de debò en remot

«L'home és qui és menys quan parla en nom propi. Dona-li una màscara i et dirà la veritat.»

— Oscar Wilde, «The Critic as Artist» (1891)

El juliol de 2024, **KnowBe4** —una empresa nord-americana de formació en ciberseguretat— va contractar un enginyer de programari remot per al seu equip d'informàtica interna sense saber que, a l'altra banda de la pantalla, hi havia un operatiu nord-coreà. El candidat havia fet servir la **identitat robada d'un ciutadà dels EUA real** i una foto d'estoc retocada amb IA perquè quadrés amb el retrat de la sol·licitud; amb això va superar **quatre entrevistes per videoconferència**, una verificació d'antecedents i la comprovació de referències. El 15 de juliol, hores després que el portàtil corporatiu arribés a la seva adreça, l'**EDR** de l'empresa va detectar intents de càrrega de programari maliciós; el centre d'operacions de seguretat va aïllar la màquina a les 22.20 i, amb Mandiant i l'FBI, va establir que el suposat empleat era un actor d'estat-nació que operava per VPN des de Corea del Nord o la Xina i que el portàtil havia anat a parar a una **«granja de portàtils» mula** en sòl nord-americà. No es va perdre cap dada, però el conseller delegat, Stu Sjouwerman, va publicar l'incident el 23 de juliol com a advertència: contractar, i no només iniciar sessió, ja és una superfície d'atac d'identitat [1].

Aquest capítol no tracta la identitat digital del ciutadà —la credencial fundacional, governamental, que aborda el capítol 47—. Aquí parlem de la **relació laboral**: la contractació, l'entrevista, la verificació d'identitat, l'*onboarding* i la continuïtat del treball en remot. La pregunta és concreta: com demostrem que **la mateixa persona verificada** va ser present a l'entrevista, a la prova d'identitat i al lliurament de credencials i del portàtil —i que qui avui té accés és, encara, aquella persona—? És la tesi del llibre aplicada al moment exacte en què una empresa decideix donar les claus de casa a un desconegut.

Contractar ja és una superfície d'atac

El cas de KnowBe4 no és anecdòtic; és el patró. El **24 de juliol del 2025**, el Departament de Justícia dels EUA va condemnar **Christina Marie Chapman**, de 50 anys, de Litchfield Park (Arizona), a **102 mesos de presó** per haver gestionat des de casa una «granja de portàtils» que va permetre a treballadors informàtics nord-coreans fer-se passar per ciutadans dels EUA en **309 empreses** nord-americanes i dues estrangeres, usant **68 identitats robades** i generant més de **17 milions de dòlars**. Allotjava els portàtils corporatius a casa seva i en va enviar **49 a l'estranger**, inclosa una ciutat xinesa a la frontera amb Corea del Nord [3].

L'escala del frau continua augmentant. En una acció coordinada del DOJ del **14 de novembre del 2025**, es va establir que facilitadors basats als EUA i a Ucraïna havien ajudat treballadors informàtics de la RPDC a obtenir feina remota fraudulenta en **més de 136 empreses** nord-americanes, comprometent més de **18 identitats** reals i generant més de **2,2 milions de dòlars** per al règim [4]. I no és un fenomen marginal: l'FBI, en l'alerta I-012325-PSA del **23 de gener del 2025**, va confirmar que els treballadors nord-coreans fan servir **IA i tecnologia de canvi de cara** durant les entrevistes en vídeo per ofuscar la identitat, i que han virat cap a l'**extorsió** dels antics ocupadors, segrestant codi i dades propietàries [2].

La porta del davant: l'entrevista i l'*onboarding*

El que abans era una formalitat —veure la cara del candidat per pantalla— s'ha convertit en el punt cec. **Gartner** prediu que, al **2028**, una de cada quatre sol·licituds (25 %) serà falsa, impulsada per *deepfakes*, síntesi de veu i *chatbots*; l'enquesta indica que un **6 %** dels candidats admeten haver fet trampes d'estil suplantació a l'entrevista [5]. La detecció de veu ho confirma des de l'altre costat: les dades de **Pindrop** mostren àudio generat per IA o reproduït en aproximadament **1 de cada 106** reunions monitorades, amb l'activitat de *deepfakes* multiplicada gairebé **13 vegades (un 1.300 % interanual)** i les veus sintètiques arribant al **0,33 %** de les trucades als centres de contacte al quart trimestre, un 173 % més que al primer [7].

Els responsables de selecció ja ho viuen com la principal amenaça. Segons un estudi del gener de 2026, el **69 % dels líders de contractació del Regne Unit** identifiquen la suplantació amb IA i les *deepfakes*

com l'amenaça emergent més sofisticada per a la integritat de la selecció (First Advantage); **Checkr** va trobar que un **23 %** de les empreses van detectar frau d'identitat entre noves incorporacions, i l'informe de **Greenhouse** indica que el **91 %** dels responsables de selecció dels EUA havien trobat o sospitat respostes d'entrevista generades per IA [6]. El frau ja no comença al *login*: comença a la primera videotrucada. El handshake de vida que blinda la videotrucada mateixa es descriu al capítol 88; aquí ens ocupa la cadena sencera de la contractació.

El marc regulador

La resposta institucional s'està construint. Com hem vist al juliol de 2025, el NIST va publicar la versió final de les SP 800-63-4 Digital Identity Guidelines, que defineixen els nivells de garantia d'identitat (IAL1/2/3) i una nova taxonomia de verificació —Remot No Atès, Remot Atès (per exemple, una sessió de vídeo), Presencial No Atès (quiosc) i Presencial Atès (en persona)—, un marc al qual les empreses poden mapar el rigor de la verificació d'identitat de l'onboarding [8]. L'FBI, en la mateixa alerta i a les seves pàgines de cerca i recomanacions sobre els «treballadors informàtics remots fraudulents de la RPDC», recomana implementar verificació d'identitat durant l'entrevista, l'onboarding i tota la relació laboral remota [2].

Hi ha, a més, una capa de risc legal especialment dura. Les sancions de l'OFAC contra la RPDC converteixen pagar o emprar un treballador nord-coreà sancionat en una infracció de responsabilitat objectiva: un error de contractació esdevé risc de sancions i de blanqueig, amb càrrecs de frau electrònic, robatori d'identitat agreujat i IEEPA en els casos Chapman i Jin Sung-Il. A això s'hi sumen la verificació d'elegibilitat laboral als EUA (Formulari I-9 / E-Verify), la porta legal que les identitats robades retocades amb deepfake volen burlar, i a Europa el marc eIDAS / eIDAS 2.0 i la cartera EUDI, amb els deures de transparència del Reglament europeu d'IA.

I un límit no menor: el RGPD i lleis biomètriques com la BIPA d'Illinois restringeixen quantes dades biomètriques o de prova de vida pot recollir un ocupador, cosa que obliga a un segellat que preservi la privacitat.

Per què la guia de l'FBI sola no salva

Cal dir-ho amb cruesa. KnowBe4 tenia EDR, feia entrevistes en vídeo, comprovava antecedents i referències —i tot i així va contractar l'operatiu—. Les recomanacions existeixen, però el problema és que **no deixen rastre verificable**: l'entrevista en vídeo es fa i s'oblida; el verificador d'identitat mira un document i una cara i en treu una conclusió que viu, en el millor dels casos, en una nota d'un sistema de recursos humans editable; el lliurament del portàtil és un albarà. Quan, mesos després, salta l'alarma —«la persona que vam contractar no és la que avui té accés»—, no hi ha cap registre inalterable amb què confrontar-ho: hi ha la memòria del departament de recursos humans i una pila de captures. Falta una manera de **lligar, amb data certa i sense desar dades sensibles, la mateixa persona verificada als tres moments crítics** de la contractació.

La prova d'existència aplicada

És aquí on **t2p** aporta la peça que falta, i ho fa sobre l'esdeveniment d'identitat de la contractació, no sobre una afirmació del currículum. En tres moments es pren una captura al dispositiu: (1) a l'entrevista en directe o per vídeo, una prova de vida del rostre del candidat més la declaració de consentiment parlada; (2) a la verificació d'identitat, el document d'identitat presentat i la coincidència amb un selfie; (3) a l'onboarding, una atestació signada que lliga aquella identitat provada a la persona concreta que tindrà les credencials i rebrà el portàtil. Cada captura es xifra amb **empremta SHA-512 al dispositiu** —el fitxer biomètric o de document no surt mai—, rep un **segell de temps RFC 3161 conforme a eIDAS**, s'ancora a la **blockchain pública** i s'empaqueta en un contenidor **.asice** verificable fora de línia, amb **GPS forense** i la prova de vida que registren on i quan hi era realment l'humà. El valor únic és la **continuïtat i el no-repudi**: una cadena inalterable i datada que demostra que el mateix humà verificat va ser present a l'entrevista, a la prova i al lliurament del dispositiu, de manera que una disputa posterior es comprova contra un registre segellat i no contra la memòria de recursos humans.

Això **complementa, mai substitueix**, els controls existents: conviu amb la verificació IAL2/3 del NIST 800-63, les comprovacions I-9/E-Verify, el cribratge d'antecedents, les auditories de currículums

duplicats i de telèfons o correus reutilitzats que recomana l'FBI, i la detecció de deepfakes en temps real (Pindrop, Reality Defender, la procedència C2PA/SynthID **com hem vist**).

Ara el límit, amb tota la cruesa. «Escombraries a l'entrada, escombraries a la cadena»: el segell prova que **un rostre, un document i una atestació concrets** es van capturar en un lloc i un instant per un autor i no s'han alterat des d'aleshores; **no prova que la persona sigui honesta**, ni que el document sigui realment seu i no una identitat robada d'alta qualitat, ni que no sigui un nacional sancionat, ni que no exfiltri dades demà ni munti una granja de portàtils. Una deepfake impecable o una identitat robada real que superi la prova de vida produeixen un segell perfectament vàlid d'un acte fraudulent. El contenidor garanteix la **integritat i la procedència de l'evidència d'onboarding**; no reemplaça el cribratge d'antecedents, el cribratge de sancions, la detecció de deepfakes, la verificació d'autenticitat del document ni la vigilància contínua de l'amenaça interna i el judici humà.

La promesa i el perill

La promesa és convertir la contractació remota en un acte amb **memòria verificable**: poder demostrar, davant d'un incident com el de KnowBe4, que la persona de l'entrevista, la de la prova d'identitat i la del lliurament del portàtil eren la mateixa —o, justament, descobrir que no ho eren— amb una prova que sobrevisca a la rotació del personal i a la pèrdua de correus. En un mercat on un portàtil corporatiu viatja a un desconegut sense cap rebut d'identitat, fer inalterable la cadena protegeix tant l'empresa honesta com el candidat legítim.

El perill demana matisos. El primer, no confondre **integritat amb veritat**: un segell impecable d'una identitat robada continua sent el segell d'un frau i pot generar una falsa tranquil·litat —«està ancorat, doncs és de fiar»— que no es correspon amb res. El segon, la **privacitat**: el rostre, el document i la prova de vida són dades biomètriques sensibles; el RGPD i la BIPA exigeixen que només en surti l'empremta, calculada al dispositiu, i mai un registre central de cares de candidats. El tercer, el **biaix i l'exclusió**: la prova de vida i la verificació de documents poden fallar més segons quins col·lectius o equips, i no poden convertir-se en una barrera d'accés a la feina. La prova d'existència és una capa de no-repudi de la contractació, no un certificat de confiança ni un substitut del judici de selecció.

A més a més, el perill de confiar només en un «clic» com a forma de consentiment s'amplia quan la informació que sustenta aquest acord és tan opaca i desproporcionada que l'usuari no pot comprendre realment què autoritza. En el cas del reconeixement facial de Facebook, Marc Goodman assenyala que les condicions d'ús tenen 9.300 paraules —un text tan extens que gairebé impossibilita una lectura crítica i, per tant, un consentiment autèntic i verificable [11]. Aquesta asimetria d'informació crea una bretxa legal: el candidat pot signar digitalment una autorització sense saber quins trets biomètrics s'emmagatzemen ni com es podran reutilitzar. Si la prova d'existència no inclou un mecanisme que demostri, de manera inequívoca i auditada, que l'individu ha entès i acceptat les condicions, el sistema queda exposat a reclamacions per violació del RGPD i la BIPA, i a una erosió de confiança que contraresta qualsevol benefici de la cadena immutable. Sense un consentiment verificable i comprensible, la tecnologia es converteix en una nova forma d'explotació de dades més que en una garantia de seguretat.

Una dimensió que el llibre *Reboot* posa sobre la taula és la crisi de la identitat digital quan les plataformes esdevenen mercats d'identitats fictícies. L'informe de la Fiscalia de Nova York (2021) va revelar 9,3 milions de comentaris a la FCC provinents d'usuaris inventats, gairebé tots creats per un sol jove de 19 anys, amb prop de 500.000 d'origen rus[12]. La solució proposta per Noveck —una prova de personalitat verificable que es genera íntegrament al dispositiu— complementa l'ancoratge neutral en blockchain: el registre immutable assegura que la prova no ha estat alterada, mentre que una «API personal» garanteix que només el propietari del dispositiu pot revelar la seva veu o la seva presència digital, sense cap base biomètrica centralitzada. Així es tanca el buit entre la immutabilitat de la cadena i l'autonomia de l'individu, evitant que identitats falses s'infiltrin en processos crítics i reforçant una confiança real.

És hora d'actuar

Per als **equips de recursos humans i contractació**: segellar els tres moments —entrevista, verificació d'identitat i lliurament del portàtil— perquè la continuïtat de la persona tingui data certa, sense desar mai les dades biomètriques. Per als **responsables de seguretat (CISO i SOC)**: exigir l'*.asice* d'onboarding com a part de l'expedient de l'empleat i confrontar-lo davant de qualsevol alerta d'amenaça interna, tal com va fer KnowBe4 amb l'EDR. Per als **proveïdors de verificació d'identitat i detecció de**

deepfakes (NIST 800-63, Pindrop, Reality Defender): integrar el segellat al dispositiu amb la verificació IAL2/3 i la detecció en temps real, perquè prova i detecció viatgin juntes. Per als **reguladors i l'FBI/IC3** (OFAC, eIDAS 2.0): reconèixer la cadena d'identitat segellada com a evidència de diligència deguda en la contractació remota i com a prova davant el risc de sancions. I per a les **plataformes de feina i marketplaces de talent remot**: ancorar la prova d'identitat de l'onboarding perquè una substitució —la persona contractada no és la que es connecta— sigui detectable.

A KnowBe4, un operatiu d'estat-nació va superar quatre entrevistes i una verificació d'antecedents abans que el portàtil fos delatat a les 22.20; com hem vist, donar a cada contractació remota una prova segellada que lligui la mateixa persona verificada de l'entrevista al teclat —sense oblidar mai que el segell no fa honesta la cara que hi ha al davant— és, en aquest front on contractar ja és atacar, **time2act**.

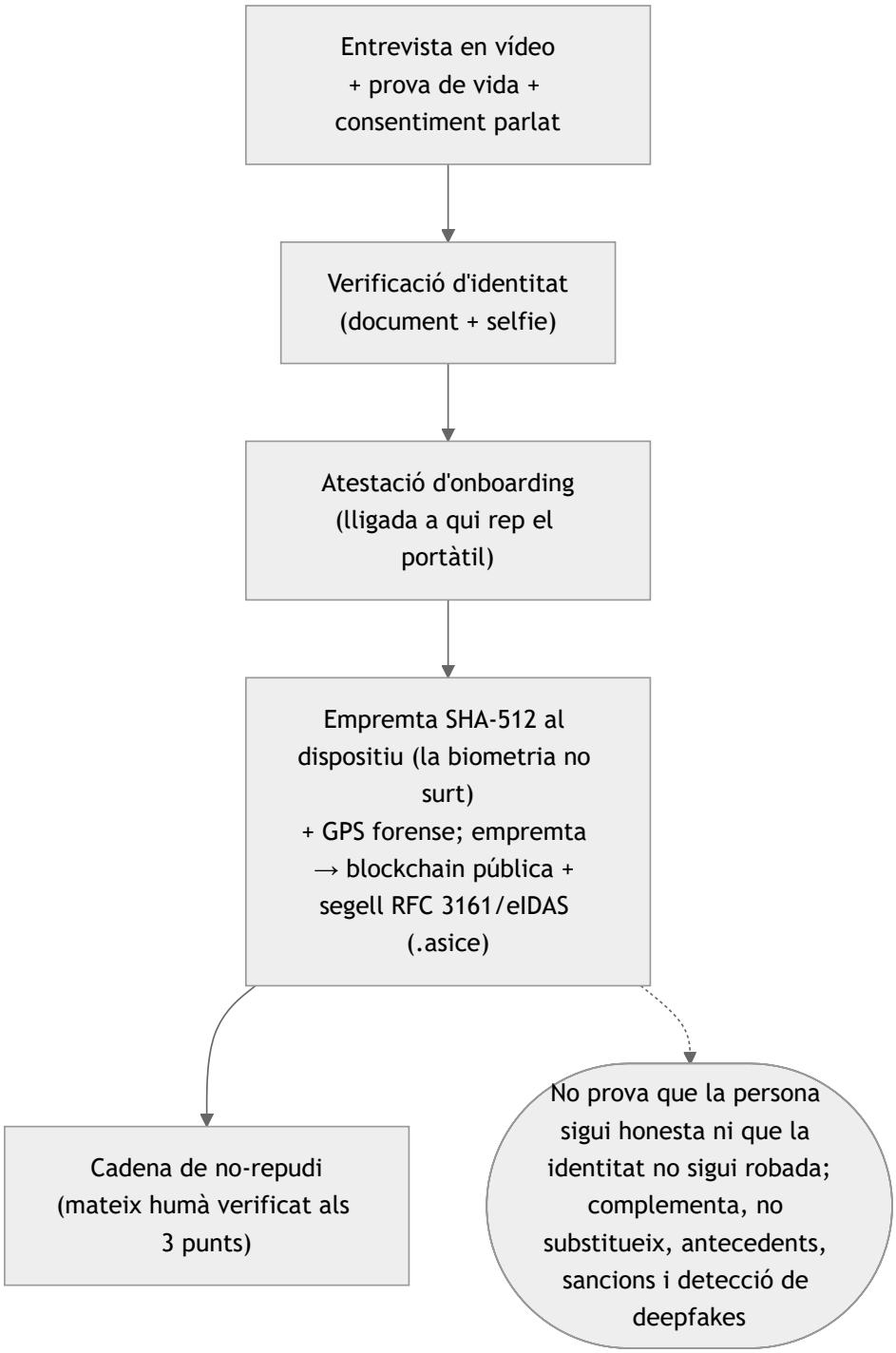


*Figura 91.1 — La contractació remota segellada en tres baules: entrevista en vídeo amb prova de vida → verificació d'identitat (document + selfie) → atestació d'*onboarding *lligada a qui rep el portàtil. A cada*

moment es calcula l'empremta SHA-512 al dispositiu (la biometria no surt), amb segell RFC 3161/eIDAS, GPS forense i ancoratge a la blockchain pública (.asice). Resultat: una cadena de no-repudi que demostra que el mateix humà verificat hi era als tres punts. Límit: el segell no prova que la persona sigui honesta, que la identitat no sigui robada ni que no sigui un nacional sancionat; complementa, no substitueix, el cribratge d'antecedents, de sancions i la detecció de deepfakes. Fonts: cas KnowBe4; cas 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; relat en primera persona: foto d'estoc retocada amb IA, quatre entrevistes en vídeo, detecció EDR del 15 de juliol de 2024, granja de portàtils 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 gener de 2025; canvi de cara amb IA a les entrevistes, gir cap a l'extorsió, recomanacions de verificació d'identitat). https://www.ic3.gov/PSA/2025/PSA250123 ↩

[3] US DOJ (USAO-DC) — *Arizona Woman Sentenced in $17M IT Worker Fraud Scheme for North Korea* (24 de juliol de 2025; Christina Chapman, 102 mesos, 309 empreses, 68 identitats robades, 17 M$, granja de portàtils, 49 portàtils enviats a l'estranger). 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 novembre de 2025; més de 136 empreses víctimes, més de 18 identitats compromeses, més de 2,2 M$ de beneficis). 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* (previsió del 25 % per al 2028; admissió del 6 % de suplantació a l'entrevista, enquesta a 3.000 candidats). 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 gener de 2026; First Advantage 69 % dels líders del Regne Unit; Checkr 23 % de frau d'identitat; 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* (àudio IA en ~1 de cada 106 reunions; ~1.300 % interanual; veus sintètiques al 0,33 % de les trucades al Q4 de 2024). https://www.pindrop.com/article/growing-trend-of-deepfakes-in-interviews/ ↩

[8] NIST — *SP 800-63-4 Digital Identity Guidelines* (final, juliol de 2025; nivells de garantia IAL1/2/3 i taxonomia de verificació Remot/Presencial × Atès/No Atès). https://pages.nist.gov/800-63-4/sp800-63.html ↩

[9] FBI — *Fraudulent Remote IT Workers from DPRK* (cerca/recomanacions; ús d'identitats robades, ordinadors intermediaris i IA, amb mitigacions per als ocupadors). 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* (credencials verificables i verificació contínua de la identitat d'*onboarding*; context de solució adjacent). 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] Fiscalia General de Nova York (2021). https://ag.ny.gov/press-release/2021/attorney-general-james-issues-report-detailing-millions-fake-comments-revealing ↩

Treball de plataforma: quan el cap és un algorisme

«...una recerca, també, de sentit diari tant com de pa diari, de reconeixement tant com de diners... d'una mena de vida en lloc d'una mena de morir de dilluns a divendres.»

— Studs Terkel, Working (1974)

Obres l'aplicació a primera hora per començar el torn i la pantalla mostra una sola línia: «Compte desactivat». Cap nom, cap telèfon, cap botó per demanar explicacions. La decisió que et costa el sou l'ha presa un sistema automatitzat, fora de la teva vista. Aquest és el punt de partida del cas conegut com a «Robo-Firing» — Drivers contra Uber i Ola —, en què un grup de conductors va haver de litigar anys, fins al Tribunal d'Apel·lació d'Amsterdam (2023), només per saber per què: el tribunal, invocant l'article 22 del Reglament General de Protecció de Dades, va estimar el seu recurs en tres sentències vinculades i va obligar Ola a explicar la lògica de la seva decisió totalment automatitzada, i Uber a donar informació significativa sobre els acomiadaments algorítmics; Uber va acabar condemnada a 584.000 euros de multes coercitives — més 4.000 euros per cada dia d'incompliment — per no complir l'ordre d'explicar-se [4]. Pensa-hi un moment: va caldre un tribunal d'apel·lació europeu i multes diàries perquè un treballador conegués el motiu del seu propi acomiadament.

Aquest capítol tracta el treball gestionat per plataformes digitals — repartidors, conductors, microtreballadors — i la relació laboral amb un cap que és un algorisme. Qui és de debò la persona que contractem en remot es tracta al capítol 91; les condicions laborals a la cadena de subministrament global, al capítol 102; què hi ha dins dels models d'IA, al capítol 79. Pregunta clau: quan el cap és un algorisme, qui aixeca acta de la relació laboral? Resposta: totes dues parts, amb evidència ancorada — el diari laboral segellat del treballador i el registre de decisions auditable de la plataforma, amb **t2p**: l'empremta SHA-512 al dispositiu, l'ancoratge de l'empremta a la blockchain pública i el segell de temps RFC 3161/eIDAS complementari dins d'un contenidor .asice [5] —, perquè els drets que Europa i Espanya ja han escrit al paper [1][2] es puguin provar als fets.

El cap que no dona la cara

Convé descriure la gestió algorítmica sense demonitzar-la. L'algorisme assigna encàrrecs en temps real, fixa tarifes dinàmiques segons l'oferta i la demanda, puntua el rendiment, ordena la cua de feina i, al límit, desconnecta. És eficient — per això existeix: sense aquesta mecànica, cap aplicació de repartiment o de transport no podria coordinar milions d'usuaris. Però l'eficiència té un cost ocult: una asimetria informativa radical.

La plataforma ho registra tot — posicions, temps de resposta, acceptacions, clics —, en registres massius que creixen cada segon. El treballador, en canvi, només veu la interfície del dia: els encàrrecs que li apareixen, la seva puntuació, la tarifa d'aquell moment. I demà la configuració pot haver canviat sense avís. Quan arriba el conflicte — davant la Inspecció de Treball, davant d'un jutge —, una part compareix amb el registre complet del sistema i l'altra amb records.

El diagnòstic ja és llei a Europa. La Directiva (UE) 2024/2831, en vigor des del 2 de desembre de 2024 i amb transposició fins al 2 de desembre de 2026, imposa transparència sobre els sistemes de seguiment i els algorismes que afecten les condicions de treball; exigeix supervisió humana de les decisions i dret a intervenció humana en les decisions importants; i prohibeix usar dades sensibles — estat emocional, biometria, converses privades — en les decisions automatitzades [1]. I estableix la peça angular: la presumpció de laboralitat quan es constaten fets que indiquen direcció i control, amb la càrrega de refutar-la sobre la plataforma [1].

Fixem-nos en la paraula decisiva: «fets». La Directiva és una màquina de convertir fets en drets. El problema és que, en aquest sector, els fets els custodia en exclusiva una de les parts. Aquest és exactament el forat que la prova d'existència tanca.

Espanya, laboratori: la Ley Rider i el cas Glovo

Espanya va arribar abans. La Llei 12/2021 — la «Ley Rider», en vigor des de l'agost de 2021 — va establir la presumpció de laboralitat per al repartiment quan l'empresa exerceix la seva organització, direcció i

control mitjançant la gestió algorítmica del servei o de les condicions de treball, i va crear un dret pioner: el comitè d'empresa ha de ser informat dels paràmetres, regles i instruccions dels algorismes que afecten les condicions de treball [2].

I el cas que va posar la llei a prova va ser Glovo. La justícia de Barcelona va obrir causa penal contra el fundador i conseller delegat, Óscar Pierre, pel model de falsos autònoms; les reclamacions per quotes no ingressades i les multes de la Inspecció de Treball sumaven uns 200 milions d'euros, i el competidor Just Eat en reclamava 295 més per competència deslleial [3]. El desenllaç va arribar entre finals de 2024 i 2025: Glovo va anunciar el pas al model laboral — entre 10.000 i 15.000 repartidors, combinant contractació directa i flotes — i Pierre va reconèixer davant la jutgessa que la regularització buscava «pau social» i evitar «discussions» amb la Inspecció, i que la pressió penal i econòmica havia forçat el canvi: «la caja no te da para operar». La matriu Delivery Hero va elevar les provisions per Glovo Espanya a entre 440 i 770 milions d'euros i va estimar uns 100 milions d'impacte en el resultat operatiu de 2025 [3].

La lliçó probatòria — que és la d'aquest llibre, no el retret polític — és aquesta: van caldre anys d'inspeccions, actes i creuaments de dades per reconstruir, des de fora i a posteriori, una realitat laboral que passava cada dia dins d'una aplicació. Cada euro de multa és també el preu d'una evidència que va costar anys d'excavar. Amb registres ancorats des del primer dia, la mateixa veritat hauria estat visible en setmanes — per a totes les parts, també per a la plataforma que hagués volgut demostrar la seva diligència.

L'acomiadament per algorisme

Tornem al «robo-firing», perquè condensa la inversió de la gramàtica laboral. En el món clàssic, l'empresari acomiada i ha de motivar; en el món de plataforma, el sistema desconnecta i és el treballador qui ha de litigar — anys, si cal [4] — només per obtenir la motivació. La Directiva europea respon generalitzant el que Amsterdam va haver d'imposar cas per cas: supervisió humana i dret a intervenció humana en les decisions importants [1].

Però fins i tot amb la motivació a la mà, queda el segon esglaó: contrastar-la. Si l'algorisme diu «vas rebutjar massa encàrrecs» o «els clients et van puntuar malament», amb què ho rebat el treballador que no té cap registre propi? La plataforma custodia les dades i el criteri; ell, ni tan sols la seva pròpia versió dels fets.

La resposta té dues meitats simètriques — i és important que siguin les dues. El treballador necessita el seu diari laboral inesborrable: la seva versió dels fets, segellada dia a dia al seu dispositiu [5]. I la plataforma necessita — per obligació legal [1][4] i per interès propi — un registre de decisions auditable: quina regla es va aplicar, sobre quines dades, amb quina revisió humana i quan. Totes dues meitats són la mateixa tecnologia; cap de les dues no pot reescriure's quan arriba el conflicte.

La prova d'existència aplicada

El mateix torn, registrat des dels dos costats de la pantalla — i cap de les dues versions no es pot reescriure.

1. El diari laboral segellat

Cada dia de feina, el treballador segella al seu dispositiu la seva jornada: hores connectat, disponibilitat, encàrrecs oferts, acceptats i rebutjats, instruccions rebudes, captures de les condicions i tarifes que l'aplicació mostrava aquell dia [5]. No és espionatge: és la seva pròpia vida laboral, documentada des del seu costat de la pantalla. El resultat és exactament allò que la presumpció de laboralitat necessita — fets datats que indiquen direcció i control [1][2] —, immune a l'argument «l'aplicació no deia això»: la captura d'aquell matí porta empremta i data certa. I si un dia arriba la desconnexió, la seva cronologia no comença de zero: ja existeix, ancorada, des del primer torn.

2. La desactivació auditable

La plataforma que decideixi — o que la llei obligui [1][4] — pot ancorar el seu registre de decisions: quan l'algorisme va assenyalar el compte, quines dades i quina regla va aplicar, quin humà ho va revisar i què va resoldre. Cada pas, empremtat i datat [5]. Davant del jutge d'Amsterdam, aquella cadena hauria estat la resposta que va costar 584.000 euros no tenir [4]; davant d'una acusació de discriminació o

d'arbitrarietat, és la defensa de la plataforma diligent; i davant del treballador, és el dret a saber — article 22 del RGPD, Directiva [1] — complert per disseny, no per sentència.

3. La inspecció que no comença de zero

El cas Glovo va exigir anys d'actes i reconstruccions per acreditar una relació laboral que l'aplicació coneixia minut a minut [3]. Amb diaris laborals segellats dels treballadors i registres de decisions ancorats de les plataformes, la Inspecció de Treball i els tribunals treballen sobre cronologies verificables des del primer requeriment: menys anys d'instrucció, menys pericials de reconstrucció, i sancions — o absolucions — assentades sobre fets amb data certa [5]. La presumpció de laboralitat [1][2] deixa de ser una batalla probatòria per esdevenir una comprovació.

4. L'algorisme amb acta

La Ley Rider dona al comitè d'empresa el dret a conèixer els paràmetres, regles i instruccions dels algorismes [2]; la Directiva imposa transparència contínua [1]. Però un document lliurat un dimarts no diu res del canvi silenciós del divendres. La solució és el versionat segellat: cada versió dels paràmetres lliurats, empremtada i datada [5], de manera que qualsevol modificació posterior sigui visible i datable. És la mateixa lògica de procedència que el llibre aplica als models d'IA al capítol 79, portada a la relació laboral: l'algorisme pot canviar, però no pot fer veure que sempre havia estat com ara.

Els límits, dits amb claredat: el segell no decideix si una relació és laboral — això ho fan les lleis i els jutges [1][2]; no obre per si sol la caixa negra de l'algorisme — això ho fan els deures de transparència [1][2] i, quan cal, els tribunals [4]; i no substitueix ni el conveni, ni el sindicat, ni la negociació col·lectiva. La prova d'existència fa exigible el dret; el dret, l'han de fer les persones.

La promesa i el perill

La promesa: treballadors que ja no discuteixen amb una pantalla muda [4]; plataformes que poden demostrar la seva diligència en lloc de pagar-la per sentència [3]; inspeccions que duren setmanes i no anys; i una presumpció de laboralitat [1][2] que s'activa amb fets datats, no amb batalles de testimonis. La gestió algorítmica, amb acta.

Els perills, amb la mateixa claredat.

El primer és **la vigilància invertida**. Seria un contrasentit tràgic que l'eina pensada per equilibrar la relació acabés justificant més monitoratge del treballador. La Directiva ja prohibeix les dades sensibles — emocions, biometria, converses privades — en les decisions automatitzades [1]; el diari laboral segellat ha de ser del treballador i per al treballador: al seu dispositiu, sota el seu control, amb revelació voluntària i revocabilitat [5]. Cap plataforma no pot exigir-lo ni accedir-hi.

El segon és **el registre esbiaixat**. Qui segella tria què segella: una plataforma podria ancorar només allò que l'afavoreix, i un treballador també. El segell acredita integritat i data, no completesa. Per això el disseny ha de ser bilateral, i els reguladors han de poder exigir a les plataformes els registres complets — recordem que els buits també queden datats [5].

El tercer és **la reputació portàtil**. Si el diari laboral segellat degenera en una «puntuació de treballador» exportable entre plataformes, haurem construït la llista negra perfecta — immutable i tot. La cronologia és per defensar drets en cas de conflicte, no per fer d'historial de conducta permanent: caducitat, revocabilitat i prohibició expressa d'usar-la com a filtre de contractació.

I el quart és **el tecnosolucionisme laboral**. Cap empremta no apuja una tarifa ni paga una cotització. Els drets del treball de plataforma van néixer de la llei [1][2], de la Inspecció [3], dels tribunals [4] i de l'organització col·lectiva; la criptografia només garanteix que, quan calgui provar, es pugui. Confondre l'eina amb la lluita seria repetir en un sector nou l'error de sempre.

És hora d'actuar

Si l'algorisme dirigeix, que quedi acta — de les seves ordres i de la teva feina.

Per als treballadors de plataforma: segella el teu diari laboral — hores, encàrrecs, instruccions, captures de condicions [5]; coneix la presumpció que t'empara [1][2]; i si arriba la desconnexió, exigeix la

motivació que Europa ja et reconeix [1][4].

Per a les plataformes: ancoreu el registre de decisions i la revisió humana [1][4][5]; el cas Glovo ensenya que la realitat acaba aflorant, i que fer-ho tard costa centenars de milions [3] — ser auditable des del primer dia és més barat que ser-ho per sentència.

Per a sindicats i comitès d'empresa: exigiu els paràmetres dels algorismes [2] amb versionat segellat [5] — la transparència sense data certa és una foto vella.

Per a la Inspecció de Treball i els jutges: demaneu i valoreu les cronologies ancorades de totes dues parts [3][5]; que la instrucció comenci amb fets datats, no amb terabytes per excavar.

Per als legisladors: en transposar la Directiva abans del 2 de desembre de 2026 [1], incorporeu el deure de registre de decisions ancorat i el dret del treballador al seu propi diari segellat — i blindeu-lo contra tot ús com a filtre reputacional.

Als conductors d'Amsterdam els va caldre un tribunal d'apel·lació i 584.000 euros en multes perquè una aplicació els digués per què els havia acomiadat [4]. Que el pròxim torn desconnectat tingui la resposta esperant-lo: datada, ancorada i exigible. Pel treball digne en l'era de l'algorisme, **time2act**.

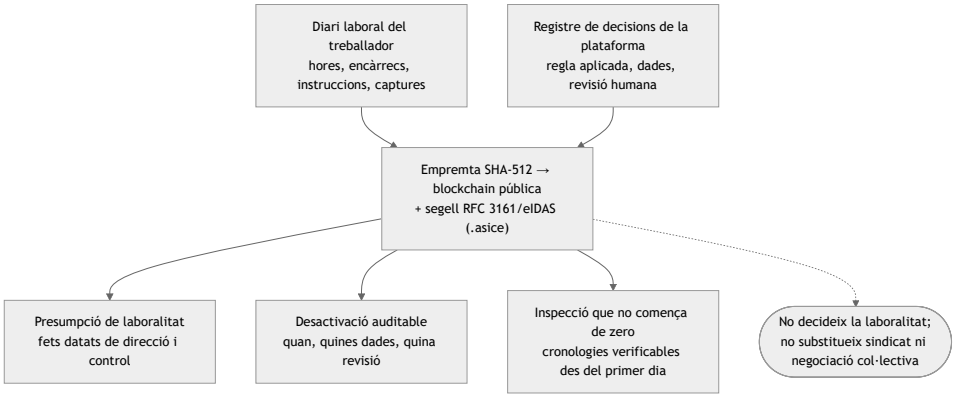


Figura 92.1 — La relació laboral de plataforma amb prova d'existència: el treballador segella el seu diari laboral (hores, encàrrecs, instruccions, captures de condicions) al seu dispositiu; la plataforma ancora el registre de decisions algorítmiques i la revisió humana (art. 22 RGPD; Directiva (UE) 2024/2831); el comitè rep els paràmetres de l'algorisme amb versionat segellat (Ley Rider). Tres sortides: la presumpció de laboralitat provada amb fets datats, la desactivació auditable i la inspecció que no comença de zero. Límits: el segell no decideix la laboralitat ni substitueix la negociació col·lectiva; el diari és del treballador, mai un filtre reputacional. Fonts: DOUE (Dir. 2024/2831); BOE (Llei 12/2021); elDiario.es (cas Glovo); Worker Info Exchange (Drivers v. Uber/Ola).

---

[1] DOUE / BOE — *Directiva (UE) 2024/2831 del Parlament Europeu i del Consell, de 23 d'octubre de 2024, relativa a la millora de les condicions laborals en el treball en plataformes* (en vigor el 2 de desembre de 2024; transposició fins al 2 de desembre de 2026; presumpció de laboralitat per fets de direcció i control amb càrrega de la prova sobre la plataforma; prohibició de dades sensibles en decisions automatitzades; transparència, supervisió humana i intervenció humana en decisions importants); 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 — *Llei 12/2021, de 28 de setembre* («Ley Rider»: presumpció de laboralitat en el repartiment mitjançant gestió algorítmica; dret del comitè d'empresa a ser informat dels paràmetres, regles i instruccions dels algorismes que afecten les condicions de treball; règim en vigor des de l'agost 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 a Barcelona; ≈200 M€ en quotes i multes; 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; provisions de Delivery Hero de 440-770 M€; impacte ≈100 M€ a l'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 sentències; Ola ha d'explicar la lògica de la decisió totalment automatitzada, art. 22 RGPD); Worker Info Exchange — *Uber ordered to pay €584,000 for failure to comply with court order in robo-firing case* (més 4.000 €/dia);

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 producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; contingut al dispositiu, revelació voluntària; els buits de la sèrie queden datats). Vegeu els capítols 13 i 15; la procedència dels models d'IA, al capítol 79. ↩

La jornada i el conflicte laboral: hores que consten

«El poder no concedeix res sense una exigència. Mai no ho ha fet i mai no ho farà.»

— Frederick Douglass, discurs de Canandaigua (1857)

Les 19:40 en un polígon industrial qualsevol. L'última comanda ha sortit tard, i el registre horari — el full de paper de la carpeta, o l'aplicació de l'empresa — marca les 18:00 en punt, com cada dia. A la cafeteria d'un centre comercial, una cambrera suma mentalment les hores que no cobrarà aquest mes. Cap dels dos gestos no farà soroll avui; tots dos pesaran el dia que hi hagi conflicte.

Les dades diuen que no són anècdotes [1]: segons l'Enquesta de Població Activa, més del 40 % de les hores extres que es fan a Espanya no es remuneren. I això amb un registre de jornada que és obligatori per a totes les empreses des del 2019. El problema no és que el registre no existeixi: és qui el custodia. El paper aguanta el que li posin; el sistema digital de l'empresa el controla l'empresa. Quan el conflicte esclata — la reclamació d'hores, la modificació de condicions comunicada de paraula, l'acomiadament que arriba just després de reclamar —, al jutjat social hi ha dues memòries i un registre de part.

Aquest capítol tracta la variable més bàsica del contracte més comú del país — i la pitjor provada. El treball governat per un cap algorísmic — repartidors, conductors — és al capítol 92; la identitat de qui contractes en remot, al capítol 91; les condicions laborals a la cadena de subministrament global, al capítol 102; l'assetjament i la tècnica de gravar converses pròpies, al capítol 75. Pregunta clau: com es discuteix la jornada quan el rellotge oficial és d'una de les parts? Resposta: amb data certa als dos costats — el diari laboral del treballador i la certificació neutral del registre oficial — mitjançant **t2p**: hash, hora i àncora — el trípode del capítol 13 [3]. I amb un context que empeny: la reforma del registre horari digital que ve exigirà exactament aquesta arquitectura.

El registre que ve: immutable per llei

La novetat legislativa [1]: el Govern va aprovar el 30 de setembre de 2025 la tramitació urgent d'un decret per al registre horari digital — desacoblat de la reducció de jornada —, amb l'objectiu d'aprovar-lo durant el 2026 (sense data d'entrada en vigor publicada encara). El que el projecte exigeix, segons la documentació pública: registres electrònics traçables i immutables; segellat de temps; registre de pauses; accés remot i en temps real per a la Inspecció de Treball; i un historial de modificacions amb autoria i data — una correcció unilateral sense coneixement del treballador es podrà considerar manipulació davant d'un tribunal [1].

Atura't en el que això significa per a la tesi d'aquest llibre — i posa-ho al costat de VeriFactu, el sistema que el capítol 34 explica: per segona vegada en pocs anys, l'Estat exigeix per norma immutabilitat, traça i data certa per resoldre un problema de confiança. Primer les factures; ara les hores. La prova d'existència ja no és una proposta: és el sentit de la marxa.

I ara, el que la reforma no dona. El registre, per immutable que sigui, viu als sistemes de l'empresa o del seu proveïdor; l'accés remot és per a la Inspecció, no per al treballador, que continua sense una còpia pròpia oposable de les seves hores. I l'empresa honesta, davant d'una acusació de manipulació, ha de provar un negatiu — que no va tocar res — amb els seus propis sistemes com a únic testimoni. La capa que falta mira els dos costats: la còpia amb data certa en mans del treballador, i la certificació neutral del registre oficial que fa el compliment de l'empresa demostrable, no només al·legable.

La prova d'existència aplicada

El conflicte laboral es guanya o es perd per fets datats; que cada part tingui els seus [3].

1. El diari laboral del treballador

Al seu dispositiu personal, el treballador segella el que l'afecta: la foto del fitxatge d'avui, la nota de les hores fetes, el torn publicat [3]. Trenta segons al final de la jornada. Només les empremtes s'ancoren; el contingut queda al seu mòbil, i no l'ha d'ensenyar a ningú — fins al dia que calgui, davant del delegat, de la

Inspecció o del jutjat social. Mesos d'entrades amb data certa pesen més que qualsevol memòria — i que qualsevol registre de part.

I una menció que aquest capítol no pot ometre: enlloc no val tant aquest diari com al treball de la llar. Les treballadores domèstiques — el contracte més informal del país: hores pactades de paraula, efectiu, sovint sense registre de cap mena — tenen en el mateix gest de trenta segons la primera evidència laboral de la seva història [3]. La dignitat d'una feina també es mesura per la seva capacitat de ser provada.

2. El fitxatge amb lloc i hora

Quan el sistema oficial «falla» — el dia que curiosament no consta, el fitxatge que algú va corregir —, la foto d'entrada i sortida amb el GPS forense de t2p — fix genuí, precisió d'uns 50 metres, antiguitat màxima d'uns 30 segons; la ubicació simulada bloqueja la certificació [3] — acredita on era el treballador i quan. El mateix val per al desplaçament que no es paga: el lloc de treball real, datat. I la línia vermella, dita aquí mateix: el moment del fitxatge, mai el seguiment continu — es documenta la jornada, no es vigila la persona.

3. El quadrant i l'ordre

El quadrant publicat, capturat amb data certa; el quadrant canviat a última hora, també; l'ordre rebuda per missatge o correu, certificada [3]. El «jo no et vaig dir això» i la modificació de condicions comunicada de paraula topen amb pantalles datades. I si la conversa és cara a cara, la gravació pròpia és lícita — la tècnica i els límits són al capítol 75.

4. El registre oficial certificat — la simetria de l'empresa

L'empresa que ho fa bé tanca cada mes el seu registre horari amb una certificació per lots: l'empremta del fitxer mensual, encadenada amb la de l'anterior [3] — la mateixa lògica que VeriFactu imposa a les factures. Davant de la Inspecció — que hi podrà accedir en remot [1] — i davant del jutjat, el seu registre no és només immutable d'ara endavant: és demostrablement no manipulat des de cada tancament. Contra la reclamació d'hores fantasma, contra l'acusació de correcció retroactiva, l'empresa honesta té dates, no al·legacions. I l'historial de modificacions que la reforma exigeix [1], ancorat, esdevé la seva coartada permanent.

Els límits, negre sobre blanc: el segell acredita hores i comunicacions — no decideix si l'hora era extra, complementària o voluntària: això ho diuen el conveni i el jutge. El diari personal del treballador no substitueix el registre legal de l'empresa — el complementa i el contrasta. I la proporcionalitat mana: cap de les dues parts no pot convertir la jornada en vigilància — ni geolocalització contínua del treballador, ni gravació ambiental de la plantilla.

La promesa i el perill

La promesa: judicis socials que discuteixen dret, no fets [1][3]; el 40 % d'hores extres impagades [1] amb una eina de reclamació a l'abast de qualsevol butxaca; empreses complidores que passen inspeccions amb registres demostrablement íntegres; i la cultura del «ja ho apuntaré» substituïda per la del fet datat — als dos costats de la nòmina.

Els perills, sense embuts.

El primer és **la vigilància disfressada de registre**. El pas del fitxatge datat al treballador rastrejat és curt i temptador. La línia legal i moral: es registra el moment — entrada, sortida, pausa —, mai el recorregut; el registre serveix la jornada, no el control de la vida.

El segon és **la desconfiança institucionalitzada**. Si cada ordre s'ha de capturar i cada torn segellar, la relació laboral es judicialitza per endavant. La resposta és la de sempre en aquest llibre: la traça és per al conflicte, no per al dia a dia — i com més verificable és el registre oficial, menys falta fa el paral·lel.

El tercer és **la bretxa del més precari**. Qui més pateix les hores impagades és qui menys eines i menys marge té per documentar-les sense por. El diari personal ajuda; però la protecció real són la Inspecció amb accés remot [1], els delegats sindicals i els convenis — la prova individual no substitueix la tutela col·lectiva.

I el quart: **confondre mesurar amb resoldre**. El registre perfecte no paga les extres: les fa visibles i reclamables. Si la reclamació continua costant la feina, el problema no és probatori. Calen inspecció,

sancions i una cultura on pagar les hores fetes sigui el mínim, no una conquesta.

És hora d'actuar

Que el rellotge de la feina tingui dos propietaris.

Per a tu, treballador: trenta segons al final de cada jornada — el fitxatge, les hores, el torn [3]; el dia que calgui reclamar, tindràs mesos de fets datats. I si la cosa va d'assetjament, el capítol 75 és el teu.

Per a les empreses: certifiqueu el registre horari per lots encadenats [3] abans que la reforma [1] us ho demani a mitges — el registre demostrablement íntegre és la vostra millor defensa davant d'Inspecció, jutjats i reclamacions infundades.

Per a sindicats i delegats: feu del diari laboral segellat una eina bàsica d'afiliació i defensa [3]; i negocieu als convenis el dret del treballador a la còpia verificable del seu registre.

Per a la Inspecció de Treball: l'accés remot que la reforma us donarà [1] val el que valgui la integritat del registre — demaneu-lo ancorat, amb historial de modificacions verificable.

Per als legisladors: la reforma del registre digital [1] és l'ocasió de tancar el cercle: registre immutable, sí — i còpia amb data certa per al treballador, i valor probatori reconegut a la certificació neutral. Que la segona meitat de la prova no es quedi al tinter.

Que les 19:40 del polígon i les hores de la cafeteria constin — i que el pròxim judici social discuteixi justícia, no memòria. Per les hores que són vida, **time2act**.

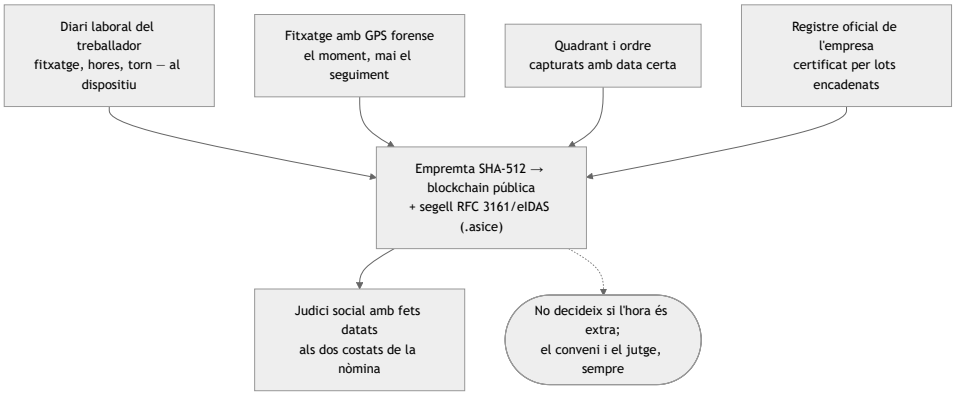


Figura 93.1 — La jornada amb prova d'existència (segellat amb t2p — capítol 13): el diari laboral del treballador (fitxatge, hores, torns — al seu dispositiu, només empremtes a la cadena), el fitxatge amb GPS forense (el moment, mai el seguiment), el quadrant i l'ordre capturats amb data certa, i el registre oficial de l'empresa certificat per lots encadenats — demostrablement íntegre davant d'Inspecció i jutjat. Context: la reforma del registre horari digital (tramitació urgent des del 30-9-2025) exigirà immutabilitat, traça i accés remot de la Inspecció; >40 % de les hores extres no es paguen (EPA). Límits: el conveni i el jutge decideixen el fons; proporcionalitat sempre. Fonts: EPA/INE; projecte de registre horari digital.

---

[1] Ministeri de Treball / premsa especialitzada — *Registre horari digital obligatori: la reforma en tràmit* (tramitació urgent aprovada pel Consell de Ministres el 30-9-2025, desacoblada de la reducció de jornada; objectiu d'aprovació durant el 2026, sense data d'entrada en vigor publicada; requisits del projecte: registres electrònics traçables i immutables, segellat de temps, registre de pauses, accés remot i en temps real per a la Inspecció de Treball, historial de modificacions amb autoria i data); EPA/INE — més del 40 % de les hores extres no es remuneren; RD-llei 8/2019 — registre diari de jornada obligatori. 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] Marc laboral general (papereta del judici social; actes de la Inspecció de Treball; paper dels delegats). Vegeu el capítol 92 per al treball de plataforma i el capítol 102 per a la cadena de subministrament laboral.

[3] t2p — manual de producte (foto amb GPS forense — fix genuí ~50 m / ≤30 s, la ubicació simulada bloqueja la certificació; captura de pantalla i correu certificades; certificar qualsevol fitxer — només l'empremta viatja; certificació en segon pla; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; les converses pròpies i l'assetjament, al capítol 75. ↩

Construcció i infraestructura: qui demostra com es va aixecar de debò

«Totes aquestes construccions s'han d'aixecar tenint en compte la solidesa, la utilitat i la bellesa.»

— Vitruvi, De architectura, I, 3 (s. I aC)

El 6 de febrer de 2023, dos terratrèmols (Mw 7,8 i 7,5) van sacsejar el sud-est de **Turquia** abans de l'alba. Van morir més de **55.000 persones** i es van ensorrar més de **160.000 edificis**, molts d'ells estructures que havien estat legalitzades a través de programes repetits d'amnistia urbanística (*imar barışı*) i aixecades amb formigó de qualitat dubtosa, sense certificar. El cas més cru és el de l'**Isias Grand Hotel**, set plantes a **Adıyaman** que es van plegar com un acordió en pocs segons i van matar **72 persones**, entre elles una delegació de voleibol d'una escola turcoxipriota: 35 dels morts eren nens, mestres i entrenadors. El desembre de 2024, després d'una vista de disset hores, un tribunal va condemnar el propietari **Ahmet Bozkurt**, el seu fill **Mehmet Fatih Bozkurt** i l'arquitecte **Erdem Yılmaz** a fins a **18 anys** cadascun per «causar la mort amb negligència conscient». Un informe tècnic de 150 pàgines va concloure que l'hotel s'havia construït amb formigó pobre barrejat amb sorra i grava de riu, no tenia cap informe d'estudi del terreny, i l'any 2016 se li havia afegit una planta sense permís [1].

Aquest capítol no tracta de qui és el propietari d'un immoble ni del seu títol legal —això és el capítol 35, el registre de la propietat. Aquí parlem del **registre d'integritat física**: les proves de materials, les inspeccions d'obra, els estudis geotècnics i els plànols *as-built*, és a dir, la prova de **com es va construir de debò una cosa i com es va verificar**, no de qui la posseeix. La pregunta és incòmoda perquè un edifici acabat amaga la seva pròpia història: un cop el formigó cobreix l'armadura, ningú no veu si les barres hi eren, si el formigó tenia la resistència declarada, ni si la prova del laboratori es va fer honestament. I quan aquesta història es falsifica, no es perden diners: es perden vides.

La història enterrada en el formigó

El cas turc no és una anomalia exòtica. S'estima que **13 milions d'edificis** turcs —més de la meitat del parc— es van aixecar incomplint la normativa, i almenys **75.000 construccions** de la zona afectada havien rebut amnisties urbanístiques abans del terratrèmol [1]. Aquestes amnisties —els *Yapı Kayıt Belgesi*, certificats de registre que legalitzaven retroactivament edificis en infracció dels codis antisísmics — van ser qualificades pels col·legis d'enginyers de Turquia com «una invitació a la mort». El problema de fons és que el paper que havia de demostrar que un edifici era segur o bé no existia, o bé es podia comprar a posteriori.

El mateix patró apareix lluny de qualsevol falla sísmica. El 24 de juny de 2021, a **Surfside**, Florida, la torre **Champlain Towers South** es va desplomar de matinada i va matar **98 persones**. La investigació del **NIST** —l'organisme federal nord-americà— va situar l'inici del col·lapse en una **fallada de punxonament** de la llosa de la coberta de la piscina: el formigó era més feble que el que exigia el codi, i l'armadura s'havia col·locat amb un recobriment excessiu que en reduïa la capacitat a tallant [3]. Una llosa, un detall constructiu, anys de degradació no documentada: 98 morts. La diferència entre Adıyaman i Surfside no és la física; és que en tots dos casos el **registre del que realment es va construir** era inexistent o no es podia confiar.

Quan la prova del material és la mentida

Hi ha un frau encara més directe: falsificar la mateixa prova que ha de garantir el material. El cas més espectacular és el del **Pont Hong Kong–Zhuhai–Macau**, una de les obres més cares del planeta. Entre 2012 i 2017, l'**ICAC** (la comissió anticorrupció de Hong Kong) va imputar **19 treballadors** del laboratori Jacobs China Limited per haver falsificat **384 informes** d'assaig de provetes de formigó: manipulaven la data de l'ordinador i substituïen les provetes febles per provetes d'alta resistència, i fins i tot per un cilindre metàl·lic de calibratge. La neteja va costar **58 milions de dòlars de Hong Kong** als contribuents, i el juny de 2024 el director Albert Leung Wing-keung va ser empresonat dos anys i mig per defraudar el govern d'uns 2 milions de dòlars de Hong Kong [4].

Als Estats Units, el president de **Testwell Laboratories**, V. Reddy Kancharla, va ser condemnat per haver falsejat proves de resistència del formigó en **més de 100 obres** de Nova York, entre elles la

Freedom Tower, el **Yankee Stadium** i el metro de la Segona Avinguda. Quan es van extreure i assajar testimonis reals, el formigó de la Freedom Tower que s'havia certificat a 12.000 PSI resultava ser, de fet, d'uns 9.000 PSI. Kancharla va rebre de set a 21 anys de presó i 225.000 dòlars de reparació [5]. La tècnica era senzilla i devastadora: en comptes d'assajar la proveta i anotar el resultat, s'escrivia directament el valor de l'especificació; el document deia el que havia de dir, però la realitat física era una altra.

I quan no és el material, és la inspecció. El 14 d'agost de 2018, el **Pont Morandi** de **Gènova** es va esfondrar i va matar **43 persones**. El juliol de 2022 van arribar a judici **59 acusats**; la fiscalia va concloure que alguns documents d'inspecció eren «clarament falsos» i que l'operadora, Autostrade, s'inspeccionava a si mateixa a través de la seva filial Spea. Com hem vist, el 7 d'abril de 2023 un jutge va acceptar un acord de 30 milions d'euros entre Autostrade i Spea [6]. L'autovigilància —ser jutge i part de la pròpia seguretat— és el forat per on s'escola la falsificació.

La llei ja demana el fil; falta l'àncora

La regulació ha reaccionat, i amb força. Al Regne Unit, després de l'incendi de la **Grenfell Tower** —com hem vist— la **Building Safety Act 2022** obliga a mantenir un «fil daurat» digital: un registre traçable i amb control de versions del disseny, els productes, els materials, les aprovacions i la informació *as-built*, conservat durant tota la vida dels edificis d'alt risc [7]. A la Unió Europea, el **Reglament (UE) 2024/3110** —la revisió del Reglament de Productes de Construcció, en vigor des del 7 de gener de 2025 i aplicable a la majoria de productes des del 8 de gener de 2026— converteix el **Passaport Digital de Producte** en un requisit legal obligatori per al marcatge CE: ha de portar la Declaració de Prestacions i Conformitat i la documentació tècnica a través d'un codi QR o portador de dades [8]. A això s'hi suma la sèrie **ISO 19650**, l'estàndard internacional per gestionar la informació amb **BIM** al llarg de tot el cicle de vida i produir un «bessó digital» *as-built* de l'actiu. La llei, doncs, ja demana exactament el que falta: un registre del *com es va construir*. Però un fil daurat emmagatzemat en un servidor que controla qui l'ha d'explicar és, en una disputa, paper de part.

Per què el fil daurat sol no salva

Cal dir-ho amb cruesa. Un registre digital, per ben dissenyat que estigui, és tan fiable com la impossibilitat d'alterar-lo en silenci. Si l'informe d'inspecció prèvia al formigonat viu en una base de dades que l'operadora pot editar —com Autostrade s'inspeccionava a si mateixa—, demà es pot retocar la data, substituir una foto o esborrar un assaig incòmode sense deixar rastre. El frau de Hong Kong va consistir, literalment, a **canviar la data de l'ordinador**; el de Testwell, a **escriure el valor de l'especificació** en lloc del valor mesurat. Cap «fil daurat» que es pugui reescriure a posteriori atura aquestes dues tècniques. El que la llei demana és un registre; el que falta és que aquest registre sigui **inalterable, datat de manera independent i lligat a un autor i un lloc**, de manera que qualsevol substitució o retrodatació posterior es pugui demostrar.

La prova d'existència aplicada

És aquí on **t2p** aporta la capa que faltava en cada fita irreversible de l'obra. **Primer**, abans del formigonat, l'inspector de camp fotografia o filma l'armadura, l'encofrat i el recobriment; el dispositiu calcula sobre la marxa l'**empremta SHA-512**, obté un **segell de temps RFC 3161 conforme a eIDAS**, l'ancoratge a la **blockchain pública** i hi afegeix el **GPS forense** i una **prova de vida** que vincula l'inspector amb aquell lloc i instant. **Segon**, el laboratori de materials segella cada resultat d'assaig de proveta —i les dades crues de l'instrument— en el moment exacte del trencament als 28 dies, de manera que la data i el valor ja no es poden retrodatar ni intercanviar (precisament com fan les tècniques de Hong Kong i Testwell). **Tercer**, l'enginyer segella el joc de plànols *as-built* signat i l'informe geotècnic en el moment de la signatura. Cada segell genera un contenidor **.asice** verificable fora de línia que flueix cap al fil daurat (BSA 2022) i al model d'informació BIM (ISO 19650), i s'aparella amb la Declaració de Prestacions i el Passaport Digital de Producte del Reglament (UE) 2024/3110. És el mateix principi de procedència C2PA dels capítols 13 i 15, aplicat aquí no a una imatge sintètica sinó a la història física d'un edifici.

Ara el límit, amb tota la cruesa. «Escombraries a l'entrada, escombraries a la cadena»: el segell demostra que *aquella* foto, *aqueix* resultat d'assaig o *aqueix* plànol existien en un instant, van ser creats per un dispositiu o autor determinat i no s'han alterat des d'alhora. **No prova que l'edifici sigui segur**, ni que

el formigó tingui la resistència real, ni que l'armadura fotografiada sigui la que va quedar al seu lloc, ni que l'assaig es fes honestament. Un inspector corrupte pot fotografiar una armadura conforme i després abocar formigó dolent; un laboratori pot segellar un assaig executat però deliberadament infracarregat; un propietari pot segellar el plànol real d'una planta il·legal. I no pot certificar retroactivament els milions d'estructures ja construïdes i sense segellar —els 13 milions d'edificis turcs no conformes. El segell estreny el frau perquè fa **demostrable** la manipulació i la fabricació posteriors; no garanteix que la realitat física de sota sigui sòlida.

La promesa i el perill

La promesa és un registre d'obra **a prova de manipulació**: que cap operadora es pugui inspeccionar a si mateixa en l'ombra, que cap laboratori pugui canviar la data de l'ordinador i que, després d'un desastre, els investigadors —com el NIST a Surfside— puguin demostrar **quins registres són autèntics i contemporanis** i quins es van fabricar. La prova d'existència no substitueix els laboratoris acreditats, la inspecció independent de tercers, la signatura del control d'obra ni la investigació forense; els fa **responsables**.

El perill demana els matisos de sempre. El primer, la **falsa confiança**: «està ancorat, doncs és segur» és exactament la mentida que el segell no autoritza —ancorar una dada no la fa certa. El segon, la **concentració i el cost**: si segellar cada fita es torna car o tècnicament feixuc, pot expulsar els petits constructors honestos en comptes de protegir-los. I el tercer, el **frau de captura**: si l'inspector corromput és qui sosté el dispositiu, pot segellar una realitat tramposa amb tota la força probatòria d'un segell; —per això el GPS forense i la prova de vida lliguen l'autor al lloc, però no el fan honest. La capa criptogràfica fa la trampa demostrable; no la fa impossible.

És hora d'actuar

Per als **laboratoris de materials i les entitats d'inspecció acreditades**: segellar cada resultat d'assaig i cada inspecció prèvia al formigonat en l'instant en què es produeixen, perquè la data i el valor no es puguin tocar mai més. Per als **promotors, constructors i enginyers**: segellar els plànols *as-built* i l'informe geotècnic en el moment de la signatura i abocar-los al fil daurat. Per als **reguladors i el control d'obra** (Building Safety Regulator, autoritats de marcatge CE sota el Reglament 2024/3110): exigir el registre segellat com a part del fil daurat i del Passaport Digital de Producte, i reconèixer-lo com a evidència. Per als **investigadors de col·lapses** (NIST i equivalents): tractar el contenidor .asice datat com la cadena de custòdia que distingeix el document autèntic del fabricat després. I per als **fabricants de productes de construcció**: ancorar la Declaració de Prestacions de cada lot, perquè una substitució posterior falli la comprovació d'empremta.

Com hem vist a Adıyaman, la mort de desenes de persones en un hotel construït amb sorra de riu i legalitzat amb un paper comprable demostra que donar a cada fita d'obra una prova segellada de com es va construir i verificar realment —sense oblidar mai que el segell no fa segur el que no ho és— és fonamental en aquest front on el formigó amaga la seva pròpia història, time2act.

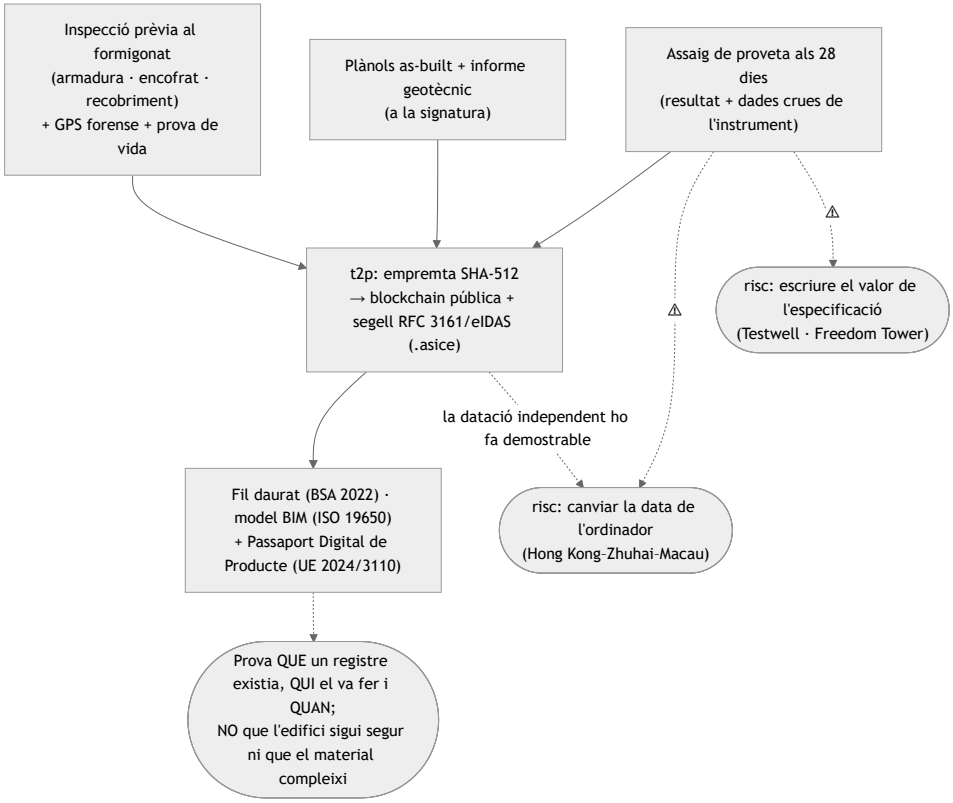


Figura 94.1 — Tres fites irreversibles d'una obra: inspecció prèvia al formigonat (armadura, encofrat, recobriment), assaig de proveta als 28 dies, i plànols as-built + informe geotècnic a la signatura. A cada fita, t2p calcula l'empremta SHA-512, hi afegeix GPS forense i prova de vida si hi ha captura de camp, segella amb RFC 3161/eIDAS i ancora a la blockchain pública (.asice); el contenidor flueix cap al fil daurat (BSA 2022) i el model BIM (ISO 19650) i s'aparella amb el Passaport Digital de Producte (Reglament UE 2024/3110). Punts de risc que la datació independent fa demostrables: canviar la data de l'ordinador (Hong Kong–Zhuhai–Macau) i escriure el valor de l'especificació (Testwell). Límit: el segell prova que un registre existia, qui el va fer i quan, no que l'edifici sigui segur ni que el material compleixi. Fonts: terratrèmols de Turquia 2023 (Isias Grand Hotel); NIST (Champlain Towers South); ICAC (pont HZMB); Testwell; pont Morandi; Building Safety Act 2022; Reglament (UE) 2024/3110.

---

[1] The Dial — *Faulty Construction* (judicis pel terratrèmol de Turquia; Isias Grand Hotel; condemnes de 18 anys el desembre de 2024; 75.000 edificis amnistiats; uns 13 milions d'edificis 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* (juliol de 2023; amnisties, no aplicació dels codis i fallades de qualitat del formigó). 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* (investigació federal oficial; 98 morts; inici per fallada de punxonament de la llosa de la piscina; formigó més feble que el codi). 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 treballadors imputats; 384 informes falsificats; manipulació de dates i substitució de provetes; Albert Leung 2,5 anys el juny 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* (febrer de 2010; Testwell/Kancharla; Freedom Tower certificada a 12.000 PSI però d'uns 9.000 PSI; 7 a 21 anys). 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* (Gènova, 14 d'agost de 2018; 43 morts; 59 acusats; documents d'inspecció «clarament falsos»; autovigilància via Spea; acord de 30 M€ el 2023). https://en.wikipedia.org/wiki/Ponte_Morandi_collapse ↩

[7] Seton UK — *Understanding the Golden Thread: Building Safety Act 2022* (registre digital traçable i amb control de versions per a edificis d'alt risc, 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* (Reglament de Productes de Construcció revisat; en vigor el 7 de gener de 2025; Passaport Digital de Producte obligatori per al marcatge CE des del 8 de gener 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* (febrer de 2025; treball experimental complet, modelització en curs, presentació tècnica el juny 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* (gestió de la informació amb BIM i registre as-built / bessó digital al llarg del cicle de vida). https://www.bsigroup.com/en-GB/products-and-services/standards/iso-19650-building-information-modelling-bim/

El pedigrí d'una peça: quan un certificat fals pot matar

«Els reglaments són paper: no esmorteiran una topada sobtada de pedra i metall.»

— Ernest K. Gann, Fate Is the Hunter (1961)

Entre el gener de 2019 i el juliol de 2023, **Jose Alejandro Zamora Yrala**, de 38 anys, va dirigir des d'un despatx a casa seva, a Surrey, una empresa britànica de comerç de peces aeronàutiques anomenada **AOG Technics**. Va vendre més de **60.000 peces de motor d'avió** —valorades en uns 6,9 milions de lliures— acompanyades de **certificats d'aptitud falsificats** (EASA Form 1 i FAA Form 8130-3) que garantien fraudulentament que les peces eren noves i aeronavegables. La majoria eren per al **CFM56**, el motor comercial més venut del món, i el pedigrí falsejat va arribar a aerolínies com American Airlines i Ethiopian Airlines. El frau es va desfer a mitjan 2023, quan una aerolínia va demanar a **Safran** que verifiqués un certificat d'AOG, Safran el va marcar com a fals i, el 4 d'agost de 2023, la CAA britànica, la FAA i l'EASA van emetre alertes de seguretat. CFM International, la joint venture de GE Aerospace i Safran, va demandar a l'High Court de Londres i va acabar identificant **126 motors sospitosos**; la Serious Fraud Office britànica va obtenir la declaració de culpabilitat de Zamora el desembre de 2025 i una condemna de **4 anys i 8 mesos** el 23 de febrer de 2026, per un frau valorat en 39,3 milions de lliures [1].

Aquest capítol no parla del silici dels xips falsificats —això és el capítol 70— ni de la traçabilitat genèrica de mercaderies del capítol 29. Aquí l'objecte és més estret i **crític per a la seguretat**: el **pedigrí documental d'una sola peça física**. El certificat d'aeronavegabilitat d'un àlep de turbina, l'entrada del quadern de bord, el comptaquilòmetres d'un cotxe. La pregunta és incòmoda: si la peça és metall que no parla, i tot el que la fa legítima és un paper que sí que es pot falsificar, com fem que aquest paper sigui inalterable i atribuïble? Perquè aquí un document fals no és una molèstia comercial: **pot matar**.

Un frau de paper sobre metall que vola

El cas AOG revela l'anatomia exacta de l'atac. Zamora no fabricava peces dolentes en una nau; manipulava i inventava els documents que les acompanyen. La demanda de CFM International va identificar 78 documents falsificats que cobrien 52 referències de peça del CFM56 i dos registres del CF6, amb àleps de turbina inclosos, i van arribar a 68 motors muntats en Boeing 737 i Airbus A320 antics; com hem vist, el recompte de motors sospitosos es va elevar a 126 [2]. El que feia letal el frau no era una falla metal·lúrgica visible, sinó la confiança cega en un certificat: un Authorised Release Certificate amb un segell i una signatura que ningú podia confrontar amb l'origen real de la peça.

AOG no és un cas aïllat, sinó la punta d'un problema sistèmic. Una estimació de la FAA citada per la indústria calcula que cada any arriben als avions uns 520.000 components falsificats o no aprovats —prop del 2 % dels 26 milions de peces en servei—, i situa el mercat global de peces falsificades per sobre dels 2.000 milions de dòlars anuals [3]. Cada una d'aquestes peces viatja amb un pedigrí de paper, i cada pedigrí és tan fort com la dificultat de falsificar-lo; avui aquesta dificultat és baixa: un PDF amb un logotip i una signatura escanejada.

El mateix forat, a quatre rodes: el comptaquilòmetres

El problema del pedigrí documental no és exclusiu de l'aviació; és el mateix forat de confiança a escala que afecta milions de consumidors. Com hem vist, al desembre de 2025 CARFAX va estimar que circulen per les carreteres dels Estats Units uns 2,45 milions de vehicles amb el comptaquilòmetres presumptament manipulat, un augment del 14 % respecte a 2024 i una pèrdua mitjana d'uns 3.300 dòlars per cotxe afectat [4]. La digitalització no ho ha resolt: revertir un quadre digital amb una eina barata resulta més net i ràpid que desmuntar el vehicle.

A Europa la magnitud és comparable. Un estudi del Parlament Europeu de 2018 va trobar manipulació del comptaquilòmetres en el 5-12 % de les vendes domèstiques de cotxes usats i en el 30-50 % de les transfrontereres, amb un dany econòmic estimat entre 5.600 i 9.600 milions d'euros anuals a la UE [5]. La història és la mateixa que a l'aviació: una peça —el vehicle— que no parla, i un historial —els quilòmetres,

el llibre de manteniment— que sí es pot reescriure. El llibre d'inspeccions amb segell de taller és, en essència, el germà humil de l'EASA Form 1.

El sistema que la indústria ja construeix

La resposta institucional existeix i avança en la direcció correcta. Després d'AOG, al febrer del 2024 es va crear l'Aviation Supply Chain Integrity Coalition —Airbus, Boeing, GE Aerospace, Safran, American, Delta, United i StandardAero— que el 9 d'octubre del 2024 va publicar 13 recomanacions centrades en tres eixos: acreditació de proveïdors, digitalització dels documents i les signatures (FAA Form 8130, EASA Form 1) i millora de la traçabilitat de les peces [6]. La clau és *digitalitzar*: la coalició reconeix que el paper signat a mà és precisament el que AOG va saber explotar.

El marc regulador ja hi és des de fa dècades. El Suspected Unapproved Parts (SUP) Program de la FAA, establert el 1995, exigeix traçabilitat fins a la fabricació segons el 14 CFR Part 21 o una determinació d'aeronavegabilitat segons el Part 43, verificada amb les etiquetes FAA Form 8130-3, i les peces sospitoses es reporten amb la FAA Form 8120-11 [7]. A Europa, l'EASA Form 1 és l'equivalent i l'EASA manté una base de dades de peces sospitoses i emet butlletins de seguretat —com el SIB 2023-05 sobre AOG Technics, de l'agost del 2023—. A la carretera, la Federal Odometer Act (49 U.S.C. ch. 327) la fa complir la NHTSA als Estats Units, i a Europa la Directiva 2014/45/UE i el sistema belga Car-Pass apunten cap a un registre de quilometratge a escala de la UE acordat el desembre del 2025; com hem vist, la llei demana traçabilitat, però falta fer-la inalterable.

Per què la digitalització sola no salva

Cal dir-ho sense embuts: digitalitzar l'EASA Form 1 o el llibre de manteniment **no impedeix el frau d'AOG per si sol**. Un PDF signat és un PDF: es pot retocar, retrodatar, copiar i tornar a emetre amb un signatari inventat, exactament com va fer Zamora. Si la digitalització només substitueix el segell de tinta per una imatge de signatura escanejada, hem canviat un paper falsificable per un fitxer falsificable. El mateix val per al quadre digital del cotxe: un registre electrònic de quilòmetres que es pot sobreescriure no és més fiable que l'agulla mecànica que reemplaça.

El problema de fons no és el suport, sinó l'absència d'una **àncora independent** que fixi *qui* va declarar *què* i *quan*, fora del control de qui podria voler reescriure-ho. Una base de dades centralitzada ajuda, però és tan forta com la confiança en l'administrador i tan vulnerable com la seva clau. El que cal és que cada esdeveniment del pedigrí —cada certificat, cada entrada de quadern, cada lectura de comptaquilòmetres— quedi lligat a una data certa i a un autor d'una manera que faci **detectable** qualsevol manipulació posterior.

La prova d'existència aplicada

Aquí és on **t2p** afegeix la capa que falta, i ho fa sobre l'**esdeveniment de pedigrí**, no sobre el metall. Quan un manteniment crea o transfereix un registre —un taller OEM/PMA que allibera una peça, un MRO que signa un formulari EASA 1 o un FAA 8130-3, un informe de desmuntatge, una entrada de quadern de bord o un paquet de traçabilitat *back-to-birth*— el tècnic o el responsable de qualitat captura el document al dispositiu. S'hi calcula localment l'**empremta SHA-512**, s'aplica un **segell de temps RFC 3161/eIDAS**, s'ancora a la blockchain pública i es genera un contenidor **.asice** verificable fora de línia. En afegir-hi un **GPS forense** i una **prova de vida**, el signatari humà queda lligat a l'acte. El resultat és una **cadena de custòdia inalterable**: qualsevol part posterior —la recepció de mercaderies d'una aerolínia, la CAMO, un regulador, un auditor o un comprador de cotxe usat que consulta el llibre segellat i la foto del comptaquilòmetres— pot verificar independentment que *aquest* certificat o *aquesta* foto existien, sense alteració, en *aquest* moment, signats per *aquest* autor a *aquest* lloc. El sistema s'assenta sota el 8130-3/Form 1 i les bases SUP i Car-Pass, encaixant directament amb la recomanació de la coalició de «digitalitzar documents i signatures + millorar la traçabilitat». Funciona al costat de les capes de procedència dels capítols 13 (C2PA) i 15.

Ara el límit, amb tota la cruesa. «Escombraries a l'entrada, escombraries a la cadena»: el segell prova **l'origen, el temps, l'autor i la integritat** del certificat, de la foto o de l'entrada de quadern; **no demostra que la peça sigui genuïna, nova, aeronavegable o ben instal·lada**, ni que la lectura del comptaquilòmetres o el registre de servei documentat siguin certs. Un falsificador encara pot **segellar**

una mentida: si AOG hagués segellat el seu propi ARC fabricat, el segell mostraria fidelment que AOG va crear *aquest* document en *aquest* instant —però no diria que el cargol és realment nou de Safran i no un de recuperat o falsificat. Una foto de quilometratge segellada indica que el quadre mostrava *aquest* número en captura, no que mai s'hagués revertit abans. El segell no fa una inspecció física, ni un assaig metal·lúrgic, ni una auditoria *back-to-birth*, ni valida que l'organització emissora tingués realment l'aprovació que afirma tenir. És una capa d'integritat i procedència que fa **detectable** la manipulació retroactiva i **traçable** la responsabilitat; mai no substitueix la inspecció acreditada, l'autenticació de l'OEM, la supervisió reguladora ni el judici d'enginyeria humà.

La promesa i el perill

La promesa és tancar el forat exacte que AOG va explotar: fer que **falsificar un certificat o inventar un signatari** deixi una empremta detectable, i convertir el pedigrí d'una peça —o l'historial d'un cotxe— en una cosa que qualsevol pot verificar sense confiar en la paraula del venedor. En una cadena on un àlep de turbina passa de mà en mà sense cap rebut inalterable, l'ancoratge de l'origen protegeix tant el comprador honest com el passatger.

El perill demana els matisos de sempre. El primer: la **falsa confiança** —«està segellat, doncs la peça és bona»—, quan el segell només garanteix el document, no el metall; un *.asice* impecable damunt d'un cargol falsificat és més perillós que cap paper, perquè inspira confiança. El segon: la **concentració**, si només els grans OEM i MRO poden segellar i els tallers petits queden exclosos del mercat per no poder-ho fer. El tercer: la dependència de la **captura honesta a l'origen** —si el primer que omple el Form 1 menteix, el segell perpetua la mentida amb data certa. La prova d'existència és una capa de governança del pedigrí, no un certificat de bondat de la peça.

És hora d'actuar

Per als OEM i la indústria del motor (GE Aerospace, Safran, CFM, Airbus, Boeing): segellar el formulari 8130-3 a l'emissió, de manera que qualsevol còpia retocada posteriorment falli la comprovació d'empremta. Per als MRO i les CAMO: verificar l'empremta segellada en rebre la mercaderia abans del muntatge i exigir-la com a requisit de compra. Per als reguladors (FAA, EASA, CAA): reconèixer el pedigrí segellat com a evidència dins el SUP Program i tractar la data certa com a diferència entre un certificat i una coartada posterior.

Per a la coalició d'integritat de la cadena: fer del segell ancorat l'estàndard tècnic recomanat per «digitalitzar documents i signatures». I per als reguladors de l'automòbil i els registres de quilometratge (NHTSA, Car-Pass, el futur registre de la UE): segellar cada lectura del comptaquilòmetres a la inspecció, perquè qualsevol reversió deixi un buit detectable.

Com hem vist, Zamora Yrala va vendre seixanta mil peces amb papers falsos des d'un despatx a casa; només quan un responsable de Safran va comprovar el certificat es va detectar el frau. Assignar a cada peça crítica un pedigrí que cap falsificador pugui reescriure sense deixar rastre —sense oblidar mai que el segell no inspecciona el metall— és, en aquest front on un document fals pot matar, time2act.

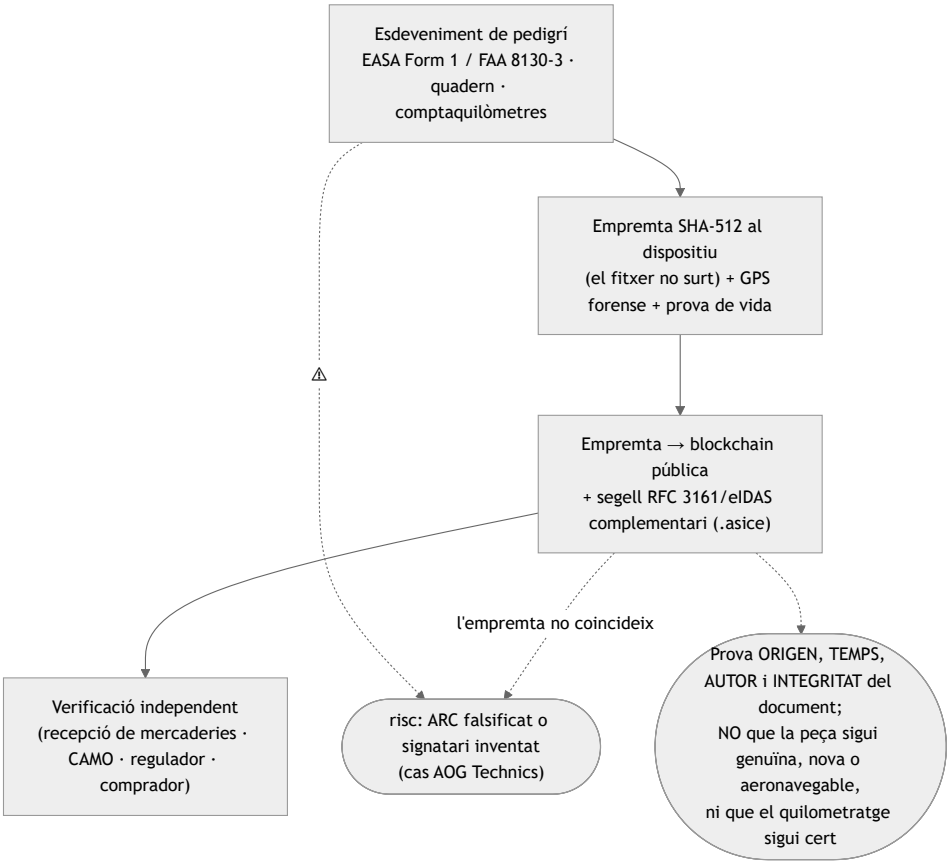


Figura 95.1 — Un esdeveniment de manteniment crea un registre (EASA Form 1 / FAA 8130-3, entrada de quadern, lectura de comptaquilòmetres). El tècnic en calcula l'empremta SHA-512 al dispositiu (el fitxer no surt), hi afegeix GPS forense i prova de vida si hi ha captura de camp, i l'empremta del conjunt s'ancora a la blockchain pública, amb segell RFC 3161/eIDAS complementari (.asice). Qualsevol part posterior —recepció de mercaderies, CAMO, regulador, comprador— verifica de manera independent qui ho va declarar i quan. Límit: el segell prova l'origen, el temps, l'autor i la integritat del document; no prova que la peça sigui genuïna, nova o aeronavegable, ni que el quilometratge sigui cert — escombraries a l'entrada, escombraries a la cadena. Fonts: cas AOG Technics (SFO); demanda de CFM International; estimacions FAA de peces no aprovades; CARFAX i Parlament Europeu sobre comptaquilòmetres; Aviation Supply Chain Integrity Coalition.

---

[1] SFO (GOV.UK) — *SFO secures 4-year prison sentence for aircraft parts fraud* (Zamora Yrala; 60.000 peces; frau de 39,3 M£; ARC falsificats; condemna de 4 anys i 8 mesos; descobriment per 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* (pàgina 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 documents falsificats, 52 referències del CFM56, 68 motors, àleps 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* (traçabilitat segons 14 CFR Part 21/43, Form 8130-3, report amb Form 8120-11). https://www.faa.gov/aircraft/safety/programs/sups ↩

[5] EASA — *Suspected Unapproved Parts* (base de dades i definicions de la UE; casos d'EASA Form 1 falsificats; marc dels SIB). https://www.easa.europa.eu/en/domains/aircraft-products/suspected-unapproved-parts ↩

[6] EASA — *Safety Information Bulletin SIB 2023-05* (butlletí sobre les peces sospitoses d'AOG Technics i accions de quarantena/reemplaçament recomanades). 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 recomanacions, 9 d'octubre de 2024; digitalitzar 8130-3/Form 1; traçabilitat; acreditació de proveïdors). 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 peces falsificades o no aprovades arriben als avions cada any, ~2 % de 26 milions; mercat de més 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* (desembre de 2025; 2,45 milions de vehicles sospitosos; +14 % interanual; ~3.300 $ de pèrdua mitjana). https://www.prnewswire.com/news-releases/carfax-odometer-rollbacks-see-dramatic-jump-of-14-to-2-45-million-vehicles-302643855.html

[10] Parlament Europeu (EPRS STU 2018-615637) — *Odometer manipulation in motor vehicles in the EU* (manipulació en el 5-12 % de vendes domèstiques i 30-50 % transfrontereres; dany de 5,6-9,6 mil milions d'euros anuals). https://www.europarl.europa.eu/RegData/etudes/STUD/2018/615637/EPRS_STU(2018615637_EN.pdf

Emissions: el sensor que mentia abans que el paper

«Quan pots mesurar allò de què parles i expressar-ho en nombres, en saps alguna cosa; quan no ho pots mesurar, el teu coneixement és migrat i insatisfactori.»

— Lord Kelvin, «Electrical Units of Measurement» (1883)

El 18 de setembre de 2015, l'**Agència de Protecció Ambiental** dels Estats Units (EPA) va emetre contra **Volkswagen** un avís de violació de la *Clean Air Act*. Els seus turismes dièsel TDI portaven un **«dispositiu de desactivació»** (*defeat device*): un programari del control del motor que reconeixia el banc de proves del laboratori —el volant quiet, la velocitat, la durada— i només llavors activava a fons el control d'òxids de nitrogen; a la carretera el rebaixava i emetia NOx fins a **40 vegades** el límit legal. Hi havia uns **11 milions de vehicles** al món (uns 590.000 als EUA, anys 2009-2016), i a mitjan 2020 l'escàndol ja havia costat a VW més de **33.300 milions de dòlars** en multes, recompres i acords, inclosa una sanció penal de 2.800 milions i una de civil de 1.450 milions [1][2]. El guió es va repetir: el gener de 2024, el fabricant de motors **Cummins** va acceptar una sanció civil de **1.675 milions de dòlars** —la més alta mai imposada sota la *Clean Air Act*— per programari de desactivació no declarat en més de **630.000** pick-ups dièsel RAM 2500/3500 dels anys 2013-2019 [3]. El fil comú és cru: la dada de compliment en què el regulador confiava semblava verídica, però havia estat **fabricada en el moment de la captura**. No es va falsejar el paper després; es va enganyar el sensor o la prova.

Aquest capítol no parla de crèdits de carboni ni de certificats d'estalvi energètic —això és cosa dels capítols 21-23, on l'actiu és un títol negociable i el risc és el doble compte o la reducció fantasma. Aquí l'actiu és una altra cosa: la **dada d'emissions del sensor i del compliment**, i el risc és la **mesura manipulada o trucada**. La pregunta és precisa: com fixem que *aquesta* lectura va sortir de *aquest* analitzador, en *aquest* lloc i instant, sense que ningú la pugui «esbiaixar» entre el sensor i el full de càlcul? La resposta toca el cor de la tesi del llibre: quan la dada ambiental val diners i decideix sancions, la seva **integritat** deixa de ser un detall tècnic i passa a ser la batalla.

Quan s'enganya el banc de proves

El cas Volkswagen va revelar una forma d'engany que no deixa empremta al paper perquè neix abans del document. El programari detectava que el cotxe era en un assaig homologat i activava un mode net que mai no es feia servir a la carretera; la lectura del laboratori era **autèntica**: allà el vehicle emetia poc, però no circulava realment. Així, el frau va perdurar anys: cada certificat era tècnicament correcte i internament coherent, i cap auditoria de documents l'hauria trobat, perquè el document no mentia; mentia la realitat que descrivia.

El cas Cummins, vuit anys després, demostra que no es tractava d'una anomalia d'una sola marca. Com hem vist, més de 630.000 camions portaven un programari no declarat, una sanció civil rècord i un acord total superior als 2.000 milions de dòlars, amb més de 325 milions per a remeis i una crida a revisar com a mínim el 85 % dels vehicles afectats en tres anys [3]. A Europa, el **Tribunal de Justícia de la UE** ha tancat la porta jurídica al truc «elegant»: el juliol del 2022 va dictaminar que el programari de **«finestra tèrmica»** —que només garanteix el control de NOx entre 15 i 33 °C— és, en principi, un dispositiu de desactivació il·legal; una sentència anterior, del desembre del 2020, ja havia declarat il·lícit el programari que reconeix el cicle de prova [8]. El missatge és clar: enganyar la prova és enganyar la llei, encara que el full surti net.

Quan es trafica el sensor que vigila la xemeneia

El truc del banc de proves té un germà industrial encara més directe: manipular el monitor continu d'emissions que vigila una xemeneia. **Berkshire Power Company** i **Power Plant Management Services** es van declarar culpables de delictes greus contra la *Clean Air Act* per esbiaixar intencionadament el **sistema de monitoratge continu d'emissions (CEMS)** de la central i subdeclarar el NOx entre el gener del 2009 i el març del 2011, com ja s'ha esmentat. La maniobra era d'una franquesa quirúrgica: introduïen un ajust fraudulent d'uns **0,5 ppm**, el **treien abans** que arribessin els auditors independents i el **tornaven a posar** quan marxaven. BPC va pagar una multa penal de 2,75 milions de dòlars; el març del 2017 les parts devien uns 7,25 milions en multes i sancions [4].

No hi havia cap document fals: el CEMS registrava i transmetia, fidelment i en temps real, una xifra fabricada. El frau vivia a la **finestra cega** entre dues auditories.

El mateix forat existeix a escala planetària amb el metà. El *Global Methane Tracker 2024* de l'**AIE** estima prop de **120 Mt** de metà del sector dels combustibles fòssils el 2023; però les xifres que les empreses de petroli i gas reporten a la **UNFCCC** són un 50 % més baixes que l'estimació de l'AIE, i les que reporten a l'OGMP 2.0 impliquen uns 5 Mt —un **95 %** més baixes [5]. El satèl·lit **MethaneSAT** (llançat el 4 de març del 2024, comunicació perduda el 20 de juny del 2025) va trobar emissions de metà de petroli i gas dels EUA **més de quatre vegades** superiors a les estimacions de l'EPA, amb una taxa de pèrdua agregada de l'1,6 % en dotze conques —vuit vegades l'objectiu del 0,2 % de la indústria [6]. La distància entre el que es declara i el que es mesura des de l'aire és, ella mateixa, la prova del problema.

El que la llei ja exigeix

La resposta reguladora s'ha endurit a banda i banda de l'Atlàntic. La *Clean Air Act* dels EUA prohibeix els dispositius de desactivació i tipifica com a delicte falsejar, manipular o **inutilitzar a consciència** qualsevol mètode de monitoratge exigit —és el ganxo legal tant del *Dieselgate* com de la manipulació de CEMS. La **norma final de metà de l'EPA** (signada el 2 de desembre de 2023, publicada el 8 de març de 2024), dins de les *New Source Performance Standards* 40 CFR Part 60 subparts OOOOb i OOOOc, crea un **Programa de superemissors**: un «esdeveniment de superemissió» és un alliberament de **100 kg de metà per hora** o més, detectat per tercers certificats per l'EPA mitjançant satèl·lit, avió/dron o sensors mòbils terrestres; l'operador ha de començar a investigar en **5 dies** i informar-ne l'EPA en **15 dies** [4][6]. S'espera que la norma eviti **58 milions de tones** de metà entre 2024 i 2038 (una reducció del ~80 %).

A la Unió Europea, el **Reglament (UE) 2024/1787** sobre la reducció de les emissions de metà al sector de l'energia imposa un **MRV** (mesura, informe i verificació) a escala de font amb **verificació independent de tercers**, un mecanisme d'alerta ràpida de superemissors basat en dades de satèl·lit, i obligacions equivalents per als importadors a partir del 2027 [10]. I l'aplicació de la llei ja mossega: el 11 de juliol de 2024, EPA i el Departament de Justícia van anunciar un acord de **241,5 milions de dòlars** amb **Marathon Oil** per infraccions de la *Clean Air Act* en gairebé 90 instal·lacions de la reserva de Fort Berthold (Dakota del Nord) —64,5 milions de sanció civil, la més alta mai aplicada a una font fixa— que retalla unes 110.000 tones de COV i metà [7]. Amb el *Waste Emissions Charge* de la *Inflation Reduction Act*, cada tona de metà declarada té un preu. Quan la dada val diners, l'incentiu a maquillar-la creix.

Per què la norma sola no salva

Cal dir-ho sense embuts, perquè aquí l'autoengany seria car. Una norma que exigeix un CEMS acreditat, un MRV verificat i un informe puntual no impedeix, per si sola, que el número que hi arriba sigui mentida des de l'origen. Com hem vist, la *Clean Air Act* prohibia els dispositius de desactivació molt abans del 2015; Volkswagen els va instal·lar igualment, i el sistema d'homologació, basat en confiar en la prova de laboratori, no els va detectar durant anys. El cas Berkshire mostra el forat encara més nu: tot el règim de CEMS funcionava sobre el paper —el sensor transmetia, el regulador rebia— mentre l'operador entrava i treia el biaix al voltant de les visites. El que falla no és el llindar legal ni el deure d'informar; és que entre el sensor i el full de càlcul hi ha una **cadena de custòdia que ningú no segella**, i un número es pot esbiaixar, retrodatar o substituir sense deixar empremta. Un informe de compliment és un PDF; res no impedeix retocar la dada abans que es converteixi en PDF.

La prova d'existència aplicada

És aquí on **t2p** aporta la baula que falta, sobre l'artefacte que importa: el **registre brut de la mesura en l'instant de la captura**, abans que es pugui «esbiaixar», trucar amb el cicle de prova o editar en silenci. El CEMS, l'analitzador de metà o el seu sistema d'adquisició —i també la càrrega de sensors d'un dron o d'un avió— calcula al mateix dispositiu l'**empremta SHA-512** de cada lectura o bloc de dades brutes; el fitxer original mai no surt. Tot seguit n'obté un **segell de temps RFC 3161/eIDAS** i **ancora l'empremta a la blockchain pública**, dins d'un contenidor **.asice** verificable fora de línia. En els vols de camp, s'hi afegeix **GPS forense** perquè la lectura de la ploma quedi lligada de manera provable a un lloc i un moment. Igual val per a una prova de certificació d'un motor o per a una notificació de superemissor: el tècnic o l'ONG **segella la traça de l'assaig** —o el fotograma de detecció del satèl·lit—

en el moment de produir-lo. Quan l'operador presenti l'informe regulador, l'auditor pot verificar que les xifres lliurades **coincideixen amb la captura bruta segellada** i que res no s'ha canviat entre el sensor i el full —tancant exactament el forat que Berkshire explotava treient i tornant a posar el biaix al voltant de les auditories. No substitueix res de la pila existent —certificació EPA/CARB, QA acreditat del CEMS, el programa OOOOb/c i de superemissors, el MRV del Reglament 2024/1787, els contrastos per satèl·lit (MethaneSAT, AIE, Copernicus)—: hi afegeix una **cadena de custòdia a prova de manipulació** del sensor a la presentació. És el complement, sobre la dada ambiental, del que els capítols 13 i 15 proposen per a la procedència C2PA del contingut.

Ara el límit, amb tota la cruesa. «Escombraries a l'entrada, escombraries a la cadena»: el segell prova origen, temps, autor i integritat d'un registre de mesura —que aquesta lectura va sortir d'aquest aparell, en aquest lloc i instant, i que no s'ha alterat des de llavors. **No prova que la lectura sigui certa** al punt de captura. Un dispositiu de desactivació que enganya el banc (VW, Cummins) produeix un resultat «net» genuïnament segellat i, alhora, buit de sentit; un CEMS esbiaixat físicament registrarà, fidelment i de manera verificable, números baixos fabricats. El segell no detecta que un sensor s'ha falsejat, que s'ha tret una sonda, que s'ha introduït aire de dilució o que el motor ha entrat en mode de reconeixement de prova; ni sap si una instal·lació **mai no va mostrejar** un component que perdia. No quantifica emissions ni jutja el compliment. És, per tant, inútil contra el frau central del *Dieselgate* si no es combina amb comprovacions independents del món real —mesura a la carretera amb equips portàtils (PEMS), auditories per sorpresa, calibratge acreditat i contrast per satèl·lit i avió— i no substitueix mai el judici del regulador, l'aplicació de la llei ni la inspecció humana.

La promesa i el perill

La promesa és tancar el buit entre el sensor i la presentació: una **cadena de custòdia inalterable i datada** que faci impossible esbiaixar un número en la finestra cega entre dues auditories, com va fer Berkshire, i que doni a l'auditor honest i al regulador una prova que els números reportats són els que el sensor va produir. En un món on la tona de metà declarada té un preu, fer l'origen de la dada a prova de manipulació protegeix tant l'operador honest com el públic.

El perill demana els matisos de sempre. El primer, no confondre **integritat amb veritat**: una mesura falsa i segellada continua sent falsa, i ara, a més, immutable —el segell podria donar una falsa tranquil·litat («està ancorat, doncs és bo») que no es correspon amb res, sobretot davant del frau que viu en el sensor, no en el paper. El segon, la **captura del custodi**: si qui segella és la mateixa part que controla el sensor manipulat, el segell només certifica amb més solemnitat un número fals; per això la verificació independent i el contrast extern són innegociables. I el tercer, la **concentració i el cost**: el segell ha d'enfortir l'MRV, no expulsar-ne els operadors petits ni els observadors independents. La prova d'existència és una capa de cadena de custòdia, no un certificat de bondat ambiental.

És hora d'actuar

Per als **operadors industrials i fabricants de motors** (Volkswagen, Cummins, centrals tèrmiques, petroli i gas): segellar la lectura bruta del CEMS i de l'analitzador, i la traça de cada assaig de certificació en el moment de la captura, perquè ningú —ni ells mateixos— la pugui esbiaixar després.

Per als **reguladors** (EPA, CARB, autoritats europees del Reglament 2024/1787): exigir la presentació amb captura segellada i contrastar-la sempre amb mesura real —PEMS a la carretera, satèl·lit a la xemeneia—, perquè cap segell NO pot substituir la inspecció.

Per als **verificadors de tercers i les ONG** del Programa de superemissors: segellar amb GPS forense el fotograma de detecció en el moment del vol, perquè la notificació de 100 kg/h, com ja s'ha indicat, sigui inatacable.

Per als **operadors de satèl·lit i la comunitat científica** (MethaneSAT, AIE, Copernicus): mantenir el contrast extern que cap segell NO pot donar, perquè la integritat de la dada i la seva **plausibilitat** són dues comprovacions diferents. I per als **legisladors**: reconèixer la captura segellada com a cadena de custòdia vàlida, i recordar que tanca el forat de Berkshire, no el de Volkswagen.

El 18 de setembre de 2015, un regulador va descobrir que durant anys havia confiat en una prova que el cotxe sabia reconèixer. Donar a cada lectura d'emissions una prova segellada del seu origen i del seu

instant —sense oblidar mai que el segell no fa certa una mesura trucada al sensor— és, en aquest front on la dada ambiental val diners i decideix sancions, **time2act**.

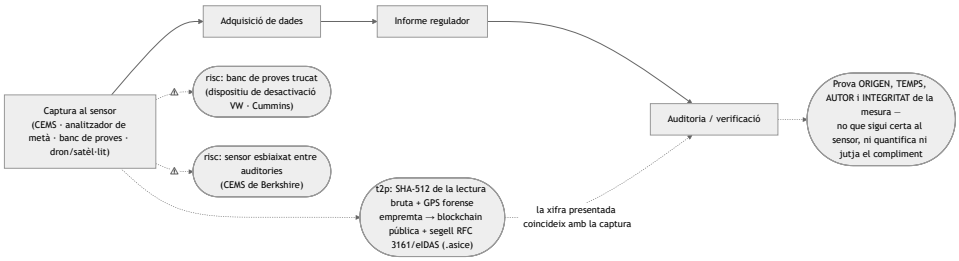


Figura 96.1 — La cadena d'una dada d'emissions en quatre baules: captura al sensor (CEMS, analitzador de metà, banc de proves, vol de dron/satèl·lit) → adquisició → informe regulador → auditoria. t2p calcula al dispositiu l'empremta SHA-512 de la lectura bruta, hi afegeix segell de temps RFC 3161/eIDAS i, en camp, GPS forense, i l'ancora a la blockchain pública (.asice); l'auditor confronta la xifra presentada amb la captura segellada. Dos punts de risc: el banc de proves trucat (dispositiu de desactivació VW/Cummins) i el sensor esbiaixat al voltant de les auditories (CEMS de Berkshire), que el segell NO detecta. Límit: el segell prova origen, temps, autor i integritat de la mesura; no prova que la mesura sigui certa al punt de captura, ni quantifica emissions ni jutja el compliment. Fonts: EPA (VW, Cummins, Berkshire, Marathon, norma de metà); AIE; MethaneSAT; TJUE (finestra tèrmica).

---

[1] EPA — *Volkswagen Clean Air Act Civil Settlement* (acords 2016-2017; sanció civil de 1.450 milions de dòlars; fons de mitigació; ~590.000 vehicles als EUA; descripció del dispositiu de desactivació). https://www.epa.gov/enforcement/volkswagen-clean-air-act-civil-settlement ↩

[2] Wikipedia — *Volkswagen emissions scandal* (NOx fins a 40 vegades el límit; ~11 milions de cotxes; ~33.000 milions de dòlars de cost total; cronologia 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 $1.675 Billion Civil Penalty* (10 de gener de 2024; la sanció civil més alta sota la Clean Air Act; 630.000+ camions RAM; 325 M$ en remeis; condicions de la revisió). https://www.epa.gov/newsreleases/united-states-and-california-announce-diesel-engine-manufacturer-cummins-inc-agrees ↩

[4] EPA — *Summary of Criminal Prosecutions: Berkshire Power* (esbiaix intencionat del CEMS, 2009-2011; ajust fraudulent retirat abans de les auditories; multa penal de 2,75 M$ a BPC; ~7,25 M$ en total el març 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* (prop de 120 Mt de metà fòssil el 2023; UNFCCC ~50 % més baix; OGMP 2.0 ~95 % més baix; esdeveniments de fuga per satèl·lit +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* (emissions mesurades >4 vegades les estimacions de l'EPA; taxa de pèrdua de l'1,6 %, vuit vegades l'objectiu del 0,2 %; 30+ vols cobrint ~70 % de la producció terrestre dels EUA). 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 $241.5M Settlement with Marathon Oil* (11 de juliol de 2024; 64,5 M$ de sanció civil, la més alta a una font fixa; ~90 instal·lacions; ~110.000 tones de COV/metà retallades). 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; definició legal del dispositiu de desactivació; sentència prèvia de desembre de 2020 sobre el reconeixement del cicle de prova). 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* (full informatiu PDF; 58 milions de tones de metà evitades 2024-2038; reducció del ~80 %; Programa de superemissors). 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] Comissió Europea — *New EU Methane Regulation to reduce emissions from fossil fuels* (Reglament (UE) 2024/1787; MRV a escala de font amb verificació de tercers; alerta ràpida de superemissors per satèl·lit; equivalència MRV per als importadors des del 2027). https://energy.ec.europa.eu/news/new-eu-methane-regulation-reduce-harmful-emissions-fossil-fuels-europe-and-abroad-2024-05-27_en ↩

Ciència ciutadana ambiental: els sensors de baix, amb data certa

«L'obligació de suportar-ho ens dona el dret de saber.»

— Jean Rostand, citat per Rachel Carson a Silent Spring (1962)

Doñana, un dels aiguamolls més valuosos d'Europa, s'encongia en silenci mentre al seu voltant els hivernacles de fresses xuclaven l'aqüífer amb pous, basses i canonades quilomètriques que cap registre oficial no comptava. Les queixes a Brussel·les es remuntaven al 2009; el 24 de juny de 2021, el Tribunal de Justícia de la Unió Europea va condemnar Espanya per haver incomplert les seves obligacions: el Pla Hidrològic 2015-2021 no computava les extraccions il·legals i no hi havia mesures per evitar el deteriorament dels hàbitats protegits [1]. La frase que ho resumeix fa mal: allò que l'administració no mesura, jurídicament no existeix — encara que s'estigui bevent un parc nacional.

El capítol 96 va tractar el sensor industrial vigilat des de dalt: la xemeneia, el mesurador oficial, el frau del sensor que menteix. Aquest capítol mira en la direcció contrària: els sensors de baix, els de la ciutadania — l'aparell de qualitat de l'aire al balcó, la foto de l'abocament, el diari del soroll, l'ull del voluntari sobre l'aqüífer. El testimoni orbital és al capítol 104; la integritat de la dada científica, al capítol 63. Pregunta clau: com pot la dada d'un ciutadà pesar prou per moure una inspecció, un expedient o una sentència? Resposta: no pretenent ser el que no és — una acta oficial —, sinó sent allò que ningú més no pot ser: una cronologia densa, local i persistent, amb data certa i integritat inatacable gràcies a **t2p** — l'empremta SHA-512 calculada a l'origen, l'ancoratge de l'empremta a la blockchain pública i el segell de temps RFC 3161/eIDAS complementari, dins d'un contenidor .asice [5].

Allò que no es mesura no existeix

Val la pena desgranar la paradoxa de Doñana, perquè és el patró de tot el capítol. La sentència europea no castiga una contaminació: castiga un buit de dades. L'Estat no computava les extraccions il·legals — la infraestructura de pous i canonades que drenava l'aigua subterrània per regar fresses en hivernacles aixecats sobre desforestacions sistemàtiques — i, en no computar-les, tampoc no en podia derivar mesures de protecció [1]. Les entitats i la ciutadania ho denunciaven des del 2009; van caldre dotze anys perquè la justícia europea digués el que el territori ja sabia [1].

La lliçó és estructural: la protecció ambiental és, abans que res, una qüestió de dades. I quan l'administració no mesura — per manca de mitjans, de voluntat o per captura d'interessos —, el buit només el pot omplir la ciutadania organitzada: plataformes veïnals, entitats de defensa del territori, voluntariat científic. Però aquest ompliment topa sempre amb el mateix mur: «i com sabem que les teves dades són de debò?». La foto sense metadades fiables, el full de càlcul del voluntari, la sèrie del sensor casolà — tot és tècnicament impugnable, i qui contamina té advocats per impugnar-ho.

La resposta no és renunciar a la dada ciutadana: és blindar-ne el que sí que es pot blindar — quan es va prendre, on, i que ningú no l'ha tocada després [5]. La qualitat metrològica es defensa amb calibratges i mètode; la integritat i la data, amb criptografia. Separar aquests dos plans — i no confondre'ls mai — és tot el secret d'aquest capítol.

La llacuna que va esdevenir persona

El Mar Menor va canviar el marc sencer. Després de dècades de degradació, una iniciativa legislativa popular va reunir 639.826 signatures, i el resultat va ser la Llei 19/2022, de 30 de setembre: el reconeixement de personalitat jurídica a la llacuna i la seva conca — el primer ecosistema d'Europa que esdevé subjecte de drets, amb dret a existir i evolucionar naturalment, a la protecció, la conservació i la restauració [2]. El Tribunal Constitucional en va confirmar la constitucionalitat, i el Reial Decret 90/2025 va regular-ne la governança: un comitè de representants de tretze membres, set dels quals de la societat civil — inicialment, del mateix grup promotor de la iniciativa [2].

El significat per a aquest llibre va més enllà de la fita jurídica: la ciutadania no només va vigilar l'ecosistema — en va esdevenir la veu legal. I una persona jurídica, per defensar els seus drets, necessita el mateix que qualsevol altra: proves. Qui parli per la llacuna davant d'un tribunal haurà d'acreditar l'estat de

l'aigua, l'episodi concret, l'abocament, la cronologia del deteriorament o de la recuperació. La ciència ciutadana passa de l'activisme al testimoni processal — i un testimoni necessita memòria infal·lible.

Aquí és on la prova d'existència tanca el cercle: cada mostra documentada, cada fotografia, cada sèrie de mesures del voluntariat, amb l'empremta SHA-512 generada a l'origen, el segell de temps i l'ancoratge a la blockchain pública [5]. La personalitat jurídica dona la legitimació; la prova d'existència, la credibilitat. L'una sense l'altra és un dret sense múscul, o un múscul sense dret.

La xarxa dels sensors de baix cost

El múscul global de la ciència ciutadana ja existeix. Sensor.Community — nascuda com a luftdaten.info — és una xarxa de sensors de qualitat de l'aire muntats per ciutadans, amb dades en temps real i presència a més de 100 països [3]; en l'àmbit hispanoparlant, xarxes com AireCiudadano ofereixen monitors de partícules amb mapa i API oberts, i projectes com CanAirIO mesuren PM2,5 amb maquinari obert i un telèfon mòbil [3].

La força d'aquestes xarxes és la que cap xarxa oficial no pot tenir: densitat i proximitat. Un sensor a cada balcó, al costat de l'escola, davant de la fàbrica — una malla tan fina que captura les variacions locals que les grans estacions de referència, per força, mitjanen. I un cost marginal gairebé zero, que converteix el manteniment en un acte col·lectiu.

La debilitat és doble, i cal dir-la sense embuts. Primera, la qualitat metrològica: un sensor de baix cost no és una estació de referència — deriva, s'embruta, li afecta la humitat. Segona, la cadena de custòdia: qui garanteix que la sèrie no s'ha retocat, que la data és la que diu, que el sensor era on diu?

La divisió del treball correcta ataca cada debilitat amb la seva arma. La primera es combat amb mètode: calibratges creuats amb estacions oficials, protocols documentats, transparència del maquinari [3]. La segona, amb prova d'existència: cada lot de lectures ancorat en origen — empremta, data certa —, de manera que el retoc a posteriori esdevé impossible i els buits de la sèrie queden igualment datats [5]. Un sensor humil amb la sèrie blindada val més, davant d'un tècnic o d'un jutge, que un sensor excel·lent amb un full de càlcul editable: la certesa del qui, què i quan pesa tant com la precisió.

El soroll: la prova a dues veus

El cas d'ús més quotidià és també el més incomprès. Quan es denuncia un excés de soroll, l'ajuntament ha de fer visita d'inspecció, i la mesura la fan tècnics municipals o la policia local amb un sonòmetre homologat i calibrat, aixecant una acta amb presumpció de veracitat i ple valor probatori — data, hora, identitat de l'infractor, tipus de soroll i mesurament [4]. El dictamen d'un pèrit acústic amb equipament homologat és prova contundent en el litigi [4]; els límits orientatius en interiors ronden els 35-45 decibels de dia i els 25-30 de nit [4]; i el Defensor del Pueblo ha hagut de recordar a les administracions que habilitin mitjans per comprovar les denúncies [4].

El forat del sistema és estructural: el soroll és intermitent i la inspecció és puntual. El local que punxa música fins a la matinada calla la nit que ve el tècnic; la màquina que vibra cada matinada descansa el dia de la visita. El veí que ho pateix té la informació que l'acta no pot capturar — la recurrència — però la seva gravació amb el mòbil no és cap acta, ni ho serà mai.

La divisió del treball, un altre cop: el ciutadà no substitueix el sonòmetre oficial; aporta la cronologia que el fa arribar a temps. Un diari del soroll segellat — registres datats nit rere nit, amb empremta i integritat acreditades [5] — no prova decibels, però prova persistència: dates, hores, durades, un patró que cap inspecció puntual no pot negar i que permet programar la visita oficial quan toca. La mesura oficial fa la foto; el diari segellat fa la pel·lícula. I un expedient necessita totes dues coses.

La prova d'existència aplicada

Un balcó, un sensor de trenta euros i una sèrie de dades que cap advocat no pot esborrar.

1. La sèrie que ningú no pot retocar

El sensor ciutadà de qualitat de l'aire ancora cada lot de lectures en origen: empremta SHA-512, segell de temps, blockchain pública [5]. Quan la plataforma veïnal presenta tres anys de dades davant de

l'ajuntament o del jutjat, la discussió sobre «dades retocades» s'acaba abans de començar: la sèrie és exactament la que era, amb els seus buits datats i tot. La crítica legítima queda circumscrita on toca — el calibratge, el mètode [3] —, que és exactament la discussió que la ciència ciutadana pot guanyar amb transparència. És el contrapès del capítol 96: allà, el sensor de la xemeneia vigilat pel regulador; aquí, la ciutadania que vigila el vigilant.

2. L'abocament fotografiat

El purí al torrent, el fum negre de matinada, la runa al descampat: la denúncia ambiental viu o mor segons la qualitat del seu rastre. Una sèrie de fotografies segellades al moment — empremta, data certa, ubicació — construeix la progressió: no una imatge solta que «podria ser de qualsevol dia», sinó una cronologia amb integritat acreditada que l'autoritat ambiental pot verificar abans d'obrir expedient [5]. I el mateix escut protegeix el denunciat honest: contra la foto vella reciclada en una campanya de descrèdit, l'absència de segell coetani parla sola.

3. El diari del soroll

El veí que pateix la màquina de cada matinada registra, nit rere nit, l'episodi: data, hora, durada, una gravació orientativa — tot segellat al seu dispositiu [5]. Al cap de tres mesos, presenta a l'ajuntament una cronologia amb integritat acreditada que converteix la seva paraula en patró verificable, i la inspecció amb sonòmetre homologat — l'única que aixeca acta amb valor probatori [4] — es programa quan el patró diu que passarà, no quan el local ho espera. El diari segellat no mesura decibels: fa que la mesura oficial arribi a l'hora de la veritat.

4. La veu de la llacuna

Els guardians del Mar Menor — la societat civil que seu al comitè de representants de l'ecosistema-persona [2] — poden donar memòria criptogràfica al seu seguiment: mostres d'aigua documentades, episodis fotografiats, sèries de sensors comunitaris [3][5]. Quan calgui defensar davant d'un tribunal el dret de la llacuna «a existir i evolucionar naturalment» [2], la seva veu legal portarà cronologies verificables, no records militants. I la mateixa lògica val per a Doñana: la cronologia ciutadana d'extraccions i assecaments, segellada any rere any, és el contrapès permanent d'aquell pla hidrològic que «no computava» [1].

Els límits, amb honestedat: el segell acredita quan i què es va registrar, no que el sensor mesurés bé — el calibratge i el mètode continuen sent la batalla científica [3]; la dada ciutadana no és una acta oficial ni un dictamen pericial, i no ha de pretendre ser-ho [4]; i la vigilància ambiental té una frontera ètica: es documenten fets, instal·lacions i episodis — mai la vida dels veïns. Sense mètode, el segell blinda soroll; sense ètica, blinda un setge.

La promesa i el perill

La promesa és una ciutadania que ja no depèn que l'administració vulgui mesurar [1]: sèries de sensors blindades [5], ecosistemes amb veu legal i memòria [2], inspeccions oficials que arriben a l'hora [4] i expedients que aguanten. La vigilància ambiental democràtica: mesurar, certificar, actuar.

Els perills demanen la mateixa claredat.

El primer és **el veïnat-policia**. La línia entre documentar la contaminació i vigilar les persones és fina. La càmera apunta a la xemeneia, no a la cuina del veí; al torrent, no al passeig de qui hi va. Es documenten fets ambientals; els rostres, les matrícules i les vides d'altri no hi tenen lloc, i el disseny de només-empremtes no legitima cap difusió [5].

El segon és **la falsa equivalència**. Segellat no vol dir exacte. Una dada mal calibrada amb data certa continua sent una dada dolenta — més perillosa i tot, perquè sembla sòlida. Si la ciència ciutadana ven el segell com a certificat de qualitat, perdrà la credibilitat que busca: el segell acredita integritat i moment; l'exactitud l'acrediten el calibratge i el mètode [3].

El tercer és **la instrumentalització**. També un interès industrial o polític pot disfressar-se de «plataforma veïnal» i inundar l'expedient de cronologies segellades esbiaixades. L'antídot no és criptogràfic sinó metodològic: transparència sobre qui mesura, amb què, com i amb quin protocol. El segell garanteix que ningú no ha retocat les dades — no que les hagin recollides de bona fe.

I el quart és **l'excusa administrativa**. Si la dada ciutadana serveix perquè l'administració es desentengui — «ja mesuren els veïns» —, haurem perdut. El TJUE va condemnar Espanya perquè l'Estat no computava [1], i el Defensor del Pueblo reclama mitjans per inspeccionar [4]: la ciència ciutadana és contrapès i complement del deure públic de mesurar, mai el seu substitut.

És hora d'actuar

La natura no pot declarar; qui la vigila, sí — si porta les dates a prova de dubte.

Per a la ciutadania i les entitats ambientals: munteu sensors amb protocols documentats [3], segelleu les sèries i les fotografies en origen [5], i penseu en cronologies llargues — la persistència és la vostra força.

Per als ajuntaments: obriu canals per rebre cronologies ciutadanes segellades i programeu la inspecció oficial — l'acta amb sonòmetre homologat [4] — quan el patró ho indiqui; el Defensor del Pueblo ja us ho recorda [4].

Per a les confederacions i agències ambientals: computeu-ho tot — la lliçó de Doñana és que el buit de dades es paga a Luxemburg [1] — i tracteu la sèrie ciutadana ancorada com el que és: un indici qualificat que mereix comprovació.

Per a les plataformes de ciència ciutadana: incorporeu l'ancoratge per defecte [3][5]: és la diferència entre un mapa bonic i un expedient que aguanta.

Per als guardians d'ecosistemes amb drets: doneu memòria criptogràfica a la veu del Mar Menor [2] — cada mostra i cada episodi, amb data certa.

Per als legisladors: reconeixeu la cronologia ciutadana segellada com a base suficient per activar inspeccions, i finançeu la xarxa pública de mesura — que el contrapès no hagi de fer de titular.

Doñana va trigar dotze anys a tenir sentència perquè les extraccions «no es computaven» [1]; el Mar Menor va necessitar 639.826 signatures per tenir veu [2]. Que la pròxima llacuna no hagi d'esperar tant: doneu-li testimonis amb data certa. Per la terra que no pot declarar, **time2act**.

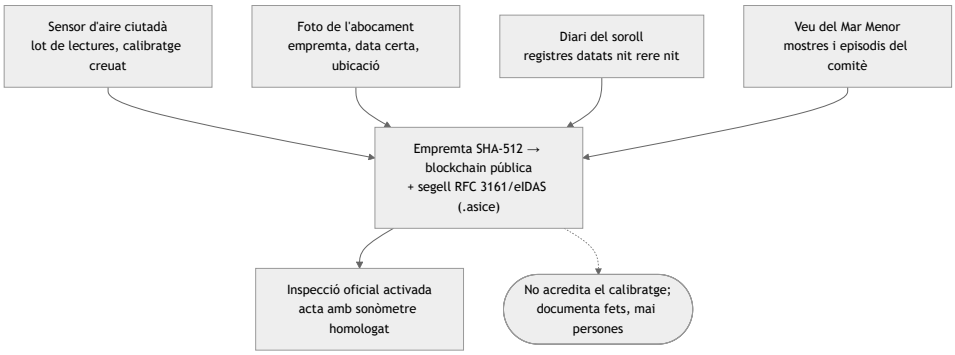


Figura 97.1 — La ciència ciutadana amb prova d'existència: el sensor del balcó, la foto de l'abocament i el diari del soroll s'ancoren en origen (empremta SHA-512, segell de temps RFC 3161/eIDAS, blockchain pública, .asice) i esdevenen cronologies amb integritat acreditada que activen la inspecció oficial (acta amb sonòmetre homologat, amb presumpció de veracitat), orienten el pèrit i donen memòria a la veu legal dels ecosistemes (Mar Menor, Llei 19/2022). Límits: el segell no acredita el calibratge ni substitueix l'acta oficial; es documenten fets, no persones. Fonts: TJUE (Doñana, 2021); BOE (Llei 19/2022); Sensor.Community; Defensor del Pueblo.

---

[1] El Ágora Diario — *Europa condena a España por no proteger el agua y hábitats de Doñana* (sentència del TJUE de 24 de juny de 2021; extraccions il·legals no computades al Pla Hidrològic 2015-2021; queixes des del 2009); Greenpeace — *Doñana, agua sin ley* (pous, basses i canonades; hivernacles de fresses; desforestacions). 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 — *Llei 19/2022, de 30 de setembre, per al reconeixement de personalitat jurídica a la llacuna del Mar Menor i la seva conca* (primer ecosistema d'Europa; drets a existir, evolucionar, protecció, conservació i restauració; ILP amb 639.826 signatures); Araoz & Rueda — *El TC reconoce la personalidad jurídica del Mar Menor*; BOE — *Reial Decret 90/2025* (comitè de representants: 13 membres, 7 de la societat 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)* (més de 100 països; sensors ciutadans de baix cost); AireCiudadano — xarxa oberta de monitors de partícules amb mapa i API; SciStarter/CanAirIO — sensors oberts 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* (inspecció municipal amb sonòmetre homologat i calibrat; actes amb presumpció de veracitat i ple valor probatori; límits interiors orientatius 35-45 dB dia / 25-30 dB nit); COITTA — *La importancia de la prueba pericial acústica*; Defensor del Pueblo — *Comprobaciones ante las denuncias de ruidos molestos* (habilitar mitjans per comprovar les denúncies). 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 producte (empremta SHA-512 a l'origen — sensor o dispositiu —; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; sèries per lots en temps real; buits datats; contingut al dispositiu i revelació voluntària). Vegeu els capítols 13 i 15; el sensor industrial, al capítol 96; el testimoni orbital, al capítol 104. ↩

El passaport del producte: qui jura el contingut reciclat, i quan

«Si els noms no són correctes, el llenguatge no s'adiu amb la veritat de les coses.»

— Confuci, Analectes, XIII, 3

El 4 de juny del 2024, **Volvo Cars** va presentar al seu nou SUV elèctric **EX90** el que la marca i el seu soci **Circulor** van anomenar «el primer passaport de bateria del món», gairebé tres anys abans que el mandat europeu el fes obligatori. Construït durant cinc anys amb l'empresa britànica de cadena de blocs Circulor, a un cost aproximat de **10 dòlars per vehicle** per a quinze anys de seguiment, el passaport permet al propietari escanejar un **codi QR** al muntant de la porta del conductor —o obrir l'aplicació de Volvo— i veure la química de la bateria, l'origen i el recorregut de producció del seu cobalt, níquel, ions de liti i grafit, el **percentatge de contingut reciclat** i la **petjada de carboni** incorporada de tot el paquet. Circulor afirma haver recollit ja més de **20.000 milions de punts de traçabilitat** a través de **150 milions de cel·les**, treballant amb proveïdors que representen aproximadament el **52 % de la producció mundial** de cel·les [5][6]. El cas és vívid precisament perquè exposa la tensió de fons del passaport digital de producte: el document registra i data fidelment tot el que la cadena de subministrament declara, però el llinatge de prova de concepte del propi EX90 —el pilot de la Global Battery Alliance del 2023 amb Audi i Tesla— admetia obertament que «la qualitat de les dades presentades no ha estat plenament verificada i s'ha complementat parcialment amb estimacions raonables» [7]. Un passaport bellament estructurat pot, doncs, transportar una declaració de contingut reciclat inflada o sense verificar. És exactament el risc de *greenwashing* que el mateix escombrat de la UE del 2020 va quantificar: prop del **42 % de les afirmacions verdes** de les empreses europees eren falses o enganyoses.

Aquest capítol tracta el **passaport de cicle de vida d'un objecte físic concret** al llarg de tota la seva vida, diferent del capítol 29 —la cadena de subministrament, que és la custòdia i la procedència dels inputs mentre les mercaderies passen d'un actor a un altre. Aquí el subjecte no és el flux de materials, sinó **una sola bateria**: el seu percentatge de contingut reciclat, les dades de reparabilitat i desmuntatge, l'**estat de salut** en ús i l'estatus de **segona vida** i fi de vida —afirmacions que persisteixen i s'actualitzen *després* que el producte s'ha venut. La pregunta no és si es pot construir un passaport bonic —Volvo ja n'ha construït un—, sinó com fer que cada xifra que conté sigui **demostrable** i no només declarada.

El document fidel a una dada que ningú no ha comprovat

Un passaport digital és, en essència, un contenidor de declaracions: estructurat, llegible per màquina i accessible amb un QR. La seva virtut —recollir-ho tot en un sol lloc verificable— és també el seu taló d'Aquil·les, perquè el document és exactament tan bo com les dades que hi entren. El pilot de la **Global Battery Alliance**, presentat a Davos el 18 de gener del 2023 amb Audi, BASF, CATL, Glencore, Tesla i Volkswagen, ho va dir amb una franquesa rara: les dades «no han estat plenament verificades» i es van «complementar parcialment amb estimacions raonables» [7]. Aquesta frase, enterrada en una nota de premsa triomfal, és la clau del capítol. El passaport no fabrica veritat; transporta el que se li dona.

I el que se li dona són **xifres falsificables amb conseqüències legals**. Des del 18 d'agost del 2031, el Reglament europeu de bateries imposa llindars mínims de contingut reciclat —**cobalt 16 %**, **plom 85 %**, **liti 6 %**, **níquel 6 %**—, que en un segon esglaó a partir del 2036 pugen a **cobalt 26 %**, **liti 12 %**, **níquel 15 %** [2]. Són percentatges precisos que el passaport ha de declarar, i cadascun és una temptació: un punt percentual de cobalt reciclat «de més» abarateix el compliment i millora la imatge. El cobalt verge reetiquetat com a reciclat a la fosa no deixa cap empremta visible al document; el passaport, dòcil, el registra com a reciclat. Aquesta és la diferència entre un sistema que **estructura** la informació i un que la **prova**.

L'estat de salut que sobreviu a la venda

Hi ha una segona família de declaracions que fa el passaport de producte radicalment diferent de la simple traçabilitat de la cadena: les que **s'actualitzen mentre l'objecte viu**. Circulor anuncia quinze anys de **monitoratge de l'estat de salut** (*state of health*) de la bateria de l'EX90 [6]. Aquesta xifra —la capacitat que conserva el paquet respecte del seu valor nou— determinarà el preu d'un EX90 de segona

mà el 2032, si una bateria és apta per a una **segona vida** com a emmagatzematge estacionari o si ha d'anar al reciclatge. És una afirmació que viu i canvia després de la venda, i el seu valor econòmic és immens.

Justament per això és manipulable. L'estat de salut surt del sistema de gestió de la bateria (el BMS); una exportació de diagnòstic és un fitxer, i un fitxer es pot retocar. Un venedor sense escrúpols té tots els incentius per maquillar la capacitat d'una bateria gastada abans de revendre el cotxe; un operador de segona vida, per declarar apta una cel·la que no ho és. El passaport, de nou, registrarà obedientment la xifra que se li lliuri. La promesa d'un mercat de segona mà i de segona vida transparent —un dels grans guanys ambientals de tota l'economia circular— depèn que aquestes lectures siguin **autèntiques**, no només **presents** al document.

El marc regulador: el passaport com a llei, no com a favor

Europa ha convertit el passaport en obligació, no en gest voluntari. El **Reglament (UE) 2023/1542** de bateries, que deroga la directiva de 2006 i s'aplica des del 18 de febrer de 2024, fa **obligatori el passaport de bateria a partir del 18 de febrer de 2027** per a tota bateria de vehicle elèctric, tota bateria industrial de més de 2 kWh i tota bateria de mitjans de transport lleugers (LMT) col·locada al mercat europeu, accessible via QR enllaçat a un identificador únic; les bateries posades al mercat després d'aquesta data sense passaport registrat **no es poden vendre legalment**, i les autoritats duaneres reben accés directe al registre a la frontera [1][3]. La **declaració de petjada de carboni** ja va començar per a les bateries de vehicle elèctric el 18 de febrer de 2025 i s'estén a les industrials de més de 2 kWh el 18 de febrer de 2026; segueix el mètode ISO 14040/44 i la PEF europea i **l'ha de verificar un organisme notificat —no es pot autocertificar** [3].

Per damunt, el **Reglament d'ecodisseny de productes sostenibles (UE) 2024/1781** (ESPR), en vigor des del 18 de juliol de 2024, eleva el passaport digital de producte a **eina horitzontal** que s'estendrà a tèxtils, ferro i acer, alumini, mobiliari i pneumàtics segons el pla de treball 2025-2030, com hem vist, adoptat el 16 d'abril de 2025; la bateria n'és el pilot legalment vinculant [8]. El comitè **CEN-CENELEC JTC 24** desenvolupa els estàndards horitzontals (identificadors únics, portadors de dades, enllaç físic-digital, interoperabilitat, drets d'accés), i els projectes **CIRPASS / CIRPASS-2**, finançats per la Comissió, defineixen el model de dades transversal. Un detall revela la prudència del legislador: les obligacions de **diligència deguda** de la cadena es van ajornar dos anys, del 18 d'agost de 2025 al 18 d'agost de 2027, mitjançant el Reglament (UE) 2025/1561, l'omnibus de «aturar el rellotge» [4]. La llei demana xifres precises; encara s'està construint el sistema que les ha de fer fiables.

Per què el passaport sol no salva

Cal dir-ho amb cruesa. Un passaport digital de producte, per ben estructurat i ple de QR que estigui, **és tan fiable com la voluntat de qui hi aboca les dades**. Un certificat de contingut reciclat penjat al passaport és un PDF; res no impedeix que el percentatge s'hagi inflat abans d'entrar-hi. Una exportació d'estat de salut és un fitxer; res al document no demostra que reflecteixi el paquet real i no una lectura del BMS retocada. Una declaració de petjada de carboni pot seguir el mètode PEF al peu de la lletra i alhora alimentar-se de dades d'activitat falses. I la verificació de l'organisme notificat, encara que sigui obligatòria per a la petjada de carboni, no s'estén a cada lectura d'estat de salut ni a cada certificat de reciclat al llarg de quinze anys de vida.

El passaport resol el problema de **tenir** la informació en un lloc accessible i estandarditzat. No resol el problema d'**acreditar** que la informació era certa i no s'ha tocat. Falta una capa que fixi, per a cada artefacte probatori subjacent —el certificat del reciclador, l'informe de l'organisme notificat, l'exportació del BMS—, **qui el va emetre, quan, i que no s'ha alterat des d'aleshores**. Sense aquesta capa, el pilot de la GBA tenia raó: les dades del passaport sovint estan «estimades» i «no plenament verificades», i el document les beneeix igualment.

La prova d'existència aplicada

És aquí on **t2p** aporta la peça que falta, i ho fa sobre l'**acte probatori** darrere de cada afirmació, no sobre l'entrada de la base de dades. En el moment en què un proveïdor o un fabricant genera un artefacte primari —un certificat de lot del reciclador amb el contingut de cobalt o ions de liti reciclat, un informe de

verificació d'empremta de carboni d'un organisme notificat, una exportació de diagnòstic d'estat de salut del BMS al final de la primera vida, un acta d'inspecció de desmuntatge o de segona vida, o una foto d'un lot de material a una mina o a una planta de triatge—, el dispositiu calcula localment l'**empremta SHA-512** (el fitxer **no surt mai** del dispositiu), obté un **segell de temps RFC 3161 conforme a eIDAS**, l'ancora a la cadena de blocs pública i l'empaqueta en un contenidor **.asice** verificable fora de línia. Per a la captura de camp —una mina, una línia de reciclatge, una badia de desballestament— el **GPS forense** i una **prova de vida** lliguen el registre a un lloc real i a una persona real en un moment real.

El QR del passaport pot transportar, al costat de l'afirmació llegible per humans, un **enllaç verificable** a aquell artefacte segellat. Qualsevol —un agent de duanes a la frontera, el comprador d'un EX90 usat que llegeix l'estat de salut de segona vida, un auditor que comprova el llindar de contingut reciclat— pot confirmar **fora de línia** que *aquest* certificat de reciclat o *aquesta* lectura d'estat de salut existia, inalterat, en *aquesta* data i d'*aquest* autor, abans que es publiqués l'afirmació. Complementa la pila regulada —la verificació de l'organisme notificat de l'article 7, el llibre de regles d'assegurament de dades de la GBA, els estàndards de portadors de dades del JTC, la traçabilitat blockchain a l'estil Circulor— donant a cada document subjacent un rastre de procedència a prova de manipulació, sense substituir mai la verificació. És, sobre el cicle de vida del producte, el germà de la marca C2PA i SynthID dels capítols 13 i 15: aquells segellen **el que un model produeix**; t2p segella **el que un objecte ha viscut**.

Ara el límit, amb tota la cruesa. **«Escombraries a l'entrada, escombraries a la cadena»**: el segell prova l'origen, l'instant, l'autor i la integritat d'un artefacte de cicle de vida; **no prova que l'afirmació que conté sigui certa**. No confirma que el cobalt reciclat fos realment reciclat i no metall verge reetiquetat a la fosa, ni que una exportació d'estat de salut segellada reflecteixi el paquet real i no un BMS manipulat, ni que una anàlisi de cicle de vida fes servir dades d'activitat honestes, ni que una bateria de «segona vida» sigui realment segura per redesplegar. Un certificat de contingut reciclat falsificat, un cop segellat, esdevé un certificat falsificat **a prova de manipulació**. t2p fixa la procedència i la inalterabilitat; no substitueix l'avaluació de conformitat de l'organisme notificat, l'auditoria de diligència deguda, l'assaig físic del material ni el judici humà que decideixen si el contingut segellat és legítim.

La promesa i el perill

La promesa és un mercat circular on el llinatge d'un producte és verificable i no només publicat: poder demostrar que aquest percentatge de reciclat, aquesta empremta de carboni i aquest estat de salut van ser declarats per aquest actor en aquella data, i que ningú no els ha retocat des d'aleshores. Per al comprador d'un EX90 usat, per a l'auditor —com hem vist— i per a l'agent de duanes, fer l'origen inalterable converteix una promesa de màrqueting en una afirmació amb conseqüències.

El perill demana els matisos de sempre. El primer, no confondre integritat amb veritat: un passaport ple d'artefactes ben segellats però amb dades inflades continua sent un passaport enganyós, ara amb una pàtina de rigor tecnològic que pot adormir l'auditor —«està ancorat, doncs deu ser cert»— quan el segell no diu res sobre la veritat del contingut. El segon, la concentració: si segellar i passaportar surt a compte només als grans fabricants —els 10 dòlars per vehicle de Volvo escalen malament per a un taller de reparació petit—, l'estàndard pot expulsar els actors petits de la reparació i la segona vida en lloc d'enfortir-los. I el tercer, la privacitat i el secret industrial: el passaport exposa dades de la cadena que poden ser sensibles, i cal equilibrar la transparència amb el dret legítim a no revelar-ho tot. La prova d'existència és una capa de governança del cicle de vida, no un certificat de bondat ambiental.

És hora d'actuar

Per als **fabricants i marques** (Volvo, els seus parells de l'automoció i, aviat, els del tèxtil i de l'electrònica): segellar cada artefacte probatori en el moment de generar-lo —certificat de reciclat, informe de petjada de carboni, lectura d'estat de salut— i enllaçar-lo des del QR del passaport, perquè cada xifra tingui data certa i autor. Per als **recicladors i organismes notificats**: segellar els certificats de lot i els informes de verificació a l'emissió, de manera que l'auditor pugui confirmar-los fora de línia sense dependre de la bona fe del registre. Per als **reguladors i les autoritats duaneres** (la Comissió sota l'ESPR, el JTC 24, les duanes amb accés directe des del 2027): reconèixer l'artefacte segellat com a evidència de la procedència que el passaport ja exigeix, i tractar la data certa com la diferència entre una declaració i una coartada fabricada posteriorment. Per als **proveïdors de plataformes de passaport** (Circulor i els seus competidors): ancoratge de l'empremta de cada document subjacent, no només estructurar-ne el contingut. I per als **compradors i operadors de segona vida**: exigir l'enllaç

verificable a l'estat de salut segellat abans de pagar per una bateria usada, perquè la lectura sigui autèntica i no només present.

A Gotemburg, el 4 de juny del 2024, un cotxe va sortir de fàbrica amb el primer passaport de bateria del món i una nota al peu que admetia que les dades no estaven «plenament verificades». Donar a cada producte una prova segellada de cada afirmació que fa al llarg de la seva vida —sense oblidar mai que el segell no fa veritable el reciclat que algú declara— és, en aquest front on un objecte ha de respondre del que diu de si mateix, time2act.

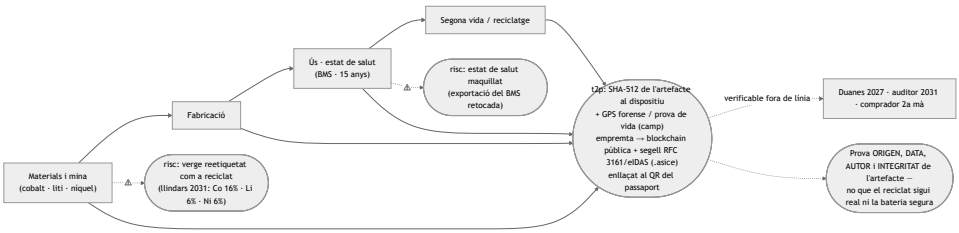


Figura 98.1 — El cicle de vida d'una bateria en quatre baules: materials i mina → fabricació → ús i estat de salut → segona vida / reciclatge. Cada baula genera un artefacte probatori (certificat de reciclat, informe de petjada de carboni de l'organisme notificat, exportació del BMS, acta de desmuntatge); t2p en calcula l'empremta SHA-512 al dispositiu i l'ancora a la blockchain pública, amb segell RFC 3161/eIDAS complementari (.asice), amb GPS forense i prova de vida en captura de camp. El QR del passaport enllaça l'afirmació amb l'artefacte segellat, verificable fora de línia per duanes, auditors i compradors de segona mà. Límit: el segell prova origen, data, autor i integritat de l'artefacte; no prova que el contingut reciclat sigui real, que l'estat de salut no s'hagi maquillat ni que la bateria sigui segura. Fonts: Volvo EX90 / Circulor; Global Battery Alliance; Reglament (UE) 2023/1542; ESPR (UE) 2024/1781.

---

[1] EUR-Lex — *Sustainability rules for batteries and waste batteries (Regulation (EU) 2023/1542 summary)* (passaport des de 2027 via QR i identificador únic; objectius de contingut reciclat des del 18 d'agost de 2031: Co 16 %, Pb 85 %, Li 6 %, Ni 6 %; accés duaner al registre). 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)* (percentatges de 2031 —Co 16/Pb 85/Li 6/Ni 6— i de 2036 —Co 26/Pb 85/Li 12/Ni 15—, les afirmacions falsificables que el passaport transporta). https://digiprodpass.com/blogs/eu-battery-regulation-recycled-content-targets ↩

[3] Circularise — *EU battery passport regulation requirements* (calendari per fases: petjada de carboni VE 18 feb 2025 / industrial 18 feb 2026; passaport 18 feb 2027; verificació per organisme notificat; àmbit VE/industrial >2 kWh/LMT). https://www.circularise.com/blogs/eu-battery-passport-regulation-requirements ↩

[4] Minespider — *EU Battery Due Diligence Obligations postponed* (diligència deguda ajornada del 18 ago 2025 al 18 ago 2027 via Reglament (UE) 2025/1561 «stop-the-clock»; guia ampliada fins al 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; cinc anys de desenvolupament amb Circulor; ~10 $/vehicle per 15 anys; QR al muntant de la porta; traça materials, contingut reciclat i petjada de carboni). 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* (més de 20.000 milions de punts de dades a 150 milions de cel·les; ~52 % dels fabricants mundials de cel·les; 15 anys de monitoratge d'estat de salut). https://spectrum.ieee.org/volvo-ex90-battery-passport ↩

[7] Global Battery Alliance — *World's First Battery Passport Proof of Concept* (Davos, 18 gen 2023; Audi/BASF/CATL/Glencore/Tesla/VW; les dades «no han estat plenament verificades i s'han complementat parcialment amb estimacions raonables»). https://www.globalbattery.org/press-releases/global-battery-alliance-launches-world%E2%80%99s-first-battery-passport-proof-of-concept/ ↩

[8] Comissió Europea (Green Forum) — *Implementing the Ecodesign for Sustainable Products Regulation (ESPR)* (ESPR en vigor el 18 jul 2024; el passaport digital de producte com a eina horitzontal; pla de treball 2025-2030 adoptat 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* (anàlisi jurídica que distingeix el pilot de bateries del desplegament horitzontal de l'ESPR; calendari d'actes delegats). https://www.hoganlovells.com/en/publications/digital-product-passports-in-the-eu-comprehensive-expansion

[10] CIRPASS — *Standardisation gaps and roadmap (v1.2, July 2024)* (model de dades del DPP, identificadors únics, portadors de dades i llacunes d'estandardització del JTC 24 — l'arquitectura on s'endolla el segell). https://cirpassproject.eu/wp-content/uploads/2024/07/CIRPASS-standardisation-gaps-and-roadmap-V1.2.pdf

Residus: on va de debò el contenidor

«On porten cada dia la seva càrrega els escombriaires, ningú no s'ho pregunta.»

— Italo Calvino, Les ciutats invisibles (1972), «Leonia»

Cada vespre, a milions de cuines, es repeteix la mateixa coreografia: esbandir el pot de iogurt, plegar la caixa de cartró, i baixar-ho tot — el groc dels envasos, el blau del paper, el marró de l'orgànica. És un gest de confiança pura: ningú de nosaltres no ha vist mai què passa després. Confiem que aquell gest té sentit, que el viatge acaba bé, que «es recicla» vol dir que es recicla.

La pregunta d'aquest capítol és exactament aquesta: on va, de debò, el contenidor? I la urgència no és retòrica [1]: Europa exporta residus a escala industrial — Turquia sola va rebre el 39 % de les exportacions europees, 12,4 milions de tones en un any —, i la trajectòria d'aquests carregaments ha estat prou fosca perquè la Unió hi hagi hagut d'intervenir: el Reglament (UE) 2024/1157 de trasllats de residus, aplicable de manera general des del 21 de maig de 2026, sotmet les exportacions de tots els residus plàstics a notificació i autorització prèvies per escrit, prohibeix exportar residus per a valorització a països de fora de l'OCDE i imposa la tramitació electrònica dels trasllats [1].

Entre el teu contenidor i el «reciclat» final hi ha una cadena — recollida, transferència, gestor, tractament, sovint un camió o un vaixell — feta de canvis de mans i papers de part. Quan tot va bé, ningú no ho mira; quan no, ho descobrim tard: el «reciclatge» que era abocament, el certificat signat sense tractament, l'etiqueta verda sense res a sota.

Aquest capítol tracta l'acte de fe col·lectiu més gran del nostre temps. El passaport del producte nou — el seu contingut reciclat, la seva segona vida — és al capítol 98; les emissions trucades, al capítol 96; l'origen de les mercaderies, al capítol 29; la cadena de custòdia del socors — la mateixa lògica, invertida —, al capítol 50; la prova ciutadana, al capítol 97. Pregunta clau: com se sosté un sistema que mou milions de gestos i milers de milions en taxes sobre albarans que ningú no pot verificar? Resposta: donant data certa a cada canvi de mans amb **t2p** — la cadena empremta–hora–àncora del capítol 13 [3] — de la bàscula al certificat de tractament final. Les regles noves del Reglament [1] valen el que valgui l'albarà que les documenta; la traça verificable és el que les fa valdre.

La cadena del residu — i on es trenca

La cadena, tal com és: el productor — la fàbrica, el comerç, la llar — genera el residu; la recollida el porta a una planta de transferència, on es consoliden fluxos; el gestor autoritzat l'encamina cap al tractament — reciclatge, valorització o eliminació —; i sovint hi ha un trasllat pel mig: un camió cap a una altra comunitat, un contenidor cap a un altre continent. La normativa ja exigeix documents d'identificació i seguiment per a cada pas, i el nou Reglament europeu els vol electrònics i amb autorització prèvia quan creuen fronteres [1].

Els punts de trencament tenen noms coneguts al sector. La subcontractació en cascada: el gestor autoritzat que delega en un altre, que delega en un tercer — i els papers es van diluint a cada esglaó. El certificat de tractament final signat lluny del tractament. El balanç de massa que no quadra: a la planta hi entren més tones que no en surten de tractades, i la diferència s'evapora en informes incomplets. L'exportació que es declara «valorització» i acaba en un abocador a l'altra punta del món. I, coronant-ho tot, el greenwashing: el «100 % reciclable», el «zero abocament» — afirmacions que cap consumidor no pot contrastar.

La clau probatòria és la de tot aquest llibre: tots aquests forats passen entre albarans de part — modificables, extraviables, sense data certa oposable. Les responsabilitats ampliades del productor paguen per tones declarades; les autoritats inspeccionen mostres; i el ciutadà, que sosté el sistema amb el seu gest i les seves taxes, no pot verificar res de res.

La prova d'existència aplicada

La mateixa cadena, baula a baula — i cada canvi de mans amb lloc, hora i pes certs [3].

1. El contenidor amb lloc i hora

A cada canvi de mans — la càrrega del camió, l'entrada a la planta de transferència, la descàrrega al gestor —, una foto amb el GPS forense de t2p: fix genuí, precisió d'uns 50 metres, antiguitat màxima d'uns 30 segons; una ubicació simulada bloqueja la certificació [3]. El contenidor que surt d'un municipi i «apareix» on no toca deixa de ser una sospita: és una cadena de captures datades amb un forat exactament allà on algú l'ha desviat. I el precintat del contenidor d'exportació, filmat amb la data i l'hora sobreimpreses [3], viatja com a evidència amb el vaixell.

2. El balanç de massa segellat

Els registres de bàscula — què entra, què surt, quan — certificats per lots amb empremtes encadenades: cada tancament, una empremta que incorpora l'anterior [3]. El balanç de massa d'una planta esdevé una sèrie datada que ningú no pot reescriure: si un mes hi entren mil tones i en surten sis-centes de tractades, la diferència té data i exigeix explicació. És la mateixa lògica que l'Estat ja imposa a les factures: la cadena d'empremtes com a normalitat comptable.

3. El certificat de tractament final

El document que tanca el cercle — «aquest residu ha estat tractat així, aquí, aquest dia» — escanejat i segellat amb data certa, lligat per empremta als albarans i captures de tota la cadena [3]. El productor que paga la seva responsabilitat ampliada sap què ha pagat; l'autoritat que autoritza un trasllat [1] pot exigir el certificat ancorat del destí; i el gestor honest — que és la majoria — té en la seva pròpia traça la defensa contra la competència deslleial de qui fa veure que tracta.

4. L'afirmació verda, congelada

El «fabricat amb 70 % de material reciclat», el «zero residus a abocador», la pàgina de sostenibilitat corporativa: capturats amb el navegador certificat de t2p — imatge completa i codi font, amb data [3]. El dia que la realitat no quadri amb l'eslògan, l'eslògan d'aquell dia existeix, exacte i datat. I el pont amb el capítol 98: el passaport del producte declara contingut reciclat — la traça del residu és l'única manera que aquella declaració tingui d'on venir.

I els límits, que també n'hi ha: el segell acredita custòdia — lloc, hora, pes, document —, no la qualitat del tractament: que el reciclatge sigui reciclatge de debò ho han de dir les inspeccions i les anàlisis. El balanç de massa pot enganyar si la primera pesada ja és falsa — la cadena val des d'on comença, i per això ha de començar a la bàscula d'entrada. I la traça és de la càrrega i dels documents, mai de les persones: la proporcionalitat amb els treballadors de planta mana, com a tots els capítols laborals d'aquest llibre.

La promesa i el perill

La promesa: taxes de responsabilitat ampliada pagades sobre tones verificades, no declarades; trasllats internacionals [1] amb expedients que el regulador pot auditar sense viatjar; gestors honestos que competeixen amb traça en lloc de patir la competència del frau; i el gest del ciutadà — el contenidor de cada vespre — correspost, per fi, amb una cadena que es pot ensenyar.

I els perills, un per un.

El primer és **el segell com a maquillatge**. Certificar albarans falsos amb data certa només fa el frau més elegant. La traça val el que val la seva primera baula: bàscules calibrades, captures al moment, inspeccions que contrasten físicament. La criptografia documenta; no substitueix el control.

El segon és **la càrrega sobre el petit gestor**. El deixaller municipal i la petita planta no poden absorbir burocràcia infinita. El gest ha de ser el de sempre — la foto de deu segons a la bàscula [3] — i el gruix documental, automàtic; si la traça esdevé barrera d'entrada, només quedaran els grans.

El tercer és **la vigilància de la planta**. Documentar càrregues no pot esdevenir vigilar treballadors. Es capturen bàscules, contenidors i documents; les persones, mai — la línia de tots els capítols laborals d'aquest llibre.

I el quart és **el tecnosolucionisme del contenidor**. La millor traça del món no redueix ni un gram de residu. La jerarquia és la de sempre: reduir, reutilitzar — i només després reciclar bé. La prova d'existència fa honest el tercer esglaó; els dos primers són decisions de producció i de consum que cap hash no pren per nosaltres.

És hora d'actuar

Que el gest de milions tingui la traça que mereix.

Per als ciutadans: el vostre gest mereix traça — exigiu als vostres municipis i als sistemes d'envasos dades verificables, no percentatges de fullet [1].

Per als gestors i les plantes: la foto a la bàscula i el balanç per lots [3] — la vostra honestedat, demostrable, és el vostre millor contracte.

Per als productors i els sistemes de responsabilitat ampliada: pagueu — i cobreu — sobre tones amb data certa; el certificat de tractament ancorat com a condició de pagament.

Per a les autoritats ambientals i la fiscalia: el nou Reglament [1] us dona la tramitació electrònica; demaneu-la ancorada — l'expedient verificable del trasllat és la diferència entre autoritzar i beneir.

Per als legisladors: que el desplegament espanyol del Reglament i el sistema de dipòsit i retorn d'envasos anunciat neixin amb data certa neutral de sèrie — seria el primer sistema de residus del món verificable de la bàscula al certificat.

Que el pot de iogurt de cada vespre tingui el viatge que li vam prometre — i que qui el desviï deixi empremtes. Pel gest de milions que mereix ser veritat, **time2act**.

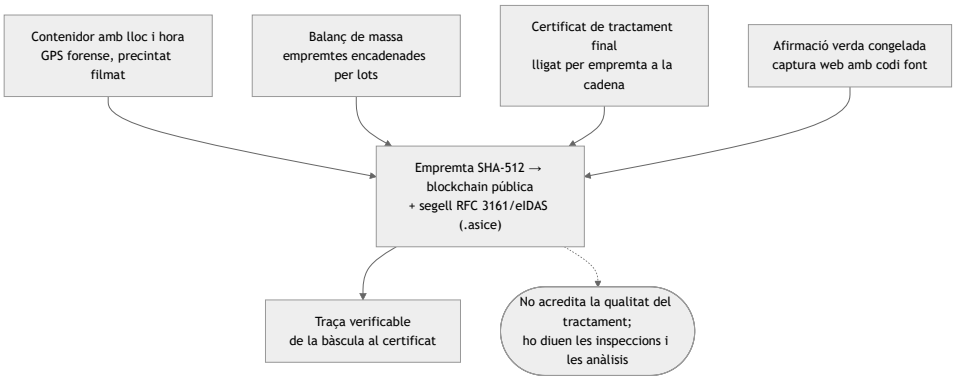


Figura 99.1 — La cadena del residu amb prova d'existència (segellat amb t2p — capítol 13): el contenidor amb lloc i hora a cada canvi de mans (GPS forense; precintat filmat amb data sobreimpresa), el balanç de massa segellat per lots encadenats (entrades vs sortides datades), el certificat de tractament final ancorat i l'afirmació verda congelada (captura web amb codi font). Context: Reglament (UE) 2024/1157, aplicable des del 21-5-2026 — notificació prèvia per a tot residu plàstic exportat, prohibició cap a països no OCDE; Turquia rebia el 39 % de les exportacions europees (12,4 Mt). Límits: la traça acredita custòdia, no qualitat de tractament; primer reduir i reutilitzar. Fonts: DOUE/BOE; RETEMA.

---

[1] DOUE/BOE — *Reglament (UE) 2024/1157, d'11 d'abril de 2024, relatiu als trasllats de residus* (deroga el Reglament 1013/2006; aplicable de manera general des del 21 de maig de 2026; exportacions de tots els residus plàstics a tercers països subjectes a notificació i autorització prèvies per escrit; prohibició d'exportar residus per a valorització a països no OCDE; tramitació electrònica); RETEMA — *Nuevo Reglamento de traslados de residuos*; Residuos Profesional — *Análisis del Reglamento (UE) 2024/1157* (context: Turquia va rebre el 39 % de les exportacions europees de residus — 12,4 milions de tones, dades 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] Marc general de residus (documents d'identificació i seguiment dels trasllats; responsabilitat ampliada del productor; jerarquia de residus). Vegeu el capítol 98 per al passaport digital de producte i el capítol 96 per a les emissions.

[3] t2p — manual de producte (foto amb GPS forense — fix genuí ~50 m / ≤30 s, la ubicació simulada bloqueja la certificació; vídeo amb data/hora sobreimpresa; escàner de documents fins a 50 pàgines; certificar qualsevol fitxer per lots — només l'empremta viatja; captura de pàgina web amb imatge completa + codi font; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; el passaport de producte, al capítol 98; la ciència ciutadana, al capítol 97. ↩

El camp i la PAC: el quadern verificable

«El sòl és el gran connector de vides, origen i destinació de tot. És el guaridor, el restaurador i el ressuscitador.»

— Wendell Berry, The Unsettling of America (1977)

El tractor aturat al marge, el mòbil a la mà bruta de terra — i una notificació de l'administració: el satèl·lit «no ha detectat activitat agrària» a la parcel·la declarada; cal aportar una fotografia georeferenciada en un termini, o l'ajuda perilla. El pagès mira el camp que va sembrar fa sis setmanes — el camp que és allà, amb les línies verdes del blat acabat de néixer — i entén el que li acaba de passar: ara ha de provar l'evident a un algorisme.

L'escena es va fent quotidiana perquè la política agrària comuna — el pressupost més gran de la Unió Europea — ha canviat de manera de vigilar [2]: de la inspecció presencial a mostres, al monitoratge per satèl·lit. Els Sentinel del programa Copernicus escanegen cada parcel·la declarada, i els sistemes classifiquen si allò que es va declarar — el cultiu, la pastura, el guaret — es veu des de dalt; quan no poden concloure — núvols, parcel·les petites, cultius tardans —, la càrrega baixa a terra: una foto georeferenciada que l'agricultor fa amb el mòbil [2].

Aquest capítol tracta la finca com a subjecte de prova. El testimoni orbital i les seves manipulacions són al capítol 104; el frau alimentari — què hi ha de debò al plat —, al capítol 101; la geolocalització de parcel·les contra la desforestació, al capítol 29; els sensors ciutadans, al capítol 97; els residus de la finca, al capítol 99. Pregunta clau: quan l'ull que reparteix les ajudes és un algorisme orbital, amb què es defensa el pagès que sí que va sembrar? Resposta: amb la seva pròpia cronologia — el quadern segellat al moment i al camp, la foto amb data certa neutral — mitjançant **t2p**: empremta al dispositiu i hora certa ancorada a la cadena (capítol 13) [3]. La simetria del capítol 104, mirada des de baix.

El quadern que ve — i el satèl·lit que ja hi és

La segona peça del tauler té calendari exacte [1]: el quadern digital d'explotació — el CUE, el registre electrònic de les actuacions de cada finca: tractaments fitosanitaris, fertilització, regs i altres pràctiques — està disponible voluntàriament des de l'1 de gener de 2024 i, després de successius ajornaments, serà obligatori l'1 de gener de 2028 per a les explotacions més grans: més de 30 hectàrees de cultiu, més de 5 de regadiu o més de 0,1 d'hivernacle. Abans, una fita intermèdia: el registre electrònic dels tractaments fitosanitaris serà obligatori l'1 de gener de 2027 — el paper s'acaba el 31 de desembre de 2026 [1].

La lectura d'aquest llibre — i ja és la tercera vegada que passa: primer les factures amb VeriFactu, després el registre horari, ara el camp: l'Estat demana registres digitals d'actuacions, i vigila amb ulls orbitals. L'arquitectura de la prova d'existència s'imposa a l'agricultura... però amb una asimetria: el satèl·lit és de l'administració, les apps són de l'administració, i el quadern viurà en plataformes que l'administració consulta. El pagès posa les dades; la prova, la custodien altres.

I el matís tècnic que ho canvia tot: el satèl·lit també s'equivoca. Núvols persistents, parcel·les petites, cultius tardans o atípics, marges — el sistema que «no detecta activitat» pot estar mirant malament [2]. Quan això passa, l'agricultor honest es troba en la posició més kafkiana d'aquest llibre: provar contra un algorisme que el seu camp existeix.

La prova d'existència aplicada

El quadern i la foto, sí — però segellats al moment, al camp, i en mans del pagès [3].

1. L'entrada del quadern, al moment i al camp

El tractament fitosanitari, l'adobada, el reg — anotats quan es fan, on es fan: l'entrada del quadern segellada amb t2p amb el GPS forense del camp — fix genuí, precisió d'uns 50 metres, antiguitat màxima d'uns 30 segons; una ubicació simulada bloqueja la certificació [3]. La diferència amb el quadern «reconstruït el diumenge a taula» és probatòria i és sanitària: el registre fet al moment és el que val quan arriba la inspecció, el residu al producte o el dubte sobre terminis de seguretat. I quan el CUE sigui obligatori [1], la versió segellada del pagès serà el seu contrast davant de qualsevol discrepància de plataforma.

2. La foto que el satèl·lit demana — amb data certa neutral

La fotografia georeferenciada que el sistema de monitoratge reclama [2], feta amb t2p: lloc i hora certs, amb el certificat i el seu codi QR [3]. No és només complir el tràmit: és que la resposta del pagès tingui el mateix rang probatori que la pregunta de l'algorisme — una evidència verificable per tercers, no una imatge més dins d'una app que fa el que fa.

3. La defensa contra l'ull que s'equivoca

La simetria decisiva: la sèrie de fotos datades del cultiu — la sembra, la naixença, el creixement — feta amb quatre gestos al llarg de la campanya [3]. Quan el satèl·lit «no vegi» el que hi és — els núvols, la parcel·la petita, el cultiu tardà [2] —, el pagès no comença de zero contra la notificació: té una cronologia ancorada que demostra l'activitat agrària abans que ningú la qüestionés. És el capítol 104 mirat des de baix: el testimoni orbital és poderós, però no infal·lible — i qui treballa la terra mereix poder-lo contradir amb fets.

4. L'expedient de l'ajuda

La sol·licitud, el quadern segellat, les fotos de campanya, les respostes als requeriments — agrupats i exportables com a paquet .asice verificable sense connexió [3]: per al recurs contra una reducció d'ajuda, per a la inspecció presencial, per a la traçabilitat que el comprador del gra o la cooperativa comencen a demanar. I el pont amb els veïns de part: el que el camp produeix entra a la cadena del capítol 101, i en surten els residus del capítol 99 — la finca verificable és la primera baula de totes dues.

Els límits, dits clarament: el segell acredita actuacions, llocs i dates — no substitueix el quadern oficial ni les plataformes de l'administració: les contrasta i les complementa [1]. No fa bones les pràctiques — els límits de fitosanitaris i les condicions de les ajudes són els que són [2]. I la bretxa digital del camp és real: l'eina ha de ser el gest de deu segons amb el mòbil que ja es duu a la butxaca, i les cooperatives i els tècnics, els aliats de qui no s'hi avé.

La promesa i el perill

La promesa: pagesos que responen als requeriments del satèl·lit amb cronologies pròpies [2][3]; quaderns que valen com a prova perquè es van escriure al moment [1]; ajudes que es cobren i es defensen amb fets datats; i una traçabilitat de finca que el mercat començarà a pagar — el gra amb pedigrí ja no és una utopia: és la continuació natural dels capítols 29 i 101.

Els perills, mirats de cara.

El primer és **el camp vigilat**. El monitoratge orbital més el quadern digital poden fer del pagès la professió més fiscalitzada del país. La resposta és la d'aquest llibre: que la traça serveixi les dues direccions — si l'administració mira des de dalt, el pagès ha de poder respondre des de baix amb el mateix rang de prova; vigilància sense simetria és submissió.

El segon és **la burocràcia que expulsa**. Cada requisit nou pesa més a la finca petita. El calendari del CUE ja ho reconeix — obligatori només per a les grans, de moment [1] —; l'eina ha de restar feina, no afegir-ne: l'anotació al moment és més ràpida que la reconstrucció del diumenge.

El tercer és **l'algorisme com a jutge**. Si la notificació del satèl·lit es tracta com a veritat per defecte, la presumpció d'innocència agrària mor. El sistema de monitoratge és un filtre, no un veredicte [2]; les seves discrepàncies s'han de resoldre amb evidència de terra — i la càrrega de la prova no pot ser tota del pagès.

Queda el quart, el més temptador: creure que amb això n'hi ha prou. Cap segell no arregla els preus en origen, la sequera ni el relleu generacional. La prova d'existència fa justes les ajudes i defensables les finques; la política agrària la fan — i l'han de fer bé — les persones.

És hora d'actuar

Que el camp que és allà es pugui demostrar des d'allà.

Per a pagesos i ramaders: l'anotació al moment amb GPS forense [3] — el quadern que es fa al camp val el doble que el que es reconstrueix; i la sèrie de fotos de campanya és la vostra pòlissa contra l'ull que s'equivoca [2].

Per a cooperatives i tècnics: sou la capa que fa possible tot això per a la finca petita — integreu el segellat als vostres serveis de quadern i de sol·licitud [1][3].

Per a l'administració agrària: el monitoratge us estalvia inspeccions [2]; retorneu la simetria — accepteu la cronologia ancorada del pagès com a contrast qualificat de les discrepàncies del satèl·lit, i que les vostres apps emetin evidència verificable, no captiva.

Per als compradors i la indústria: la finca amb traça pròpia és el primer graó de la vostra cadena — els capítols 29 i 101 en són la continuació; pagueu-la com el que val.

Per als legisladors: el CUE arribarà [1]; que arribi amb la prova en mans de qui la genera — el quadern segellat pel pagès, amb data certa neutral, com a registre amb valor probatori ple.

Fa deu mil anys que la pagesia alimenta el món sense que ningú li demanés provar-ho; ara que li ho demanen des de l'espai, que almenys tingui les eines. Pel camp que és allà — i que es pugui demostrar —, **time2act**.

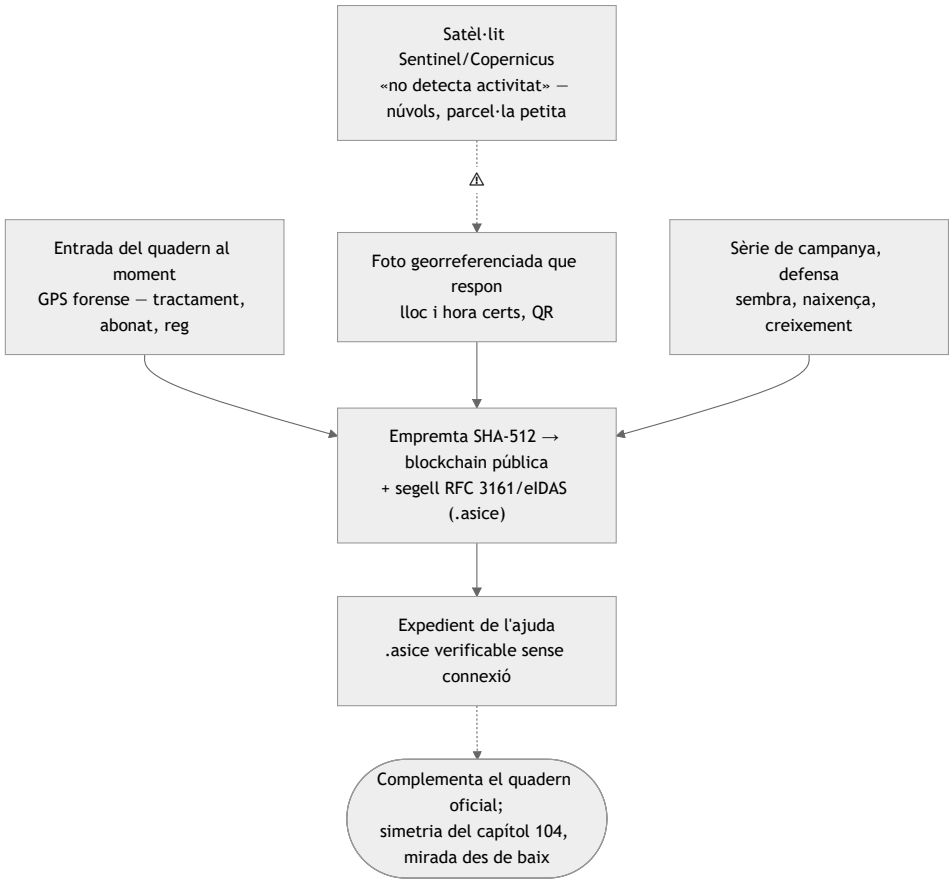


Figura 100.1 — El camp amb prova d'existència (segellat amb t2p — capítol 13): l'entrada del quadern segellada al moment i al camp (GPS forense), la foto georeferenciada que el monitoratge demana — amb data certa neutral —, la sèrie de campanya com a defensa contra el satèl·lit que s'equivoca (la simetria del capítol 104, mirada des de baix) i l'expedient de l'ajuda en .asice. Context: PAC vigilada per Sentinel/Copernicus; quadern digital (CUE) voluntari des de 2024, fitosanitaris electrònics des de l'1-1-2027, CUE obligatori l'1-1-2028 (>30 ha). Límits: complementa el quadern oficial, no el substitueix; la bretxa digital del camp exigeix cooperatives i tècnics com a aliats. Fonts: FEGA/normativa CUE; PAC 2023-2027.

---

[1] Agrodigital — *El cuaderno digital de explotación será obligatorio a partir del 1 de enero de 2028* (CUE voluntari des de l'1-1-2024; ajornaments; obligatori des de l'1-1-2028 per a explotacions >30 ha de cultius, >5 ha de regadiu o >0,1 ha d'hivernacle; registre electrònic de tractaments fitosanitaris obligatori des de l'1-1-2027 — paper fins al 31-12-2026); FEGA/Agronews — aclariments d'entrada en vigor; Govern d'Aragó — *Cuaderno digital (CUE)* (contingut: actuacions fitosanitàries, fertilització, regs i altres pràctiques). 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 seguiment per monitoratge (imatges Sentinel/Copernicus sobre les parcel·les declarades al SIGPAC; requeriments de fotografies georeferenciades a l'agricultor quan el sistema no pot concloure). Marc general del FEGA i

de la Comissió Europea. Vegeu el capítol 104 per a la integritat del testimoni orbital. ↩

[3] t2p — manual de producte (foto amb GPS forense — fix genuí ~50 m / ≤30 s, la ubicació simulada bloqueja la certificació; certificació en segon pla — el camp sense cobertura; certificar qualsevol fitxer per lots; escàner de documents; projectes per a l'expedient d'una campanya; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; el satèl·lit, al capítol 104; els aliments, al capítol 101; els residus, al capítol 99. ↩

Frau alimentari: quan l'etiqueta menteix sobre el que t'has menjat

«Digues-me què menges i et diré què ets.»

— Jean Anthelme Brillat-Savarin, Physiologie du goût (1825), aforisme IV

La nit del 8 al 9 de juliol de 2024, el Comandament dels Carabinieri per a la Tutela de la Salut (NAS) d'Itàlia, dins del marc OPSON coordinat per Europol, va escorcollar divuit magatzems de la regió de la Pulla i va comissar unes **42 tones d'oli adulterat** ja envasat i etiquetat com a «oli d'oliva verge extra italià», més unes 71 tones d'una «substància oliosa», per prop d'un milió de dòlars. El detall que ho explica tot: els investigadors van trobar **623 litres de clorofil·la** que s'afegien a olis barats per falsejar el color verd del verge extra autèntic, amb etiquetes «verge extra» falsificades i **1.145 segells d'impostos especials** sospitosos de ser falsos. Set persones van ser acusades d'associació delictiva, adulteració d'aliments per a la venda, frau en subministraments públics i militars i adulteració per a l'exportació [3]. Tot venia de l'Operació Omegabad de novembre de 2023 (Guàrdia Civil + Carabinieri + Europol), que va comissar **260.000 litres** d'oli —«lampante» barat tallat i venut com a verge extra a Ciudad Real, Sicília i la Toscana—, va detenir onze sospitosos i va confiscar 91.000 euros en efectiu [4]. L'onada seguia el preu rècord del verge extra a l'engròs, uns 10,50 €/kg a començament de 2024, després que la sequera andalusa reduís les collites a gairebé la meitat.

Aquest capítol tracta una pregunta diferent de la dels seus veïns. El capítol 29 cobreix la cadena de subministrament genèrica —custòdia, logística i procedència de mercaderies—; el capítol 72, l'extracció il·legal i l'origen conflictiu d'una matèria primera. Aquí parlem específicament de l'**autenticitat i l'origen de l'aliment**: l'adulteració (tallar l'oli amb lampante o gira-sol, la mel amb xarop de sucre), la substitució d'espècie (cavall per vedella) i les **falses al·legacions geogràfiques** de denominació protegida. La pregunta és simple i antiga: *és aquest producte el que diu l'etiqueta?* I la tesi del llibre hi encaixa: davant d'un frau que viu de la **paperassa falsa** —etiquetes, certificats, segells—, la prova d'existència fixa qui va declarar què, on i quan, sense poder retrodatar-ho.

Un negoci d'uns 40.000 milions que viu del premi de l'origen

El frau alimentari afecta aproximadament l'1 % de la indústria mundial i suposa un cost anual d'entre 10.000 i 40.000 milions de dòlars [7]. La Xarxa de Frau Agroalimentari de la UE va registrar 758 sospites el 2023, un 26 % més que l'any anterior, amb substitució de carn, adulteració de mel i oli mal etiquetat al capdamunt [7]. El valor de vendes anual dels productes amb indicació geogràfica de la UE era de 74.800 milions d'euros el 2017, prop del 7 % de les vendes d'aliments i begudes, i un producte amb denominació protegida es ven en mitjana al doble del preu d'un comparable sense certificar [6]; com més valuosa és la denominació, més temptador resulta falsificar-la.

L'**Operació OPSON XIII** (resultats anunciats l'octubre de 2024) va confiscar unes 22.000 tones d'aliments per uns 91 milions d'euros, desmantellant onze xarxes i denunciant 278 persones; a Itàlia es van trobar 42 tones de fals verge extra i 623 litres de clorofil·la, i a Espanya 45.000 litres d'oli i 120.000 llaunes de tonyina [1]. L'**Operació OPSON XIV** (anunciada el 2025) va elevar la xifra a uns 95 milions d'euros —11.566 tones d'aliments i 1,4 milions de litres de begudes—, amb 631 persones denunciades i tretze grups de crim organitzat desarticulats en 31 països [2].

La mel que no és mel i el cavall que era vedella

L'oli no és l'únic front. En l'acció coordinada europea «From the Hives» (mostres de novembre de 2021 a febrer de 2022, resultats publicats el 21 de març del 2023), **147 de 320 partides de mel importada — el 46 %—** van resultar sospitoses d'adulteració amb xarops de sucre, un augment enorme respecte al 14 % registrat el 2015-17. El càlcul és transparent: la mel real costava de mitjana uns 2,32 €/kg importada i el xarop d'arròs entre 0,40 i 0,60 €/kg; la UE n'importa unes **175.000 tones l'any**, prop del 40 % del consum [5]. Així, una de cada dues partides arribava sota sospita de no ser mel veritable.

I cap repàs no és complet sense l'episodi que va sacsejar Europa. En l'escàndol de la carn de cavall de 2013, la lasanya de vedella de Findus contenia més del 60 % —fins al 100 %— de carn de cavall. Al judici de París del 16 d'abril del 2019, l'exresponsable de Spanghero, Jacques Poujol, va rebre dos anys (divuit

mesos suspesos) i una multa de 100.000 euros; el comerciant neerlandès Jan Fasen, dos anys i una prohibició permanent del sector càrnic, per la venda de més de **500 tones de carn de cavall** canalitzades a través de Comigel cap a 28 empreses de tretze països [9]. Una etiqueta pot mentir al llarg de mitja Europa abans que ningú no ho noti.

La llei de l'origen: un registre reforçat, però de paper

La resposta normativa ha estat substancial. El règim d'indicacions geogràfiques de la UE es va revisar amb el **Reglament (UE) 2024/1143**, en vigor des del **13 de maig de 2024**, que fusiona les regles de DOP, IGP i IG per a aliments, vins i begudes espirituoses en un únic marc de registre i reforça la protecció de les indicacions usades com a ingredient i venudes en línia [8]. El **Reglament (UE) 2017/625** de controls oficials dona base legal als controls al llarg de la cadena i a la **Xarxa de Frau Agroalimentari (FFN)** de la DG SANTE, connectada al sistema d'alertes RASFF. Els estàndards de l'oli (Reg. 2022/2104 i 2022/2105) defineixen les categories —verge extra, verge, lampant—, i la Directiva de la mel 2001/110/CE es va reforçar el 2024 amb la Directiva (UE) 2024/1438. Als Estats Units, els controls preventius de la **FSMA** obliguen a protegir-se contra l'adulteració per motius econòmics (EMA); l'exemple canònic és l'oli barat venut com a 100 % oli d'oliva [10]. I OPSON hi aporta la força operativa cada any.

El problema és que tota aquesta arquitectura descansa sobre **documents**: certificats de conformitat, números de lot, informes de laboratori, segells d'impostos i etiquetes de denominació. Un document, com hem vist a la Pulla, es pot falsificar, clonar, reciclar o retrodatar; el registre 2024/1143 indica quina denominació mereix protecció, però no garanteix que aquest certificat sigui genuí ni que aquesta analítica cobreixi aquest lot.

Per què el certificat sol no salva

Cal dir-ho amb cruesa. Un certificat de conformitat en PDF, un número de lot imprès o un informe de laboratori signat no demostren res si es poden alterar sense deixar empremta. Com hem vist a la Pulla, els defraudadors van crear les etiquetes «verge extra» i segells d'impostos per fer passar la mentida pels controls. Un certificat genuí d'un lot petit pot servir per emparar un enviament molt més gran diluït després; un informe autèntic d'un lot honest es pot adjuntar, retocant-ne la data, a un lot adulterat; i si el segell d'impostos és falsificable, tota la cadena de garanties s'esquerda. El que falta no és més paper: cal un ancoratge inalterable que fixi qui va emetre cada artefacte d'autenticitat, sobre quin lot i en quin instant, de manera que no es pugui clonar ni retrodatar.

La prova d'existència aplicada

És aquí on **t2p** aporta la capa que falta, sobre la paperassa i l'acte de camp, no sobre la química. Funciona en tres fases. Primer, en crear el lot, el productor captura fotos i vídeo geoetiquetats i amb prova de vida de l'olivar, del rusc o de la línia d'envasat; el dispositiu calcula l'empremta SHA-512 al mateix aparell —el fitxer no surt mai—, l'ancora a la **blockchain pública**, hi afegeix un segell de temps complementari RFC 3161 conforme a eIDAS, i el GPS forense vincula l'acte al territori DOP/IGP reclamat, fixant *on* i *quan* es va produir el lot abans que cap barreja pugui passar. Segon, se segellen els artefactes d'autenticitat: l'informe del laboratori acreditat (perfil NMR/IRMS, ràtio isotòpica, pol·len per a la mel, àcids grassos per a l'oli), el certificat de conformitat, el número de lot, els documents d'impostos i l'art de l'etiqueta DOP/IGP, cadascun empremtat i segellat en un contenidor **.asice** verificable fora de línia i lligat a un identificador de lot. Tercer, qualsevol inspector, importador o tribunal pot verificar, sense connexió, que el certificat, l'informe i les fotos d'origen existien aleshores, els va emetre aquell organisme i no s'han alterat ni retrodatat —desactivant etiquetes falsificades, segells clonats i certificats reciclats vistos a OPSON i Omegabad. És el complement, sobre l'etiqueta i el document, del que proposen els capítols 13 i 15 amb C2PA per a la procedència de la imatge i del certificat, i pot alimentar el passaport digital de producte del capítol 98.

El límit és clar: «escombraries a l'entrada, escombraries a la cadena». El segell prova origen, temps, autor i integritat d'un artefacte capturat; **no** comprova que el contingut segellat sigui veritat, legítim ni segur. No pot dir si l'oli de l'ampolla és realment verge extra, si la mel està tallada amb xarop d'arròs o si l'al·legació geogràfica és químicament certa: això només ho determina l'anàlisi de laboratori (NMR, IRMS, ADN, pol·len). Un productor deshonest encara pot segellar una foto autèntica d'un olivar equivocat, empremtar un certificat genuí que cobreix menys lot del que s'expedeix o segellar paperassa correcta d'un

producte adulterat. No atura la substitució aigua avall ni val res si l'organisme certificador mateix és corrupte; és una eina probatòria i antiretrodatació *sobre* —mai en lloc de— l'autenticació de laboratori, els controls oficials, la certificació acreditada i el judici humà.

La promesa i el perill

La promesa és un ecosistema agroalimentari on l'origen i la garantia documental siguin **verificables i no retrodatables**: poder demostrar amb data certa que aquell certificat, aquell informe i aquelles fotos de l'olivar existien, els va emetre l'organisme legítim i no s'han tocat. En un sector on el premi de la denominació es ven al doble i el frau costa fins a 40.000 milions l'any, **com hem vist**, fer l'origen inalterable protegeix el productor honest, l'importador prudent i el consumidor.

El perill demana els matisos de sempre. Primer, no confondre **integritat amb veritat**: una paperassa falsa i segellada continua sent falsa, i ara, a més, immutable; el segell podria donar una falsa tranquil·litat —«està ancorat, doncs és genuí»— sense correspondència amb la química real. Segon, la **dependència de l'organisme certificador**: si el consell regulador o el laboratori són captius o corruptes, el segell n'eternitza la mentida amb aparença de rigor. I tercer, la **bretxa digital**: imposar un segell avançat podria expulsar el petit cooperativista o el productor del sud global sense laboratori acreditat ni eina a l'abast, concentrant encara més el mercat de la qualitat.

És hora d'actuar

Per als **consorcis i consells reguladors de DOP/IGP**: segellar el número de lot, l'art de l'etiqueta i el certificat en emetre'ls, perquè una etiqueta clonada com les de la Pulla falli la verificació. Per als **laboratoris acreditats i organismes de control**: ancorar l'informe analític (NMR/IRMS, pol·len, àcids grassos) i el certificat de conformitat al moment d'emissió, vinculant-los a l'identificador de lot. Per als **productors i cooperatives**: capturar la prova de camp geoetiquetada amb prova de vida i GPS forense a la collita, al rusc o a la línia d'envasat, abans de qualsevol barreja. Per als **inspectors i duanes** (NAS, Guàrdia Civil, OPSON, OLAF): verificar fora de línia l'autenticitat i la data dels segells i certificats, en lloc de fiar-se'n a ull. I per als **reguladors i la DG SANTE**: reconèixer l'artefacte segellat com a evidència de la documentació exigida i alimentar-hi la xarxa d'alertes —com hem vist al Reg. 2024/1143—.

A la Pulla, una nit d'estiu, set persones omplien ampolles d'oli barat tenyit amb **623 litres** de clorofil·la i hi enganxaven etiquetes i segells falsos perquè passessin per verge extra italià. Donar a cada lot honest una prova segellada del seu origen, la seva data i el seu certificat —sense oblidar mai que el segell no fa veritat el que s'hi declara— és, en aquest front on l'etiqueta pot mentir sobre el que ens mengem, time2act.

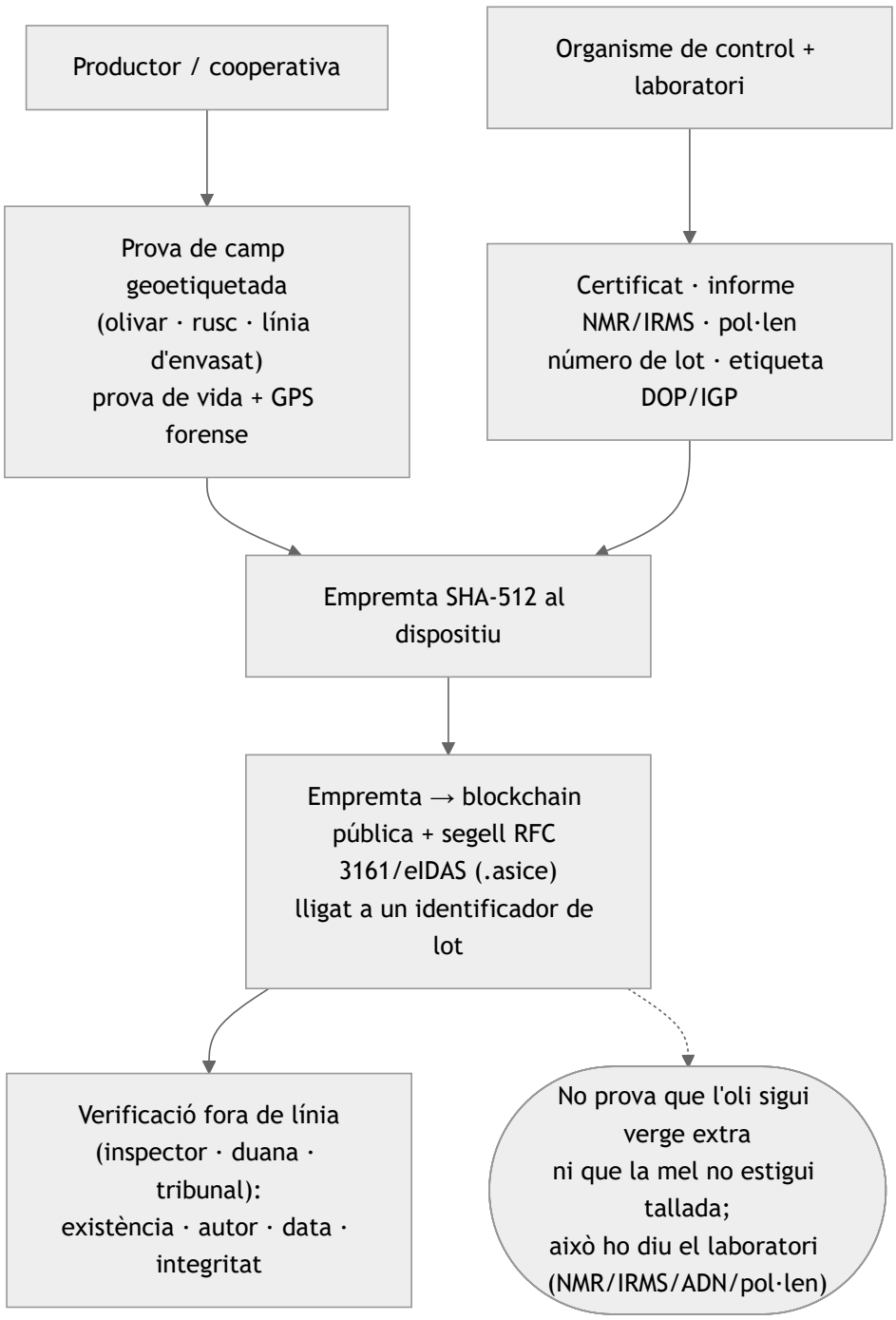


Figura 101.1 — El productor captura la prova de camp geoetiquetada amb prova de vida i GPS forense (olivar, rusc, línia d'envasat) i en calcula l'empremta SHA-512 al dispositiu; en paral·lel, l'organisme de control i el laboratori segellen el certificat, l'informe analític, el número de lot i l'etiqueta DOP/IGP. L'empremta de tot plegat s'ancora a la blockchain pública, amb segell RFC 3161/eIDAS complementari (.asice), lligat a un identificador de lot. Qualsevol inspector, duana o tribunal ho verifica fora de línia: existència, autor, data i integritat. Límit: el segell prova el paper i l'acte de camp, no que l'oli sigui verge extra ni que la mel no estigui tallada —això ho diu el laboratori (NMR/IRMS/ADN/pol·len). Fonts: OPSON XIII i XIV (Europol); cas Pulla; Operació Omegabad; «From the Hives»; Reg. (UE) 2024/1143.

---

[1] Europol — *EUR 91 million worth of counterfeit and substandard food seized in Europe-wide operation* (Operació OPSON XIII; 22.000 t d'aliments, 91 M€, 11 xarxes; Itàlia: verge extra i clorofil·la; Espanya: oli i tonyina). 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* (Operació OPSON XIV; 95 M€, 11.566 t, 631 denunciats, 13 grups de crim organitzat, 31 països). 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 juliol de 2024; escorcoll dels Carabinieri a la Pulla, 42 t de fals verge extra, 623 L de clorofil·la, 7 acusats, etiquetes i segells 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* (desembre de 2023; Operació Omegabad: 260.000 L comissats, 11 detencions, lampante venut com a verge extra, Ciudad Real/Sicília/Toscana, 91.000 € en efectiu). https://www.foodsafetynews.com/2023/12/spanish-and-italian-investigators-uncover-olive-oil-fraud/ ↩

[5] Comissió Europea (DG SANTE) — *EU coordinated action on honey ('From the Hives')* (mostres 2021-2022; 46 % de 320 partides sospitoses d'adulteració amb xarop de sucre; metodologia i països participants). 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 les IG de la UE: 74.800 M€ el 2017; prima de preu d'unes 2 vegades per als productes protegits). https://www.foodnavigator.com/Article/2020/04/22/Geographical-Indications-worth-a-mouth-watering-75-billion-study/ ↩

[7] Comissió Europea — *EU Agri-Food Fraud Network: reports and publications* (el frau afecta ~1 % de la indústria i costa 10.000-40.000 M$/any; 758 sospites el 2023, +26 %; carn, mel i oli al capdamunt). 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 maig de 2024; marc únic de DOP/IGP/IG i ETG; protecció com a ingredient i en línia). 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* (judici de 2019; Poujol (Spanghero) 2 anys + 100.000 € de multa, Fasen 2 anys + prohibició permanent; Comigel, 500+ t cap a 13 països). https://www.foodsafetynews.com/2019/04/four-sentenced-in-france-for-roles-in-horse-meat-scandal/ ↩

[10] FDA — *Economically Motivated Adulteration (Food Fraud)* (definició d'EMA, p. ex. oli barat venut com a 100 % oli d'oliva; deure de controls preventius 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; estat de l'art en segellat/ancoratge de la procedència de l'oli i en autenticació analítica NMR/IRMS). https://www.mdpi.com/1424-8220/24/24/8189

Qui ho va fer, i en quines condicions: la diligència deguda en la mà d'obra

«Considereu si això és un home: / que treballa dins el fang, / que no coneix la pau, / que lluita per mig pa, / que mor per un sí o per un no.»

— Primo Levi, «Shemà», Si això és un home (1947)

A finals de gener i durant el febrer de 2024, la duana dels Estats Units va retenir milers de cotxes de luxe del **grup Volkswagen** —models **Porsche, Bentley i Audi**— als ports nord-americans. El motiu no era el motor, ni la carrosseria, ni l'acer alemany: era una **peça electrònica diminuta**, amagada en la profunditat de la cadena, amb material rastrejable fins a **Xinjiang**, la regió on la *Uyghur Forced Labor Prevention Act* presumeix que tot bé es fabrica amb treball forçat. Volkswagen va declarar que no havia sabut l'origen del component al nord-oest de la Xina fins que un proveïdor el va avisar a mitjan gener de 2024, després que les autoritats nord-americanes ja l'haguessin marcat el desembre de 2023; va prometre substituir la peça en tots els cotxes venuts arreu del món i va treballar per alliberar els vehicles [4]. L'episodi és la dimensió laboral en estat pur: els cotxes i el seu acer eren «d'Alemanya», però la pregunta que els va aturar al moll era **qui havia fet una peça minúscula molt avall de la cadena, i en quines condicions**.

Aquest capítol és diferent del capítol 29 —la integritat de la cadena de subministrament—, que segella **d'on** ve un bé i la seva custòdia física: l'origen de l'objecte. Aquí parlem de la capa **social** que s'hi superposa: qui el va fabricar i sota quines condicions laborals, el registre de diligència deguda en drets humans i el testimoni dels treballadors, no la geografia del material. La pregunta del capítol és: com es fixa, amb data certa i de manera que no es pugui retrodatar ni desestimar com a *deepfake*, **la prova del que sabíem i del que vam fer** sobre les persones que hi ha al final de la cadena. L'episodi de Volkswagen ho cristal·litza: una multinacional pot quedar cega davant d'un proveïdor de quart o cinquè nivell que no veu.

Una xacra de 28 milions de persones i 236.000 milions de dòlars

La magnitud és aclaparadora. L'**OIT** estima que **27,6 milions de persones** estaven en treball forçat en un dia qualsevol del 2021, 2,7 milions més que el 2016; **17,3 milions** són explotades a l'economia privada i els **treballadors migrants** corren un risc **tres vegades** més gran [1]. El treball forçat genera **236.000 milions de dòlars** de beneficis il·legals l'any —64.000 milions més (un 37 %) que el 2014—, amb els beneficis més alts a Europa i l'Àsia Central (**84.000 milions**) [2]. Com hem vist, no és un problema de països llunyans: és un model de negoci global i una part dels diners es fa a casa.

L'episodi de Volkswagen no va sortir del no-res. El febrer del 2024, **Human Rights Watch** va publicar l'informe *Asleep at the Wheel*, que documentava l'exposició dels fabricants d'automòbils —VW, BMW, Mercedes-Benz, GM i d'altres— al treball forçat uigur a la cadena de l'alumini i els components [5]. El juny del 2023, l'**ECCHR** havia presentat una denúncia davant la **BAFA** alemanya, al·legant que Volkswagen, BMW i Mercedes-Benz havien incomplert la Llei alemanya de cadenes de subministrament pels seus vincles amb Xinjiang. El risc no era invisible: ja estava documentat i denunciat abans que la duana actués.

El risc migra de la roba al cotxe

Durant anys, el treball forçat es va associar al tèxtil; ja no. Entre juny de 2022 i juliol de 2025, la duana nord-americana (**CBP**) va retenir **16.755 enviaments** valorats en **3.690 milions de dòlars** sota la UFLPA; només el 2024 va retenir mercaderia per **1.340 milions**, i gairebé el **48 %** de les retencions d'aquell any van acabar amb l'entrada denegada [3]. La xifra que ho diu tot: les retencions al sector de l'**automòbil i l'aeroespacial** van créixer quasi un **1.600 %** el 2024 respecte al 2023 —de 59 a 991 enviaments entre gener i novembre—, una prova que el risc de treball forçat ha emigrat de la roba als béns manufacturats complexos [3].

I la pressió creix. El **14 de gener de 2025**, el **DHS** va fer la seva ampliació més gran de l'*Entity List* de la UFLPA, afegint **37 empreses** xineses d'energia i tèxtil i portant la llista negra de presumpció refutable a **144 entitats** [3] —com hem vist anteriorment—. Cada nom afegit converteix una cadena fins llavors

tranquil·la en un camp de mines documental: el comprador ha de demostrar, amb proves «clares i convincents», que el seu producte no en conté cap.

La llei ja exigeix vigilar tota la cadena

El marc normatiu s'ha endurit a ambdues ribes de l'Atlàntic. Als **EUA**, la **UFLPA** (vigent des del 21 de juny de 2022) presumeix que tot bé fet totalment o parcial a Xinjiang, o per una entitat de la llista, és producte de treball forçat i queda barrat, llevat que proves «clares i convincents» ho refutin. A la **UE**, la **Directiva de diligència deguda en sostenibilitat corporativa (CSDDD, Directiva 2024/1760)** va entrar en vigor el **25 de juliol de 2024**, cobrint les empreses amb 5.000 empleats i 1.500 milions d'euros de facturació (i les de fora amb 1.500 milions de facturació a la UE); després de les esmenes Òmnibus, la transposició s'ajorna fins al **26 de juliol de 2028** i l'aplicació al **26 de juliol de 2029** [6]. El **Reglament europeu de treball forçat**, vigent des del **13 de desembre de 2024** i aplicable a partir del **14 de desembre de 2027**, prohibeix qualsevol producte fet amb treball forçat, però sense presumpció geogràfica —la càrrega de la prova recau en les autoritats, a diferència de la UFLPA [7]. A **Alemanya**, la **LkSG** s'aplica a les empreses de 1.000 empleats des de l'1 de gener de 2024; la BAFA pot imposar multes de fins a **800.000 euros o el 2 % de la facturació mundial**, i el 2023 va fer **486 auditories** [8]. Sota tot hi ha el marc internacional: els convenis 29 i 105 de l'OIT i els Principis Rectors de l'ONU sobre empreses i drets humans.

Per què l'auditoria social sola no salva

Cal dir-ho amb cruesa, perquè aquí la complaença mata literalment. L'eina que la indústria diu que vigila la mà d'obra —l'auditoria social i els certificats com SA8000, BSCI o SMETA— falla repetidament en allò mateix per què existeixen. La fàbrica del Rana Plaza, auditada sota BSCI, es va ensorrar el 24 d'abril de 2013 i va matar 1.131 persones; la fàbrica d'Ali Enterprises al Pakistan, certificada SA8000, es va incendiar el 2012 i va matar més de 250 treballadors. Totes dues havien passat la inspecció poc abans del desastre [9]. No són casos aïllats: l'informe de Human Rights Watch de novembre de 2022 va documentar com les auditories trampegin de manera rutinària —consultories que ensenyen els treballadors a mentir, dobles llibres de comptes, nòmines falses i nens amagats durant la inspecció [10].

I hi ha un buit més fonamental, anterior al frau: el certificat només verifica el compliment d'un mínim legal que sovint és misèria. Com hem vist, els salaris legals són molt per sota d'un salari digne en tots els grans centres tèxtils —al voltant del 31 % a l'Índia, el 37 % a la Xina i Bangladesh, el 33 % a Cambodja i el 13 % a Sri Lanka [11]. Un PDF de conformitat pot dir «tot correcte» sobre una fàbrica on ningú no cobra prou per viure. El document, sol, no salva: és tan fiable com la voluntat de qui el signa i tan honest com la inspecció que el va emetre.

La prova d'existència aplicada

És aquí on **t2p** aporta la capa que falta, i ho fa sobre la **prova contemporània i contextualitzada** de les condicions i de les persones, no sobre el producte —com hem vist al capítol 29—. En el moment de la captura, un treballador, un representant sindical, un auditor de camp sense avís previ o una ONG local de confiança grava amb el seu dispositiu una foto o un vídeo curt del taller, d'un dormitori, d'una sortida d'emergència encadenada, d'una nòmina o d'un full de torns. L'aplicació calcula al dispositiu l'**empremta SHA-512** del fitxer —que mai no surt del telèfon—, obté un **segell de temps RFC 3161/eIDAS** i ancora l'empremta a la **blockchain pública**, produint un contenidor **.asice** verificable fora de línia. Per a les captures de camp d'una persona o un lloc s'hi afegeix un **GPS forense** (que demostra que la foto es va fer dins *aquella* fàbrica o *aquell* dormitori de reclutament) i una **prova de vida** (que demostra que va ser un treballador real, no un testimoni *deepfake* aleccionat, qui va donar el relat en aquell moment).

El mateix mecanisme segella la cara corporativa de la cadena: la **declaració del proveïdor** i l'atestació de custòdia que una marca recull per refutar la presumpció de la UFLPA, el **registre de diligència deguda** de la LkSG o la CSDDD, la **queixa d'un treballador** presentada per una aplicació tipus WOVO, o les **troballes en brut d'un auditor** sense avís previ abans que cap fàbrica hagi tingut temps de «preparar-se». Complementa el sistema existent atacant els dos forats documentats per reguladors i HRW: les auditories es trampegen amb treballadors aleccionats i documents fabricats, i una marca que combat una retenció de la CBP ha de demostrar **quan** va saber realment les coses i quan va actuar. Una queixa o una troballa segellades amb data, GPS i prova de vida són molt més difícils de retrodatar, editar o

desestimar com a *deepfake* que un informe en PDF —i això reforça el testimoni del treballador, el rastre de queixes i l'expedient que una empresa presenta a la CBP, la BAFA o una autoritat competent de la UE.

Ara el límit, amb tota la cruesa, perquè aquí enganyar-se faria mal. «Escombraries a l'entrada, escombraries a la cadena»: el segell prova **l'acte** —que aquesta persona, en aquest lloc i moment verificats, va gravar aquesta imatge o va signar aquesta declaració, i que res no s'ha alterat des de llavors. **No prova que les condicions siguin bones** ni que el salari sigui digne; una foto segellada i geolocalitzada d'un taller endreçat i muntat per a la inspecció continua sent una posada en escena. No confirma que la declaració d'un proveïdor sigui veraç, ni que la fàbrica de tercer nivell que apareix sigui realment la que fa la peça, ni que el testimoni d'un treballador s'hagi donat lliurement i no sota coacció — la prova de vida derrota una cara sintètica, no una d'espantada. No verifica que els béns estiguin lliures de contingut de Xinjiang ni que satisfacin la UFLPA o les obligacions de la CSDDD i la LkSG; tot això encara exigeix investigació, traçat documental, visites sense avís i judici humà. El segell fa la prova inalterable i datada; mai no substitueix l'auditoria, el regulador ni la credibilitat del mateix treballador. És el complement laboral del que els capítols 13 i 15 proposen amb el C2PA i la procedència del contingut.

La promesa i el perill

La promesa és convertir el testimoni més fràgil de la cadena —la veu d'un treballador, sovint atemorit i sense poder— en una **prova datada, geolocalitzada i admissible** que cap fàbrica NO pot esborrar i cap advocat NO pot desestimar com a fabricada després. La marca honesta guanya un expedient de diligència deguda que aguanta davant la CBP i la BAFA; el treballador guanya que la seva paraula deixi de ser «la seva paraula contra la de l'empresa».

El perill demana els matisos més estrictes. El primer, i de vida o mort: la **seguretat del testimoni**. Un treballador que segella una prova contra el seu ocupador s'exposa a represàlies; el sistema ha de protegir la seva identitat, no exposar-la. El segon, no confondre **integritat amb veritat**: una declaració de proveïdor falsa i segellada continua sent falsa, i ara, a més, immutable; el segell podria donar una falsa tranquil·litat —«està ancorat, doncs compleix»— que no es correspon amb res. I el tercer, la **concentració**: si només les grans marques poden segellar i documentar, l'estàndard pot tornar-se una barrera que expulsa el petit proveïdor honest en lloc d'enfortir el treballador. La prova d'existència és una eina de dignitat i de rendició de comptes, no un certificat de bondat.

És hora d'actuar

Per als **treballadors i els sindicats**: poder segellar al dispositiu una queixa, una nòmina o una imatge del taller com a prova datada i geolocalitzada, sense que la foto surti del telèfon i amb la identitat protegida. Per a les **marques i els compradors** (Volkswagen, BMW, Mercedes-Benz i la resta): segellar la declaració del proveïdor i el registre de diligència deguda en el moment de recollir-los, perquè l'expedient presentat a la CBP o la BAFA tingui data certa i no sembli fabricat posteriorment. Per als **auditors de camp i les ONG**: ancorar les troballes en brut abans que cap fàbrica es «prepari», convertint la inspecció sense avís en prova inalterable. Per als **reguladors** (CBP, BAFA, autoritats de la UE sota el Reglament de treball forçat): reconèixer la prova segellada amb segell de temps com a evidència vàlida del que una empresa sabia i quan, i tractar la data certa com a diferència entre diligència i coartada. I per als **legisladors** (UFLPA, CSDDD, LkSG): exigir que el rastre de diligència deguda sigui verificable i ancorat, no un PDF que es pugui retocar demà.

Als ports nord-americans, milers de cotxes de luxe es van aturar per una peça que ningú a la seu sabia que existia. Donar a cada treballador del final de la cadena una prova segellada del que va viure i a cada marca honesta una prova del que sabia i quan va actuar —sense oblidar mai que el segell no fa dignes les condicions— és, en aquest front, el moment d'actuar time2act.

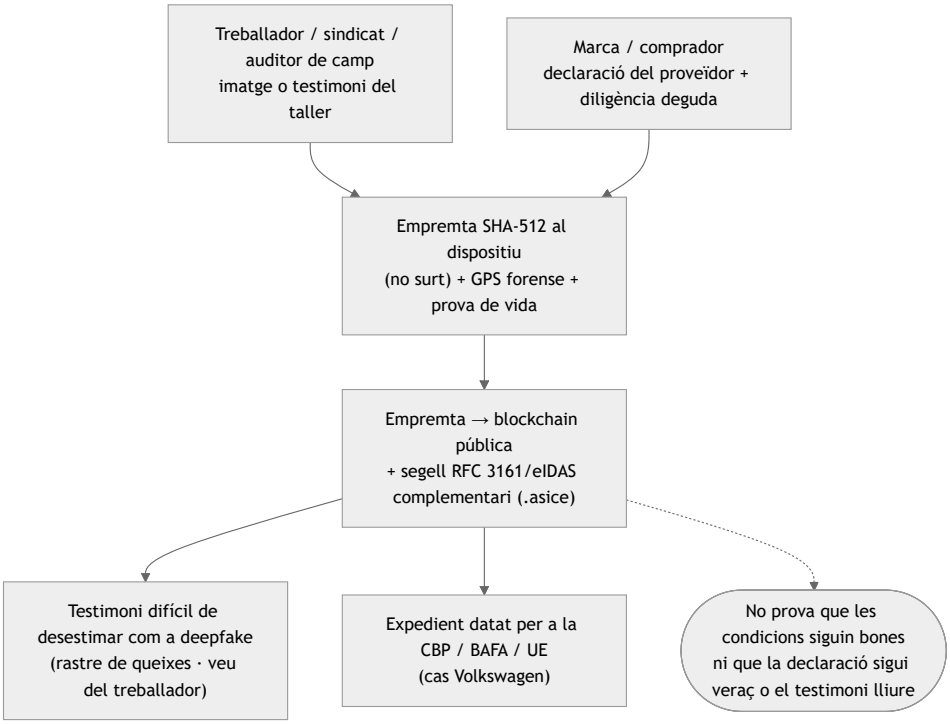


Figura 102.1 — Dues fonts de prova: el treballador, el sindicat o l'auditor de camp capturen al dispositiu una imatge o un testimoni del taller (empremta SHA-512 que no surt del telèfon, GPS forense, prova de vida); la marca segella la declaració del proveïdor i el registre de diligència deguda. L'empremta de tot plegat s'ancora a la blockchain pública, amb segell de temps RFC 3161/eIDAS complementari (.asice). Resultats: testimoni del treballador més difícil de desestimar com a deepfake, i expedient datat per a la CBP, la BAFA o l'autoritat de la UE. Límit: el segell prova l'acte, el lloc i la data; no prova que les condicions siguin bones, que la declaració sigui veraç ni que el testimoni fos lliure. Fonts: cas Volkswagen/CBP; OIT; Miller & Chevalier (UFLPA); HRW (auditories i automòbil); ECCHR (certificats).

---

[1] OIT — *Data and research on forced labour (Global Estimates 2022)* (27,6 milions de persones en treball forçat el 2021; 17,3 milions a l'economia privada; els migrants tripliquen el risc). 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* (març de 2024; +37 % des de 2014; 84.000 milions a Europa i l'Àsia 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 enviaments i 3.690 M$ retinguts; 1.340 M$ el 2024; 48 % d'entrades denegades; +1.600 % a l'automòbil; *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* (marques, subcomponent, cronologia desembre 2023 – mitjan gener 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* (febrer de 2024; VW, BMW, Mercedes, GM i la cadena de l'alumini). https://www.hrw.org/report/2024/02/01/asleep-wheel/car-companies-complicity-forced-labor-china ↩

[6] Comissió Europea — *Corporate Sustainability Due Diligence (CSDDD)* (Directiva 2024/1760, en vigor el 25 de juliol de 2024; transposició fins al 26 de juliol de 2028, aplicació des del 26 de juliol de 2029 després de l'Òmnibus). 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* (desembre de 2024; en vigor el 13 de desembre de 2024, aplicació el 14 de desembre de 2027; model d'investigació sense presumpció geogràfica). 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* (aplicació a empreses de 1.000 empleats des de l'1 de gener de 2024; multes fins al 2 % de la facturació mundial; 486 auditories el 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 morts, BSCI; Ali Enterprises, més de 250 morts, SA8000; totes dues havien passat la inspecció). 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* (novembre de 2022; treballadors aleccionats, dobles llibres, nòmines falses, nens amagats). 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 salari mínim legal és el 31 % d'un salari digne a l'Índia, el 37 % a la Xina i Bangladesh, el 33 % a Cambodja, el 13 % a Sri Lanka). https://cosh.eco/en/articles/living-wages-eu-garment-workers ↩

Integritat marítima: on és de debò aquell vaixell, i és qui diu ser?

«El mar mai no ha estat amic de l'home. Com a màxim, ha estat el còmplice de la inquietud humana.»

— Joseph Conrad, El mirall del mar (1906)

El 29 d'abril de 2026, l'empresa d'intel·ligència marítima **Windward** va destapar un esquema de contraban de cru iranià valorat en uns **800 milions de dòlars**. Quatre superpetroliers VLCC sancionats pels Estats Units —**Alicia** (IMO 9281695), **RHN** (IMO 9208215), **Star Forest** (IMO 9237632) i **Aqua** (IMO 9248473)—, cadascun amb uns **2 milions de barrils** a bord, emetien missatges AIS de destinació falsos i traçats erràtics per semblar fondejats davant de Basra i carregant al port iraquià de **Khor al Zubair**. En realitat, s'esquitllaven cap a terminals iranianes, hi carregaven cru iranià i fabricaven una **coartada digital** d'origen iraquià legítim. Windward va resseguir una desena de petroliers sancionats falsejant posicions davant de l'Iraq, i més de vint vaixells a l'oest de l'estret d'Ormuz amb senyals delators d'*spoofing*: traçats circulars en forma de «cercles de collita», escales portuàries inventades [2].

Aquest capítol és diferent del capítol 54 —el frau documental del comerç internacional, que segella albarans i cartes de crèdit— i del capítol 72 —la pesca il·legal, que mira si una captura es va fer on i com tocava. Aquí l'objecte segellat no és cap paper ni cap captura: és el **fet físic d'on és un vaixell i qui és**, aigües amunt de qualsevol document. Al mar, la posició i la identitat declarades són **assercions de ràdio autoinformades** que es poden fabricar a l'engròs. La pregunta del capítol és com fer que un vaixell pugui **provar de manera no repudiable** on era i qui era en un instant donat —i, sobretot, com fer que un vaixell sancionat **no pugui** fabricar a posteriori un rastre que el situï a Khor al Zubair quan mai no hi va ser.

El senyal que es pot inventar

L'AIS —el sistema d'identificació automàtica— neix per a la seguretat: que els vaixells es vegin entre ells. Però el que un vaixell emet (posició, rumb, identitat MMSI, destinació) és el que **ell mateix decideix** emetre. Aquí rau el frau. Entre el gener de 2024 i el juliol de 2025, **Kpler** va identificar **261 vaixells** que van falsejar el seu AIS abans de ser sancionats —la categoria de pràctica enganyosa més nombrosa—, inclosos petits gasers que inventaven escales a Khor al Zubair per fabricar històries de viatge plausibles [3]. La firma britànica **Lloyd's List Intelligence** documenta la mecànica del *blanqueig d'identitat*: el frau del número IMO, el salt de bandera, la manipulació de la «encaixada» AIS perquè dos cascos intercanviïn identitats al mar [11]. L'altra cara és l'apagada deliberada: el desembre de 2024, l'OFAC va designar els operadors del **MS ENOLA**, que «continuava fent servir pràctiques enganyoses, inclosa l'apagada de l'AIS» per ocultar transferències il·lícites de petroli iranià sota l'ordre executiva 13902 [9].

La flota fantasma i el mapa que menteix

L'escala és industrial. La **flota fantasma russa** compta més de **1.000 petroliers** envellits i infraassegurats —al voltant del **17 %** de la flota petroliera mundial—; el catàleg d'intel·ligència ucraïnès en llistava **1.337** al febrer de 2026, i el 2024 la flota va generar uns **9.400 milions de dòlars** d'ingressos russos addicionals esquivant el sostre de preu [6]. Viuen del falsejament: posicions inventades, identitats prestades, transbordaments vaixell a vaixell (STS) lluny de tota mirada. I no és només petroli: el 25 de desembre de 2024 el petroler **Eagle S**, de bandera de les Illes Cook i part de la flota fantasma, va arrossegar l'àncora i va malmetre el cable submarí Estlink 2 entre Finlàndia i Estònia, reforçant una dimensió de **seguretat híbrida** [10].

Per damunt del frau deliberat hi ha el **soroll de fons** que el fa indistingible: la interferència massiva del GNSS. Al segon trimestre de 2025, més de **10.000 vaixells** van patir oficialment interferència de GPS —vuit vegades més que els uns 1.250 del primer trimestre—, amb gairebé **3.000 vaixells** afectats al golf Pèrsic i Ormuz durant el pic del juny de 2025 [4]. Durant la guerra Israel-Iran d'aquell mes, l'*spoofing* a Ormuz —per on passa el **20 %** del petroli mundial— posava les pantalles dels superpetroliers «sobre terra ferma» i a través d'una central nuclear; el professor Todd Humphreys, de la Universitat de Texas, ho deia sense embuts: «Estic ben segur que són els iranians els qui fan aquest *spoofing*» [1]. L'1 de març de 2026, més de **1.100 vaixells** del golf van patir interferència en 24 hores, amb 21 nous nuclis que situaven

vaixells dins de la central nuclear de Barakah; els trànsits per Ormuz van caure una tercera part [5]. El mapa global de seguiment s'ha convertit ell mateix en una **falsificació**.

La llei demana traçabilitat; el frau la ridiculitza

El marc existeix. El **conveni SOLAS, capítol V, regla 19**, de l'OMI, obliga a portar AIS en tots els vaixells de 300 GT o més en viatges internacionals i a mantenir-lo «en funcionament en tot moment» tret que la seguretat justifiqui apagar-lo —cosa que converteix la navegació «a les fosques» i l'*spoofing* deliberat en una **infracció de seguretat**. Les sancions de l'**OFAC**, sota l'ordre 13902, i el règim del sostre de preu rus citen explícitament la manipulació de l'AIS, la navegació fosca i el blanqueig d'identitat com a pràctiques enganyoses [9]. La **UE** va llistar més de **444 vaixells** de la flota fantasma cap al desembre de 2025 (n'hi va afegir 41 el 18 de desembre) [7], i el 18è paquet, del 18 de juliol de 2025, va rebaixar el sostre del cru rus de 60 a **47,60 dòlars** amb un mecanisme dinàmic que el manté un 15 % per sota del mercat [8]. El Comitè Jurídic de l'OMI treballa contra la **matriculació fraudulenta**: el LEG 111 (abril de 2024) i el LEG 112 (març de 2025) van publicar directrius sobre registre de vaixells, previstes per al 2027, per frenar el salt de bandera i el frau del número IMO. La llei demana traçabilitat; el problema és que descansa sobre un senyal que el mateix infractor controla.

Per què el mandat de l'AIS sol no salva

Cal dir-ho amb cruesa. Que SOLAS obligui a portar l'AIS encès no impedeix ni l'apagada ni l'spoofing; només els converteix, sobre el paper, en infracció. El problema de fons és que l'AIS és **autoinformat**: el vaixell indica on és i qui és, i el receptor s'ho creu. Una posició AIS sense ancoratge independent no distingeix el vaixell honest del que fabrica un traçat; una fallada d'AIS pot ser una avaria o una tapadora; i quan el frau s'amaga dins d'un mar de **diversos** vaixells amb interferència real, la maniobra dolosa es torna **indistingible** del soroll legítim. Detectar l'anomalia —cosa que Windward, Kpler o Pole Star fan molt bé— no és el mateix que **provar-la davant d'un tribunal**, ni impedeix que un operador sancionat al·legui que el seu rastre sospitós era una víctima més de la interferència. Falta una capa que converteixi «aquest traçat sembla anòmal» en «aquesta posició verificada és criptogràficament provable, i l'absència de segell és en si mateixa una bandera vermella».

La prova d'existència aplicada

És aquí on **t2p** tanca el forat d'integritat de la posició i de la identitat autoinformades. Quan es pren una fixació, una unitat de bord resistent a la manipulació —com un inspector de confiança de la guàrdia costanera o del port, o una aplicació d'escala o de proveïment de combustible— captura el **registre de navegació**: la fixació GNSS amb hora, IMO i MMSI, el calat i la trama AIS tal com s'emet. Al mateix dispositiu es calcula l'**empremta SHA-512** del registre —el rastre cru no ha de sortir del vaixell—, se li afegeix un **segell de temps RFC 3161 conforme a eIDAS** i s'ancora a la blockchain pública, dins d'un contenidor **.asice** verificable fora de línia. Quan un inspector comprova físicament el casc, el nom i la placa IMO en una escala o un transbordament STS, s'hi incorpora una **fixació GPS forense** i una **prova de vida** de l'inspector i de l'escena.

El resultat és un **llibre major de posició i identitat**, continu i ancorat independentment: un vaixell pot demostrar posteriorment on i qui era, i —com hem vist— un vaixell sancionat **no pot** fabricar a posteriori un rastre segellat que el situï a Khor al Zubair quan no n'existeix cap segell contemporani. Això **complementa** els sistemes existents (AIS, LRIT, detecció per RF i SAR de satèl·lit, cribratge OFAC i UE) afegint una àncora datada, no repudiable i de grau judicial. Com els capítols 13 i 15 fan amb la procedència C2PA del que un dispositiu **produeix**, aquí se segella el que un vaixell **fa i és**.

El segell prova l'origen, l'hora, l'autor i la integritat d'un registre de posició —**no que el senyal GNSS subjacent fos genuí**. Si el receptor rep un senyal de satèl·lit falsejat, un segell vàlid ancorarà una posició falsa: la criptografia certifica «aquest dispositiu va registrar aquesta fixació en aquest instant», no que la fixació fos real. Per tant, sense receptors multiconstel·lació i anàlisi forense, el segell no distingeix una ubicació honesta d'una falsejada; només l'absència de segell es converteix en prova. Complementa la procedència C2PA/SynthID però **mai substitueix** l'auditoria de bandera, el control del port ni el judici humà.

La promesa i el perill

La promesa és convertir l'oceà en un espai amb **memòria verificable**: que un vaixell honest pugui demostrar la seva posició i identitat amb un ancoratge que cap operador pot retocar, i que el silenci —la manca de segell— passi a ser una dada acusatòria. En un sector on un casc canvia de nom, de bandera i de número IMO sense deixar rebut, fer l'origen inalterable protegeix tant la naviliera neta com l'asseguradora i l'estat costaner.

El perill demana els matisos de sempre. El primer, no confondre **integritat amb veritat**: una posició falsejada però segellada continua sent falsa, i ara, a més, immutable; el segell podria donar una falsa tranquil·litat —«està ancorat, doncs és real»— que no es correspon amb res. El segon, la **voluntarietat**: cap règim no pot obligar un petroler fantasma a segellar la seva posició, de manera que el sistema protegeix sobretot els honestos i deixa la prova en l'absència. I el tercer, la **governança** de qui opera les unitats de bord i les claus: si les controla qui té incentius per mentir, el segell perd el sentit. La prova d'existència és una capa d'integritat del senyal, no un certificat de legalitat ni un substitut de l'ull humà que sap llegir un mar.

És hora d'actuar

Per als **estats de bandera i l'OMI**: incorporar el segell de posició i identitat a les directrius de registre del 2027 i al règim SOLAS, de manera que un forat d'AIS sense segell contemporani pesi com a indici. Per a les **autoritats de control de l'estat del port i les guàrdies costaneres**: segellar amb GPS forense i prova de vida cada inspecció de casc, nom i placa IMO en escales i transbordaments STS. Per als **reguladors de sancions** (OFAC, Consell de la UE): reconèixer l'absència de rastre segellat com a senyal de risc en el cribratge, i el segell com a evidència de grau judicial. Per a les **asseguradores i els clubs P&I**: exigir el llibre major de posició ancorat com a condició de cobertura, perquè el petroler infraassegurat de la flota fantasma quedi fora del mercat. I per a les **firmes d'intel·ligència marítima** (Windward, Kpler, Pole Star): connectar la seva detecció d'anomalies amb l'àncora segellada, perquè «sembla *spoofing*» esdevingui «provablement no era on deia».

Com hem vist el 29 d'abril del 2026, quatre superpetroliers van pintar al mapa una geografia que no existia per amagar 800 milions de dòlars de cru iranià. Donar a cada vaixell honest una prova segellada d'on era i qui era —i convertir el silenci del defraudador en la seva pròpia acusació—, sense oblidar mai que el segell no fa real un senyal manipulat; és, en aquest front on l'oceà mateix s'ha tornat falsificable, **time2act**.

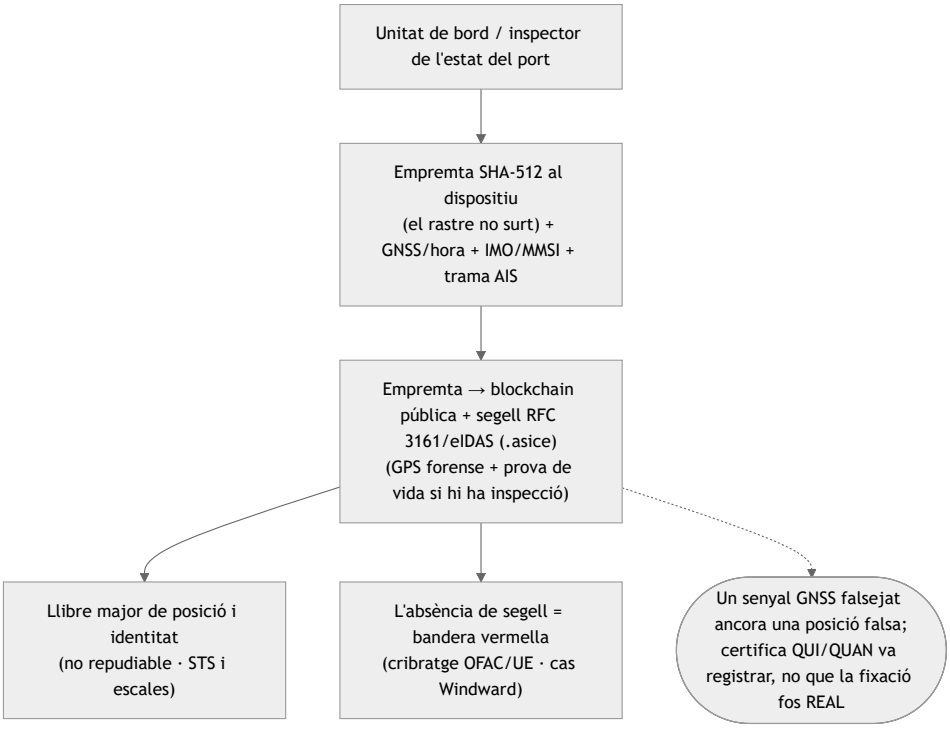


Figura 103.1 — En prendre una fixació, una unitat de bord o un inspector de l'estat del port captura el registre de navegació (GNSS + hora, IMO/MMSI, calat, trama AIS) i en calcula l'empremta SHA-512 al dispositiu; l'empremta del conjunt s'ancora a la blockchain pública, amb segell RFC 3161/eIDAS complementari (.asice), amb GPS forense i prova de vida quan hi ha inspecció física. Dos resultats: a l'esquerra, un llibre major de posició i identitat no repudiable; a la dreta, l'absència de segell esdevé una bandera vermella per al cribratge de l'OFAC/UE. Límit: el segell certifica que el dispositiu va registrar aquesta fixació en aquest instant, no que el senyal GNSS fos genuí; un senyal falsejat ancora una posició falsa. Fonts: cas Windward (esquema de 800 M$); Kpler (261 vaixells); GPSPATRON (10.000+ vaixells); Scientific American (Ormuz); OFAC (MS ENOLA).

---

[1] GPS spoofing is scrambling ships in the Strait of Hormuz — *Scientific American* (spoofing a Ormuz durant la guerra Israel-Iran de 2025; vaixells sobre terra i centrals nuclears; atribució d'Humphreys a l'Iran; ~20 % del petroli mundial per l'estret). 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* (revelació de Windward, 29 d'abril de 2026; VLCC amb números IMO; escales falses a 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 vaixells van falsejar l'AIS abans de ser sancionats, gener 2024-juliol 2025; escales falses a 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+ vaixells afectats el 2T 2025, vuit vegades més que el 1T; punts calents regionals). 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 març de 2026: 1.100+ vaixells en 24 h, 21+ nuclis; fixacions falses a Barakah i Al Hamra; Ormuz un terç avall). 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* (mida de la flota; ~17 % de la flota petroliera mundial; 9.400 M$ d'ingressos extra el 2024; pes creixent de la bandera russa). 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 — *Consell de la UE (Consilium)* (18 de desembre de 2025: el total de la UE arriba a 444+ vaixells; prohibicions d'accés a port i de serveis). 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 — *Consell de la UE (Consilium)* (18 de juliol de 2025: sostre del cru rebaixat de 60 a 47,60 $ amb mecanisme dinàmic 15 % per sota del mercat). 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* (desembre de 2024; acció de l'OFAC sota l'E.O. 13902 citant el MS ENOLA «apagant l'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* (petroler Eagle S de bandera de les Illes Cook, 25 de desembre de 2024, dany al cable submarí del Bàltic; dimensió d'amenaça 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* (blanqueig d'identitat, frau del número IMO, encaixada AIS i mecànica de l'spoofing de posició). https://www.lloydslistintelligence.com/resources/blog/the-secret-lives-of-the-shadow-fleet-ais-spoofing-vessel-identity-manipulation ↩

Observació de la Terra: el testimoni orbital que també es pot falsificar

«Torneu a mirar aquest punt. Això és aquí. Això és casa nostra. Això som nosaltres.»

— Carl Sagan, Pale Blue Dot (1994)

L'abril del 2022, després que les forces russes es retiressin de **Bucha**, a Ucraïna, el Kremlin va afirmar que les imatges de cossos escampats pels carrers s'havien «escenificat» un cop els seus soldats havien marxat. Però els satèl·lits **WorldView** de **Maxar Technologies** ja havien fotografiat aquells carrers: imatges d'alta resolució del 18, el 19 i el 31 de març de 2022 mostraven cadàvers estesos al carrer Iablónska i una fossa comuna acabada d'excavar —una rasa d'uns 14 metres al costat d'una església de cúpula daurada—, totes datades en setmanes en què les tropes russes encara ocupaven la ciutat. *The New York Times* va geolocalitzar els cossos dels fotogrames orbitals fins a la posició exacta que després es veuria als vídeos a peu de carrer, refutant de manera demostrable la negació de Moscou i alimentant les investigacions per crims de guerra [2][3]. I tanmateix, aquell mateix «testimoni» en òrbita és avui un objectiu de falsificació: el 2021, el geògraf **Bo Zhao**, de la Universitat de Washington, va encunyar el terme **«geografia *deepfake*»** i va demostrar, a *Cartography and Geographic Information Science*, que la IA podia empeltar les textures de Pequín sobre un mapa de Tacoma per fabricar escenes de satèl·lit falses i convincents [1].

Aquest capítol és transversal i toca tres veïns sense confondre-s'hi. El capítol 20 fa servir la imatge de satèl·lit com a **prova judicial** d'un crim de guerra; el capítol 22 la fa servir per **mesurar el carboni** (biomassa, desforestació); el capítol 96 per **vigilar emissions**. Tots tres tracten la imatge com una *font* de prova sobre una altra cosa. Aquí el subjecte és la imatge mateixa: la **integritat del fotograma orbital**, alhora testimoni i objectiu de falsificació. La pregunta és incòmoda: si l'ull al cel pot ara mentir tan bé com qualsevol *deepfake*, com fixem que *aquest* píxel, d'*aquest* sensor, va existir en *aquest* instant — abans que ningú no el discutís? És la tesi del llibre aplicada al lloc més inesperat: la fotografia de la Terra des de dalt.

Quan la imatge orbital és l'únic testimoni

La imatge de satèl·lit s'ha convertit en prova de primera línia precisament on a peu de terra no hi arriba ningú. El 2020, l'equip de **BuzzFeed News** —la sèrie *Built to Last*, després guanyadora d'un Pulitzer— va combinar imatges de **Planet** i d'altres satèl·lits amb els quadres en blanc que la censura xinesa deixava sobre els seus propis mapes per identificar **268 camps de detenció** acabats de construir a Xinjiang, i **428 emplaçaments sospitosos** en total [4]. Sense un sol periodista sobre el terreny, l'òrbita va documentar un sistema d'internament massiu. A Bucha, el patró es repeteix a la inversa: l'òrbita havia datat el crim setmanes abans que el negador pogués inventar-se una coartada. En tots dos casos, la imatge no era una il·lustració: era *l'evidència*, i tota la cadena —tribunal, Nacions Unides, opinió pública— hi descansava.

Aquesta dependència és, alhora, la seva vulnerabilitat. Quan tot un edifici de prova reposa sobre un fotograma, qui pugui falsificar-lo —o només sembrar el dubte que es pot falsificar— enderroca l'edifici sencer. I aquí és on el 2021 va canviar les regles.

El testimoni que ara es pot fabricar

Bo Zhao no va parlar en hipotètic. El seu estudi va construir un conjunt de detecció de **8.064 imatges de satèl·lit** —la meitat autèntiques de Seattle, Tacoma i Pequín; l'altra meitat *deepfakes* de Tacoma amb textures empeltades de Pequín i de Seattle— i va advertir que la imatge falsificada per IA és una **amenaça per a la seguretat nacional** [1]. Quatre anys després, el perill ja és operatiu, no teòric. El novembre de 2025, un estudi de detecció provava classificadors contra imatges aèries forjades amb **StyleGAN2** i **Stable Diffusion** sobre més de **130.000 imatges** etiquetades, i trobava que els *Vision Transformers* les detecten molt millor que les xarxes convolucionals: **95,11 % enfront del 87,02 %** d'encert; les falsificacions GAN deixen distorsions d'alta freqüència, mentre que les de difusió mostren «dissonància semàntica» —terreny repetit, carreteres que s'acaben de cop, ombres mal aparellades [5].

El risc puja quan l'objectiu és estratègic. El 2024, investigadors de verificació nuclear (Nguyen, Glaser i Biessmann, de Princeton) van demostrar que els models de text a imatge poden generar imatges de satèl·lit **fotorealistes d'instal·lacions concretes** —centrals nuclears incloses—, «difícils de distingir de les dades reals», amb implicacions directes per al control d'armament i la verificació [6]. La pròpia **NGA** —l'agència d'intel·ligència geoespacial dels EUA— ha advertit que la imatge manipulada amb GAN podria desviar combois davant ponts o carreteres que no existeixen. L'ull al cel, durant dècades el patró d'or de la prova incontestable, ha entrat a l'era en què cal preguntar-li, també a ell, «com sé que ets real?».

La cursa institucional: autenticar el senyal i la imatge

La resposta institucional avança en dos fronts. El primer és la geolocalització: el 24 de juliol de 2025 el servei OSNMA de Galileo entra en operació, convertint-se en el primer GNSS mundial que emet una signatura digital criptogràfica (protocol TESLA) perquè els receptors rebutgin senyals de posicionament falsificats [7]. És la columna vertebral del *on* i del *quan* d'una captura —tot i que no atura la interferència (jamming). El segon front és el reconeixement automàtic: com hem vist, el 2024 la NGA llança el programa Sequoia d'etiquetatge de dades, valorat fins a 708 milions de dòlars en set anys —el seu contracte de dades més gran de la història— per entrenar la visió per computador (Maven) sobre imatges de satèl·lit [8]. Com més decisions automàtiques pengen de la imatge, més car és que aquesta menteixi.

El tercer front és l'estàndard de confiança. La UE ha bastit el seu Programa Espacial (Reglament 2021/696, 14.800 milions d'euros per a 2021-2027) i l'agència EUSPA, encarregada de la seguretat de Copernicus, Galileo i EGNOS. L'Open Geospatial Consortium va publicar a l'abril de 2025 una iniciativa anual d'Integritat, Procedència i Confiança (IPT) que defineix la integritat (el maneig al llarg del cicle de vida), la procedència (l'origen i qui ha modificat les dades) i la confiança (ben documentada, consistent, inalterable) per a les dades geoespacials [9]. És el marc conceptual que faltava, però té un buit decisiu.

Per què el marc IPT sol no salva

Cal dir-ho amb cruesa. La iniciativa IPT de l'OGC defineix magníficament què volem dir amb integritat i procedència, però es basa en estàndards de metadades, no en signatura criptogràfica ni cadena de blocs [9]. Una metadada és tan fiable com el sistema que la custodia: un camp de procedència en un fitxer es pot reescriure, retrodatar o suavitzar després d'una disputa, sense deixar cap empremta independent. El mateix passa amb les altres capes: el C2PA —les Content Credentials que la guia conjunta de la NSA, l'ODNI i la CISA del 29 de gener de 2025 recomana per a la integritat de la imatge— signa la procedència si s'aplica al moment de la captura, però no diu res si el forjador segella la seva pròpia falsificació. I els detectors de Vision Transformer, per bons que siguin, donen una probabilitat, no una prova datada: el seu 95 % d'encert vol dir que un de cada vint forjats passa, i que cada generació nova de difusió els obliga a reentrenar-se. Cap d'aquestes capes fixa, de manera inalterable i independent, qui va lliurar quins píxels i quan. Falta la cadena de custòdia.

La prova d'existència aplicada

És aquí on **t2p** aporta la capa que falta, i ho fa sobre l'artefacte digital —l'escena— en el punt més primerenc defensable de la cadena. L'artefacte segellat és **l'escena de satèl·lit crua o de nivell L1** més les metadades portadores (identificador de sensor, òrbita/efemèrides, hora de recepció a l'estació de terra, projecció i paràmetres de processament). Hi ha dos ancoratges complementaris. **Primer**, a l'*ingest* de l'estació de terra: l'operador (Maxar, Planet, el segment de terra de Copernicus de l'ESA) calcula l'**empremta SHA-512** de l'escena lliurada sobre el sistema receptor —el fitxer no surt d'allà—, n'obté un **segell de temps RFC 3161 conforme a eIDAS**, ancora l'empremta a la cadena pública i emet un contenidor **.asice** verificable fora de línia que viatja amb cada tessel·la i informe derivats. **Segon**, a l'extrem de l'analista, periodista o investigador —un equip OSINT geolocalitzant els fotogrames de Bucha o de Xinjiang—: el retall concret, la capa d'anotació i les coordenades GPS i l'hora d'adquisició afirmades es tornen a segellar, amb **GPS forense** lligant qualsevol captura de camp que ho corrobori i una **prova de vida** quan una persona verifica un lloc sobre el terreny.

El segell fixa *quins píxels* van existir, de *quin sensor*, en *quin instant* UTC, atribuïts a *quin operador o analista*. Així, una escena forjada o generada per difusió més tard no es pot fer passar per l'original, i un tribunal —o un auditor de carboni MRV— pot demostrar que la imatge va entrar al registre *abans* de qualsevol disputa. Complementa, no substitueix: la procedència de l'IPT de l'OGC, l'autenticació de posició

de Galileo OSNMA, les *Content Credentials* del C2PA dels capítols 13 i 15, i els detectors de *deepfake* de *Vision Transformer* —aportant la capa de **custòdia a prova de manipulació** que tots ells no tenen.

Ara el límit, amb tota la cruesa. «Escombraries a l'entrada, escombraries a la cadena»: el segell prova l'origen, l'instant exacte, l'autoria i la integritat bit a bit d'una escena; **no prova** que l'escena mostri el que s'afirma, que el sensor estigués ben calibrat, que el núvol, l'ombra, l'angle fora de nadir o la resolució no enganyin, ni que la geolocalització sigui correcta. Si un forjador genera una central nuclear falsa amb Stable Diffusion —o una escena de desforestació adulterada— i segella *això*, el segell datarà fidelment una mentida: només fixa que *aquesta* imatge exacta va existir en *aquest* moment, signada per *aquest* signant, no que sigui observació autèntica de la Terra. No pot autenticar de manera retroactiva una imatge segellada només després de manipular-la, no atura la interferència del GNSS, ni dictamina si un pont, una fossa comuna o un bosc arrasat són reals. Detectar píxels sintètics segueix exigint classificadors forenses i judici expert; el carboni MRV, inventaris a peu de terra; l'ús per a crims de guerra, corroboració sobre el terreny i avaluació judicial. El segell reforça la cadena de custòdia; mai no substitueix la verificació de la veritat del contingut.

La promesa i el perill

La promesa és un registre de l'observació de la Terra on cada escena arrossega un **rebut inalterable** del seu origen, hora i autor —de manera que el negador de Bucha ja no pugui al·legar «escenificació» sobre una imatge datada criptogràficament setmanes abans, i l'auditor de carboni o el fiscal puguin demostrar que la prova és anterior a la disputa. En un món on l'ull al cel pot mentir, fer l'origen inalterable protegeix tant la víctima com el verificador honest.

El perill demana els matisos de sempre. El primer, no confondre **integritat amb veritat**: una escena forjada i segellada al moment de forjar-la continua sent falsa, i ara, a més, porta un segell que pot donar una falsa tranquil·litat —«està ancorat, doncs és real»— que no es correspon amb res. El segon, la **concentració de poder**: si només un grapat d'operadors comercials i agències estatals poden segellar a l'estació de terra, l'estàndard pot consolidar qui controla la veritat orbital i deixar fora l'investigador independent. I el tercer, l'ús **autoritari**: la mateixa cadena que dona pes probatori a la imatge de Xinjiang pot donar pes a la vigilància; la integritat de la imatge no en jutja l'ús legítim. La prova d'existència és una capa de custòdia, no un certificat d'autenticitat ni un substitut del judici expert que sap llegir un fotograma.

És hora d'actuar

Per als **operadors de satèl·lit** (Maxar, Planet, el segment de terra de l'ESA Copernicus): segellar l'escena crua o L1 a l'ingest de l'estació de terra —empremta SHA-512, segell eIDAS, ancoratge a la blockchain pública, contenidor .asice— perquè cada tesela derivada arrossegui una procedència inalterable des del minut zero. Per als **investigadors OSINT, periodistes i ONG de drets humans** (els qui van geolocalitzar Bucha i Xinjiang): tornar a segellar el retall, l'anotació i les coordenades afirmades, amb GPS forense i prova de vida quan hi hagi captura de camp. Per als **organismes d'estàndards** (OGC, dins la iniciativa IPT): afegir la signatura criptogràfica i l'ancoratge inalterable a la capa de metadades, omplint el buit que avui deixa l'IPT. Per als **estats i agències** (EUSPA, NGA, el programa Galileo OSNMA): combinar l'autenticació del senyal de posició amb el segellat de la imatge, perquè el *quan* i l'*on* i els *píxels* es defensin junts. I per als **tribunals i auditors de MRV** (la CPI, els verificadors de carboni): reconèixer el segell datat com la cadena de custòdia que distingeix una prova anterior a la disputa d'una imatge presentada després —sense oblidar mai que el segell no decideix si el que es veu és real.

A Bucha, l'ull al cel havia datat el crim setmanes abans que el negador pogués inventar-se la coartada. Donar a cada escena de satèl·lit una prova segellada del seu origen, hora i autor —sense oblidar que el segell fixa l'existència, no la veritat del que mostra— és, en aquest front on el testimoni orbital és alhora la nostra millor prova i un nou objectiu de falsificació, time2act.

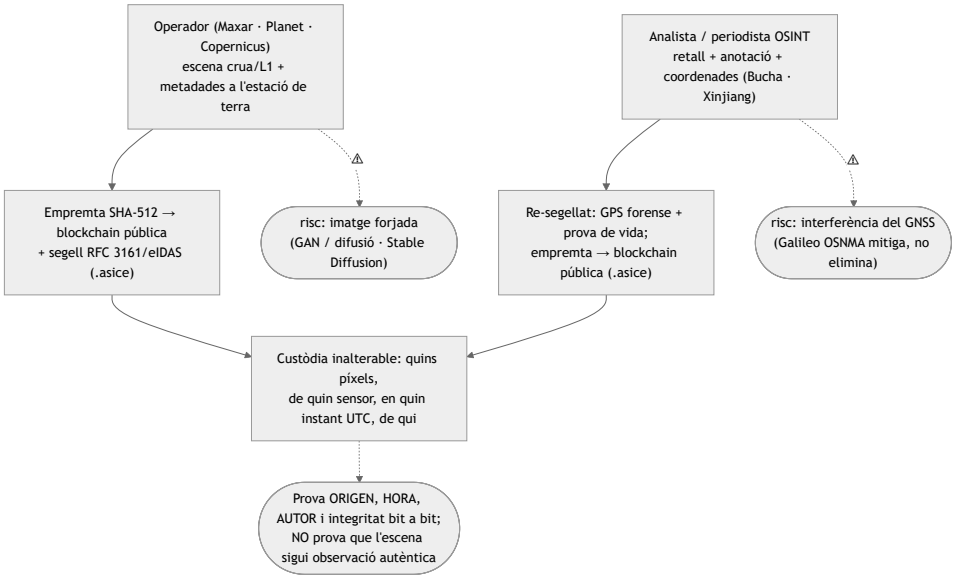


Figura 104.1 — La cadena de l'observació de la Terra en dues baules de segellat. A l'origen, l'operador (Maxar, Planet, Copernicus) calcula l'empremta SHA-512 de l'escena crua/L1 més les metadades a l'ingest de l'estació de terra; l'empremta s'ancora a la blockchain pública, amb segell RFC 3161/eIDAS complementari (.asice). A l'altre extrem, l'analista o periodista OSINT torna a segellar el retall, l'anotació i les coordenades, amb GPS forense i prova de vida. Punts de risc: imatge forjada amb GAN/difusió (Stable Diffusion, StyleGAN2) i interferència del GNSS, que la signatura de Galileo OSNMA i els detectors de Vision Transformer mitiguen però no eliminen. Límit: el segell prova origen, hora, autor i integritat bit a bit; no prova que l'escena sigui observació autèntica ni que la interpretació sigui correcta. Fonts: cas Bucha (Maxar); Bo Zhao (geografia 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 d'abril de 2021; Bo Zhao encunya «geografia deepfake» a *Cartography and Geographic Information Science*; conjunt de 8.064 imatges; amenaça per a la seguretat 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 d'abril de 2022; nou imatges de Maxar del 18/19/31 de març; cossos al carrer Iablónska; fossa comuna de 14 metres). 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 recollida intensiva de Maxar; ús del *New York Times* el 4 d'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* (mètode guanyador d'un Pulitzer; imatge de Planet i tessel·les censurades; 268 camps nous i 428 emplaçaments sospitosos). https://www.buzzfeednews.com/article/alison_killing/satellite-images-investigation-xinjiang-detention-camps ↩

[5] *Deepfake Geography: Detecting AI-Generated Satellite Images* (arXiv 2511.17766, novembre de 2025; ViT 95,11 % enfront de CNN 87,02 % sobre més de 130.000 imatges; artefactes GAN enfront de difusió). 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 i Biessmann; imatge sintètica fotorealista d'instal·lacions incloses centrals nuclears; control d'armament). https://arxiv.org/abs/2404.07754 ↩

[7] Comissió Europea — *Observer: How Galileo OSNMA helps counter GNSS spoofing* (OSNMA operatiu el 24 de juliol de 2025; primera autenticació mundial del senyal del Servei Obert d'un GNSS via signatures criptogràfiques 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 $700 million program to help AI make sense of satellite images* (contracte d'etiquetatge Sequoia de fins a 708 M$ en 7 anys, 2024; alimenta la visió per computador Maven; el contracte de dades més gran de l'agència). 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 Integritat, Procedència i Confiança, abril de 2025; defineix integritat/procedència/confiança, però sense signatura criptogràfica ni cadena de blocs). 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 gener de 2025; guia conjunta que recolza la signatura de procedència C2PA per a la integritat de la imatge, aplicable a l'observació de la

Terra). https://media.defense.gov/2025/Jan/29/2003634788/-1/-1/0/CSI-CONTENT-CREDENTIALS.PDF

Protecció civil i emergències: qui sabia què, i quan

«Però si el sentinella veu venir l'espasa i no toca la trompeta, i el poble no és advertit [...] demanaré comptes de la seva sang a la mà del sentinella.»

— Ezequiel 33,6

La tarda del 29 d'octubre de 2024, l'estació d'aforament de la rambla del Poio, al sud-oest de València, va enviar les seves últimes dades. A les 16:13, un correu de la Confederació Hidrogràfica del Xúquer (CHJ) a Emergències informava d'un cabal de 28,7 metres cúbics per segon: semblava que allò remetia [5]. A les 17:00, el cabal era ja de 325,52; a les 17:40, la mateixa CHJ registrava al Poio un cabal cinc vegades superior al de l'Ebre [6]; a les 18:00, la sèrie marcava 1.725,89 [5]. A les 18:43, un altre correu avisava: 1.686 metres cúbics per segon i risc elevat [5]. A les 18:55, el sensor va marcar 2.282. Cap a les 19:00, la força de l'aigua va arrossegar i va destruir l'estació mateixa [5]. I l'alerta ES-Alert no va sonar als mòbils fins a les 20:11, quan els barrancs ja s'havien endut carrers sencers [1]. El balanç: 229 morts a la província de València i 237 a tot Espanya, més de 2.600 ferits, uns 141.000 vehicles i 11.242 habitatges afectats, 800 quilòmetres de carreteres malmeses [4], unes pèrdues estimades de 17.800 milions d'euros [3].

Aquest capítol tracta la protecció civil i les emergències: riuades, incendis, allaus, l'estat de les carreteres i les alertes a la població. La veritat de les comunicacions oficials en general es tracta al capítol 86; el testimoni orbital dels satèl·lits, al capítol 104; els sensors industrials, al capítol 96; la reclamació d'assegurances ordinària, al capítol 28. La pregunta que vertebra les pàgines següents és una altra: com es reconstrueix, de manera que ningú no la pugui discutir, la cronologia d'una emergència? Perquè després de cada catàstrofe comença una segona batalla —judicial, política i asseguradora— que sempre gira sobre el mateix: qui sabia què, i quan. La resposta d'aquest llibre és segellar cada dada en origen amb **t2p**: l'empremta SHA-512 calculada al dispositiu o a la font, l'ancoratge de l'empremta a la blockchain pública i el segell de temps RFC 3161/eIDAS complementari, dins d'un contenidor .asice, tal com hem vist als capítols 13 i 15 [23]. Una prova d'existència així és neutral per construcció: pot exculpar una administració o incriminar-la, blindar el ciutadà davant l'asseguradora i desarmar bulos. No té bàndol. Per això serveix.

La cronologia com a camp de batalla

Reconstruïm les cinc hores decisives amb el que se sap. El CECOPI —l'òrgan que coordina l'emergència— es va convocar a les 15:00 i es va reunir a les 17:00; passades les 18:00, el president de la Confederació hi va plantejar la possibilitat d'enviar alertes massives als mòbils [2]. La primera ES-Alert va sortir a les 20:11, i una segona, a les 21:03; en una emergència de nivell 2, la gestió i la petició d'enviament corresponen a la comunitat autònoma [1]. Entre la proposta i el so als telèfons van passar unes dues hores; entre el correu del risc elevat i l'alerta, gairebé una hora i mitja. Sobre aquests minuts s'ha construït des d'aleshores una batalla de versions que ha ocupat portades, compareixences i declaracions creuades.

I una instrucció judicial. Des del 10 de març de 2025, el Jutjat d'Instrucció número 3 de Catarroja, amb la jutgessa Nuria Ruiz Tobarra al capdavant, investiga l'exconsellera Salomé Pradas i l'exsecretari autonòmic d'Emergències Emilio Argüeso per presumptes omissions greus en la gestió d'aquella tarda [9]. L'Audiència de València va confirmar la imputació d'Argüeso; el Tribunal Superior de Justícia valencià va rebutjar investigar l'expresident Mazón; el març de 2026, la causa encara «afrontava la recta final» [10]. Més de cinc-cents dies per fixar una cronologia de cinc hores.

La ironia central del cas mereix aturar-s'hi. La jutgessa va haver de requerir a À Punt «totes les gravacions d'imatge i so» de la reunió del CECOPI, i de reclamar els vídeos originals a la productora —contractada, precisament, per la mateixa secretaria d'Emergències— per poder «determinar l'hora exacta de cada vídeo» [11]. Un any després de la riuada, l'instrument central de la instrucció era un grapat de fitxers la data dels quals ningú no podia acreditar. Aquest és exactament el problema que resol la prova d'existència: si cada acta, cada vídeo i cada ordre s'hagués segellat en el moment de crear-se, la cronologia seria avui un fet verificable en qüestió d'hores, no una hipòtesi processal que consumeix anys. I convé subratllar-ho: el segell no prejutja res ni assenyala ningú per endavant. Només fixa el rellotge — per a tothom.

Dades que desapareixen quan més importen

El sensor del Poio va morir treballant: segons el comunicat de la CHJ del 4 de novembre, la força de l'aigua va arrossegar els sistemes de mesura cap a les 19:00, després de dues hores reflectint la crescuda [5]. Fins aquí, la fragilitat física. El que va passar després il·lustra una fragilitat pitjor: la de la dada mateixa. A primers de novembre, enmig de la batalla de versions, les dades del Poio van desaparèixer del web públic de la CHJ, i van reaparèixer dies més tard; la premsa en va dir «l'apagó informatiu» [7]. I les revelacions posteriors van afegir inquietud: barrancs clau que no formaven part de la xarxa de control i un mesurador a Massanassa que no es mostrava públicament [8].

No cal cap conspiració perquè una dada crítica s'esvaeixi. N'hi ha prou amb un servidor que es reinicia, un web «en manteniment» o un funcionari espantat. Però l'efecte és sempre el mateix: la ciutadania perd la capacitat de distingir entre l'error, la negligència i l'ocultació, i el buit l'omple la sospita. En plena crisi, quan la confiança és l'únic recurs que no es pot improvisar, cada dada que desapareix erosiona totes les que queden.

La solució estructural és ancorar la telemetria en origen. Si cada lectura del Sistema Automàtic d'Informació Hidrològica (SAIH) es converteix, en néixer, en una empremta SHA-512 ancorada a la blockchain pública, amb segell de temps complementari [23], esborrar-la del web ja no la fa desaparèixer: l'existència i el contingut queden acreditats per sempre, i qualsevol ciutadà pot verificar que la sèrie publicada coincideix amb la segellada. Fins i tot els forats es tornen provables: allò que no es va mesurar tampoc no es pot maquillar a posteriori, perquè l'absència d'empremtes datades és, en si mateixa, un fet demostrable [8]. La confiança deixa de dependre de la bona fe de l'organisme i passa a dependre de la matemàtica. El sensor del Poio va morir enviant dades; el registre del que va enviar no hauria de poder morir mai.

La mentida durant l'emergència

Els dies posteriors a la riuada, el pàrquing inundat del centre comercial Bonaire, a Aldaia, es va convertir en l'epicentre d'una teoria de la conspiració: «ens amaguen els morts». Vídeos d'altres aparcaments presentats com si fossin de Bonaire; camions frigorífics i cotxes fúnebres descontextualitzats com a presumptes trasllats de cadàvers; una falsa acta municipal que parlava de «més de 220 cadàvers» extrets el primer dia; documents falsos que elevaven el total per sobre de les 800 víctimes. Quan la recerca oficial va acabar, la conclusió va ser rotunda: cap víctima mortal al pàrquing [12]. Tant era: la maquinària ja girava. Newtral va desmentir més de 60 bulos sobre la DANA només durant el primer mes [13], amb la IA generativa com a principal facilitador —imatges i vídeos versemblants a partir d'un text, veus clonades amb pocs segons d'àudio—; i aquella marea de falsedats va arribar a generar problemes d'ordre públic i a interferir en les tasques dels equips d'emergència [14].

En una emergència, el dubte mata dues vegades: quan el ciutadà no creu l'alerta oficial, i quan creu el bulo. La crisi de la veritat que vam descriure al capítol 10 té aquí la seva versió més letal, perquè el temps de reacció es mesura en minuts i no hi ha marge per a la verificació artesanal.

La prova d'existència no detecta mentides —no és un detector de bulos— però permet l'estratègia inversa: que tota peça oficial neixi segellada. Fotos de drons, comunicats, ordres d'evacuació, balanços: si cada element porta l'empremta i la data ancorades des de l'origen, qualsevol persona, mitjà o verificador pot comprovar-ne l'autenticitat sense dependre de ningú, i allò que circula sense segell queda automàticament sota sospita. El «dividend del mentider» —despatxar la prova incòmoda com a falsa— es desactiva quan la prova porta ancoratge criptogràfic: el responsable que voldria negar un retard ja no pot dir que el registre és un muntatge, i el conspiracionista que agita una «acta» apòcrifa topa amb un ecosistema on els documents autèntics es reconeixen per l'empremta. La veritat oficial es torna comprovable; la mentida, orfe de segell.

Focs, neu i asfalt: el patró es repeteix

L'agost de 2025, Espanya va viure la pitjor onada d'incendis forestals en més de trenta anys: prop de 400.000 hectàrees cremades fins al 19 d'agost, amb una vintena de grans incendis declarats en dues setmanes [17][18]. Ourense, amb unes 150.000 hectàrees —una setena part de la província—, León i Zamora van concentrar prop de la meitat de la superfície cremada; el foc d'Uña de Quintana va arrasar unes 40.000 hectàrees i el d'A Rúa, més de 38.000; a Molezuelas de la Carballeda, més de 700 persones van haver de ser evacuades, i el Govern va desplegar 500 militars addicionals de la UME sobre els més de 1.400 ja actius [17]. Quan el fum es va dissipar, va començar la pregunta de sempre, la mateixa de la DANA

però amb foc: es va avisar a temps aquell poble? Cada ordre d'evacuació, cada tall de carretera i cada part de mitjans desplegats és un document datat que després es discutirà.

La neu repeteix el patró en silenci. El Centre de Lauegi d'Aran publica cada dia el butlletí de perill d'allaus a partir de sortides al terreny i tests del mantell, complementat amb la cartografia ATES d'exposició del terreny, i adverteix que aquesta informació «no substitueix la formació, l'experiència i el bon judici» [19]; l'ICGC cobreix el Pirineu català i l'AEMET, la resta de massissos [20]. Quan hi ha un accident, la pregunta —d'asseguradores, famílies i, si escau, jutjats— és sempre la mateixa: quin nivell de perill estava publicat quan el grup va sortir? Un butlletí segellat en publicar-se fa la resposta indiscutible, i protegeix tothom alhora: el predictor pot acreditar què va publicar i quan; la víctima i els seus, sobre quina informació es va prendre la decisió.

I l'asfalt. L'article 106.2 de la Constitució i la Llei 40/2015 obliguen l'Administració a indemnitzar els danys causats pel funcionament dels serveis públics: un accident per mal estat de la via és indemnitzable si hi ha nexe causal i no hi intervé força major, l'atestat de la Guàrdia Civil és la peça probatòria central, i el silenci administratiu de sis mesos aboca el ciutadà al contenciós [22]. Registres de manteniment, inspeccions i talls de carretera segellats en origen tallen la discussió pels dos costats: l'Administració diligent pot provar que va actuar; el conductor, que el sot hi era. En els tres escenaris —focs, neu, asfalt— la constant és la mateixa que a València: la segona batalla es guanya o es perd segons qui pugui acreditar les seves dates.

La prova d'existència aplicada

Imaginem un centre de coordinació d'emergències, el pròxim octubre. Res no ha canviat a la vista: les mateixes pantalles, les mateixes trucades. Però cada acta, cada correu del SAIH, cada ordre i cada alerta es va segellant a mesura que es produeix, sense cap esforç afegit per als operadors: l'empremta SHA-512 es calcula a la font, rep el segell de temps RFC 3161/eIDAS i s'ancora a la blockchain pública dins d'un contenidor .asice [23]. La cadena de custòdia es construeix sola, mentre tothom fa la seva feina.

1. El registre de la decisió

L'òrgan de coordinació d'una emergència —el CECOPI valencià o qualsevol altre— produeix actes, vídeos i ordres que dirigeixen la resposta. Segellats en el moment de crear-se, esdevenen una cronologia no repudiable: si l'enviament d'una alerta es planteja passades les 18:00 i s'executa a les 20:11 [1][2], el registre ho acredita sense requeriments judicials a televisions ni a productores [11], i una instrucció que avui consumeix anys [9][10] es redueix en bona part a verificar empremtes. La neutralitat és la clau de volta: el mateix segell que pot evidenciar la lentitud d'un responsable acredita la diligència del que va actuar bé. Les autoritats poden demostrar que van decidir a temps; la ciutadania disposa d'una base verificable per exigir responsabilitats quan no va ser així.

2. El sensor que no pot desaparèixer

Les lectures del SAIH —com la seqüència del Poio: 28,7, 325,52, 1.725,89, 2.282 metres cúbics per segon [5]— s'ancoren en origen, per lots i en temps real. Ni un «apagó informatiu» al web [7] ni la destrucció física de l'estació [5] no esborren el registre: l'empremta acredita què es va mesurar i quan, i els buits de la sèrie queden igualment datats. La xarxa de control es torna auditable des de fora [8]: qualsevol persona amb el fitxer de dades pot comprovar que coincideix, bit a bit, amb el que es va segellar aquell dia. La discussió sobre «quines dades hi havia» s'acaba abans de començar.

3. La foto del ciutadà

El Consorci de Compensació d'Assegurances ha pagat per la DANA 212.237 sinistres per un import de 4.378 milions d'euros, amb un cost total estimat d'uns 4.800 milions (dades del març de 2026) [15][16]. Cada expedient comença amb el mateix material fràgil: fotos i vídeos del cotxe submergit, del baix inundat, de la collita perduda. Una foto segellada al dispositiu en el moment de fer-la —l'empremta amb la data, sense que la imatge hagi de sortir del telèfon [23]— accelera el peritatge, blinda el ciutadà honest davant la sospita i deixa sense marge el frau de qui recicla fotos d'una altra riuada: sense segell coherent amb la data del sinistre, la imatge reciclada no s'aguanta. L'escala ho fa decisiu: 251.249 expedients de cop [16], una allau administrativa que distingeix l'emergència del flux ordinari d'assegurances que hem vist al capítol 28.

4. El butlletí i la carretera

El butlletí de perill d'allaus [19][20], l'ordre d'evacuació d'un poble amenaçat pel foc [17], el tall preventiu d'una via o el registre de manteniment d'una carretera [22] comparteixen una mateixa naturalesa: són documents públics el valor probatori dels quals depèn del fet que ningú no pugui discutir-ne l'hora de publicació. Segellats en publicar-se, protegeixen alhora el tècnic que va avisar, el conductor que reclama i la família que vol saber si l'avís va arribar a temps. La data certa no té bàndol: és de qui la necessita.

Cal dir amb la mateixa claredat el que el segell no fa: no prediu riuades, no apaga focs, no fa sonar cap sirena; no detecta bulos ni impedeix crear-los. Només fa indiscutible què existia i quan. És infraestructura de prova, no substitut de la inversió en prevenció.

La promesa i el perill

La promesa és una emergència amb totes les dades crítiques segellades en origen: sensors, actes, alertes, ordres, fotos. La reconstrucció posterior es faria en hores i no en anys [9][10][11]; el Consorci podria tramitar les allaus d'expedients sobre proves no repudiables, amb peritatges més curts i menys frau [16]; i el bulo perdria força perquè tot allò oficial seria verificable per qualsevol [12][13]. La segona batalla —la de les versions— quedaria desactivada abans de començar.

Els perills exigeixen la mateixa franquesa.

El primer és la **vigilància**. Segellar la recepció d'alertes o les fotos dels ciutadans no pot esdevenir mai un rastre centralitzat d'on era cadascú. El disseny ha de ser el del llibre: les empremtes es generen i es custodien al dispositiu de cada persona; cap contingut ni cap ubicació no viatja a cap registre central, i el sistema no pot servir per desanonimitzar ningú [23].

El segon és l'**administració defensiva**. Si el segell es converteix en escut burocràtic, el funcionari pot acabar dedicant més energia a «quedar cobert» que a decidir bé. La cultura del paraigua ja existeix; la criptografia no l'ha d'amplificar. El segell documenta l'acció: no la substitueix ni l'eximeix.

El tercer és la **revocabilitat**. Les empremtes de les fotos personals de danys han de poder invalidar-se a petició del ciutadà. La immutabilitat és per a la dada pública —el cabal, l'acta, l'ordre—, no per a la vida privada de les víctimes, que conserven el dret a l'oblit.

I el quart és el **tecnosolucionisme**. Cap cadena de blocs no salva vides. Salven vides les sirenes, els plans d'emergència assajats, els barrancs nets, la cultura d'autoprotecció i, sobretot, la decisió presa a temps [2]. El segell garanteix només que, després, la veritat sigui indestructible. Però això, ben entès, també és prevenció: qui sap que la seva inacció quedarà acreditada per sempre té un incentiu poderós per actuar.

És hora d'actuar

La DANA de València va deixar 229 morts [4], una instrucció judicial que compta els dies per centenars [10] i una lliçó que cap país no hauria de necessitar aprendre dues vegades: la veritat d'una emergència és massa important per confiar-la a la memòria de les reunions, als webs que «es mantenen» i als vídeos sense hora.

Per a les administracions de protecció civil i els centres 112: segelleu en origen actes, ordres i alertes. L'ES-Alert —nascut de l'article 110 de la Directiva europea 2018/1972, transposada per la Llei 11/2022, i operatiu des del 2022-2023 [21]— ja arriba a tots els mòbils; feu que la cronologia de la pròxima emergència sigui un fet verificable des del primer minut, i no una investigació d'anys [9][10].

Per a les confederacions hidrogràfiques i els operadors de sensors: ancoreu cada lectura del SAIH en temps real, que cap «apagó informatiu» [7] no torni a ser possible i que fins i tot els buits de mesura quedin acreditats [8].

Per a les asseguradores i el Consorci: accepteu i prioritzeu la foto segellada al dispositiu. Davant 251.249 expedients de cop [16], la prova no repudiable és peritatge més ràpid, menys frau i més respecte per l'assegurat honest.

Per als mitjans i els verificadors: exigiu i comproveu el segell del material oficial d'emergència, i tracteu amb cautela per defecte allò que circuli sense ancoratge [12][13].

Per a tu, ciutadà: documenta els danys amb l'empremta al dispositiu, i recorda que el segell no substitueix l'alerta: quan soni el mòbil [1], deixa el cotxe i puja al pis de dalt.

Per als legisladors: reconeixeu valor probatori ple al registre segellat d'emergències i imposeu-lo com a estàndard de la Xarxa d'Alerta Nacional [21].

El sensor del Poio va morir a les 19:00 enviant la veritat [5]. Que mai més cap veritat d'emergència no depengui de la supervivència d'un aparell ni de la memòria d'una reunió. En aquest front, **time2act**.

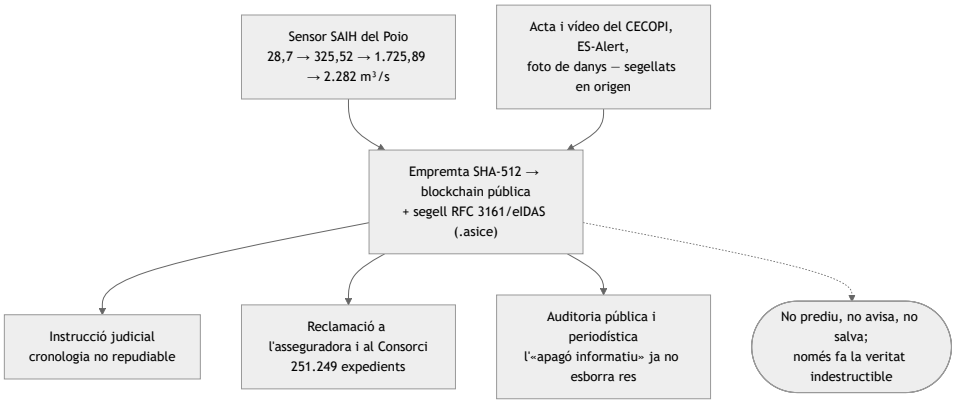


Figura 105.1 — La dada d'emergència se segella en origen: la lectura del sensor (SAIH/Poio), l'acta i el vídeo de l'òrgan de coordinació (CECOPI), l'alerta (ES-Alert), l'ordre d'evacuació i la foto de danys del ciutadà reben l'empremta SHA-512 al dispositiu o a la font, l'ancoratge de l'empremta a la blockchain pública i el segell de temps RFC 3161/eIDAS complementari (.asice). Tres sortides: la instrucció judicial (cronologia no repudiable), la reclamació a l'asseguradora i al Consorci, i l'auditoria pública i periodística. Límit: el segell no prediu, no avisa i no salva; només fa la veritat indestructible. Fonts: Maldita.es; CHJ/SAIH; Consorci de Compensació d'Assegurances; Lauegi.

---

[1] Maldita.es — *Quién envió la alerta de las 20:11 horas en Valencia, qué dice el protocolo* (31 d'octubre de 2024; ES-Alert a les 20:11 i 21:03; en nivell 2 la petició correspon a la comunitat autònoma). 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 convocat a les 15:00, reunit a les 17:00; proposta d'alerta massiva passades les 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 d'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 morts en total: 229 a la província de València, 7 a Castella-la Manxa, 1 a Màlaga; més de 2.600 ferits; 11.242 habitatges; ≈141.000 vehicles; 800 km de carreteres). 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 novembre de 2024; correus de la CHJ de les 13:42, 15:04, 16:13 i 18:43; cabals de les 17:00 i les 18:00; 2.282 m³/s a les 18:55; l'estació d'aforament, destruïda per l'aigua cap a les 19:00, segons el comunicat de la CHJ del 4 de novembre). 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 febrer 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 novembre 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* (instrucció oberta el 10 de març de 2025; Jutjat d'Instrucció núm. 3 de Catarroja, jutgessa 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 març de 2026; el TSJ rebutja investigar 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 d'octubre de 2025); El Español — *La jueza requiere a À Punt «todas las grabaciones de imagen y sonido» de la reunión del Cecopi* (els vídeos, d'una productora contractada per la secretaria d'Emergències; se'n demanen els originals per fixar l'hora exacta de cadascun). 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 d'octubre de 2025; falsa acta municipal de «més de 220 cadàvers»; documents falsos amb més de 800 víctimes; cap víctima mortal al pàrquing). 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 novembre 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 com a principal facilitador); elDiario.es — *Los bulos y falsedades sobre la DANA de València* (interferència en les tasques d'emergència). 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 novembre de 2025; 210.106 indemnitzacions). 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 març de 2026; 212.237 sinistres pagats; 251.249 expedients; el 99,3 % tramitats; cost total estimat ≈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 fins al 19 d'agost; Ourense ≈150.000 ha; Uña de Quintana ≈40.000 ha; A Rúa >38.000 ha; Molezuelas de la Carballeda, més de 700 evacuats; 500 militars addicionals de la UME sobre més 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 vintena de grans incendis en dues setmanes, més de 300.000 ha; la pitjor temporada en més de 30 anys). https://www.vallfirest.com/noticias/oleada-incendios-forestales-2025 ↩

[19] Centre de Lauegi d'Aran (Conselh Generau d'Aran) — *Butlletí de perill d'allaus i cartografia ATES* (butlletí diari; «la informació no substitueix la formació, l'experiència i el bon judici»). https://lauegi.conselharan.org/ates/?lang=en ↩

[20] ICGC — *Butlletí de Perill d'Allaus (BPA)* (Pirineu català); AEMET — *Boletín de peligro de aludes* (resta de massissos). 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 (Espanya) — *Public Warning System / ES-Alert* (art. 110 de la Directiva (UE) 2018/1972, transposat per la Llei 11/2022 General de Telecomunicacions; sistema operatiu des del juny de 2022 i a disposició dels 112 autonòmics des del 2023; tecnologia *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; Llei 40/2015; nexe causal; l'atestat de la Guàrdia Civil com a prova central; silenci administratiu de 6 mesos). https://www.administracionpublica.com/responsabilidad-patrimonial-por-danos-por-el-estado-de-la-calzada/ ↩

[23] t2p — manual de producte (empremta SHA-512 al dispositiu o a l'origen de la dada; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice). Vegeu els capítols 13 i 15. ↩

Eleccions verificables: del «dividend del mentider» a l'evidència ancorada

«Si tothom et menteix sempre, la conseqüència no és que et creguis les mentides, sinó que ja ningú no creu res.»

— Hannah Arendt, entrevista amb Roger Errera (1973)

El **28 de setembre de 2023**, dos dies abans de les eleccions parlamentàries eslovaques, va començar a circular per Telegram i Facebook una gravació d'àudio en què el líder del partit Eslovàquia Progressista, **Michal Šimečka**, i la periodista del diari Denník N **Monika Tódová** semblaven discutir com amanyar les eleccions: comprant vots de la minoria gitana, manipulant el recompte i subornant periodistes. L'àudio era una falsificació generada amb IA; tots dos ho van negar immediatament i els verificadors de l'AFP hi van trobar els senyals de la manipulació. Però va arribar en el pitjor moment possible: dins de la **moratòria electoral de 48 hores**, quan ni els mitjans ni els polítics podien desmentir-lo amb detall; i, en ser àudio i no vídeo, va esquivar el forat de la política de «mitjans manipulats» de Meta, que llavors només cobria el vídeo. Va superar les **100.000 visualitzacions** a Facebook i les **30.000** a Instagram, i va córrer per cadenes de correu amb la transcripció inclosa. El partit de Šimečka va perdre davant l'Smer de Robert Fico; els analistes encara debaten quant hi va influir l'àudio, però el cas s'ha convertit en el primer estudi de cas d'una mentida que arriba quan ja no queda temps per desmentir-la [12].

Quatre mesos després, a New Hampshire, una veu clonada de **Joe Biden** demanava per telèfon als votants que no anessin a les primàries —el cas que hem analitzat al capítol 68—, i la FCC va acabar sancionant-ne el responsable [1]. El problema de fons és el mateix a totes dues ribes de l'Atlàntic: quan la falsificació arriba més de pressa que el desmentiment, la confiança electoral queda sense àncora. Aquesta és la qüestió d'aquest capítol.

Aquestes escenes es converteixen en la il·lustració d'una paradoxa profunda: l'amenaça més fonamental no és que ens enganyin amb una mentida, sinó que abandonem la fe en qualsevol veritat. Beth Noveck, a *Reboot*, descriu aquest fenomen com el «liar's dividend», on la possibilitat de crear falses narratives permet descartar les realitats incòmodes com a enganys deliberats [2]. Així, una simple gravació d'àudio pot desencadenar un efecte dominó que minva la credibilitat del procés democràtic sencer.

L'impacte d'incidents com aquests es mesura millor en l'escala de les eleccions de 2024: l'any electoral més gran de la història, amb més de quatre mil milions de persones cridades a votar en més de quaranta països [3]. En un context on cada vot compta i una àmplia fracció de la població depèn d'un procés transparent, l'erosió de la confiança esdevé una crisi sistèmica. Les tecnologies emergents —IA per a la generació de contingut sintètic i plataformes socials que amplifiquen el seu abast— han transformat les mentides en eines de pressió política, creant un entorn on la veritat necessita una defensa més robusta que la simple detecció del fals.

La resposta que proposa aquest capítol, i que constitueix el fil conductor de la Part XII, no és només afinar els filtres contra deepfakes o reforçar les lleis com l'SB 131 d'Utah, que obliga a etiquetar mitjans sintètics amb procedència tamper-evident [4]. El veritable gir de timó es troba en una prova d'existència ancorada a la blockchain: el t2p descrit al capítol 13. Aquesta àncora neutral i immutable ofereix un registre verificable que no depèn de tercers de confiança ni de la integritat del creador original; és, per tant, una evidència d'autenticitat inalterable que pot ser consultada independentment del contingut visual o sonor. La integritat del procés mateix — el cens, l'urna, el recompte vist des de dins — l'hem tractada al capítol 48; el front d'aquest capítol és l'evidència pública que envolta l'elecció.

En lloc de centrar-nos exclusivament en detectar falsos —una cursa sovint perduda, com demostra el capítol 15— la nostra missió és demostrar què és real amb una prova immutable. Només així podem contrarestar el «dividend del mentider» i restaurar la confiança que sustenta les eleccions democràtiques. En aquest escenari, la blockchain esdevé no només una infraestructura tecnològica, sinó el fonament d'una nova era de transparència electoral.

El dividend del mentider

Quan la tecnologia crea imatges i àudios tan perfectes que ningú pot discernir el veritable de l'engany, la simple existència d'una deepfake esdevé una arma poderosa contra la veritat. No només el fals enganya; la **possibilitat** que qualsevol prova pugui ser un muntatge generat per IA genera un dubte universal:

«potser tot això és una manipulació». Aquest escenari, anomenat per Beth Noveck *dividend del mentider*, transforma cada fragment de l'evidència electoral —des d'una fotografia del col·legi fins al registre digital d'un vot— en una possible ficció. Quan cap imatge, àudio o acta es pot creure amb certesa, el vot perd el seu ancoratge en la realitat compartida i es converteix en un gest aïllat, desproveït de confiança col·lectiva.

Aquesta erosió del fonament democràtic no és una mera hipòtesi. Com hem vist, el 2024 va ser l'any electoral més gran de la història, amb més de **4.000 milions** de persones cridades a les urnes en més de quaranta països [3]. En aquest context massiu, qualsevol incertesa sobre la validesa dels resultats pot desencadenar crisis polítiques que travessen fronteres. La detecció de deepfakes, encara que avançada, es converteix en una cursa armamentística: cada nou algoritme capaç d'identificar manipulacions és avaluat i superat per tècniques d'engany més sofisticades, com retalls o compressions que alteren el senyal original. Com indica el capítol 15, confiar exclusivament en la detecció és una **cursa perduda**; els defensors del veritable es veuen constantment superats per l'evolució de les tècniques falses.

La solució no és perseguir el fals amb més zel. El que cal és un fonament positiu, una **àncora neutral i immutable** que pugui demostrar, sense dubte, que una cosa autèntica va existir i no ha estat alterada. Aquí entra la prova d'existència basada en blockchain: el t2p que ja hem esmentat al capítol 13. Aquesta tecnologia ofereix una marca de temps criptogràfica verificable per qualsevol actor, sense necessitat d'un tercer de confiança ni depenent de credencials que puguin ser revocades o falsificades. En lloc de buscar el fals, es demostra el **veritable**: cada acta electoral, cada registre de vot i cada transmissió en viu pot ser «ancorat» a la cadena, assegurant que no ha patit cap alteració posterior.

Les marques d'aigua i els estàndards de procedència, tot i la seva importància com a complement —com mostra el *Tech Accord* de 2024 [5]— són insuficients si es consideren per separat. Noveck insisteix que «les marques d'aigua i els estàndards de procedència soles no resoldran el problema»; cal combinar-los amb una infraestructura immutable que proporcioni **confiança verificable** a tot moment [10]. Així, la IA deixa de ser un instrument per crear dubte i es converteix en una eina per reforçar la veritat, etiquetant cada fragment d'evidència amb una prova inalterable.

En resum, el dividend del mentider no és només un efecte col·lateral de les deepfakes; és una amenaça estructural que desestabilitza la confiança en les eleccions. La resposta no es troba en una guerra interminable contra els falsos, sinó en establir una base neutra i immutable —la blockchain com a testimoni immutable del fet real— que permeti a cada votant confiar que el seu vot és comptat tal com va ser emès, sense l'ombra d'un possible engany. Aquesta és la veritable clau per restaurar la credibilitat democràtica en una era de manipulació digital.

El complement: llei i indústria (necessaris, insuficients)

A la primavera del 2024 l'estat d'Utah va aprovar la SB 131, una norma que obliga a qualsevol anunci polític que contingui «mitjans sintètics» a incloure una cadena de procedència tamper-evident: ha de quedar clar qui és l'autor original, quins editors hi han intervingut i si s'ha fet servir IA generativa. La sanció prevista —1.000 dòlars per infracció— pretén crear un desincentiu econòmic perquè els actors polítics no puguin amagar la veritat darrere d'una imatge o una veu manipulada [4]. Aquesta llei reconeix, de manera explícita, que la clau per combatre les deepfakes és rastrejar l'origen del contingut. No obstant això, el seu enfocament es basa en un model de confiança depenent del creador i dels intermediaris: si l'autor no registra correctament la informació o si una plataforma decideix no aplicar-la, el mecanisme queda desactivat.

Al mateix temps, a febrer del 2024 es va signar el *Tech Accord to Combat Deceptive Use of AI in Elections* durant la Conferència de Seguretat de Munic. Vint empreses líders —Adobe, Amazon, Google, IBM, Meta, Microsoft, OpenAI i altres— es van comprometre voluntàriament a desenvolupar eines per detectar contingut electoral enganyós i a «rastrejar l'origen» d'aquest material [5]. L'acord no comporta sancions legals ni cap mecanisme de verificació externa; es recolza únicament en la bona fe dels participants. Això significa que, si una empresa decideix ignorar les seves pròpies directrius o si un nou proveïdor entra al mercat sense adherir-se a l'acord, el buit de confiança persisteix —com hem vist.

Beth Noveck, autora de *Reboot* (2026), posa el punt final a aquest dibuix incomplet: «les marques d'aigua i els estàndards de procedència soles no resoldran el problema», perquè depenen de la cooperació del creador i de la plataforma [10]. En les seves paraules, aquestes solucions són només un «complement menor» davant d'una crisi que requereix una àncora independent. La IA pot ajudar a classificar i filtrar contingut, però sense una font immutable que no pugui ser alterada per cap part, la confiança continua sent fràgil.

—És aquí on l'ancoratge en blockchain entra com a protagonista indiscutible. A diferència de les credencials de contingut descrites al capítol 13 —com hem vist—, que es basen en un taló d'Aquil·les i depenen d'una autoritat central per validar-se, la prova d'existència ofereix una veritat immutable. Un cop el votant o el registre electoral queda gravat en una cadena de blocs amb hash SHA-512 i Merkle tree, qualsevol intent posterior de modificar-lo esdevé detectable instantàniament i, més important encara, impossible sense deixar empremta. Aquesta neutralitat total elimina la necessitat de confiar ni en qui va crear el contingut ni en quina plataforma s'allotja.

—En resum, les iniciatives legislatives com la SB 131 d'Utah —com hem vist— són passos imprescindibles per establir un marc normatiu i cultural que reconegui la importància de la procedència. Tanmateix, sense una capa addicional que proporcioni una prova d'existència inalterable, aquestes mesures es queden curtes. La veritable solució a la crisi de confiança electoral no és només rastrejar l'origen; és crear un testimoni immutable que pugui ser consultat per qualsevol ciutadà, sense dependre de tercers. Això és el que ofereix *t2p*: un ancoratge neutral i independent que converteix la veritat electoral en un bé públic, immutable i verificable per a tots.

L'àncora neutral: provar l'autèntic

En un món on el «dividend del mentider» s'ha convertit en una arma política –«la capacitat de desestimar fets veritables però incòmodes com a falsos»[2]– la confiança en les eleccions es troba al límit d'un precipici. La solució no és només rastrejar l'origen del contingut, sinó crear un testimoni immutable que qualsevol ciutadà pugui consultar sense dependre de cap tercer de confiança; com hem vist, *t2p* ofereix una prova d'existència en blockchain que actua com a ancoratge neutral i independent, convertint l'evidència electoral en un bé públic verificable.

L'ancoratge es fonamenta en tres principis. Primer, la cadena no pren partit; cada bloc és generat per una xarxa distribuïda on cap entitat única controla el consens. Segon, no cal que el creador conservi cap credencial o clau secreta: un cop l'evidència s'ha inscrit, el seu hash es converteix en una empremta digital irreversible que qualsevol pot validar contra la cadena pública. Tercer, aquesta neutralitat permet que partits, observadors independents, mitjans de comunicació i ciutadans puguin utilitzar el mateix mecanisme sense temer manipulacions internes.

Un exemple viu d'aquesta aplicació es troba al projecte Voto Libre del Perú i Amèrica Llatina. Allà, la IA classifica les imatges fotogràfiques recollides durant les fases de recompte i, juntament amb blockchain, genera un informe «segur, transparent i en temps real»[6]. Quan el govern peruà va aprovar la llei 32270 per al vot digital amb blockchain l'any següent, es va establir que cada prova fotogràfica de frau hauria d'estar ancorada a la cadena, garantint que ningú pugui alterar-la sense deixar rastre. Així, les imatges es converteixen en testimonis verificables per qualsevol ciutadà o organització internacional.

A Taiwan, l'exministra digital Audrey Tang va impulsar una campanya de «prebunking» on els electors gravaven el seu propi col·legi electoral i pujaven aquests metratges a una plataforma basada en blockchain[7]. Cada vídeo es registra amb un hash únic; quan es consulta, qualsevol pot comprovar que el contingut coincideix exactament amb l'estat original del fitxer. Aquest procés ha transformat les gravacions personals en proves verificables del que realment va passar a les urnes, contrarestant les teories conspiratives i reforçant la legitimitat del resultat.

Com hem vist al capítol 13, un ancoratge neutral pot aplicar-se a tot tipus d'actuació electoral: recomptes de vots, comunicats oficials de la junta electoral, vídeos ciutadans dels col·legis o fins i tot declaracions públiques dels candidats. Un cop registrat en la cadena, cada element adquireix una capa de confiança que no depèn del dispositiu de votació (el «frontend») sinó del seu registre posterior (el «backend»). Això vol dir que, encara que la infraestructura de vot electrònic sigui vulnerable, la prova d'existència manté la integritat de l'evidència i permet a qualsevol revisitar el procés amb una veritat immutable.

Beth Noveck adverteix que les marques d'aigua i els estàndards de procedència «soles no resoldran el problema»[10]; cal combinar-los amb mecanismes com la prova d'existència per crear un ecosistema on l'educació mediàtica i les institucions sòlides puguin recolzar una confiança real. En aquest sentit, *t2p* ofereix la peça clau que falta: una cadena neutral que converteixi cada fragment de la veritat electoral en un testimoni públic, immutable i verificable per a tothom. (Vegeu el capítol 13 per al detall tècnic de la prova d'existència.)

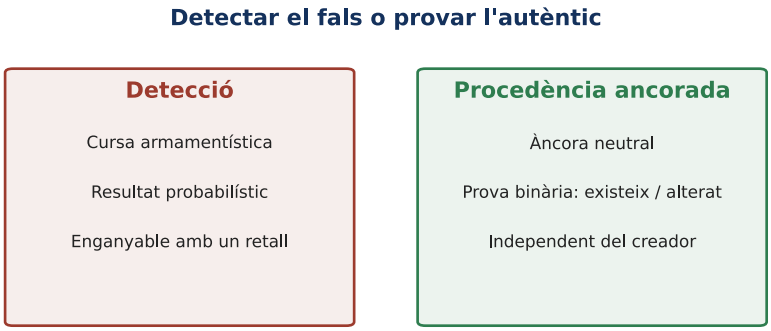


Figura 106.1 — Davant la cursa sovint perduda de la detecció, l'ancoratge neutral demostra que una cosa autèntica va existir i no s'ha alterat.

Quan el candidat és un avatar

En la primavera de 2024, mentre es recollien vots a Wyoming, una figura inesperada va aparèixer al ple de l'ajuntament: **VIC**, el Virtual Integrated Citizen. El xatbot, programat com a «titella de carn» del seu creador, es va presentar com a candidat a alcalde i, sorprenentment, va obtenir **327 vots**[8]. A les Illes Samoa Americana, un altre avatar —**PalmerAI**, amb la veu i la imatge d'en Jason Palmer— es va proclamar vencedor del caucus demòcrata amb **51-40** punts de votació[8]. I a Albània, el setembre de 2025 ha marcat l'arribada de **Diella**, la primera ministra d'IA del món, encarregada de les compres públiques i autoritzada per un vistiplau humà final[8].

Aquests casos fan desaparèixer la pregunta tradicional: *«És real aquest vídeo?»* La resposta ja no és rellevant. El que ara preocupa a votants, periodistes i reguladors és **qualsevol declaració provinent d'una entitat digital que pot reproduir-se infinitament**. Quan un avatar diu «prometo reduir els impostos per a les petites empreses», la veritat de l'enunciat depèn tant del contingut com de qui —o què— ha generat aquell missatge. La **procedència verificable**, que la prova d'existència en blockchain garanteix, passa a ser el criteri clau per autoritzar o desautoritzar una rèplica digital.

Aquesta nova frontera es troba al cor del *dividend del mentider* que descriu Beth Noveck: «la capacitat de descartar com a falsos els fets veritables però incòmodes»[2]. Els avatars d'IA amplifiquen aquest fenomen; la seva habilitat per generar discursos coherents i persuasius facilita que els humans deleguin la veu a una entitat sense cara. En el moment en què **el votant no pot distingir si el missatge ve del candidat real o del seu avatar**, l'elecció es converteix en un camp de batalla d'autenticitat digital més que de polítiques.

És aquí on la prova d'existència (t2p) entra en joc. Registrant cada declaració oficial —text, àudio i vídeo— amb una empremta criptogràfica immutable a una cadena **neutral**, es crea un testimoni públic inalterable del qui ha parlat i de què s'ha dit. Aquest ancoratge no depèn d'un tercer de confiança; la seva neutralitat total elimina la necessitat que el creador mantingui credencials o que les marques d'aigua siguin considerades suficients[10]. Com hem vist, iniciatives com el **Tech Accord** i la legislació d'Utah sobre mitjans sintètics reconeixen que les marques de procedència són només un complement menor, sense capacitat per resoldre la crisi de confiança per si soles[5][4].

No obstant això, la solució encara és parcial. El capítol 81 detalla els **drets de rèplica digital**, que permeten a una persona exigir l'eliminació o la correcció d'un contingut difós sense el seu consentiment. Quan un avatar d'IA repeteix una declaració errònia, la víctima pot invocar aquest dret, però només si disposa d'una prova inequívoca de la font original. Sense la **prova d'existència**, la cadena de responsabilitat es trenca i el debat es desvia cap a litigis interminables.

Així, la pregunta que queda oberta és com integrar aquesta capa de verificació en els processos electorals sense enganyar la ciutadania amb una nova forma de burocràcia digital. La resposta passa per **convertir cada missatge electoral en un registre immutable** i, al mateix temps, establir mecanismes legals que reconeguin aquest registre com a prova vinculant davant les autoritats. Només llavors podrem dir que la democràcia ha trobat una eina per fer governable el repte de l'avatar polític, mantenint viva la confiança en la veritat electoral mentre es conserva la llibertat d'expressió digital.

La promesa i el perill

En una jornada d'eleccions a la capital peruana, una observadora va gravar amb el seu telèfon un taulell de votació on apareixia clarament el paper de l'urna i el número del col·legi electoral. Uns minuts més tard, aquella imatge es va pujar a les xarxes socials i, sense cap marca d'aigua ni etiqueta que en certifiqués l'origen, alguns grups polítics van començar a qüestionar-la com a «fotomuntatge». La mateixa escena, reproduïda amb una IA generativa, podria haver estat desmentida en pocs segons si la prova d'existència registrada a la blockchain hagués pogut demostrar que aquell instant havia quedat fixat de manera immutable i neutral. Aquesta és la promesa central del *t2p*: convertir el «no pots provar res» en «això existia i no s'ha alterat», oferint una àncora independent que no depèn d'un tercer de confiança ni de credencials que puguin ser revocades.

L'impacte d'aquest ancoratge és immediat. Quan la veritat es pot corroborar amb un hash immutable, el «dividend del mentider» —el poder de desestimar fets incòmodes alegant que són falsos— perd força ([2]). En lloc d'una cursa infructuosa per detectar deepfakes, les eleccions passen a ser una prova verificable: la simple existència del registre és suficient per desactivar l'argument de «potser no va passar». Això no només reforça la confiança dels votants, sinó que ofereix als mitjans i a les autoritats un punt d'inici sòlid per a qualsevol investigació posterior. La neutralitat total de la blockchain —sense cap entitat central que pugui manipular el registre— assegura que la prova sigui acceptada tant en tribunals com en processos electorals internacionals.

Però aquesta promesa ve acompanyada d'un perill inevitable. Primer, les marques d'aigua i els estàndards de procedència, tan ben intencionats com són, no poden resoldre el problema sols ([10]). Sense una alfabetització mediàtica robusta —com demostra l'estudi coreà que ha reduït la intenció de compartir informació falsa ([11])—, la població continua vulnerable a les narratives manipulades. La tecnologia només pot proporcionar evidència; no pot substituir el judici humà ni la confiança col·lectiva en institucions sòlides.

Segon, el tecnosolucionisme pot enganyar amb l'idea que una àncora immutable garanteix la veritat del contingut. El *t2p* només certifica que un document o una imatge van existir i no han estat alterats posteriorment; no avalua si les declaracions contingudes són veraces o no. Així, una acta electoral podria estar perfectament ancorada però plena d'errors de comptatge o manipulació humana anterior a la seva captura. La tecnologia ha de ser complementària a processos de verificació i auditories independents, no un substitut.

Finalment, qui controla la cadena? El capítol crític 112 alerta que la infraestructura que garanteix la veritat pot convertir-se en una eina de vigilància si es deixa sense governança democràtica. Sense mecanismes clars d'auditoria i participació ciutadana, la mateixa blockchain podria ser utilitzada per entitats autoritàries o corporatives per registrar i monitorar comportaments polítics, consolidant un nou tipus de poder centralitzat. Això subratlla la necessitat d'un marc legal que reconegui el registre com a prova vinculant però també limiti l'abús.

En resum, l'àncora neutral del *t2p* és una eina indispensable per restablir la confiança electoral en un entorn on les deepfakes erosionen constantment la veritat. No obstant això, la seva eficàcia depèn d'una alfabetització mediàtica sòlida, de processos humans que verifiquin el contingut i d'un govern democràtic sobre la infraestructura blockchain. Només així podrem dir que l'eina és necessària —i no només suficient.

És hora d'actuar

Les autoritats electorals són les primeres guardes de la confiança ciutadana. Han d'ancorar cada acte oficial —acta de vot, recompte preliminar i comunicat de resultats— amb una prova d'existència en blockchain (t2p) i publicar-ne el hash verificable al portal electoral. Això converteix qualsevol intent de manipulació en un canvi impossible sense deixar rastre, i permet que qualsevol observador contrasti la integritat del document amb una sola consulta a la cadena.

Els mitjans han d'adoptar el mateix rigor. Cada informe que inclogui material sensible —vídeos de debat, declaracions gravades o documents filtrats— ha de ser segellat amb un segell d'existència i publicar-ne l'identificador al final de l'article. Això ofereix als lectors una prova immutable que el contingut no s'ha alterat des del moment en què es va pujar a la xarxa, i els capacita per verificar-lo sense dependre d'un tercer de confiança. Els periodistes també han de formar les seves redaccions en l'ús de les eines de

comprovació basades en IA que integren blockchain, tal com demostra el projecte Voto Libre al Perú [6], on la combinació ha permès un reportatge «segur, transparent i en temps real».

La ciutadania, per la seva part, es converteix en l'última línia de defensa. Davant d'un vídeo «explosiu» que circula a les xarxes durant una campanya, el votant ha de demanar-ne la prova d'existència abans de compartir-lo. Si no existeix cap hash verificable, el contingut s'ha de tractar com a potencial deepfake i es recomana notificar les plataformes corresponents. A més, qualsevol testimoni directe—una gravació del seu col·legi electoral o una foto del tauler de votació—ha d'anar immediatament a una xarxa pública de blockchain, tal com va fer Taiwan amb la iniciativa Cofact liderada per Audrey Tang [7]. Això converteix l'acte individual en una àncora neutra que reforça el teixit col·lectiu de la veritat.

Els reguladors han d'establir marcs legals que garanteixin la interoperabilitat i la procedència verificable del contingut electoral, inspirant-se en l'exemple de Utah amb la Llei SB 131, que exigeix etiquetes «tamper-evident» per a mitjans sintètics [4]. No obstant això, aquesta regulació no ha de delegar tot el control a la tecnologia; cal combinar-la amb programes d'alfabetització mediàtica i de formació en IA, tal com recomana Beth Noveck: les marques d'aigua per si soles no resolen el problema [10].

En resum, la cadena de confiança es construeix pas a pas: autoritats que ancoren dades oficials, mitjans que publiquen amb segell immutable, ciutadans que verifiquen abans de difondre i reguladors que imposen estàndards sense abdicar del control democràtic.

Les eleccions no es demanen; es comproven. És time2act.

---

[1] FCC — *Robocalls de veu clonada i eleccions (cas 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 i eleccions 2026 al 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/ ; i *Reboot*, cap. 3 (Voto Libre). ↩

[7] Beth Simone Noveck — *Reboot* (2026), cap. 3 (Taiwan, 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), introducció i cap. 3 («possibilist, not Pollyanna»; la procedència «alone will not solve the problem»). ↩

[11] Beth Simone Noveck — *Reboot* (2026), cap. 3 (assaig coreà sobre alfabetització mediàtica i deepfakes). ↩

[12] IPI / VSquare / HKS Misinformation Review — *el deepfake d'àudio Šimečka–Tódová a Eslovàquia* (28-09-2023; moratòria de 48 hores; forat de la política d'àudio de Meta; el debat sobre la influència real en el resultat). 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 registre que es pot comprovar

«Els models són opinions incrustades en matemàtiques.»

— Cathy O'Neil, Weapons of Math Destruction (2016)

Era una tarda freda d'octubre a Londres quan James Whitaker, subdirector de l'oficina regional de Correus del Regne Unit, va rebre la notificació oficial que canviaria la seva vida. Un correu electrònic, enviat des del departament legal de la corporació, li anunciava una acusació de frau per part d'un programa anomenat Horizon, desenvolupat per Fujitsu i implementat al servei de gestió de transaccions postals. Whitaker, que havia dedicat més de tres dècades a la logística postal i gaudia d'una reputació impecable entre col·legues i ciutadans, es trobava ara davant d'un delicte que mai havia comès.

El programa Horizon, segons el seu disseny, registrava cada moviment de diners en les seves 600 sucursals. Però una sèrie d'errors informàtics va crear «descoberts» inexistents: transaccions fictícies que sumaven milions de lliures. Sense cap registre independent que pogués ser consultat o verificat per un tercer, la sola declaració del software es convertí en prova feixuga. Whitaker i més de 900 subdirectors d'oficina van ser condemnats injustament, perdent les seves llars, la seva reputació i, en alguns casos, la vida mateixa; el cas s'ha vinculat a com a mínim tretze suïcidis [1].

La investigació pública presidida per Sir Wyn Williams, conclosa al desembre de 2024, va revelar que l'absència d'un registre auditable havia permès que el sistema fos manipulat sense cap rastre visible. No es tractava només d'una falla tècnica, sinó d'una falta estructural: ningú –ni els funcionaris del govern ni la pròpia agència postal– podia reconstruir pas a pas com s'havien generat aquells suposats errors. El resultat fou una catàstrofe de confiança i responsabilitat que va sacsejar el sector públic britànic.

En aquest context, la veu de Noveck en *Reboot* ressona amb claredat: «Cal comprar la IA com a infraestructura cívica — verificable, auditable i responsable per a les persones que afecta» [1]. La lliçó no és evitar la intel·ligència artificial, sinó exigir que cada decisió assistida per una màquina es pugui rastrejar i comprovar de manera independent. Un registre tamper-evident, ancorat amb prova d'existència (t2p), seria el fonament mínim per a qualsevol auditoria futura; sense ell, les decisions automatitzades romanen en la foscor, inaccessibles a la revisió ciutadana i vulnerables a l'impunitat.

Així, l'escena de Whitaker, un home honrat convertit en víctima d'un algoritme invisible, il·lustra el perill més insidiós de delegar decisions públiques a una IA sense un marc de responsabilitat clar: la irresponsabilitat. No és només que el programa fos biaixat; és que no hi havia cap mecanisme per a comprovar què havia passat realment i qui en era responsable. La proposta de Noveck —exportació de registres per a revisió independent, escrows de tercers o accés restringit d'avaluadors— es converteix, doncs, en una necessitat urgent per a restaurar la confiança pública en les tecnologies governamentals [2].

En les seccions que segueixen veurem com un registre immutable basat en blockchain pot garantir neutralitat i no-repudiabilitat, convertint cada acció de la IA pública en un esdeveniment verificable i auditable, i obrint la porta a una democràcia realment responsable davant les noves formes d'automatització.

Les apostes: del biaix a la irresponsabilitat

Els governs ja confien en sistemes d'intel·ligència artificial per assignar prestacions socials, adjudicar contractes públics i definir les prioritats de polítiques urbanes. En els debats públics el focus sovint recau en el biaix dels algorismes: si una IA aprèn de dades històriques esbiaixades, pot perpetuar discriminacions invisibles. Però la veritable crida d'alerta és més profunda. Quan les decisions són preses per una màquina i ningú pot reconstruir el camí que ha conduït a elles, desapareix l'essència mateixa de la rendició de comptes. Com diu Noveck, cal evitar una «accountability in name only»: un teatre democràtic on les explicacions són només narratives plausibles, però no verificables [9].

Aquesta irresponsabilitat esdevé especialment perillosa en l'àmbit de la contractació pública, que és la palanca més potent per modelar l'economia i la confiança ciutadana. Noveck insisteix que la compra d'IA ha d'exigir «exportació de registres per a revisió independent» i, quan el sistema sigui tancat, la creació d'un escrow o un accés restringit per a auditors externs, de manera que qualsevol resultat pugui ser reproduït i verificat [2]. Sense aquests mecanismes, els reglaments es converteixen en simples formalitats:

els proveïdors poden emmagatzemar logs en servidors propietaris, i les administracions poden modificar o suprimir dades sense deixar rastre.

És aquí on entra el protagonisme del registre immutable basat en blockchain. Un bloc encadenat actua com a testimoni neutral, impossible de ser alterat ni per l'administració ni pel proveïdor. Cada acció de la IA —des de la selecció d'una oferta fins al càlcul d'una prestació— queda anotada amb una prova d'existència (t2p) que fixa el *què* i el *quan*, sense revelar el *com*. Aquesta mínima informació és, per si sola, el fonament indispensable per a qualsevol auditoria: comprovar que l'esdeveniment va existir, però no necessàriament conèixer la lògica interna del model. Així es garanteix la neutralitat i la no-repudiabilitat, mentre es manté la confidencialitat de les propietats intel·lectuals i de les dades sensibles.

Els registres algorítmics públics que van sorgir a Helsinki i Amsterdam el 2020 —i que posteriorment s'han replicat al Canadà i Espanya— ja demostren com una catalogació transparent d'algoritmes pot reforçar la confiança ciutadana [4]. No obstant, sense un mecanisme immutable, aquests inventaris són vulnerables: poden ser editats o esborrats, i el seu valor queda limitat a una declaració de bona fe. La integració amb blockchain transforma aquest registre en una evidència forense fiable, que es pot consultar per part d'auditors independents, tribunals i ciutadans interessats.

En resum, la transició de l'enfocament del biaix cap a la responsabilitat implica tres passos clau: (1) exigir l'exportació i auditabilitat dels logs com a condició de compra; (2) establir escrows o accés restringit per a auditors externs quan els sistemes siguin tancats; i (3) ancorar aquests registres en una infraestructura immutable que garanteixi neutralitat i no-repudiabilitat. Només així la IA pública pot deixar de ser un instrument d'opacitat i convertir-se en una infraestructura cívica verificable, tal com proposa Noveck: «verificable, auditable i responsable per a les persones que afecta» [1]. Aquesta és la base sobre la qual podem construir una democràcia realment responsable davant l'automatització creixent.

El registre que es pot comprovar

Al laboratori del GovLab a Washington, la primera versió de **Policy Synth** es va desplegar l'estiu del 2024 com una eina oberta per a decisions automatitzades en àmbits tan diversos com les licitacions públiques i el disseny de polítiques urbanes. Cada acció d'un agent d'IA queda registrada en un «log» detallat que indica qui ha actuat, quina decisió s'ha pres, quan i quines fonts de dades l'han alimentada; a més, cada entrada ve acompanyada d'una citació automàtica de les dades utilitzades, tal com descriu Noveck: «desa un registre detallat de les accions dels seus agents, que permet als responsables polítics auditar i explicar les decisions; totes les sortides estan referenciades i citades» [3].

El que converteix aquest registre en una veritable **infraestructura cívica** és l'ancoratge amb la prova d'existència descrita al capítol 13. Quan cada entrada es «timesta» a través d'una cadena de blocs immutable, el registre passa de ser un simple arxiu digital a convertir-se en una evidència **no-repudiable**: ningú —ni l'agència que ha desplegat l'IA, ni els proveïdors del model— pot modificar retroactivament la informació registrada. Això elimina el perill d'una responsabilitat difusa i la substitueix per una traçabilitat clara i verificable.

Aquesta neutralitat és clau perquè, com assenyala Noveck, el veritable repte no són els biaixos del model sinó l'**irresponsabilitat**: «qui assumeix la responsabilitat quan un agent d'IA autònom recomana una acció que acaba en un resultat perjudicial?» [3]. Un registre immutable respon directament a aquesta pregunta. Si una decisió de contractació pública ha conduït a un sobrecost o a la selecció d'un proveïdor corrupte, el log mostrat per Policy Synth indica exactament quin agent va recomanar l'acció, quines dades la van recolzar i en quin moment es va generar. Un auditor —o fins i tot un tribunal— pot reproduir aquest escenari sense dependre de la bona fe d'una part o de la disponibilitat de codi font.

Com hem vist a Helsinki, el registre municipal d'algorismes del 2020 es va enllaçar amb una capa de prova d'existència per garantir que les decisions sobre assignació d'habitatges socials fossin totalment verificables [4]. A Amsterdam, l'enregistrament de les polítiques de vigilància urbana segueix el mateix patró: cada alerta generada per un model predictiu és horodatada i ancorada a la cadena, cosa que permet als ciutadans sol·licitar una explicació completa i immutable. Aquestes experiències demostren com la **neutralitat** del registre —la cadena no jutja el contingut, només fixa el fet— es converteix en l'element fonamental per a una auditoria real.

En resum, ancorar el log de Policy Synth amb prova d'existència transforma un simple historial operatiu en una font de veritat indiscutible. La pregunta de Noveck sobre la responsabilitat deixa de ser abstracta i es converteix en una resposta concreta: el registre indica **qui**, **què**, **quan** i **amb quines dades**. Això

ofereix a les institucions públiques un mecanisme d'auto-control que no depèn de l'autosuficiència del proveïdor, sinó d'una infraestructura pública verificable i auditable —exactament el que Noveck defensa com a «verificable, auditable i responsable per a les persones que afecta» [1]. La democràcia, així, pot avançar cap a una era en què la confiança es basa en proves inalterables, no només en promeses.



Figura 107.1 — La decisió d'IA pública deixa un registre citat que, ancorat amb prova d'existència, esdevé una auditoria independent i no-repudiable.

Registres i procedència: del catàleg a la prova

A l'estiu del 2020, Helsinki i Amsterdam van publicar els primers inventaris algorítmics municipals, documents que enumeraven cada sistema d'IA desplegat en serveis públics, des de la gestió d'escombraries fins al control de trànsit. Aquells catàlegs no eren simples llistats; incloïen les finalitats del model, els conjunts de dades d'entrenament i les mesures de supervisió humana aplicades. L'objectiu era clar: transformar la «confiança en la web de la ciutat» en una confiança fonamentada en proves verificables [4]. Quan aquestes entrades es van ancorar amb la prova d'existència descrita al capítol 13, qualsevol ciutadà o auditor extern podia demostrar que un registre havia estat creat en un moment determinat i no s'havia modificat posteriorment. Això elimina l'opció de «editar a posta» els logs després d'una decisió controvertida i ofereix una base neutra per a la revisió.

Els esforços europeus van inspirar iniciatives similars al Canadà, amb el projecte Tracking Automated Government, i a Espanya, on l'Observatori Algorítmic ha consolidat un repositori nacional que recull les IA utilitzades en àrees com les compres públiques i la seguretat ciutadana. Aquestes plataformes es converteixen en punts de partida per a auditories independents: els auditors poden descarregar el registre, comprovar-ne l'horari amb la prova d'existència i comparar-lo amb les decisions efectives del sistema. La combinació d'inventaris públics i ancoratge criptogràfic crea una capa de transparència que supera la simple «doble opacitat» descrita per Noveck, on el coneixement científic i comercial es manté separat i ocult [5].

A escala de procedència del model, el concepte d'AI-BOM (Bill of Materials) ha guanyat tracció gràcies a les directrius de Noveck, que insisteixen en incloure no només els pesos del model sinó també les dades d'entrenament i la configuració completa de la infraestructura [8]. DeepSeek R1, llançat al gener del 2025 amb pesos oberts sota llicència MIT i un cost de desenvolupament de 5,6 milions de dòlars, ha demostrat que és possible publicar tota la cadena de subministrament d'una IA avançada sense comprometre la propietat intel·lectual essencial [7]. Quan aquest AI-BOM es registra mitjançant la prova d'existència, qualsevol entitat pot verificar que les dades declarades són exactes i que no s'han afegit ni suprimit elements posteriors a l'entrenament. Això ofereix el fonament mínim sobre el qual una auditoria externa pot construir-se: es coneixen tant els ingredients com el moment en què van ser combinats.

El marc regulador californià, amb la SB 53 i la creació de CalCompute, ja obliga a grans proveïdors a publicar informes de seguretat estandarditzats i a mantenir un núvol públic on les execucions es registren de forma immutable [6]. Aquesta infraestructura pública proporciona l'«escrow» que Noveck demana per a sistemes tancats: els logs del nucli d'execució són accessibles a auditors independents, garantint la traçabilitat completa des del moment en què s'ha generat una recomanació fins al seu desplegament final.

En resum, l'anomenada «doble opacitat» no és un obstacle insalvable si es combina un catàleg algorítmic públic amb la prova d'existència i un AI-BOM complet. El registre passa de ser una simple declaració a una evidència inalterable que permet tant al ciutadà com a l'institució verificar què va existir i quan, obrint el camí per a auditories reals i responsabilitat efectiva. Aquesta és la clau perquè la IA pública es converteixi en infraestructura cívica verificable, auditable i, finalment, responsable.

La promesa i el perill

Imagina una ciutat on cada licitació, cada decisió de polítiques socials o cada alerta policial generada per un algorisme es registra en una cadena de blocs immutable. Un funcionari pot obrir l'aplicació, veure la transacció amb el seu hash, comprovar que el model d'IA va existir i quan, i consultar les metadades que indiquen quins pesos i dades van ser utilitzats. Això transforma la confiança cega en una verificació directa: «confia en l'administració» es converteix en «comprova-ho tu mateix». La prova d'existència (t2p) ofereix, com ja s'ha vist al capítol 13, el fonament mínim per a qualsevol auditoria independent; la simple declaració passa a ser una evidència inalterable que pot ser revisada per ciutadans i entitats externes.

Aquesta capacitat de fer auditable cada acció assistida per IA és la promesa central del registre tamper-evident. La iniciativa Policy Synth, desenvolupada pel GovLab de Noveck, ja demostra com un log detallat permet als responsables polítics rastrejar i explicar les decisions d'un agent autònom, amb totes les sortides citades i vinculades a fonts verificables[3]. A més, la normativa californiana (SB 53) obliga els proveïdors de models «frontera» a publicar informes de seguretat i a posar a disposició del públic registres d'ús, creant un ecosistema on el control es pot exercir des de fora de les empreses creadores[6].

Tanmateix, la mateixa infraestructura que garanteix la transparència pot engendrar perills greus si no s'acompanya d'una auditoria externa i de supervisió humana. La simple existència del registre no explica la procedència ni la justícia del model: el problema de la «doble opacitat», on la ciència és incomprensible i el comerç es manté tancat, persisteix encara que cada transacció sigui immutable[5]. Sense mecanismes d'auditoria independent, el registre pot convertir-se en una mera «accountability in name only», un teatre democràtic on les explicacions són plausibles però no veritables[9].

Un altre perill es manifesta quan la confiança en l'informació registrada es confon amb la legitimitat de la decisió. El cas Diella, primera ministra d'IA d'Albània que va promoure compres públiques «100 % lliures de corrupció» amb un vistiplau humà a cada fase, il·lustra com una cadena impecable pot amagar decisions injustes si el criteri subjacent del model és defectuós[10]. Un registre immutable no pot corregir una política que ja es basa en un biaix o una errada de programació; només pot demostrar que la decisió va ser presa i quan.

Finalment, la qüestió de qui controla la cadena i els nodes és fonamental. El capítol 112 detalla com el mateix registre immutable que fa responsable el govern pot, si es gestiona inadequadament, convertir-se en una eina de vigilància massiva sobre els ciutadans, rastrejant cada interacció amb l'IA i potencialment restringint drets digitals. Per tant, la infraestructura és necessària però no suficient: cal establir governs de dades, mecanismes d'escrow per a tercers i un marc legal que asseguri que el control del registre es manté en mans neutres i democràtiques[2].

En resum, l'ancoratge de les decisions públiques en una prova d'existència ofereix la clau per a auditories reals i responsabilitat efectiva. Però aquesta promesa només s'assoleix si es complementa amb auditoria externa, supervisió humana i una governança clara del registre mateix; altrament, el risc de teatre democràtic i vigilància excessiva pot eclipsar qualsevol benefici esperat.

És hora d'actuar

La confiança de què depèn la democràcia no pot quedar-se en una promesa abstracta; ha de ser verificable i, sobretot, reproduïble. Per això cada actor del sector públic ha de prendre mesures concretes que transformin la IA pública en una infraestructura cívica realment auditable.

Compradors públics —tant les administracions centrals com les entitats locals— han de fer obligatòria, en els contractes, la inclusió d'un registre ancorat a blockchain i provat per *t2p*. Aquest registre ha de ser exportable per a una revisió independent i, quan el sistema sigui tancat, s'ha d'establir un «escrow» de tercers o un accés restringit d'avaluadors tal com recomana Noveck: «exportació de registres per a revisió independent» i «escrow de tercers o accés d'avaluador restringit» són condicions imprescindibles per garantir que cap decisió es perdi en una caixa negra irreproduïble[2]. La clàusula contractual ha de

preveure sancions si el proveïdor no compleix amb aquests requisits, evitant així l'escenari del cas Horizon, on dades errònies van conduir a condemnes injustes i fins a tretze suïcidis[1].

Administracions —com a propietàries d'aquestes plataformes— han de publicar inventaris algorítmics que incloguin cada entrada ancorada al registre immutable. Els exemples pioners de Helsinki i Amsterdam, llançats el 2020, demostren que és possible detallar dades d'entrenament, ús, supervisió humana i avaluació de biaix en un catàleg públic accessible[4]. Aquests inventaris han d'anomenar explícitament la procedència dels models (AI-BOM) i les dades utilitzades, tal com es descriu al capítol 79, perquè qualsevol auditor pugui rastrejar l'origen i el moment exacte en què una decisió va ser generada.

Auditors i tribunals — com a guardians de la responsabilitat — han d'exigir l'empremta ancorada com a base mínima de revisió. La prova d'existència no només certifica que una acció ha existit, sinó que estableix el moment exacte en què es pot reproduir el procés decisional, convertint la inspecció en una tasca factible i evitant l'«accountability in name only», on les explicacions són merament escenificades sense fonament real[9].

Ciutadania — ha d'haver reconegut el dret a reconstruir i impugnar qualsevol decisió algorítmica que li afecti. Aquest dret es materialitza només si els registres són públics, no manipulables i accessibles per a revisió independent. La legitimitat d'una política pública no s'auto-declara; es comprova amb el registre que mostra quins passos es van seguir i quan es van executar.

En resum, la combinació de **neutralitat** (un registre immutable que ningú pot alterar) i **auditabilitat** (capacitat d'accedir, exportar i revisar els registres) converteix la IA pública en una eina responsable. Aquesta promesa només es materialitza si cada actor assumeix les seves obligacions: contractes amb clàusules d'exportació i escrow per a compradors; inventaris ancorats per a administracions; exigència de l'empremta per a auditors; i dret de reconstrucció per a ciutadans. La legitimitat no es proclama, es comprova. És *time2act*.

---

[1] Beth Simone Noveck — *Reboot: AI and the Race to Save Democracy* (Yale University Press, 2026), cap. 8 ; i *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 ; i *Reboot* (2026), cap. 8 (Canadà, Espanya). ↩

[5] Beth Simone Noveck — *Reboot* (2026), cap. 8 («double opacity»; auditories externes). ↩

[6] Govern de Califòrnia — *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 (codi obert: els cinc elements; registre de consultes i entrenaments). ↩

[9] Beth Simone Noveck — *Reboot* (2026), introducció i cap. 6 («accountability in name only»; la IA com a objecte). ↩

[10] TIME — *Albania's AI minister Diella* (2025). https://time.com/7324934/albania-ai-minister-diella/ ↩

Participació autèntica: una persona, una veu, sense vigilància

«No diem que qui no s'interessa per la política sigui algú que es fa càrrec dels seus afers; diem que aquí no hi té res a fer.»

— Pèricles, oració fúnebre (Tucídides, II, 40)

Era l'estiu del 2017 quan la Federal Communications Commission (FCC) va llançar una consulta pública sobre la neutralitat de la xarxa. El formulari en línia es va omplir amb més de **22 milions** de comentaris; el soroll que inundava la plataforma era tan intens que, uns mesos després, un informe de la FCC revelà que **18 milions** d'aquests missatges eren falsos i **9,3 milions** contenien identitats inventades o robades. La majoria d'aquestes intervencions provenien d'un sol jove de 19 anys que havia programat un bot per inundar el debat, mentre que prop de **500.000** comentaris arribaven des d'adreces russes vinculades a una campanya secreta finançada per la indústria de banda ampla[1].

Aquell escenari, tan concret com emblemàtic, mostrava la paradoxa que ara es repeteix en cada àmbit digital: quan el soroll supera el senyal i no podem distingir una veu humana d'un algoritme, la participació ciutadana es transforma en un **teatre de buits**. Les plataformes democràtiques, que haurien de ser escenaris per a l'expressió autèntica, acaben convertint-se en espais on l'«opinió» és només una capa superficial d'informació fabricada. La confiança es desintegra; la veu del ciutadà, sense cap prova verificable que la recolzi, perd tot valor i es converteix en un murmuri que ningú escolta.

En aquest context, la necessitat d'una **prova de personalitat** —una persona, una veu— es fa imperiosa. No només cal garantir que cada vot o suport a una iniciativa prové d'un individu real; també s'ha d'evitar que aquesta garantia depengui d'una base biomètrica centralitzada, que podria convertir-se en un instrument de vigilància massiva. La solució ha d'estar basada en la **prova d'existència** i la **prova de vida al dispositiu**, com es descriu al capítol 13: una signatura digital que combina un vídeo-selfie amb verificació biomètrica realitzada íntegrament dins del propi telèfon, sense que cap entitat externa tingui accés o emmagatzemi les dades biològiques[7].

A diferència de sistemes com Worldcoin, que escaneja l'iris per «provar que ets humà» i ha estat objecte de prohibicions i multes en més de nou jurisdiccions, incloent la declaració d'inconstitucionalitat a Kenya i la destrucció obligada de les dades recollides a Colòmbia[4], aquesta aproximació descentralitzada garanteix que la prova de personalitat sigui **neutral** i **no centralitzada**, evitant que cap empresa o govern pugui utilitzar-la com a punt d'entrada per a la vigilància.

Així doncs, el repte que planteja Noveck —escala, acció i institucionalització de la participació digital— es pot abordar només si superem l'obstacle fonamental del **soroll indistinguible**. Només amb una prova de personalitat verificable, sense dependre d'una infraestructura biomètrica centralitzada, podrem transformar la participació digital d'un simulacre a una força real que decideixi i no només que cridi. Aquest és el primer pas cap a una democràcia en què cada ciutadà tingui una veu autèntica, reconeguda i respectada.

Els dos fracassos de la participació

En els últims anys, les plataformes digitals han convertit el vot ciutadà en un espectacle: enquestes massives que recullen milers de veus però mai arriben a transformar cap decisió política. Aquest fenomen, que Noveck descriu com «participació sense integració», esdevé un teatre on la democràcia actua només com a escenari d'una representació buida [6]. Les consultes obertes, les peticions en línia i els referèndums digitals són sovint recollits per entitats que no disposen de cap mecanisme per canalitzar aquests inputs cap al poder legislatiu o executiu. El resultat és una acumulació de soroll que es difumina entre la multitud i desapareix sense deixar empremta ni impacte real.

A aquest primer fracàs s'afegeix un altre, més insidiós: l'escalada d'identitats falses i bots que ofeguen el debat. Un informe de la FCC indica que, de més de 22 milions de comentaris enviats a través de les xarxes neutres, uns 18 milions eren falsos [1]; la Fiscalia General de Nova York confirma que 9,3 milions d'aquests missatges provenien d'identitats fictícies controlades per un sol xicot de 19 anys amb programari automatitzat i una xarxa de gairebé 500.000 adreces russes [1]. Com hem vist, aquesta inundació de falsedats distorsiona la percepció del consens ciutadà i desincentiva la participació autèntica: els usuaris

reals es veuen obligats a lluitar contra una marea d'informació enganyosa i, finalment, abandonen el procés.

El perill no resideix només en l'abundància de soroll; és la manca de confiança que aquesta pràctica genera. Un estudi citat per Noveck indica que el 51 % dels europeus enquestats estarien disposats a substituir alguns polítics per intel·ligència artificial, una xifra que denuncia un profund esgotament de la fe en les institucions democràtiques [8]. Aquesta estadística no és només un baròmetre d'insatisfacció; és una senyal clara que el model actual de participació digital ha perdut legitimitat. Més soroll, més plataformes obertes i més consultes sense conseqüències només empitjoren la percepció que les veus individuals són irrellevants.

Per sortir d'aquest bucle cal redefinir dos requisits bàsics. En primer lloc, la participació ha de decidir: els inputs ciutadans han d'estar connectats directament a processos de decisió real, com demostra el portal e-Cidadania del Senat brasiler, on una «Idea Legislativa» que arribi a 20.000 suports passa a ser examinada per la Comissió de Drets Humans i pot convertir-se en llei —exemple recent és la «Llei Joca», aprovada l'abril de 2025 després d'un moviment popular massiu [2]. En segon lloc, aquesta decisió ha de provenir exclusivament de persones reals. La prova de personalitat verificada per t2p ofereix una solució: un certificat que combina vídeo-selfie i verificació biomètrica al dispositiu sense que cap tercera part emmagatzemi les dades [7]. A diferència del model centralitzat d'iris de Worldcoin, prohibit i multat en nou jurisdiccions per vulnerar la privacitat [4], aquesta prova manté la integritat de la identitat a escala local, evitant el control massiu i garantint que cada veu sigui autèntica.

En resum, el fracàs actual de la participació digital es deu tant al fet que no decideix com al fet que s'enfonsa en una massa d'identitats artificials. La solució passa per dos pilars imprescindibles: una connexió directa amb les estructures de poder i una verificació descentralitzada que asseguri que cada contribució prové d'una persona real. Només així podrem transformar el soroll indistinguible en una força democràtica capaç de decidir, i no només de cridar.

Participació que decideix

En el Senat brasiler, el portal e-Cidadania ha transformat la veu del ciutadà en una obligació parlamentària sempre que una proposta arriba a un llindar de vint mil suports [2]. Això no és només una petita mostra d'interès: el cas conegut com «Llei Joca», nascut d'una denúncia popular sobre un gos mort per error d'una aerolínia, —com hem vist— es va convertir en llei a l'abril de 2025 [2]. Avui el sistema registra més de cent vint mil idees legislatives i desenes de milions de suports, convertint la massa de comentaris digitals en una força normativa concreta.

A Taiwan, el model vTaiwan combina deliberació oberta amb decisions vinculants. Les «tecnologies plurals» descrites per Tang i Weyl connecten els debats ciutadans amb les institucions, de manera que les propostes recolzades superant un llindar preestablert passen a ser considerades oficialment per l'executiu [3]. No es tracta només d'una plataforma on la gent comenta; és una infraestructura que tradueix el consens digital en acció legislativa real.

Aquests dos exemples il·lustren una regla fonamental: la tecnologia només pot potenciar la democràcia quan hi ha un marc institucional clar i un compromís ferm de resposta. Sense aquest marc, fins i tot les eines més sofisticades es converteixen en simples escenaris d'entreteniment, on les veus no tenen cap pes real. El perill és que, a mesura que la participació digital s'expandeix, el soroll generat per identitats falses i bots amenaça de desvirtuar aquest procés.

Les dades recents mostren com aquesta vulnerabilitat es materialitza: **com hem vist**, més del 80 % dels comentaris d'aquella consulta de la FCC van resultar falsos o manipulats [1]. Quan una iniciativa depèn d'un nombre mínim de suports per avançar, l'efecte de les identitats artificials es tradueix directament en decisions polítiques. Un grup organitzat pot crear milers de comptes ficticis, inflar artificialment el suport a una proposta i, sense una verificació fiable, fer que els legisladors prenguin mesures basades en un consens inventat.

Aquesta fragilitat és la porta d'entrada per al següent pas: garantir que cada suport prové d'una persona real i present. La prova d'existència de **t2p** ofereix exactament això—una signatura vinculada a un vídeo-selfie i una verificació biomètrica realitzada exclusivament al dispositiu, sense que cap entitat externa accedeixi a la informació [7]. A diferència del model centralitzat d'iris de **Worldcoin**, prohibit i multat en diverses jurisdiccions per vulnerar la privacitat [4], el mecanisme descentralitzat de **t2p** manté la identitat segura i invisible per a tercers.

Així, mentre Brasil i Taiwan demostren com la tecnologia pot canalitzar la participació cap a resultats tangibles, la seva efectivitat depèn d'un component essencial: una verificació fiable que impedeixi que els bots substitueixin les veus autèntiques. Només amb aquesta capa de confiança podrem transformar el soroll digital en una força democràtica capaç de decidir realment, i no simplement de cridar.

Una persona, una veu, sense vigilància

En un cafè de São Paulo, a la vora d'una pantalla que mostrava en temps real les signatures digitals del portal e-Cidadania, una jove activista anomenada Lúcia observava com el nombre de suports per la «Llei Joca» superava els 20.000 i, d'un cop, es convertia en proposta legislativa. El moment era electrificant: un ciutadà havia aconseguit transformar una petita queixa en una iniciativa nacional només perquè el seu vot, el seu suport, estava vinculat a una identitat verificable i única. Però aquest èxit no seria possible sense una capa fonamental de confiança que garanteixi que darrere cada signatura hi ha una persona real i present, i no un bot o una identitat falsa.

La crisi actual de la participació digital es manifesta en dues dimensions. D'una banda, molts espais en línia són merament escenaris on les veus s'alcen sense cap capacitat d'influir: un «teatre» de comentaris que mai arriben a les decisions polítiques [6]. De l'altra, la proliferació d'identitats falses i bots ha inundat les plataformes amb suports artificials; com hem vist, la FCC va constatar que gairebé tots els comentaris rebuts en una consulta pública del 2017 eren falsos [1]. Aquest doble problema paralitza la democràcia digital i alimenta la desconfiança ciutadana.

Una solució aparent ha estat el projecte Worldcoin, que pretén demostrar que un usuari és humà escanejant l'iris i centralitzant aquesta biometria en una cadena de blocs. Com hem vist, aquest model s'ha revelat perillós: entre 2024 i 2025 va ser prohibit i multat en més de nou jurisdiccions; el Kenya el va declarar inconstitucional i n'hi va ordenar la destrucció total de les dades recollides [4]. La centralització d'una característica tan sensible com l'iris genera un malson de vigilància, on una entitat —pública o privada— controla informació biològica que podria ser explotada per fins autoritaris o comercials.

La via neutral ofereix la prova d'existència i de vida desenvolupada per t2p. Aquesta tecnologia combina un vídeo-selfie amb verificació biomètrica completament al dispositiu, sense que cap tercer vegi ni emmagatzemi la imatge o les dades biomètriques [7]. Quan l'usuari captura el seu rostre i veu, es genera una signatura criptogràfica única que vincula l'acte (vot, comentari, suport) a una persona present. La prova no depèn de cap base de dades centralitzada; la confiança resideix en la integritat del dispositiu mateix, garantint que la identitat és autèntica però sense revelar-la.

A més, les «APIs personals» proposades per Noveck permeten al ciutadà controlar la seva pròpia identitat i dades en línia [5]. En lloc de ser producte d'una plataforma, l'individu es converteix en gestor del seu perfil digital, decidint quina informació compartir i amb qui. Aquesta arquitectura reforça la distinció crucial entre prova de personalitat –el fet de ser una persona única– i identificació –qui ets exactament–. La primera assegura que només persones reals poden participar; la segona es manté reservada i no és necessària per a l'actuació cívica.

Com hem vist, la prova d'existència amb vida al dispositiu ofereix una resposta directa al problema de les veus falses sense crear un centre de vigilància. És la mateixa neutralitat que ha sostingut l'èxit de plataformes com e-Cidadania o vTaiwan: cap tercer controla la clau de la confiança, i cada vot es converteix en una declaració autèntica d'una sola veu humana. Aquesta arquitectura és el fonament sobre el qual podem transformar el soroll digital en decisió real i democràtica.

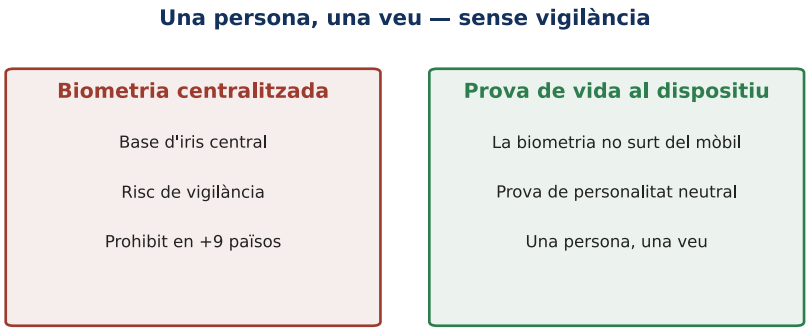


Figura 108.1 — La prova de personalitat es pot fer al dispositiu, sense bases biomètriques centralitzades: una persona, una veu, sense vigilància.

La promesa i el perill

Imaginem una jornada electoral digital on cada vot es registra amb la mateixa seguretat d'una empremta física, però sense que cap entitat pugui accedir a les dades biomètriques que l'han generat. Aquesta és la visió que ofereix la prova de personalitat neutral de **t2p**: una signatura digital basada en un vídeo-selfie i una verificació biomètrica completament **en el dispositiu**, que vincula cada acte a una persona real i present sense que cap tercer no vegi ni guardi aquella informació sensible [7]. En teoria, aquest mecanisme pot transformar el soroll de milers d'identitats fictícies en decisions autèntiques, convertint la participació massiva en un veritable exercici democràtic. La promesa és clara: una única veu humana per cada vot, sense l'esclat de bots ni la manipulació de perfils falsos que ha paralitzat les iniciatives digitals d'última dècada.

No obstant això, el camí cap a aquesta confiança plena està ple de riscos que no podem ignorar. Primerament, qualsevol sistema de prova de personalitat corre el perill de convertir-se en una **arquitectura de vigilància** si la biometria se centralitza. L'exemple de Worldcoin il·lustra aquest escenari: la proposta d'escanejar l'iris per demostrar que un usuari és humà ha estat prohibida, multada o obligada a esborrar dades en més de nou jurisdiccions, i tant Kenya com Colòmbia han declarat inconstitucional el seu model per la seva dependència d'una base d'iris centralitzada [4]. Aquesta experiència demostra que una idea ben intencionada pot convertir-se en un instrument de control massiu quan les dades biomètriques es converteixen en actius gestionats per entitats externes. La línia vermella, per tant, és clara: **mai** bases biomètriques centralitzades.

En segon lloc, la prova de personalitat només és emancipadora si s'integra al poder institucional. Noveck recorda que la participació digital es troba atrapada en tres reptes recurrents —escala, acció i institucionalització—; sense una connexió efectiva amb les estructures de decisió, el resultat continua sent un **teatre** on els ciutadans parlen però no decideixen [6]. Les experiències exitoses de Brasil (e-Cidadania) i Taiwan (vTaiwan/Pol.is) mostren que la clau és una arquitectura neutral on cap tercer controla les claus de confiança, permetent que cada vot es converteixi en una declaració autèntica d'una sola veu humana [2] [3]. Però aquesta integració requereix un marc regulador que garanteixi que les signatures digitals siguin reconegudes i valorades per les institucions legislatives.

Finalment, la qüestió de **qui controla la cadena** on es registren aquestes proves és fonamental. Si la infraestructura subjacent fos gestionada per entitats privades o per estats amb interessos polítics, el potencial emancipador podria ser usurpat com a instrument d'hegemonia digital. El capítol 112 detalla les limitacions del model de Worldcoin i la necessitat d'una governança oberta i democràtica sobre qualsevol cadena que emmagatzemi proves de personalitat.

En conclusió, la prova de personalitat neutral ofereix una oportunitat única per a una participació ciutadana autèntica —una persona, una veu— però només si es manté **descentralitzada**, s'integra al poder real i està sotmesa a una governança transparent. Sense aquestes garanties, el risc és que la tecnologia, en comptes d'alliberar, es converteixi en una nova capa de vigilància que domestiqui la democràcia que pretén reforçar. La decisió final recau en nosaltres: dissenyar i defensar un sistema on la confiança sigui **neutral**, no una moneda per al control.

És hora d'actuar

Els parlaments i ajuntaments han d'abandonar les consultes que només recullen veus sense poder decidir. Cal establir llindars obligatoris, com el model del portal e-Cidadania del Senat brasiler, on una iniciativa que arribi a 20.000 suports passa a la Comissió de Drets Humans i es converteix en projecte de llei [2]. De manera similar, Taiwan ha integrat les tecnologies plurals de vTaiwan/Pol.is per transformar cada aportació ciutadana en un pas concret cap a l'acció legislativa [3]. L'adopció d'aquests marcs hauria d'anar acompanyada d'una prova de personalitat al dispositiu: una signatura amb vídeo-selfie i verificació biomètrica que es realitza íntegrament dins del telèfon, sense que cap entitat externa accedeixi ni emmagatzemi la dada biomètrica [7]. Aquest mecanisme elimina els bots i les identitats falses detectades a la consulta de la FCC del 2017, on 9,3 milions de comentaris eren ficticis —incloent un sol jove de 19 anys — i prop de mig milió provenien de Rússia [1].

Els dissenyadors cívics han de reconèixer que la prova de personalitat no és sinònim d'identificació. L'objectiu és garantir que cada vot o proposta prové d'una persona real i present, però sense crear una base centralitzada d'informació biomètrica com la que va intentar imposar Worldcoin amb l'escaneig d'iris —un projecte prohibit i multat en nou jurisdiccions per vulnerar drets fonamentals [4]. La lliçó és clara: les solucions han de ser descentralitzades, mínimes i totalment controlades pel dispositiu de l'usuari. Qualsevol arquitectura que requereixi repositoris biomètrics centrals ha d'estar prohibida per la normativa, tal com preveu el marc regulador europeu sobre dades sensibles.

La ciutadania ha d'exigir una participació que decideixi i eines que li permetin ser participant, no producte. Les «APIs personals» proposades per Noveck ofereixen un panell de control on cada individu gestiona la seva pròpia identitat digital sense cedir-la a tercers [5]; així la veu ciutadana es converteix en una força real d'influència i trenca el cercle viciat de «participació sense integració» que reduïa la democràcia a un simulacre [6].

Finalment, els reguladors han de protegir la prova de personalitat descentralitzada i vetar qualsevol forma de repositori biomètric central. Això implica legislar contra l'emmagatzematge massiu d'iris o empremtes fora del dispositiu i establir sancions per a les empreses que intentin crear «capes de vigilància» sota la capa de confiança. La normativa ha d'estar alineada amb el principi de neutralitat: la tecnologia ha de ser un instrument que reforça la confiança, no una moneda per al control.

En resum, una democràcia que escolta persones —sense haver de vigilar-les— pot transformar la participació digital en autèntica acció cívica adoptant llindars decisoris, implementant proves de personalitat al dispositiu i garantint marcs reguladors estrictes. És el moment d'aplicar aquestes mesures concretes: **time2act**.

---

[1] Fiscalia General de l'Estat de Nova 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] Senat Federal del Brasil — *Portal e-Cidadania / Llei Joca* (2024-2025) https://www12.senado.leg.br/ecidadania/ ; i *Reboot* (Noveck, 2026), cap. 7. ↩

[3] Audrey Tang i E. Glen Weyl — *Plurality: The Future of Collaborative Technology and Democracy* (2024) ; i *Reboot* (2026), cap. 7. ↩

[4] Biometric Update / ICLG — *Worldcoin/World ID: prohibicions i ordres de supressió (Kenya inconstitucional; Colòmbia)* (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 personals). ↩

[6] Beth Simone Noveck — *Reboot* (2026), cap. 7 (escala, acció, institucionalització; «participation without integration»). ↩

[7] time2act — capítol 13 (t2p: signatura amb vídeo-selfie i prova de vida al dispositiu) ; T2P-Manual (v1.0, 2026). ↩

[8] Beth Simone Noveck — *Reboot* (2026), cap. 3 (enquesta Univ. de Madrid: 51% substituirien polítics per IA). ↩

Manifestacions: la prova simètrica al carrer

«La injustícia en qualsevol lloc és una amenaça per a la justícia a tot arreu.»

— Martin Luther King Jr., «Carta des de la presó de Birmingham» (1963)

Minneapolis, 25 de maig de 2020. Al vespre, davant d'una botiga de barri, una noia de disset anys que passava per allà aixeca el telèfon i grava. Es diu Darnella Frazier, i el seu vídeo contradiu la versió inicial dels fets i esdevé prova central al judici contra l'agent Derek Chauvin per l'assassinat de George Floyd [2]. L'11 de juny de 2021, el jurat del Premi Pulitzer li concedeix una menció especial per «informar amb coratge de l'assassinat de George Floyd, un vídeo que va esperonar protestes contra la brutalitat policial arreu del món, subratllant el paper crucial de la ciutadania en la cerca de la veritat i la justícia per part dels periodistes» [1]. Una adolescent amb un telèfon va canviar la història perquè el seu vídeo va ser cregut. I aquesta és exactament la pregunta que vertebra aquest capítol: en l'era del deepfake, què passarà el dia que un vídeo així es pugui despatxar amb dues paraules — «és fals»?

Aquest capítol tracta el dret de manifestació i l'ordre públic: la documentació del carrer, en les dues direccions. La prova en conflictes armats i drets humans és al capítol 20; el fotoperiodisme, al capítol 17; les eleccions i el «dividend del mentider», al capítol 106; la participació cívica, al capítol 108. La pregunta clau: com es reconstrueix una càrrega policial, un aldarull o una detenció sense que guanyi, simplement, la versió del més fort? La resposta d'aquest llibre és simètrica per construcció: evidència ancorada en captura per totes dues parts — **t2p**: l'empremta SHA-512 calculada al dispositiu mentre es grava, l'ancoratge de l'empremta a la blockchain pública i el segell de temps RFC 3161/eIDAS complementari dins d'un contenidor .asice [14]. Ni el manifestant ni l'agent no poden reescriure el que va quedar segellat. La prova no té bàndol: aquesta és la seva força democràtica.

El vídeo contra l'atestat

El cas espanyol que ho condensa va passar arran d'una protesta del moviment «Rodea el Congreso», a Madrid. Tres agents antidisturbis van acusar una manifestant d'haver-los clavat puntades i cops de puny; l'atestat inicial, però, només recollia insults, i les acusacions van anar creixent durant la instrucció i el judici — fins que van aparèixer els vídeos, que no mostraven cap agressió. La frase de la crònica judicial ho diu tot: «Ella no está condenada porque había un vídeo» [3]. L'epíleg és incòmode: els agents que l'havien acusada van acabar absolts — el tribunal va reconèixer que no hi havia proves de les agressions que ells afirmaven amb rotunditat, però no hi va veure delicte [4]. Sense el vídeo, una condemna probable per a ella. Amb el vídeo, cap conseqüència per a ningú.

Convé entendre el terreny processal, sense èpica. L'atestat policial no és una sentència anticipada: si els agents que el van redactar no el ratifiquen al judici, sota publicitat i contradicció, no té eficàcia probatòria per si sol [5]. Però a la pràctica la paraula de l'agent pesa, i en l'àmbit administratiu — el de les multes — la presumpció de veracitat de l'autoritat deixa el ciutadà gairebé indefens si no disposa d'imatges. Aquell dia, el vídeo va anivellar el camp. Per pura casualitat: algú gravava.

La lliçó del cas no és contra ningú; és contra la casualitat. La veritat d'una plaça no pot dependre que algú tingués el mòbil a la mà, ni que el fitxer sobrevisqui, ni que el jutge se'l cregui quan l'altra part insinuï que està editat. I la lliçó simètrica val igual: què protegeix l'agent honest acusat en fals d'una brutalitat que no va cometre? La mateixa resposta: evidència ancorada en el moment de la captura, de sèrie, per a tothom [14].

Gravar la policia: un dret amb multa

A Espanya, el dret a documentar el carrer ha viscut una dècada de zona grisa. L'article 36.23 de la Llei de Seguretat Ciutadana — la «llei mordassa», de 2015 — sanciona l'ús d'imatges d'agents en intervencions policials; el Tribunal Constitucional en va anul·lar el terme «no autoritzat», tancant la porta a la censura prèvia, i, segons les cròniques, els cossos policials ja no apliquen la infracció en la seva forma original [6]. PSOE i Sumar van pactar el 2024 una reforma perquè el risc per als agents en difondre imatges hagi de ser «constatable» i reflectir-se motivadament [6]. El context més ampli explica la desconfiança: als deu anys de la llei, el març de 2025, se n'havien imposat més de 400.000 multes — del conjunt de la llei, no només d'aquest article — i el tercer intent de reforma continuava en tràmit [7]; Amnistia Internacional en parla com de «deu anys de vulneracions de drets humans i promeses incomplertes» [8].

Gravar la policia en l'exercici de funcions públiques, de bona fe i sense posar ningú en perill, és una garantia democràtica: ho va demostrar Frazier a Minneapolis [1] i ho va demostrar el vídeo de «Rodea el Congreso» a Madrid [3]. Però qui grava s'exposa encara a la incertesa sancionadora, i el material que capta és fràgil: un mòbil confiscat o trencat, un fitxer esborrat, i la prova mor amb ell.

La resposta de t2p és doble. Primer, l'ancoratge en captura: si l'empremta de cada segment s'ancora mentre es grava [14], ni la destrucció del dispositiu no esborra l'existència datada del material — el que es va gravar queda acreditat, encara que calgui recuperar-ne una còpia més tard. Segon, la protecció del gravador: el disseny de només-empremtes no publica res, no identifica ningú i no difon cap imatge; fixa que allò existia, i prou. Documentar deixa de ser un acte de risc amb prova fràgil per ser un acte discret amb prova indestructible.

La càmera corporal: la mirada de l'altre costat

La simetria comença pels cossos policials, i el desplegament ja és un fet. Els Mossos d'Esquadra han estès les càmeres corporals Axon Body 3 al 98 % del territori, amb 800 unitats i 300 més previstes; 5.000 agents han rebut la formació necessària i s'han habilitat hores d'autorització per a 7.000 policies, amb 1.500 més en camí; el reglament d'ús s'està actualitzant, i els sindicats en reclamen la generalització [9] [10]. La Policia Nacional estén gradualment el seu «Dispositiu de Gravació Unipersonal» (model AB3) entre els agents de seguretat ciutadana, i està previst que arribi també a la Guàrdia Civil; l'objectiu declarat és doble: protegir la ciutadania i protegir els agents davant d'acusacions falses [11].

Però el desplegament no resol el punt crític: la custòdia. Qui guarda les imatges? Qui decideix quin fragment es publica, quin «es perd», quin acompanya el comunicat de premsa? Una càmera corporal sense integritat verificable és, en essència, la memòria d'una sola part: pot documentar l'agressió a l'agent, i pot desaparèixer quan documenta l'excés. La confiança que genera depèn, tota, de la confiança en qui la custodia.

Aquí és on la proposta d'aquest llibre completa el que les càmeres han començat: una cadena d'empremtes contínua, ancorada en captura [14]. Cada segment de vídeo se segella en néixer, de manera que qualsevol tall, buit o edició posterior esdevé matemàticament detectable. L'agent honest hi guanya el primer: ningú no podrà dir que el seu vídeo exculpatori és un muntatge. I el ciutadà hi guanya alhora: cap supressió selectiva no passarà desapercebuda, i el comandament que publiqui un fragment haurà d'assumir que el context existeix, està datat i és exigible judicialment. La càmera corporal amb ancoratge deixa de ser la memòria del més fort per ser la memòria de tothom.

«Això és IA»: el dividend del mentider arriba al carrer

L'agost de 2024, Donald Trump va afirmar falsament que la fotografia de la multitud que esperava Kamala Harris a l'aeroport de Detroit era «generada per IA». La foto l'havia feta un membre de l'equip de campanya i no estava manipulada; hi havia unes 15.000 persones, i periodistes d'Associated Press i d'altres mitjans, presents a la mateixa pista, havien documentat la multitud des de tots els angles; els verificadors ho van desmentir en cadena [12][13]. La lliçó és de gel: si una multitud fotografiada per desenes de professionals es pot negar amb dues paraules, què no es podrà negar d'un vídeo incòmode de deu segons gravat per un manifestant anònim — o per una càmera corporal?

El «dividend del mentider» — el concepte que vam introduir al capítol 106: la capacitat de despatxar com a falsa la prova autèntica però incòmoda — talla en dues direccions quan arriba al carrer. En una, el poder pot negar el vídeo real d'un excés policial: «muntatge», «IA», «descontextualitzat». En l'altra, un grup violent pot negar el vídeo real dels seus aldarulls — o, pitjor, fabricar-ne un de fals per criminalitzar una protesta pacífica, amb les mateixes eines de síntesi que ja hem vist aplicades a veus i imatges en capítols anteriors.

En tots dos escenaris, la sortida estructural és la mateixa: que el material autèntic porti data i empremta ancorades des del primer segon [14], i que el material sense ancoratge valgui cada dia menys davant d'un tribunal i davant de l'opinió pública. La veritat del carrer no es pot defensar a crits; es defensa amb matemàtica.

La prova d'existència aplicada

Una plaça plena, i dos rellotges que graven: el mòbil d'una manifestant i la càmera corporal d'un agent. Cap dels dos relats no podrà ser reescrit.

1. El manifestant que documenta

Una manifestant grava una intervenció policial. Mentre grava, el dispositiu calcula per segments l'empremta SHA-512 i l'ancora amb el segell de temps RFC 3161/eIDAS [14]. No publica res: l'ancoratge no revela ni contingut ni identitat. Si el mòbil es perd, es trenca o li és confiscat, l'existència i la data del material queden acreditades. Si l'acusen d'haver agredit algú — com a «Rodea el Congreso» [3][4] —, el vídeo íntegre apareix amb una autenticitat que cap impugnació genèrica no pot tombar. Si algú crida «això és IA» [12], l'empremta anterior al desmentit el desmenteix. I si l'agressió la va cometre ella, el mateix segell servirà l'acusació: la prova no té bàndol.

2. L'agent amb la càmera ancorada

La càmera corporal de l'agent [9][11] genera una cadena contínua d'empremtes: cada segment, segellat en captura [14]. Davant d'una queixa falsa per brutalitat, el seu vídeo és inatacable. Davant d'una sospita de supressió selectiva, la cadena mostra si hi ha buits, i els auditors — interns, judicials o parlamentaris — poden inspeccionar la seqüència sencera. El cos policial que publica un fragment ho fa sabent que el context és datat i exigible. La transparència deixa de dependre de la bona voluntat del moment.

3. L'observador i el periodista

Els observadors de drets humans i els fotoperiodistes que cobreixen la manifestació (capítols 17 i 20) treballen amb equips que segellen en captura: el seu material esdevé un paquet probatori amb cadena de custòdia des del carrer fins a la sala de vistes [14]. I poden fer-ho sense exposar les seves fonts: primer l'empremta; la publicació, només si cal i quan sigui segur — el mateix model d'evidència verificable que el llibre ha mostrat per als conflictes armats al capítol 20.

4. La reconstrucció simètrica

El jutjat rep els dos corrents ancorats — mòbils ciutadans i càmeres corporals — i, en lloc de paraula contra paraula, obté una línia de temps fusionada i verificable: què va passar primer, qui va respondre què, amb quina proporcionalitat. L'atestat, que per si sol necessita ratificació [5], arriba acompanyat de material la data i la integritat del qual no admeten discussió. Les instruccions s'escurcen; les sentències s'assenten sobre fets.

Els límits, dits amb la mateixa claredat: el segell no atorga cap dret a gravar-ho tot en tota circumstància — la reforma de la llei de seguretat ciutadana continua pendent [6][7], i la intimitat de tercers compta; no valora la proporcionalitat d'una càrrega ni la legalitat d'una detenció, que corresponen al jutge; no substitueix testimonis ni pericials; i un clip autèntic pot continuar sent enganyós si es retalla el context. L'ancoratge acredita existència i integritat; no acredita completesa.

La promesa i el perill

La promesa: que mai més la veritat d'una plaça no depengui de la casualitat que algú gravés [1][3], ni de la custòdia unilateral d'unes imatges [9], ni de la credulitat davant del «això és IA» [12]. Evidència simètrica, ancorada i neutral: la infraestructura probatòria d'una democràcia que es manifesta. Els perills, però, són seriosos, i cal mirar-los de cara.

El primer és **la inversió vigilant**. Les eines per documentar el poder no poden acabar identificant els qui protesten. Ancorar un vídeo no ha d'implicar cap registre de qui era a la plaça: el disseny de només-empremtes no revela contingut ni identitat, i el reconeixement facial sobre material de manifestacions és una línia que una democràcia no ha de creuar (vegeu el capítol 108: participació sense vigilància). Cap registre central, cap desanonimització.

El segon és **l'autèntic descontextualitzat**. El segell acredita que un clip existia; no acredita què va passar fora de pla. Un fragment verídic retallat amb malícia és la desinformació més difícil de combatre. Les mitigacions: cadenes contínues en lloc de clips solts, metadades de seqüència i una cultura del context — el segell mai no pot ser un argument d'autoritat total.

El tercer és **el gel sobre el carrer**. Si manifestar-se implica saber-se gravat per totes bandes i per sempre, la por pot buidar les places — el mateix efecte esmorteïdor que les sancions de la llei mordassa

han projectat sobre fotògrafs i activistes durant una dècada [7][8]. Per això la revocabilitat i la caducitat de les empremtes personals, i la publicació sempre voluntària, no són extres tècnics: són condicions democràtiques del sistema.

I el quart és **la coartada tecnològica**. Cap càmera no substitueix la reforma legal pendent [6][7], ni la formació policial, ni els mecanismes independents de rendició de comptes. El segell fa la veritat recuperable; la justícia, l'han de fer les institucions.

És hora d'actuar

La plaça és de tothom, i la seva veritat també ho ha de ser.

Per a manifestants i ciutadania: grava de bona fe quan calgui, segella en captura [14] i no publiquis rostres de tercers sense necessitat; coneix el marc legal vigent [6] i recorda que l'empremta et protegeix encara que no publiquis mai res.

Per als cossos policials: desplegueu les càmeres corporals amb cadena d'empremtes ancorada [9][11] [14] i publiqueu les polítiques de custòdia i conservació. L'agent honest és el primer beneficiari d'una prova que ningú no pot posar en dubte.

Per a jutges i fiscals: exigiu integritat ancorada al material d'ambdues parts; una línia de temps verificable val més que cent ratificacions d'atestat [5].

Per als legisladors: culmineu la reforma de l'article 36.23 amb un dret explícit a documentar de bona fe [6][7]; reconeixeu presumpció d'autenticitat a l'evidència segellada en captura; i prohibiu el reconeixement facial massiu sobre material de protestes.

Per als mitjans i els observadors de drets humans: incorporeu el segell en captura als vostres equips de sèrie (capítols 17 i 20), verifiqueu l'ancoratge abans de publicar material de tercers i tracteu el material sense empremta amb la cautela que mereix [12][13].

Darnella Frazier tenia disset anys i un telèfon, i el món la va creure [1][2]. La pròxima Darnella potser no serà creguda — llevat que el seu vídeo porti una data que cap poderós no pugui esborrar. Perquè la plaça continuï dient la veritat, **time2act**.

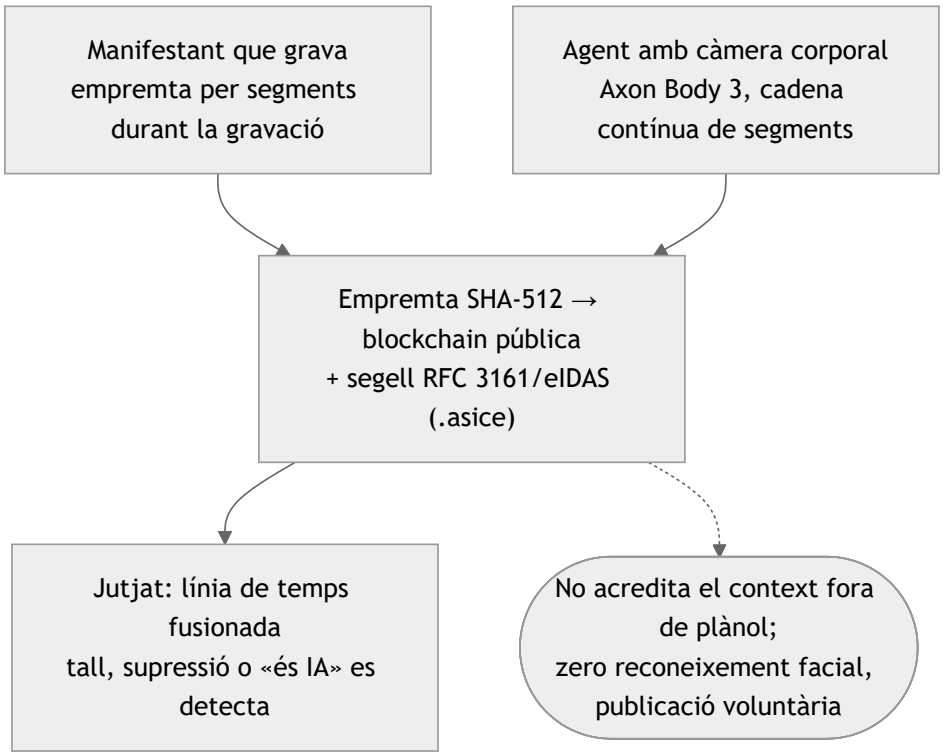


Figura 109.1 — La prova simètrica al carrer: el vídeo del manifestant i la càmera corporal de l'agent se segellen en captura, per segments (empremta SHA-512 al dispositiu, segell de temps RFC 3161/eIDAS, ancoratge a la blockchain pública, .asice), sense publicar res ni identificar ningú. Al jutjat, les dues cadenes es fusionen en una línia de temps verificable; qualsevol tall o

supressió es detecta. Límits: el segell no acredita el context fora de pla, no valora la proporcionalitat i exigeix revocabilitat, publicació voluntària i zero reconeixement facial. Fonts: 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 juny de 2021; menció especial; citació literal del jurat). 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 anys en gravar; el vídeo com a prova al judici 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»* (cas «Rodea el Congreso»; l'atestat inicial només recollia insults). 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'* (absolució; el tribunal no veu delicte tot i l'absència de proves de l'agressió). 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 l'eficàcia probatòria de l'atestat). 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 juliol de 2024; art. 36.23; el TC anul·la el terme «no autoritzat»; reforma pactada: risc «constatable» i motivat). 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 març de 2025; multes del conjunt de la llei). 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] Amnistia Internacional Espanya — *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 territori amb 800 càmeres; 5.000 agents formats; autorització per a 7.000 i 1.500 més; reglament en actualització). 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 càmeres més previstes; peticions de generalització). 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 model AB3; extensió gradual; previst per a la Guàrdia Civil; objectiu: protegir ciutadania i agents). 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* (agost de 2024; foto d'un membre de l'equip, sense manipular; periodistes d'AP a la pista; 15.000 assistents). 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* (verificació). https://www.univision.com/noticias/fotografias-eventos-campana-kamala-harris-no-ia-como-afirman-trump-y-redes ↩

[14] t2p — manual de producte (empremta SHA-512 al dispositiu, per segments durant la gravació; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; cadena d'empremtes contínua per a càmeres corporals; publicació opcional). Vegeu els capítols 13 i 15. ↩

Clavar els talons: el cost de no fer res

«Odio els indiferents. Crec que viure vol dir prendre partit. [...] La indiferència és el pes mort de la història.»

— Antonio Gramsci, «Indifferenti», La città futura (1917)

El 2050, a la primera tarda d'un juliol que sembla no acabar-se mai, el sol s'alça com un disc incandescent sobre una plana deshabitada al sud del Sahel. Les dunes, ara recobertes per capes de pols fina que reflecteixen la llum en tons de gris metàl·lic, són l'únic rastre visible d'una civilització que va decidir clavar els talons davant el canvi climàtic. A la frontera entre el que queda de Mali i el que abans era una ciutat costanera, un grup de refugiats —homes i dones amb les seves possessions més precioses embolcallades en draps desgastats— es reuneix al voltant d'un pou de sorra que encara conserva aigua. No és només aigua; és l'últim recurs que pot salvar-los d'una mort segura per deshidratació. En aquest món, les asseguradores fa temps que es van retirar de regions que abans consideraven de «risc moderat», i la cobertura davant els desastres climàtics s'ha convertit en un luxe inabastable per a la majoria.

Aquesta escena no és una predicció: és un dels futurs que encara podem escollir o evitar. I el que la fa esfereïdora és que el 2026 ja sabíem prou per impedir-la. Els informes de l'IPCC mostraven que mantenir l'escalfament global per sota dels 2 °C requeriria una transició energètica decidida i inversions de l'1-2 % del PIB mundial[3]. Però les polítiques de la dècada anterior no van aplicar aquestes mesures, i van deixar que les emissions continuessin el seu camí ascendent. En aquell futur, l'escalfament ha superat els 3 °C respecte al nivell preindustrial, tal com advertien les projeccions per a les polítiques vigents[1]. A aquest nivell, els models econòmics indiquen que el PIB per càpita mundial podria caure més del 50 % cap a l'any 2100 si arribem a 2 °C per sobre del nivell actual[1]; i a 3 °C, la producció acumulada disminueix entre un 15 % i un 34 % respecte al que s'esperava[1].

Els efectes es deixen sentir a cada racó del planeta. Les onades de calor s'allarguen durant setmanes, tensen els sistemes sanitaris i en disparen la despesa quan s'hi sumen les malalties relacionades amb l'exposició prolongada a la calor i la desnutrició. El cost net de la inacció arriba a representar entre un 11 % i un 27 % del producte acumulat mundial —tres vegades la despesa sanitària global projectada fins al 2100 —, una càrrega que cap economia no pot suportar sense conseqüències[2]. I els punts d'inflexió del sistema climàtic, un cop traspassats, poden costar fins a 2,4 bilions d'euros l'any[2]. Les migracions massives s'han convertit en una realitat quotidiana; ciutats costaneres senceres es troben inundades i abandonades.

Així, aquell 2050 no és només un any més avançat en la cronologia; és el reflex d'una decisió col·lectiva que hauria preferit la comoditat de la inacció a l'energia de la transformació. El preu de la procrastinació es mesura en vides perdudes, economies desintegrades i una confiança global erosionada —un doble perill, climàtic i de credibilitat, que s'alimenta mútuament. La pregunta que queda pendent, i que ressona entre les dunes i les ciutats abandonades, és simple però profunda: quina quantitat de futur estem disposats a sacrificar per mantenir-nos quiets?

Cap a on anem

Els números no menten: les polítiques vigents ens arrosseguen cap a un escenari de **més de 3 °C d'escalfament global**, i això ja és una realitat documentada [1]. La distància entre les promeses que es fan a les cimeres de les COP i la realitat del terreny, descrita al capítol 6, no és només un tema de diplomàcia; es paga en graus. Cada dècim perdut representa vides que s'esvaeixen, sectors econòmics que col·lapsen i una confiança global que es trenca com el vidre sota pressió.

Com hem vist, les projeccions indiquen una caiguda del PIB per càpita superior al 50 % i pèrdues entre el 15 % i el 34 % de la producció mundial fins al 2100, amb costos que podrien arribar fins a **2,4 bilions d'euros anuals** [2]; aquestes xifres reflecteixen una economia que s'esfondra davant fenòmens climàtics cada cop més intensos —sequeres prolongades, inundacions devastadores i incendis forestals que arrasen infraestructures clau.

En contraposició, la inversió necessària per limitar l'escalfament per sota dels 2 °C és sorprenentment modesta: **entre l'1 % i el 2 % del PIB mundial** [3]. Aquesta xifra representa només una fracció del que costaria mantenir-nos en l'estat de passivitat actual, sense comptar les oportunitats perdudes d'un creixement sostenible basat en tecnologies netes. Per tant, assumir que actuar implica costos prohibitius és un error econòmic i moral; el veritable cost és l'abstenció.

A més, el doble perill —climàtic i de confiança— es retroalimenta. Cada grau addicional empitjora les condicions ambientals i alimenta la desconfiança en les institucions i els processos democràtics, ja que la població percep una incapacitat d'actuar davant la crisi. Aquesta erosió de credibilitat redueix la capacitat col·lectiva per mobilitzar recursos i suport polític necessari per a mesures ambicioses, generant un cercle viciós cada cop més difícil d'escapar.

Com hem vist, les polítiques actuals ens porten directament cap a una temperatura que supera els 3 °C, traduint-se en pèrdues econòmiques massives i un augment de la despesa sanitària. La inversió per frenar aquest camí és relativament petita comparada amb el cost de no fer res; ara cal trencar aquesta inèrcia, reconèixer que cada grau perdut és una advertència i actuar immediatament, ja que només així es pot preservar tant el planeta com la confiança en les nostres institucions.

El preu de no fer res

Imagina una escala que mesura el benestar econòmic mundial com un termòmetre: cada grau addicional d'escalfament global retalla el PIB per càpita i la diferència és brutal. Com hem vist, un augment de 2 °C podria reduir aquest indicador més del 50 % cap al final del segle, mentre que superar els 3 °C provocaria una caiguda entre el 15 % i el 34 % de la producció acumulada fins al 2100 [1]. Aquest descens no és només una xifra abstracta; significa que bona part de les persones del planeta veurien reduïda a la meitat la seva capacitat de compra, d'estalvi i d'inversió, i es traduiria en menys recursos per a educació, salut i innovació.

Però el cost econòmic directe no és l'únic factor que pesa sobre aquesta balança. El cost net de la inacció —la diferència entre les despeses addicionals generades pel canvi climàtic i els beneficis d'una política d'adaptació o mitigació— se situa entre l'11 % i el 27 % de la producció acumulada [2]; com hem vist, aquesta franja equival a tres vegades la despesa sanitària global projectada fins al 2100, revelant com les conseqüències del canvi climàtic s'estendran a tots els àmbits de la vida humana: des de l'augment de malalties relacionades amb la calor fins a l'aparició d'epidèmies emergents per la migració de vectors.

A més, hi ha punts d'inflexió que amenacen de trencar el sistema en moments crítics. Les estimacions indiquen que aquests canvis estructurals poden costar fins a 2,4 bilions d'euros l'any [2]. Aquestes xifres no són merament costos addicionals; representen la necessitat urgent d'invertir en infraestructura resilient, tecnologies netes i sistemes de governança capaços de gestionar l'augment dels riscos. Cada any que passa sense una resposta coordinada acumula aquest cost ocult i el converteix en una càrrega cada cop més pesada per a les generacions futures.

En resum, la inacció no és un estat neutre: és una aposta econòmica i social que costa molt més del que qualsevol inversió preventiva podria demanar. Les xifres mostren clarament que el preu de quedar-nos quiets supera de manera significativa el d'actuar ara, tant en termes de pèrdua de benestar material com de deteriorament de la confiança institucional. La clau per evitar aquest escenari desolador és reconèixer que cada grau perdut incrementa els costos i reduir immediatament les emissions per mantenir l'escalfament per sota dels 2 °C, una tasca que suposa només l'1-2 % del PIB mundial [3]. És un compromís assequible comparat amb la factura colossal de la inacció.

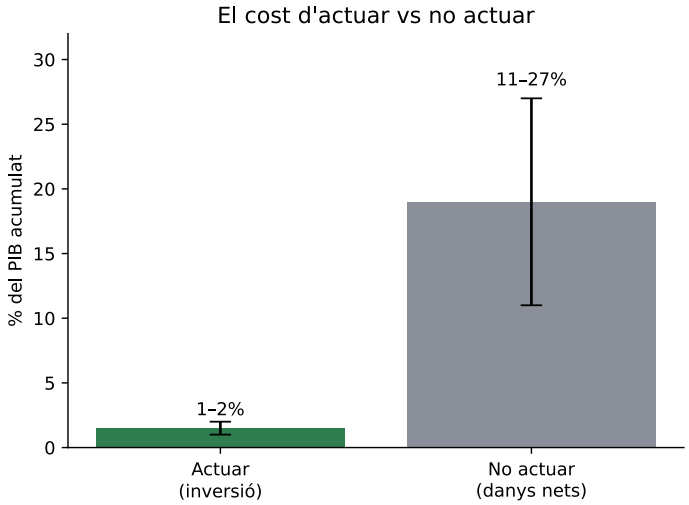


Figura 110.1 — Com més puja la temperatura, més cau l'economia: el cost de no actuar es dispara amb cada dècim de grau.

El risc sistèmic doble

En el cor d'una crisi que es bifurca entre veritat i clima, les dues s'enreden en una espiral de retroalimentació que amplifica cada vulnerabilitat. La incertesa alimentada per *deepfakes* sofisticats, informes de *greenwashing* i narratives manipulades erosiona la confiança institucional i impedeix una governança eficaç de la transició energètica; sense dades fiables, les polítiques climàtiques es converteixen en projectes a l'aire, vulnerables a pressions econòmiques i a desinformació que dilueix el consens científic. Cada retard incrementa els costos climàtics.

A l'inrevés, un escenari més càlid genera una crisi de veritat encara més profunda: fenòmens extrems —inundacions, incendis forestals i sequeres prolongades— produeixen fluxos d'informació caòtica que sovint es tradueixen en notícies sensacionalistes o falsificades per interessos particulars. Quan les comunitats pateixen danys reals, la percepció pública es fragmenta; alguns busquen explicacions científiques i altres adopten narratives conspiratives que minimitzen la responsabilitat humana, dificultant l'aplicació de mesures d'adaptació o mitigació per part dels governs.

Les dades mostren clarament com aquesta doble crisi multiplica el risc global; si les polítiques actuals segueixen la seva trajectòria, l'escalfament mundial superarà els 3 °C i el PIB per càpita caurà dràsticament —com hem vist—. El cost net de la inacció equival a una part important de la producció acumulada global, superant tres vegades la despesa sanitària prevista fins al final del segle, i els punts d'inflexió podrien arribar fins a 2,4 bilions d'euros l'any si no es prenen mesures urgents [1][2].

En contrast, contenir l'escalfament per sota dels 2 °C només requereix una inversió modestíssima —entre l'1 i el 2 % del PIB mundial [3]—, una xifra assequible comparada amb la factura colossal de la inacció. Aquesta disparitat demostra que el veritable perill no resideix tant en les tecnologies o els costos inicials, sinó en l'esclat d'una crisi de confiança que paralitza la resposta col·lectiva; reforçar institucions fiables i sistemes de verificació transparent és tan urgent com qualsevol política climàtica.

Així, el doble risc sistèmic —clima i veritat— no són fenòmens independents, sinó dos costats d'una mateixa moneda. La incapacitat de confiar en les dades impedeix governar la transició; la manca de govern eficaç empitjora el clima, que al seu torn genera més incertesa i desinformació. Trencar aquest cercle viciós és l'objectiu central de *time2act*: demostrar que, amb intel·ligència artificial i cadena de blocs per garantir la integritat de la informació, podem restaurar la confiança i impulsar accions climàtiques decisives abans que els costos esdevinguin insostenibles.

El cost de la mentida, front a front

El cost de no actuar no es mesura només en graus. Hi ha una segona factura, més silenciosa, que ja s'està pagant: la de la confiança que s'esfondra. I, com la climàtica, creix amb cada any de retard. Recorrem-la pels cinc fronts que aquest llibre ha examinat.

A les **finances**, una sola videotrucada falsificada va costar uns 25,6 milions de dòlars a l'enginyeria Arup el 2024 [4]; i la consultora Deloitte projecta que el frau impulsat per la intel·ligència artificial podria arribar als 40.000 milions de dòlars anuals als Estats Units el 2027 [5]. Cada estafa erosiona una mica més la confiança que greixa el comerç.

A la **sanitat**, una imatge mèdica manipulada —un tumor injectat o esborrat— no costa diners: costa diagnòstics encertats, tractaments a temps i, en última instància, vides. A l'**educació**, els títols falsos i l'autoria impossible de verificar deprecien el mèrit de tota una generació. I a la **democràcia i la defensa**, les *deepfakes* electorals i la desinformació de guerra fan miques la base de fets compartida sense la qual cap societat es pot posar d'acord per actuar —ni tan sols sobre el clima.

I aquests cinc fronts només són el principi. Al llarg del llibre, la mateixa factura de la desconfiança ha anat apareixent a cada racó de la vida col·lectiva: al **clima**, on els crèdits de carboni inflats i el greenwashing buiden de sentit cada tona estalviada; a l'**economia real**, des de l'assegurança i la cadena de subministrament fins als immobles, la tokenització d'actius, la propietat intel·lectual i les licitacions públiques; i, en aquest darrer tram, al teixit mateix de la societat: la **identitat** dels qui no tenen document per provar que existeixen, la **integritat electoral** de les actes i l'escrutini, l'**ajuda humanitària** que ha d'arribar a la persona real, els **testaments**, el **comerç internacional**, l'**auditoria** dels comptes, el **frau publicitari**, els **registres de ciberseguretat**, el **patrimoni artístic** i la protecció dels

denunciants que s'hi juguen la llibertat. I encara més enllà, a les noves fronteres: la **ciència**, on una dada fabricada corromp el coneixement; el **cos**, des de les pensions i el dopatge fins a la dada genètica que també és de la teva família; les **màquines**, que decideixen accidents i guarden la seva pròpia caixa negra; els **mercats** especialitzats de la música, el maquinari i les matèries primeres; i la **justícia mateixa**, on una gravació autèntica es pot negar com a falsa. A cada front, el mecanisme del dany és el mateix —una prova que es pot fabricar o negar— i la defensa també: una prova d'existència que ningú no pugui alterar impunement.

Perquè aquí els dos costos convergeixen. Una societat que no es posa d'acord sobre què és real no es posarà d'acord sobre què cal fer davant els 3 °C. El «dividend del mentider» —la possibilitat de descartar qualsevol prova incòmoda titllant-la de falsa— paralitza l'acció climàtica tant com la desinformació directa. La crisi de la veritat i la crisi del clima no són dues emergències separades; són la mateixa emergència vista des de dos angles, i s'alimenten mútuament [6].

La conclusió torna a ser la mateixa, i per això és tan poderosa: l'assegurança més barata contra totes dues factures és la veritat verificable. Ancorar les dades —climàtiques, financeres, mèdiques, educatives, probatòries— perquè ningú no les pugui alterar impunement no és una despesa tècnica; és la condició prèvia perquè qualsevol altra inversió tingui sentit. Sense una base de fets fiable, fins i tot l'1-2 % del PIB que cal per frenar l'escalfament es gastaria enmig del soroll i la sospita. Amb ella, cada euro compta. El cost de la mentida, com el del carboni, només puja mentre no actuem.

L'aposta racional

Imaginem una sala de reunions plena d'alts càrrecs que observen un gràfic de línies ascendents: cada grau addicional d'escalfament s'acumula com una càrrega invisible sobre les economies del món. En aquell moment, una veu trenca el silenci i, com hem vist, assenyala que només una petita fracció del PIB mundial invertida en la transició podria mantenir l'escalfament per sota dels 2 °C. Aquesta és la promesa de les polítiques climàtiques amb suport científic, i el cost de no actuar és una bomba de rellotge que batega més fort a cada instant.

Les projeccions actuals mostren que les polítiques insuficients ens porten cap a un escenari d'escalfament superior als 3 °C abans de la fi del segle [1]. En aquest context, l'impacte econòmic és devastador: com hem vist, si el planeta arriba a una temperatura de 2 °C per sobre del nivell actual, el producte interior brut per càpita podria caure més del 50 % al 2100, i a 3 °C la producció acumulada mundial es reduiria entre un 15 % i un 34 % [1]. Paral·lelament, el cost net de la inacció s'estima entre l'11 % i el 27 % de la producció acumulada —equivalent a tres vegades la despesa sanitària global fins al 2100— amb punts d'inflexió que podrien arribar a 2,4 bilions d'euros l'any [2].

En contrast, destinar entre l'1 % i el 2 % del PIB a finançar la transició cap a fonts d'energia renovable, millorar l'eficiència energètica i desplegar sistemes que garanteixin la transparència de les dades climàtiques representa una despesa comparativament petita [3]. Aquesta inversió no és un cost addicional, sinó una assegurança econòmica sense precedents: el retorn es mesura en reducció de riscos i preservació del creixement a llarg termini. Cada euro invertit ara evita dècades de pèrdues massives, des d'inundacions que devasten infraestructures fins a crisis sanitàries alimentades per l'augment de les temperatures.

A més, la inversió en intel·ligència artificial i cadena de blocs ofereix una doble capa de protecció. D'una banda, la IA pot optimitzar els processos de generació i distribució d'energia, reduir el consum innecessari i augmentar la resiliència del sistema; d'altra banda, la cadena de blocs assegura que les dades climàtiques siguin verificables i difícils d'alterar, contrarestant l'onada de desinformació i *deepfakes* que minen la confiança pública. Aquesta combinació aspira a crear un ecosistema on la informació fiable alimenti decisions polítiques encertades, trencant el cercle viciós entre incertesa climàtica i pèrdua de credibilitat.

En definitiva, l'aposta racional consisteix a reconèixer que el cost d'actuar és una fracció diminuta del producte mundial, mentre que el preu de la inacció s'estén durant dècades i afecta tots els sectors de la societat. La decisió no és entre pagar o no pagar; és entre invertir en un futur sostenible o deixar que les conseqüències econòmiques i socials ens sobrepassin. Com a ciutadans, empresaris i líders, tenim l'oportunitat —i la responsabilitat— d'aportar aquest 1-2 % del PIB mundial, i assegurar així una economia més robusta i un planeta habitable per a les generacions futures. La pregunta que queda és: estem disposats a fer aquesta petita aposta per garantir el nostre benestar col·lectiu?

La promesa i el perill

A la vora del límit climàtic, les eines que fa uns anys semblaven fantasies de ciència-ficció són ara recursos tangibles i econòmicament viables. Les fonts d'energia renovable —solar fotovoltaica, eòlica marina i hidrogen verd— han abaratit els seus costos de manera espectacular i, en bona part dels mercats, ja són més barates que les fòssils. Així, la transició esdevé tant una necessitat ambiental com una oportunitat per reduir els costos operatius empresarials.

Aquesta nova abundància energètica es veu potenciada per la intel·ligència artificial, capaç d'optimitzar el balanç entre oferta i demanda en temps real, minimitzant pèrdues i maximitzant l'aprofitament dels recursos intermitents. Els algoritmes de predicció meteorològica, cada cop més precisos, s'integren a les xarxes intel·ligents, reduint la necessitat de reserves costoses i augmentant la fiabilitat del subministrament. Paral·lelament, la cadena de blocs ofereix transparència i traçabilitat que contraresta l'opacitat dels mercats energètics tradicionals; els contractes intel·ligents poden automatitzar el pagament d'energia verda i assegurar que cada quilowatt-hora prové realment d'una font neta, minimitzant el risc de *greenwashing*.

Com hem vist, invertir només entre un i dos per cent del PIB mundial permetria mantenir l'escalfament global per sota dels 2 °C, el llindar establert pel pacte de París [3]. Es tracta d'una despesa modesta comparada amb la reducció de pèrdues per desastres climàtics i amb l'increment de productivitat que comporta.

Tanmateix, el perill es presenta com una força invisible però potent: la inèrcia institucional i la resistència cultural al canvi. La desinformació —alimentada per xarxes socials i interessos econòmics— distorsiona les dades reals i fa que el públic percebi les solucions com a costoses o arriscades quan, en realitat, són més barates que el cost de la inacció; **com hem vist** [1].

A més, els costos ocults de la inacció ja es comencen a fer sentir: el cost net estimat de no actuar s'eleva fins a un 11 %-27 % de la producció global acumulada fins al 2100, equival a tres vegades la despesa sanitària mundial d'aquell període i podria arribar a 2,4 bilions d'euros l'any [2]. Aquest impacte no només afecta l'economia; erosiona la confiança social i institucional i genera un cercle viciós on la incertesa alimenta més inacció.

Com hem vist, disposem d'una caixa d'eines tecnològiques ja demostrades com a eficients i econòmiques. El repte no és trobar solucions, sinó superar les barreres psicològiques i polítiques que ens empenyen cap al camí més car: la inacció. Si triem aquest últim, el cost acumulat serà molt superior al de qualsevol inversió responsable avui. La decisió es converteix, per tant, en una qüestió de visió: preferim invertir un petit percentatge del nostre producte interior brut per garantir un futur sostenible i fiable, o deixarem que la inèrcia i la desinformació ens portin a un cost molt més alt i irreversible?

Les dues corbes

Imaginem una sala de control on es projecten dos gràfics simultanis: d'una banda, la corba aparentment ascendent del PIB mundial si les polítiques actuals continuen tal com són; de l'altra, el descens abrupte del producte interior brut quan l'escalfament supera els 3 °C. La primera mostra un creixement aparent, però a llarg termini revela una caiguda de la producció acumulada d'entre el 15 % i el 34 % si arribem a aquest llindar crític [1]; la segona indica que el cost net de la inacció podria absorbir entre l'11 % i el 27 % del producte global, l'equivalent a tres vegades la despesa sanitària mundial fins al 2100, amb punts d'inflexió que arriben a 2,4 bilions d'euros l'any [2] —com hem vist.

En contrast, la inversió necessària per mantenir l'escalfament per sota dels 2 °C se situa entre l'1 % i el 2 % del PIB mundial [3]. Aquesta xifra, comparada amb els percentatges de producció que es perdran si no fem res, és poc més que un ajust de pressupost. És, per tant, una decisió d'escala humana: destinar una petita part del nostre producte interior brut a la transició energètica i a les infraestructures digitals que garanteixin transparència i traçabilitat.

El pla ha de ser tan clar com el mapa d'una ruta marítima. Primer, establir fites intermèdies amb terminis curts i finançar projectes pilot que combinin la intel·ligència artificial per optimitzar l'ús energètic i la cadena de blocs per certificar la procedència neta dels recursos. Segon, crear mecanismes de rendició de comptes basats en contractes intel·ligents: si una empresa supera els objectius establerts, rep incentius; si falla, es deriven conseqüències verificables. Tercer, mobilitzar capital privat mitjançant bons verds i fons d'impacte que siguin auditables en temps real gràcies a la cadena de blocs.

Aquest full de ruta no és una mera llista de mesures —és un contracte col·lectiu entre governs, empreses i ciutadans. Cada acció ha de ser mesurable, verificable i, sobretot, ajustable si els resultats no coincideixen amb les expectatives. La confiança es reconstrueix quan el públic pot veure, en temps real, com s'inverteixen els diners i quin impacte tangible genera. Així, la doble amenaça —climàtica i de confiança— es desactiva simultàniament: una reducció efectiva d'emissions disminueix les pressions ambientals que alimenten la incertesa social, i una infraestructura transparent reforça la credibilitat institucional.

En última instància, el repte és tan polític com tecnològic. Cal que els líders adoptin una visió a llarg termini i reconeguin que el cost d'una inacció prolongada supera de molt les despeses immediates d'un pla de transició. El moment és ara; la ruta està dibuixada i només queda decidir si avancem amb passos ferms o ens quedem atrapats en l'estancament, deixant que la història registri una oportunitat perduda i un futur empobrit.

---

[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] (síntesi de modelització climàtica-econòmica) 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* (cas 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/ ↩

Com hi arribem? Un full de ruta

«Caminant, no hi ha camí: / es fa camí en caminar.»

— Antonio Machado, «Proverbios y cantares», XXIX (1912)

El 2035 la ciutat de Barcelona s'alça com a testimoni viu d'una decisió presa deu anys enrere: el 2026, els governs i les empreses van decidir actuar. Des del primer moment que es va aprovar el marc regulador per a la prova d'existència basada en IA i blockchain, les infraestructures de confiança van començar a proliferar com filaments d'una xarxa neuronal col·lectiva. Avui, al passeig de la Rambla, els turistes no només consulten mapes digitals; escanegen codis QR que, amb un simple gest, verifiquen l'origen i la integritat de cada producte —des del vi de la DO Penedès fins a les peces d'art fabricades per impressió 3D. Cada etiqueta porta una petita cadena de blocs que registra, en temps real, els passos de producció, transport i consum, tot sense consumir gairebé energia: la blockchain moderna, després del Merge, ha reduït el seu cost energètic prop d'un 99,95 % respecte al model anterior, de manera que ancorar la veritat ja no malgasta el planeta [2].

A les façanes dels edificis es projecten dades verificables d'impacte climàtic: gràfics que mostren com els sistemes urbans han optimitzat el consum gràcies a la intel·ligència artificial. Aquestes plataformes intel·ligents ajusten el consum d'electricitat dels edificis en funció de la demanda real i la disponibilitat d'energia renovable, minimitzant els residus i maximitzant l'eficiència. La inversió necessària per a aquest canvi es va estimar entre l'1 i el 2 % del PIB mundial —una xifra que molts crítics van considerar massa alta en aquell moment, però molt més barata que el cost de no fer res— i la recuperació d'aquests costos ha estat ràpida, impulsada per l'estalvi operatiu i la nova confiança del mercat [1].

A les escoles, els estudiants aprenen a fer servir eines d'IA que ajuden a verificar documents i notícies, dificultant la propagació de deepfakes. En un centre de recerca, una jove investigadora mostra com un sistema entrenat per reconèixer manipulacions digitals pot contrastar en mil·lisegons una imatge viral contra el seu origen, enviant immediatament el resultat a una cadena de blocs pública. Aquest procés —la prova d'existència, el cor de *t2p*— ha esdevingut un pilar de la confiança digital: cada dada que circula per la xarxa és rastrejable fins al moment en què va ser segellada, i qualsevol alteració queda al descobert.

Al mercat laboral, les empreses ja no depenen únicament d'auditories anuals per validar certificacions; moltes credencials s'emeten i es verifiquen a l'instant a través de contractes intel·ligents. Un enginyer informàtic pot demostrar, amb una sola transacció, que ha completat un projecte de codi obert, i el seu historial queda registrat de manera verificable per a futurs col·laboradors.

Aquest escenari no és una utopia; és la culminació possible d'una sèrie de decisions concretes preses al llarg d'una dècada. Cada actor —govern, empresa, ciutadà— pot adoptar un conjunt de principis clars, que van des del compromís amb l'estandardització de la prova d'existència fins a la tria de protocols de consens de baix consum energètic. El resultat és una societat on la confiança es construeix sobre dades verificables, i on les tecnologies emergents treballen com a infraestructura per a un futur sostenible i just.

Els tres actors

Governants — liderar el marc de confiança. El primer pas d'un govern responsable és establir un preu al carboni que reflecteixi el cost real del dany climàtic i incentivi la descarbonització a tots els nivells de l'economia. Aquest preu ha d'estar recolzat per estàndards internacionals de verificació i monitoratge (MRV) basats en la prova d'existència. La blockchain moderna, després del Merge, consumeix molt menys energia que les cadenes de blocs tradicionals, com hem vist, i pot convertir-se així en la columna vertebral d'un registre immutable i verificable de dades d'emissions [2]. Els governs poden finançar xarxes de verificació a escala nacional i regional, donar suport a la recerca de protocols de consens ultraeficients i establir legislació que orienti les empreses cap a informes ESG certificats de manera comprovable. D'aquesta forma es crea una cadena de confiança on cada declaració d'impacte es pot auditar gairebé en temps real, reduint el risc de greenwashing i augmentant la credibilitat davant d'inversors i ciutadans.

Empreses — transformar les dades en actius sostenibles. Per a les organitzacions, la clau és invertir en una infraestructura neta que garanteixi la traçabilitat dels seus processos productius. Això implica desplegar solucions de blockchain per ancorar dades ESG i utilitzar proves d'existència per validar cada pas del cicle de vida del producte, des de l'extracció de matèries primeres fins al reciclatge final. Les empreses que adopten aquest model no només compleixen la normativa emergent, sinó que també hi

guanyen un avantatge competitiu: els consumidors i els inversors prefereixen marques que ofereixen transparència verificable. A més, l'adopció d'aquestes tecnologies redueix els costos associats a auditories externes i certificacions tradicionals, alliberant recursos per a la innovació i el creixement sostenible. El principi és senzill: invertir en net, ancorar les dades i no fer greenwashing.

Ciutadania — ser vigilant i actiu. Cada individu disposa de petites però potents palanques: optimitzar el consum energètic a la llar, adoptar mobilitat elèctrica i verificar les declaracions abans de compartir-les. Les eines basades en blockchain permeten que qualsevol usuari comprovi la traçabilitat d'una informació amb només uns clics, evitant la propagació de desinformació i reforçant la confiança col·lectiva. A més, la participació ciutadana en programes de monitoratge distribuït —com les xarxes de sensors per a la qualitat de l'aire o els comptadors intel·ligents d'energia— alimenta dades accessibles públicament i serveix de fonament per a polítiques locals més efectives. La combinació d'acció personal amb eines de verificació descentralitzada crea un ecosistema on la responsabilitat es distribueix, augmentant la pressió sobre governs i empreses perquè actuïn amb integritat.

Com hem vist, els **governants** han d'establir preus al carboni i marcs reguladors robustos; les **empreses** han de convertir les seves dades ESG en actius immutables i transparents; i la **ciutadania** ha d'exercir una vigilància activa, aprofitant les eines de prova d'existència per validar la informació. Aquesta sinergia multiplica l'impacte de cada palanca, convertint el desafiament global en una oportunitat col·lectiva. És hora de posar-nos en marxa: **time2act**.

La infraestructura de confiança

La transició cap a una economia neta i resilient es fonamenta en una única premissa: sense dades fiables no hi ha acció efectiva. Durant tot *time2act* hem mostrat com les tecnologies emergents poden transformar la incertesa en seguretat, i ara és el moment de consolidar aquest fil conductor. La intel·ligència artificial (IA) i la blockchain formen una sinergia que permet generar, validar i compartir informació amb un grau d'integritat fins ara difícil d'assolir. En aquest ecosistema, la prova d'existència —el concepte central de *t2p*— actua com a ancoratge immutable per a tota mena d'evidències: des de les emissions de carboni d'una fàbrica fins als certificats d'energia verda d'un microgrid comunitari.

1. Dades immutables, decisions àgils

La blockchain garanteix que cada registre d'emissió o certificat ESG es mantingui inalterable i verificable per a qualsevol part interessada. Això redueix la necessitat de processos d'auditoria costosos i prolongats, escurçant el temps de validació de setmanes a minuts. Aquesta eficiència no només impulsa la competitivitat, sinó que crea una base sòlida per a polítiques públiques fonamentades en evidències reals.

2. IA com a motor d'anàlisi i predicció

Els algorismes d'IA processen grans volums de dades en temps real, identificant patrons ocults i projectant escenaris futurs amb una precisió cada cop més alta. Quan aquestes prediccions es recolzen en registres immutables, la seva credibilitat augmenta: els resultats deixen de ser només estimacions difícils de contrastar i passen a estar ancorats en una capa de confiança verificable. Això permet a governs i empreses prendre mesures proactives —com ajustar la producció d'energia renovable o reorientar inversions— sense la paràlisi del dubte sobre la veracitat de les dades.

3. Prova d'existència: l'estampilla de la veritat

t2p ofereix una solució tècnica per a qualsevol informació que requereixi autenticació. Mitjançant un hash criptogràfic i el registre en una cadena de blocs pública, es genera una prova d'existència que pot ser consultada per qualsevol actor —des del consumidor fins al regulador— sense necessitat d'intermediaris. Aquesta capacitat és crucial a l'era de les deepfakes i la desinformació: cada declaració, certificació o reclamació pot contrastar-se amb una prova immutable, reforçant la confiança social i mercantil.

4. Governança descentralitzada i participació ciutadana

La blockchain no només emmagatzema dades; també habilita mecanismes de governança transparent. Mitjançant contractes intel·ligents, les organitzacions poden establir regles clares per a la gestió d'actius digitals, recompensar comportaments sostenibles i penalitzar infraccions de manera automàtica. A més, els ciutadans disposen d'eines de verificació que els permeten exercir una vigilància activa sobre les polítiques públiques i les pràctiques corporatives, convertint la supervisió en un procés col·lectiu i continu.

5. Ruta cap a l'acció: principis per a tots els actors

1. **Adoptar plataformes blockchain de baix consum energètic** — el Merge ha reduït el consum d'energia de les cadenes modernes prop d'un 99,95 % [2].
2. **Integrar la IA per al processament i l'anàlisi de dades ESG**, assegurant que cada model es nodreixi de registres verificats.
3. **Implementar la prova d'existència com a estàndard de validació** en certificats, informes i declaracions públiques.
4. **Fomentar la participació ciutadana mitjançant portals oberts**, on qualsevol usuari pugui consultar i validar les dades amb un clic.
5. **Establir marcs reguladors que reconeguin la cadena de blocs com a font de verificació**, simplificant els processos d'auditoria.

Com hem vist, la confiança és el pont entre la visió d'un futur sostenible i la realitat operativa actual. La combinació d'IA i blockchain, reforçada per *t2p*, crea una infraestructura que converteix dades en veritat i veritat en acció. El repte ja no és tecnològic sinó col·lectiu; depèn de cada empresa, govern i ciutadà posar-se en marxa. És hora d'actuar amb decisió i conviccions clares: **time2act**.

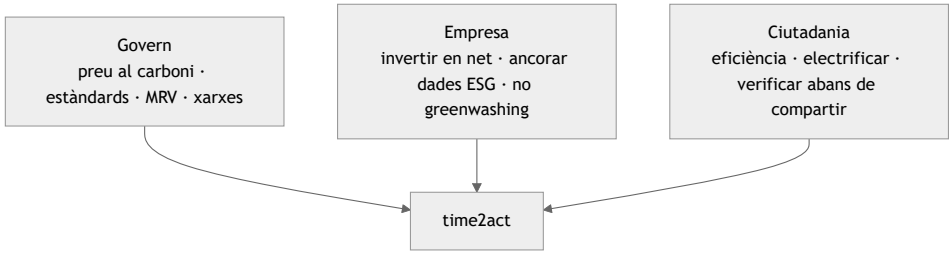


Figura 111.1 — Cada actor —govern, empresa i ciutadania— té accions concretes a curt, mitjà i llarg termini.

Els principis de l'acció

1. Electrificar-ho tot el possible. La transició energètica ja no és una opció, sinó la base sobre la qual es construeix qualsevol model sostenible. Cada equipament industrial, cada flota de transport i cada infraestructura urbana hauria de ser alimentada per electricitat, preferentment generada a partir de fonts renovables. La clau és establir un calendari de migració escalable: identificar els punts crítics, substituir els equips per motors d'alta eficiència i aprofitar les oportunitats de càrrega intel·ligent per equilibrar la demanda.

2. Fer-ho amb energia neta i ferma. No n'hi ha prou d'electrificar si l'electricitat prové d'origen fòssil. La combinació d'IA per optimitzar la despesa energètica i de blockchain per registrar en temps real la procedència del corrent ajuda a garantir una cadena de subministrament veritablement neta. Quan cada quilowatt-hora es pot certificar mitjançant un contracte intel·ligent, l'energia neta deixa de ser només una aspiració ambiental i esdevé també una palanca de competitivitat i de confiança per al consumidor.

3. Mesurar i verificar de manera incorruptible. La veritat de les dades es converteix en el nou actiu més valuós. Mitjançant *t2p*, cada registre d'energia consumida, d'emissions o de resultats operatius es pot codificar en una cadena de blocs immutable, dificultant les manipulacions i facilitant auditories molt més ràpides. La mesura precisa i la verificabilitat instantània són, per tant, els pilars que sustenten qualsevol estratègia d'impacte real.

4. Alinear incentius. El preu del carboni ha de reflectir el seu cost social. Aplicar un preu a les emissions i eliminar les subvencions als combustibles fòssils crea un marc econòmic on les decisions verdes són també les més rendibles. Aquest alineament incentiva comportaments responsables i orienta la inversió cap a les tecnologies netes, sense necessitat d'intervencions reguladores excessives.

5. Protegir la veritat com a bé públic. En una era de deepfakes i desinformació, la confiança es converteix en un recurs escàs. La infraestructura basada en blockchain, reforçada per *t2p*, fa que la informació crítica sobre energia, emissions i impacte social sigui immutable i accessible a tots els interessats. Les polítiques públiques han de reconèixer la veritat com un bé comú, establint marcs legals que protegeixin les dades certificades i dissuadeixin les manipulacions. Així, cada ciutadà, empresa o govern pot confiar en una font verificable per prendre decisions informades.

Aquests cinc principis no són només recomanacions teòriques; són passos concrets que qualsevol actor —des de la start-up més àgil fins al govern nacional— pot començar a implementar avui mateix. En seguir-los, convertim el potencial de la IA i la blockchain en una infraestructura de confiança capaç de transformar dades en veritat i veritat en acció. **time2act**.

L'horitzó regulador

Cap full de ruta no estaria complet sense mirar el marc legal que s'acosta, perquè la regulació recompensarà els qui s'avancin. A Europa, l'article 50 del Reglament d'Intel·ligència Artificial (l'EU AI Act) obligarà a marcar en format llegible per màquina el contingut generat per IA i a etiquetar les *deepfakes*; les seves obligacions s'apliquen a partir del 2 d'agost de 2026 [3]. En paral·lel, el reglament eIDAS 2.0 desplega la cartera d'identitat digital europea i introdueix figures noves —els registres electrònics qualificats i l'arxivament electrònic qualificat— que donen reconeixement legal al model de traça d'auditoria immutable que aquest llibre defensa [4].

A l'altra banda de l'Atlàntic, els Estats Units han aprovat la TAKE IT DOWN Act (signada el maig de 2025), que penalitza la imatge íntima no consentida —incloses les generades per IA— i obliga les plataformes a retirar-la en 48 hores; i la DEFIANCE Act, aprovada pel Senat el gener de 2026, hi afegeix una via civil perquè les víctimes puguin reclamar [5].

El missatge per a governs i empreses és inequívoc: l'expectativa legal ja no és només «guardar» la informació, sinó poder DEMOSTRAR-NE l'origen i la integritat. Les organitzacions que avui adopten la prova d'existència —ancorar el hash de cada dada crítica abans de compartir-la— no compliran la norma a contracor i a última hora, sinó que hi arribaran preparades, perquè ja hauran convertit la verificabilitat en un hàbit. La regulació no és, doncs, una càrrega afegida a la transició: és el mateix camí, senyalitzat.

La promesa i el perill (síntesi)

Per primera vegada en la història contemporània disposem d'un diagnòstic clar, d'eines provades i d'una infraestructura capaç de protegir la veritat que sustenta les nostres decisions. La intel·ligència artificial, alimentada per grans volums de dades netes i verificades, pot transformar informació dispersa en coneixement accionable amb una precisió que fa dècades era impossible. Paral·lelament, la blockchain —en la seva forma més eficient després del Merge, que ha reduït el consum energètic prop d'un 99,95 %— ofereix una capa d'imparcialitat i immutabilitat que converteix cada transacció, cada registre de propietat intel·lectual o cada certificació climàtica en una prova d'existència difícil de falsejar [2]. Aquesta combinació crea una infraestructura de confiança on la veritat no només es detecta, sinó que es manté intacta davant d'intents de manipulació, com els deepfakes i les campanyes de desinformació massiva.

No obstant això, el relat de l'oportunitat està inevitablement entrellaçat amb un perill imminent. Actuar té un cost —entre l'1 i el 2 % del PIB mundial per mantenir l'escalfament per sota dels 2 °C—, però és molt més barat que el cost de no actuar, que creix amb cada any de retard [1]. A més, la tecnologia, tot i ser poderosa, no és una panacea. La blockchain pot garantir la integritat dels registres, però sense una voluntat política i empresarial decidida a adoptar-la, aquests registres romanen inactius, com arxius en un dipòsit tancat. De manera similar, els models d'IA poden oferir prediccions útils, només si es disposa de dades fiables i de processos de governança que n'assegurin la utilització ètica i transparent.

La finestra per aprofitar aquesta sinergia és limitada. Cada any que passa sense una acció coordinada augmenta el cost econòmic i complica el camí tecnològic, perquè les infraestructures legals i reguladores es queden enrere respecte al ritme d'innovació. Les barreres d'adopció —des de la manca de talent especialitzat fins a l'oposició d'interessos establerts— s'enfonsen quan el moment clau desapareix. Per això, cal una voluntat col·lectiva que impulsi polítiques públiques, inversions estratègiques i col·laboracions intersectorials per desplegar aquesta infraestructura de confiança a escala global.

Disposem d'eines i del marc conceptual necessaris perquè la veritat sigui el fonament de cada decisió; però si no actuem ara, la porta es tancarà, els costos augmentaran i la nostra capacitat d'actuar amb informació fiable quedarà compromesa. La clau és combinar la potència tecnològica amb una voluntat decidida a transformar aquesta promesa en realitat concreta. És el moment de dir **time2act**.

Aquesta visió es veu reforçada per Beth Noveck, qui després de l'escàndol Horizon —on més de 900 condemnes injustes van conduir a almenys tretze suïcidis— proposa que la intel·ligència artificial sigui una infraestructura cívica, **verificable, auditable i responsable davant les persones que impacta** [6].

El seu marc de contractació obliga governs i empreses a exigir registres ancorats en blockchain neutral i independents del creador, assegurant que cada model d'IA pugui ser revisat i reproduït sense caixes negres. Aquest requisit converteix la prova d'existència en una condició mínima per a qualsevol licitació pública, transformant dades i algoritmes en actius oberts que es poden validar en temps real, i completa el nostre full de ruta: no només protegim la veritat, sinó que fem obligatòria la seva transparència des del primer moment d'adquisició.

És time2act

Fa vint anys, Paul Roberts, a *The End of Oil* (2004), va pintar el quadre d'un món que es quedava sense energia fàcil, amb una geopolítica fragmentada i un clima que mostrava les primeres fissures irreversibles. El seu diagnòstic, tan precís com alarmant, encara ressona en cada sala de consells directius i en cada aula universitària. Però el panorama ha canviat: avui disposem no només del coneixement dels riscos, sinó també d'una infraestructura tecnològica capaç de restablir la confiança que la crisi ha erosionat.

Principi 1 — Veritat com a base operativa. La prova d'existència converteix qualsevol dada —des de certificats d'origen energètic fins a resultats d'auditories climàtiques— en un registre immutable i verificable. Això redueix la incertesa que alimenta els deepfakes i les manipulacions de mercat, i permet decisions basades en fets contrastables.

Principi 2 — Eficiència energètica com a requisit. Com hem vist, la blockchain moderna consumeix molt menys energia que les primeres iteracions [2]. Això significa que la infraestructura de confiança no es converteix en una nova font de demanda desbocada, sinó en una eina que pot conviure amb els sistemes ja existents.

Principi 3 — Cost d'adopció sostenible. Mantenir l'escalfament per sota dels 2 °C requereix invertir entre l'1 i el 2 % del PIB mundial, una xifra que es paga amb escreix si es compara amb el cost de la inacció: increment de desastres climàtics, pèrdua de confiança en els mercats i augment del preu de les matèries primeres [1]. La transició no és gratuïta, però és molt més barata que el seu contrari.

Principi 4 — Escalabilitat per a tots els actors. Des de governs nacionals fins a start-ups d'energia renovable, la combinació d'IA per al processament de dades i blockchain per a la seva certificació crea una capa que es pot adoptar progressivament. Cada entitat pot iniciar un pilot local —per exemple, validar l'origen de l'energia en una zona industrial— i escalar cap a cadenes de subministrament més àmplies.

Principi 5 — Governança participativa. La transparència inherent a aquests sistemes permet incloure ciutadans, acadèmics i ONG en processos de verificació i auditoria, reforçant el contracte social i generant un ecosistema on la confiança no és una concessió sinó una conseqüència natural.

El camí que s'obre davant nostre és clar: integrar IA i blockchain com a pilars d'una nova arquitectura de confiança, desplegant la prova d'existència per garantir que cada decisió es fonamenti en dades autèntiques. No només cal implantar tecnologia; cal transformar mentalitats, establir marcs reguladors àgils i crear col·laboracions intersectorials que catalitzin el canvi.

Així doncs, la crida no és a més diagnòstics ni a promeses buides, sinó a posar en marxa les eines que ja tenim. El moment de parlar ha passat; ara toca actuar amb decisió i precisió. **És time2act**.

---

[1] (cost d'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, article 50 (transparència del contingut generat per IA; aplica 2-ago-2026). https://artificialintelligenceact.eu/article/50/ ↩

[4] Signaturit — *eIDAS 2.0: registres i arxivament electrònics qualificats*. https://www.signaturit.com/blog/eidas-2-regulation/ ↩

[5] Orrick — *TAKE IT DOWN Act becomes law*; DEFIANCE Act (Senat, gen-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 segell i la cadena: qui controla la prova, i qui hi queda atrapat

«El poder tendeix a corrompre, i el poder absolut corromp absolutament.»

— Lord Acton, carta a Mandell Creighton (1887)

A l'entrada d'un laboratori improvisat a Nairobi, una fila de cotxes esperava per ser inspeccionada. Entre ells, joves estudiants, venedors ambulants i famílies amb nens petits s'alineaven sota un pòster que anunciava «World ID — Demostra que ets humà». Un equip d'enginyers, amb màscares de protecció i una càmera d'alta resolució, escanejava l'iris de cada persona mentre un monitor mostrava números que semblaven confirmar la seva identitat. En menys de dos minuts, el sistema registrava una «prova» immutable a una cadena de blocs pública, assignant-li un crèdit criptogràfic com a recompensa per participar.

Aquesta escena, que podria aparèixer en qualsevol reportatge optimista sobre la lluita contra bots i deepfakes, és exactament el que *time2act* ha defensat: un mecanisme fiable per demostrar que darrere d'un avatar hi ha una persona real. No obstant això, l'ironia esdevé palpable quan, només dos anys després, el mateix projecte Worldcoin/World ID s'enfronta a prohibicions i multes en més de nou jurisdiccions. Kenya va declarar-lo inconstitucional, i tant Kenya com Colòmbia van ordenar la destrucció total de les dades biomètriques recollides. El que havia començat com una solució per reforçar la confiança digital es transforma en un exemple clar del perill que amaga qualsevol infraestructura immutable [1].

Aquesta paradoxa és el punt d'arrencada d'aquest capítol. La infraestructura que permet *t2p* —biometria, registre immutable i cadena de blocs— pot ser, simultàniament, l'arquitectura de la vigilància massiva. No es tracta d'un rebuig del concepte; el mecanisme és necessari per combatre la falsificació digital. El que sí cal reconèixer, tal com estableix Snowden, és que «el credo del sistema de vigilància massiva era 'recull-ho tot, processa-ho tot, aprofita-ho tot, associa-ho tot'», i que aquest patró ja ha deixat una empremta indeleble en la nostra història recent [20].

Aquest capítol es presenta com el contrapès honest del llibre. Seguint el mandat de *time2act* —«la promesa i el perill»— recull, en un sol lloc, les crítiques que fins ara havien estat disperses entre informes d'ètica, anàlisis legals i testimonis de whistleblowers. La tesi central és clara: la descentralització tècnica no garanteix una governança democràtica; el veritable problema són les relacions de poder que s'estableixen al voltant del control de la prova. Qui defineix les regles d'entrada a aquest registre? Qui pot eliminar o modificar les dades sense rendició de comptes? Quins interessos es beneficien quan una sola entitat controla tant l'accés com la verificació?

En el context actual, on els grans L2 d'Ethereum operen amb un únic seqüenciador corporatiu i el 42 % dels blocs són censurats segons les llistes OFAC [5], la pregunta que queda oberta és qui verifica el verificador. La cadena de blocs pot dir «no confiïs, verifica», però sense una auditoria independent i transparent, aquesta verificació es converteix en una forma subtil de control, com recorda Dominic Frisby: «el lema de la cadena de blocs és «no confiïs, verifica»; però la pregunta que queda oberta és qui verifica el verificador» [32].

Així, aquest capítol d'obertura posa en relleu que, tot i les promeses de confiança restaurada, la mateixa tecnologia pot ser utilitzada per consolidar poder i imposar una vigilància que limita la llibertat individual. La resposta no és desestimar la biometria ni la cadena immutable, sinó construir marcs de governança democràtica que assegurin que el «segell» serveixi per protegir-nos i no per atrapar-nos. El proper pas del lector serà confrontar aquestes tensions i considerar com garantir que el control de la prova es mantingui al servei de la societat, i no a les mans d'una elite tecnològica.

La neutralitat que no existeix

Al capvespre del 2026, la infraestructura que sosté la xarxa Ethereum es veu dominada per una sola entitat: un seqüenciador corporatiu gestionat per Coinbase a través de Base. No és només una qüestió de rendiment; aquest únic node decideix quin bloc s'inclou i en quina cadena de confirmació passa, exercint una forma de censura que afecta el 42 % dels blocs d'Ethereum via relays que apliquen les llistes OFAC. A més, la capa segona de validació que t2p fa servir avui ha concentrat la producció de blocs en un grup reduït de validadors triats després de l'actualització «Rio» (2025) [5].

Aquesta concentració contradiu el mite popular que la blockchain és inherentment descentralitzada i neutral. La veritat és que qui programa i opera els nodes determina quins registres es guarden i qui hi té accés. Com assenyala Cathy O'Neil, els models matemàtics que sostenen aquestes infraestructures són «opacs i invisibles per a tothom excepte per als grans sacerdots del sector: els matemàtics i els enginyers informàtics» [4]. La seva observació revela que la confiança no recau en el codi, sinó en les persones que l'escriuen i el mantenen.

Marc Goodman ho resumeix amb claredat: «qui controli el codi controlarà el món, per a bé i per a mal» [3]. Això no és una hipèrbole; la capacitat de definir les regles d'una cadena immutable es tradueix en poder sobre la identitat digital, els drets de propietat intel·lectual i fins i tot la capacitat d'excloure actors polítics o socials. Edward Snowden confirma aquesta dinàmica: «aquestes màquines fan el que fan perquè algú els ho mana, d'una manera molt concreta i minuciosa; i aquest algú pot ser fins i tot un nen de set anys» [2].

A la taula on es redacten les regles del joc, el marge per saltar-se-les és enorme. Jack Watling observa que «ser a la taula on s'estableixen les regles del joc augmenta el marge d'un estat per saltar-se aquestes mateixes regles en benefici propi» [6]. Aquest poder no es limita als estats; infraestructures privades com Starlink, controlades per corporacions sense rendició de comptes democràtica, s'han convertit en actius estratègics que modelen la comunicació global i, per tant, la capacitat de vigilància i control [7].

El paral·lelisme històric és revelador. Dominic Frisby recorda com Isaac Newton, com a únic responsable de la seca reial (Master of the Mint), va concentrar el control de la validació de la moneda i va perseguir els falsificadors amb una rigorositat implacable [8]. La centralització del poder de verificació no és un fenomen nou; només ha canviat de metall a bits.

Sense una governança democràtica explícita que reguli qui pot ser validador, quines són les seves obligacions i com se supervisen les decisions, la prova d'existència (t2p) corre el risc de transferir el poder dels intermediaris tradicionals —bancs, notaris, autoritats públiques— a una elit tècnica que opera en l'ombra; com hem vist. La infraestructura immutable es converteix així en un nou tipus d'intermediari: invisible però decisivament influent, i sense mecanismes de rendició de comptes que garanteixin la seva neutralitat.

El consentiment cristal·litzat

En el marc del «consentiment verificat» que sustenta la prova d'existència, el llibre ha presentat aquest segell com a garantia de transparència i responsabilitat. Tanmateix, la mera existència d'una acceptació registrada no assegura que sigui autònoma ni lliure. Carissa Véliz recorda que «no tens marge per negociar els termes i les condicions, que, a més, poden canviar en qualsevol moment sense avís previ»[9]; i l'opinió del Comitè Europeu de Protecció de Dades subratlla que el model «consentir o pagar» no constitueix un consentiment «lliurement prestat»[10]. Això vol dir que, quan la cadena blockchain segella permanentment aquell «accepto», transforma una possible elecció voluntària en un fet immutable i, per tant, ineludible.

Dos exemples concrets il·lustren com aquesta dinàmica es materialitza en infraestructures de registre. A la Casa de Contractació de Sevilla, el registre d'obligacions s'imposava mitjançant juraments obligatoris i sancions que arribaven fins a dos-cents assots per incompliment[11]. Aquell «registre immutable» servia com a eina de coacció: l'acte de signar no era una manifestació lliure, sinó un requisit legal que, si es rebutjava, comportava penes econòmiques i personals severes. En aquest context, la blockchain podria consolidar la memòria d'aquells juraments, convertint-los en testimonis eterns d'una pressió institucional.

Un altre vector de coerció prové de la dependència energètica que sosté les xarxes descentralitzades. Jack Watling descriu aquesta situació com un «dit posat damunt la gola»[12], una condició que invalida l'autonomia del consentiment perquè els operadors no poden dissociar-se de la infraestructura crítica sense comprometre el seu funcionament. La necessitat d'un subministrament energètic constant per a nodes i validadors crea una vulnerabilitat estructural: el «clic» que dona fe del consentiment esdevé un acte forçat, motivat pel temor a perdre accés a recursos essencials.

Aquests casos revelen una contradicció fonamental en la proposta de t2p. Si la tecnologia registra i verifica qualsevol acceptació sense discernir entre voluntat i imposició, el resultat és una forma d'autoritarisme digital que reforça les jerarquies de poder existents. La solució no consisteix només a afegir més capes de seguretat criptogràfica; cal introduir mecanismes de governança que puguin validar la legitimitat del

consentiment mateix. Això implica, per exemple, establir protocols d'auditoria independent que revisin les condicions contractuals i assegurin que el registre no es converteixi en una eina de coacció estructural.

En definitiva, la cadena pot ser un testimoni fiable només si el seu testimoni és genuí. Distincions clares entre consentiment real i forçat han de ser incorporades al disseny de t2p; d'altra manera, el «clic» etern que es registra podria acabar per perpetuar les formes de control que pretén combatre. El repte, doncs, no és només tecnològic sinó institucional: cal garantir que la verificació del consentiment sigui acompanyada d'un marc democràtic que protegeixi l'autonomia dels individus i impedeixi que el segell es converteixi en una cadena de vigilància.

La plusvàlua de la prova

Quan tokenitzem l'experiència humana com a «prova d'existència», el que aparentment és una eina per restablir la confiança es converteix, en realitat, en un actiu negociable. Shoshana Zuboff descriu aquest fenomen com el capitalisme de la vigilància: «l'experiència humana [és] matèria primera gratuïta» que les plataformes extreuen, prediuen i venen [13]. Cada vegada que una empremta biomètrica o un segell temporal es registra en una cadena immutable, s'afegeix una nova unitat de valor a la base de dades que alimenta el mercat de la informació personal. La mateixa Zuboff recorda que «els acaparats som nosaltres; la nostra experiència és l'objecte d'extracció» [14], subratllant que el control del flux de dades es tradueix en poder econòmic i polític.

Aquesta dinàmica no és només teòrica. El 2024, la Federal Trade Commission dels Estats Units va prohibir per primera vegada a corredors de dades la venda de localitzacions sensibles i va multar Avast amb 16,5 milions de dòlars [15]. El mateix any, l'Autoritat de Protecció de Dades neerlandesa (DPA) imposà una sanció de 30,5 milions d'euros a Clearview AI per haver creat una base biomètrica de trenta mil milions de fotografies extretes sense consentiment. Aquestes accions demostren que la mercantilització del registre immutable ja ha generat un model d'ingressos basat en l'explotació de les proves d'identitat, i que els mecanismes reguladors encara lluiten per mantenir el pas.

L'avís històric de Dominic Frisby sobre la degradació silenciosa dels estàndards ofereix una perspectiva de llarg termini. El denari romà, segons Frisby, va passar del 95-98 % de plata a menys d'un 1 % sense que ningú se n'adonés [16]. Aquest declivi es va produir perquè no hi havia una auditoria independent i contínua que vigilés la qualitat i la integritat del sistema monetari. De manera paral·lela, les tecnologies de registre immutable poden patir una erosió similar si el seu funcionament queda sotmès a interessos privats sense supervisió pública. La falta d'una auditoria permanent deixa oberta la porta a manipulacions subtils: canvis en els algoritmes de consens, inserció de nodes controlats per entitats corporatives i, finalment, una concentració del poder que contradiu l'ideal descentralitzat.

Per tant, cal establir salvaguardes concretes contra la mercantilització de les dades registrades. Primer, el protocol ha d'incloure mecanismes de verificació externa, amb auditors independents acreditats per institucions democràtiques i no per empreses que en treuen profit. Segon, s'ha d'instaurar un marc legal que obligui a la transparència del propietari dels segells i de les cadenes associades, garantint que qualsevol transferència de valor sigui pública i reversible. Finalment, cal un sistema de governança participativa on els usuaris puguin exercir control sobre les polítiques d'ús i les tarifes aplicades a la seva pròpia prova.

Només amb aquestes mesures es pot evitar que el «segell» es converteixi en una «cadena» d'explotació. La plusvàlua de la prova no resideix únicament en la seva capacitat tècnica per validar l'autenticitat, sinó en la manera com la societat regula qui n'obté beneficis i quins límits imposa al seu ús. Sense una auditoria permanent i una governança democràtica, el risc és que, tal com ha passat amb les monedes antigues, els estàndards tècnics es degradin silenciosament fins a perdre completament la seva funció protectora.

El dret a l'oblit eliminat

En el moment que una informació es grava en una cadena immutable, la seva existència deixa d'estar subjecta al caprici de les institucions ni al pas del temps. La immutabilitat, celebrada com a garantia de confiança, es converteix simultàniament en l'ancoratge d'un rastreig permanent que impedeix qualsevol possibilitat d'oblit. Edward Snowden descriu aquest fenomen amb una precisió inquietant: «em resultava atroç estar tan inextricablement i tecnològicament lligat a un passat del qual em penedia del tot, però que tot just recordava»[20]. No és només una reflexió personal; és la realitat d'un sistema dissenyat per «recollir-ho tot, processar-ho tot, aprofitar-ho tot, associar-ho tot» i que, al centre de les seves operacions,

el centre de dades de Bluffdale es va construir per emmagatzemar «el patró de vida del planeta sencer»[17].

Aquests processos van més enllà d'una simple acumulació de dades: la xarxa ha imposat una «fidelitat a la memòria, la uniformitat identitària i, per tant, la conformitat ideològica»[18]. Quan el registre és immutable, qualsevol error, dada obsoleta o informació que en un futur pugui resultar perjudicial per al subjecte es converteix en una ferida permanent. No hi ha mecanisme de supressió ni d'anul·lació; la memòria digital es manté viva i accessible indefinidament.

Com el 2026 ja s'ha assenyalat, aquest poder de rastreig s'ha materialitzat en l'ús massiu d'eines d'anàlisi de cadena per part d'agències federals nord-americanes. ICE, IRS i FBI han adquirit solucions com Chainalysis o TRM Labs amb l'objectiu explícit de desanonimitzar el registre immutable, vinculant adreces digitals a persones concretes[19]. Aquestes tecnologies permeten seguir el flux d'actius digitals, identificar transaccions i, finalment, rastrejar els individus fins al seu origen biològic o geogràfic. El resultat és una forma de vigilància que transcendeix les fronteres tradicionals del control estatal: la informació ja no depèn només del consentiment d'un usuari, sinó que es converteix en un testimoni immutable de cada acció.

Frisby destaca que fins i tot l'or, considerat l'«únic diner que no és una promesa», esdevé vulnerable quan la seva propietat i ubicació són totalment transparents: «un objectiu fàcil de confiscació o d'impostos»[21]. De manera anàloga, un registre immutable esdevé un actiu que qualsevol autoritat pot aprofitar per imposar sancions, confiscar béns o limitar drets civils. La impossibilitat d'eliminar o revocar dades errònies significa que els ciutadans no disposen de cap recurs efectiu davant decisions injustes basades en informació inexacta.

Aquesta situació planteja una contradicció fonamental: la immutabilitat, que el llibre ha celebrat com a pilar de confiança, esdevé també l'instrument que elimina qualsevol possibilitat d'oblit i, per tant, impedeix la rectificació o la supressió de dades perjudicials. Sense una auditoria permanent i una governança democràtica, aquest registre immutable gira contra el ciutadà, convertint-se en una eina de coerció més que en una garantia de transparència. El repte, doncs, no és només tecnològic sinó polític: cal establir mecanismes de revocabilitat i de caducitat per a registres erronis o transitoris, assegurant que la immutabilitat no es tradueixi en un estigma d'injustícia permanent.

Algoritmes inapel·lables

En el moment que una entitat decideix segellar la procedència d'una dada, el criteri que sustenta aquell segell queda ocult darrere d'un mur de codi i de matemàtiques incomprensibles per a la majoria. Com avisa Cathy O'Neil, els veredictes emesos per aquests models són «inapel·lables» i, alhora, «opinions incrustades en matemàtiques» que només els grans sacerdots del sector –enginyers i científics de dades– poden llegir i qüestionar [22]. Aquesta opacitat converteix el segell en una autoritat incontestable i crea un poder que supera qualsevol control democràtic.

Carissa Véliz reforça aquesta perspectiva: predir el comportament humà equival a intentar controlar-lo, una dinàmica que condueix inevitablement cap a l'autoritarisme quan les prediccions s'utilitzen per regular o restringir llibertats [23]. El model que garanteix la «veracitat» d'un registre immutable pot ser emprat per imposar límits a l'individu sense que aquest en tingui coneixement ni capacitat d'impugnar-lo. Edward Snowden afegeix: «la predictibilitat és manipulació». Quan un sistema anticipa les accions futures, no només ofereix informació; crea un mecanisme subtil de coacció que condiciona les decisions presents per tal d'ajustar-les al patró preestablert [24]. Així, el segell deixa de ser una simple garantia de procedència i es converteix en un instrument de conformitat.

Aquesta concentració de poder algorítmic es veu reforçada pel fet que qui estableix les regles del joc té marge per trencar-les. Jack Watling assenyala que «qui fa les regles té marge per saltar-se aquestes mateixes regles en benefici propi» [6]. En un ecosistema on la infraestructura de cadena de blocs i el registre immutable són controlats per uns pocs actors corporatius, aquesta capacitat es tradueix en una vulnerabilitat estructural: el segell pot ser modificat o ignorat segons els interessos d'aquells que l'han creat.

Com hem vist, el marc legal del 2026 retrocedeix davant aquestes amenaces; l'ajornament de les obligacions per a la IA d'alt risc dins del paquet «Digital Omnibus» i la derogació de la llei d'IA del Colorado deixen un buit regulador que facilita l'expansió indiscriminada dels sistemes de segellat [25].

Sense una normativa clara que imposi transparència i revisió independent, els algoritmes inapel·lables poden operar sense cap fre ni contrapès.

La fragilitat del segell queda evident també en el camp de la geolocalització. Durant la guerra d'Ucraïna, la interferència electrònica va enganyar els senyals GPS, demostrant que ni el temps ni la posició són invulnerables a manipulacions deliberades [26]. Això revela una veritat fonamental: la força vinculant del segell només és tan segura com la fiabilitat de les infraestructures subjacents. Si aquestes poden ser falsificades, cal desenvolupar mecanismes d'explicabilitat verificable i de rectificació que tinguin la mateixa robustesa legal que el registre immutable original.

En resum, la concentració del poder algorítmic converteix el segell en una arma potencial de control. La solució no resideix només en millorar la tecnologia, sinó en establir governança democràtica capaç d'imposar transparència, revisió independent i mecanismes de rectificació que impedeixin que el «codi» esdevingui l'únic guardià del futur.

L'autocensura del registre permanent

A la primavera de 2024, una jove escriptora catalana va retirar un assaig sobre les pràctiques d'intel·ligència artificial en el període electoral, temorosa que el simple fet de publicar-lo pogués atraure la vigilància estatal. Aquest comportament no és anecdòtic; segons Carissa Véliz, entre un terç i dos terços dels escriptors eviten certs temes per por de la vigilància governamental [27]. La causa profunda resideix en el que els estudiosos anomenen *mission creep*: una infraestructura dissenyada per a un propòsit —com la prova d'existència t2p— s'estén progressivament cap a usos no previstos, transformant-se en una arma de control social.

El registre immutable, l'element central de qualsevol cadena de blocs que pretén garantir integritat i traçabilitat, es converteix així en un «segell» que pot ser aprofitat per imposar límits funcionals i temporals a la llibertat d'expressió. Un exemple recent és Eurodac, el sistema europeu d'empremtes digitals per a processos d'asil. El 2024 s'ha abaixat l'edat mínima de recollida biomètrica de dotze a sis anys, obrint la base a un accés policial ampliat i facilitant una vigilància precoç sobre infants [28]. Aquesta expansió no és merament tècnica; és una decisió política que transforma una eina de gestió migratòria en una font d'informació per al control social.

La proliferació del registre permanent també alimenta efectes dissuasius més subtils però igualment devastadors. A Síria, durant la guerra, la desinformació orquestrada per actors russos va crear una incertesa fabricada que paralitzà les respostes internacionals i locals [29]. Quan el coneixement esdevé incert, la capacitat d'actuar de manera autònoma s'esvaeix: la població comença a autocensurar-se per evitar ser objecte de possibles sancions o persecucions. Aquest fenomen es reflecteix en l'observació de Shoshana Zuboff que el poder fonamental del sistema és determinar «qui sap, qui decideix i qui decideix qui decideix» [30]. En aquest escenari, el registre immutable deixa d'ésser una garantia de transparència per convertir-se en un mecanisme que consolida la informació al servei d'unes poques autoritats.

La legitimitat d'aquest poder es qüestiona quan les plataformes esdevenen «els àrbitres reals del que la gent pot dir», com assenyala Véliz: cal preguntar-se si disposen de la mena adequada de legitimitat per exercir aquest control [31]. El «protegir» dades biomètriques o transaccions digitals sovint es presenta com a eufemisme de «controlar» el comportament i les identitats dels individus. La conseqüència directa és una autocensura que s'estén més enllà del discurs, limitant la iniciativa creativa, inhibint la investigació crítica i encoratjant l'auto-exclusió de temes incòmodes.

Per evitar que una eina d'un fi es converteixi en infraestructura d'un altre, cal establir límits explícits tant funcionals com temporals. Això implica definir clarament quines dades poden ser registrades, durant quant temps i sota quina supervisió independent. Només amb mecanismes de revisió transparent i la participació democràtica es pot garantir que el segell digital no es converteixi en una cadena d'opressió. En aquest equilibri delicat entre confiança i vigilància, el perill real resideix no tant en la tecnologia mateixa sinó en qui la controla i com s'hi permet l'expansió del seu abast.

El contraargument que t2p ha de sobreviure

En el llarg viatge d'aquest llibre hem mostrat com la prova d'existència pot restaurar la confiança en un món saturat de deepfakes i falsificacions digitals. Ara ens trobem davant del reflex més incòmode: la mateixa infraestructura —biometria, registre immutable i cadena de blocs— és l'esquelet d'una

arquitectura de vigilància que podria convertir el segell digital en una cadena d'opressió. La clau per a no perdre-nos en un escenari de tecnoutopisme és reconèixer que **la descentralització tècnica no equival a governança democràtica**; el problema fonamental són les relacions de poder que es configuren al voltant del control i la supervisió.

El lema de la cadena, «no confiïs, verifica», s'ha convertit en un axioma universal per a la seguretat distribuïda. No obstant això, com assenyala Dominic Frisby, la pregunta oberta és **qui verifica el verificador**? [32] Si el procés de verificació es manté dins d'una caixa negra operada per uns pocs actors, el que hauria de ser una garantia de transparència es transforma en un instrument de coacció. **Com hem vist, el 2026 el 42 % dels blocs es construeixen a través de relays que apliquen censura OFAC**; la cadena que t2p fa servir avui concentra la producció de blocs en un grup reduït de validadors triats. [5] Aquesta concentració revela com, malgrat una arquitectura descentralitzada al nivell del protocol, el control efectiu recau en mans corporatives i estatals.

Per tal que **t2p** pugui complir amb la seva missió sense esdevenir un instrument de vigilància, cal establir quatre exigències imprescindibles:

1. **Governança democràtica dels nodes** — Qui opera, valida i audita els nodes ha d'estar sotmès a processos oberts i participatius, evitant la concentració observada en les cadenes L2. La supervisió ha de provenir d'entitats independents i representatives, no només de grans plataformes financeres.
2. **Auditoria transparent dels algoritmes** — Els mètodes de verificació han de ser subjectes a revisions periòdiques per part d'experts externs, amb resultats publicats en formats accessibles. Així es contraresta l'opacitat descrita per Cathy O'Neil, segons la qual els models són «opinions incrustades en matemàtiques», llegibles només per als «grans sacerdots del sector». [4]
3. **Mecanisme de revocabilitat i correcció** — Quan un registre immutable conté errors o dades recollides sense consentiment (com Eurodac que ha reduït l'edat biomètrica a sis anys i permet accés policial), s'ha d'incloure una via segura per a la rectificació o supressió, garantint el dret a l'oblit i evitant l'ús coercitiu de dades errònies. [28]
4. **Control de la plusvàlua de les dades** — Cal definir clarament qui captura i comercialitza la informació derivada del registre; sense aquest control, es perpetua una economia de vigilància on la informació personal es converteix en béns d'alts rendiments per a corporacions i estats. [15]

En resum, **la cadena segella probabilitats, no veritats**; un segell immutable pot ancorar la coacció tan eficaçment com l'autenticitat. Reconèixer aquesta dualitat no debilita el missatge de *time2act*, sinó que el blinda: només confrontant les limitacions del poder i establint regles estrictes de governança podem garantir que la prova d'existència sigui una eina de confiança i no un instrument d'opressió.

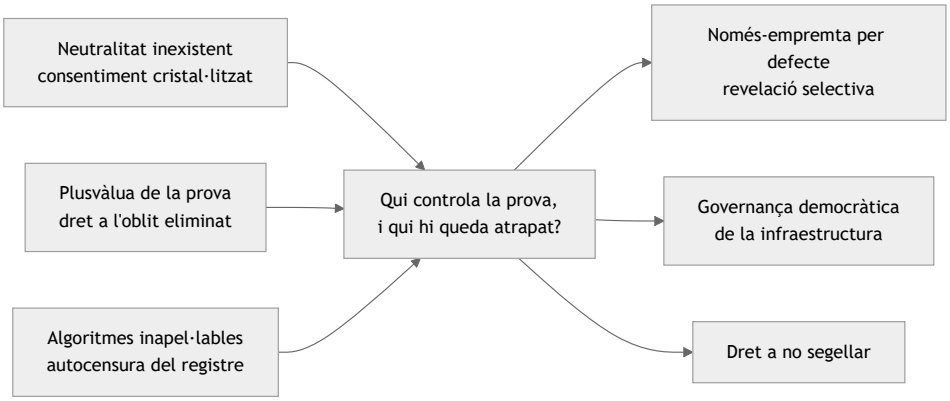


Figura 112.1 — El segell i la cadena: qui controla la prova, i qui hi queda atrapat. Els riscos que el capítol desgrana — la neutralitat que no existeix, el consentiment cristal·litzat, la plusvàlua de la prova, el dret a l'oblit eliminat, els algoritmes inapel·lables i l'autocensura del registre permanent — i els contrapesos que reclama: només-empremta per defecte, revelació selectiva, governança democràtica de la infraestructura i el dret a no segellar.

És hora d'actuar

La prova d'existència que hem construït al llarg de *time2act* és, com qualsevol segell, una doble eina: autentica la veritat i, simultàniament, pot convertir-se en l'ancoratge d'una nova forma de coerció. Per tal

que aquest instrument es mantingui al servei de la confiança i no del control, cal establir cinc principis de disseny que guiïn la seva governança.

1. Governança de nodes transparent i distribuïda. La descentralització tècnica no garanteix per si sola una democràcia digital; el poder segueix concentrat en qui controla els punts d'entrada. Com hem vist, el 2026 el 42 % dels blocs d'Ethereum es construeixen a través de relays que imposen censura OFAC i les xarxes L2 operen amb un únic seqüenciador corporatiu com Base de Coinbase [5]. Per tant, els nodes que registren la prova han d'estar subjectes a una auditoria pública continuada i a una selecció basada en criteris oberts (competència tècnica, diversitat geogràfica i compromís amb valors democràtics). La transparència ha de ser verificada per entitats independents, tal com recorda Frisby: «no confiïs, verifica», però la pregunta clau és *qui* verifica el verificador [32].

2. Dret a la revocació i a la caducitat. Un registre immutable no pot ser etern si pretén respectar els drets fonamentals de les persones. La legislació europea ha avançat cap al model «consentir o pagar», però sense un mecanisme que permeti retirar el consentiment, aquest model es converteix en una forma de captivitat [10]. Cal establir protocols que possibilitin la revocació del certificat d'identitat i la caducitat automàtica dels registres biomètrics quan deixin d'estar necessaris o siguin vulnerables a l'abús.

3. Minimització biomètrica real. La centralització de bases biomètriques, com el projecte Eurodac que ha abaixat l'edat de recollida a sis anys i la comparteix amb forces policials [28], demostra com una infraestructura pensada per a la seguretat pot ser convertida en eina de vigilància massiva. La solució passa per evitar bases centralitzades i, en el seu lloc, utilitzar proves descentralitzades basades en tècniques de «zero-knowledge» que no revelen dades sensibles però permeten validar l'existència d'un individu.

4. Auditoria algorítmica independent. Els models matemàtics que sustenten les decisions automatitzades són, segons O'Neil, opacs i accessibles només per a «els grans sacerdots del sector» [4]. Per tal de garantir que la prova no esdevingui un instrument d'injustícia, cal instituir comissions independents amb poder legal per revisar i validar els algoritmes que processen les dades biomètriques i blockchain.

5. Encriptació d'extrem a extrem com a defensa real. Snowden afirma que l'encriptació d'extrem a extrem és l'única protecció efectiva contra la vigilància, ja que converteix les dades interceptades en soroll incomprensible sense les claus [34]. Tota transmissió de proves ha d'estar protegida per aquest nivell d'encriptació, i les claus han de ser gestionades de manera descentralitzada, evitant punts únics de fallada.

Aquests principis estableixen límits funcionals contra el *mission creep* que, com avisa Zuboff, transforma l'experiència humana en matèria primera gratuïta per a l'extracció i la venda [13]. Només si s'instal·len controls democràtics —auditories independents, revocació de consentiment i una arquitectura transparent — la prova d'existència pot mantenir-se com a eina emancipadora i no com a instrument de captura. **El segell pot garantir la veritat; la cadena ha d'impedir que aquesta veritat esdevingui una gàbia**.

---

[1] Biometric Update / ICLG — *Worldcoin/World ID: prohibicions i ordres de supressió (Kenya inconstitucional; Colòmbia)* (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 — *Estat de descentralització dels L2 d'Ethereum (seqüenciadors)* (2026). https://l2beat.com/scaling/summary — i MEV Watch, *blocs amb 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 — *Accions contra data brokers (X-Mode/Outlogic) i 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 — i 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 — *Agències federals dels EUA i l'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] Consell de la UE / Pinsent Masons — *«Digital Omnibus»: ajornament de les regles d'IA d'alt risc* (maig 2026). https://www.pinsentmasons.com/out-law/news/rules-high-risk-ai-delayed-under-eu-omnibus-deal — i 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 — *Expansió d'Eurodac (edat 12→6; accés policial), Pacte de Migració 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 — *Guia d'estil (STYLE.md): «la promesa i el perill»; «res de tecno-utopia sense evidència»*.

[34] Edward Snowden — *Vigilancia permanente* (Planeta, 2019). ↩

El setge a la veritat: el testimoni que no es pot silenciar

«La nostra missió és informar d'aquests horrors de la guerra amb exactitud i sense prejudicis.»

— Marie Colvin, «Truth at all costs», St Bride's, Londres (2010)

Cap a les deu del matí del 25 d'agost de 2025, la càmera de Reuters instal·lada al capdamunt d'una escala exterior de l'hospital Nasser, a Khan Younis, al sud de Gaza — el punt que els equips de televisió feien servir des de feia dies per la seva vista de la ciutat —, emetia en directe, com cada matí. El primer míssil va impactar exactament allà. El senyal es va tallar en sec: Hussam al-Masri, el càmera de Reuters que filmava, va morir amb la seva lent. Uns deu minuts després, quan rescatadors i periodistes ja s'havien enfilat escales amunt a buscar els ferits, va arribar el segon impacte — la tàctica coneguda com a «doble toc» [3]. El balanç: almenys 22 morts, entre ells cinc periodistes — al-Masri (Reuters), Mariam Dagga (col·laboradora d'Associated Press), Mohammed Salama (Al Jazeera), Moaz Abu Taha (col·laborador de Reuters) i Ahmed Abu Aziz (Middle East Eye i Quds News Network) [1][3]. Les anàlisis posteriors dels vídeos, per part d'NBC i de CNN, hi van comptar fins a quatre municions [3]. L'oficina del primer ministre Netanyahu en va dir «un contratemps tràgic», i l'exèrcit va anunciar una investigació [3].

Hi ha una ironia atroç en aquesta escena, i convé mirar-la de cara: la prova de l'atac va quedar filmada per la mateixa càmera que l'atac destruïa. El directe de Reuters és alhora l'última imatge de Hussam al-Masri i l'evidència de com va morir. En aquesta guerra, la imatge ja no acompanya els fets: és el camp de batalla.

L'escena passa, a més, en una guerra que el món no ha pogut anar a veure: des de l'octubre de 2023, la premsa internacional té vetada l'entrada independent a Gaza [6]. I passa en el conflicte que el Committee to Protect Journalists (CPJ) descriu com «l'esforç més letal i deliberat per matar i silenciar periodistes» que hagi documentat mai [1]. Tancar la porta als de fora, matar o assenyalar els de dins, i negar les imatges que malgrat tot en surten — «muntatge», «actors», «això és IA» —: tres estratègies que convergeixen en un mateix objectiu, que cap prova no sobrevisqui. Aquest llibre sencer ha defensat que la confiança es pot tornar verificable; aquest penúltim capítol la porta on tot és més difícil i més necessari alhora: allà on informar mata i on negar és gratis. La tesi és la de sempre, portada al límit: si cada foto i cada vídeo neixen amb una prova d'existència ancorada en una cadena pública que cap estat, cap plataforma i cap consorci no controla, matar el testimoni deixa de matar la prova — i negar-la deixa de sortir de franc.

Aquest capítol camina sobre pedres que el llibre ja ha posat: la imatge com a testimoni i les credencials de contingut, al capítol 17; l'evidència de crims de guerra amb empremtes i blockchain — eyeWitness, l'Starling Lab, el Protocol de Berkeley —, al capítol 20; el testimoni orbital, al capítol 104; el dividend del mentider a les urnes, al capítol 106; la prova simètrica al carrer, al capítol 109; i la cadena de custòdia del socors — inclòs el terratrèmol de Veneçuela —, als capítols 49 i 50. Aquí totes aquestes peces es troben en el seu escenari extrem.

Un setge també informatiu

La primera capa del setge és la porta tancada. Des de l'inici de la guerra, Israel no permet l'entrada independent de periodistes estrangers a Gaza; només visites puntuals escortades per l'exèrcit, cas per cas — un format que la Foreign Press Association, que agrupa els corresponsals estrangers, denuncia com a insuficient per a cap cobertura real [6]. La cronologia judicial ho diu tot: el gener de 2024, el Tribunal Suprem israelià va rebutjar la primera petició de la FPA — no hi ha «cap dret adquirit» a entrar, va dir, i pesen les raons de seguretat —; la FPA va tornar a recórrer al setembre de 2024; van seguir pròrrogues i més pròrrogues; i el gener de 2026, ja amb l'alto el foc en vigor, el govern va tornar a dir al tribunal que el vet s'havia de mantenir «per raons de seguretat» — i el tribunal va tornar a ajornar la decisió [6]. Més de dues dotzenes d'organitzacions informatives de tot el món han reclamat conjuntament poder entrar [6]. El resultat és una anomalia històrica: la primera gran guerra d'aquest segle que el món ha vist gairebé exclusivament a través dels ulls de qui la pateix.

La segona capa és el que ha passat als que eren dins. El CPJ comptabilitza 263 periodistes i treballadors de mitjans morts des del 7 d'octubre de 2023 — a més de 108 empresonats i 174 ferits — i sosté que cap altre actor no havia matat tants periodistes des que l'organització recull dades, el 1992 [1]. L'informe «News Graveyards» del projecte Costs of War de la Universitat de Brown (abril de 2025) hi va posar una perspectiva difícil d'oblidar: més periodistes morts a Gaza que a la Guerra Civil americana, les dues

guerres mundials, Corea, el Vietnam, Iugoslàvia i l'Afganistan combinades — una comparació que cal agafar amb el matís que la mateixa base de dades històrica en què es basa desaconsella comparar èpoques amb mètodes de recompte diferents [2]. Reporters Sense Fronteres (RSF), que compta més de 210 morts i té motius raonables per creure que almenys 56 van ser atacats deliberadament per la seva feina, ha presentat cinc denúncies davant la Fiscalia del Tribunal Penal Internacional — l'última, el 30 de setembre de 2025 —, i hi documenta també el patró del doble bombardeig: un segon míssil que arriba quan els rescatadors i els reporters ja són sobre el terreny del primer [7].

Dos noms condensen el mecanisme. Anas al-Sharif, corresponsal d'Al Jazeera, va morir el 10 d'agost de 2025 en l'atac contra la tenda de premsa davant l'hospital al-Shifa, amb quatre companys més; l'exèrcit israelià el va declarar «operatiu de Hamàs», una acusació que Al Jazeera i el CPJ rebutgen. El detall que importa és anterior: ja al juliol, el CPJ i la relatora especial de les Nacions Unides Irene Khan havien alertat de la campanya de descrèdit contra ell i del risc que corria la seva vida [4]. Primer el dubte, després el míssil. I Wael al-Dahdouh, cap de la corresponsalia d'Al Jazeera a Gaza, va saber en directe, mentre informava, que un atac aeri acabava de matar la seva dona, el seu fill Mahmoud, la seva filla Sham i el seu net Adam, el 25 d'octubre de 2023. Va continuar informant [5].

I quan la premsa de fora és a la porta i la de dins és sota les bombes, el buit l'omple el testimoni. La guerra l'han explicada al món figures com Bisan Owda — reportera de vint-i-cinc anys, amb quatre milions de seguidors, que el setembre de 2024 va guanyar un Emmy per «It's Bisan From Gaza — and I'm Still Alive», malgrat una campanya per desqualificar-la — o el fotoperiodista Motaz Azaiza, les imatges del qual van donar la volta al món [8]. A Gaza, la frontera entre el fotoperiodista professional i el testimoni ciutadà s'ha esborrat: sovint són la mateixa persona, amb el mateix mòbil. I això fa inevitable la pregunta d'aquest capítol: quina força probatòria té el que graven?

«Fake»: el dividend del mentider en temps de guerra

El llibre ha vist el dividend del mentider a les urnes (capítol 106) i sap que detectar no basta (capítol 15). La guerra n'ensenya la forma més crua: no cal falsificar res — n'hi ha prou de dir «fals» a tot. «Pallywood», l'acusació que els palestins escenifiquen el patiment, va viure una explosió mesurable: BBC Verify va comptar un pic de 220.000 usos del terme a X només el novembre de 2023 [9]. Les «proves» que l'acompanyaven solien ser material reciclat — una protesta egípcia de 2013, una disfressa de Halloween tailandesa, un rodatge publicitari a Algèria —, presentat com si fos Gaza [9].

Dos casos ensenyen les dues cares del mecanisme. El primer: el Jerusalem Post va publicar — i després va haver de retirar — que el cos d'un nadó palestí de cinc mesos era una nina; el compte oficial d'Israel a X va amplificar l'acusació; la BBC va localitzar la família i els fotògrafs i va confirmar que era el cos real d'un infant [9]. El segon, invers i encara més corrosiu: una foto difosa per Israel del cos carbonitzat d'un nadó assassinat el 7 d'octubre va ser titllada massivament de «generada per IA» perquè un detector comercial, «AI or Not», va donar positiu. L'empresa va acabar reconeixent el fals positiu — culpa de la compressió i d'una etiqueta difuminada —, i diversos experts van considerar la foto genuïna [9]. La lliçó talla en els dos sentits: els detectors s'equivoquen amb fotos falses i amb fotos reals, i un detector dolent és el somni del negacionista — qualsevol imatge autèntica es pot «desmentir» amb una eina gratuïta i una captura de pantalla.

El sociòleg Ron Dudai ho ha descrit amb precisió: les velles teories conspiratives, elaborades i laborioses, han donat pas a una forma més crua de negacionisme — la documentació es descarta amb una sola paraula, «Fake» [9]. I el descrèdit no es queda en la retòrica: RSF documenta com les acusacions de «muntatge» contra els periodistes gazians — el que anomena «Gazawood» — els converteixen en objectius [7]. És el camí que va recórrer al-Sharif: el dubte sembrat al juliol va precedir el míssil de l'agost [4].

El dividend del mentider no té bandera: el cobra qualsevol poder interessat que una imatge no existeixi — a Gaza, a Síria, on sigui —, i el paga sempre el mateix: el testimoni que diu la veritat i no ho pot demostrar. Contra un «fals!» que costa zero, la resposta no pot ser un peritatge que costa mesos. Ha de ser una prova que ja existia.

Quan el setge és a casa: Minneapolis, hivern de 2026

No cal una zona de guerra ni una dictadura perquè el mecanisme es dispari. El desembre de 2025, el Departament de Seguretat Nacional dels Estats Units va llançar sobre Minneapolis i Saint Paul l'operació Metro Surge — «la major operació de control migratori mai duta a terme», en paraules del mateix

departament —: milers d'agents del Servei d'Immigració i Duanes (ICE) i de la Patrulla Fronterera, més de quatre mil al punt àlgid segons les xifres que un jutge va haver d'obligar a revelar, i prop de tres mil vuit-centes detencions en dos mesos, menys d'una quarta part amb antecedents penals [21]. La ciutat era, precisament, aquella on el vídeo d'una adolescent amb un mòbil havia canviat la història el 2020 (capítol 109). El que hi va passar és l'experiment més net que existeix sobre la pregunta d'aquest llibre: què val el testimoni quan qui nega és el mateix estat.

Renée Good: tres trets i massa càmeres

El 7 de gener de 2026 al matí, Renée Good — trenta-set anys, escriptora, ciutadana nord-americana — era al volant del seu cotxe en un carrer del sud de Minneapolis, aturada perpendicularment al pas d'uns vehicles federals; hi anaven també la seva parella, una criatura de sis anys i el gos [22]. L'agent d'ICE Jonathan Ross li va disparar tres trets. La versió oficial va arribar en hores i des de dalt de tot: la secretària de Seguretat Nacional, Kristi Noem, va afirmar que Good havia intentat «atropellar i envestir» els agents i que duia tot el dia «assetjant i obstruint» l'operatiu — d'això últim no se n'ha presentat mai cap prova —, i el president Trump va escriure que havia atropellat l'agent «de manera violenta, deliberada i acarnissada» i que aquest «es recuperava a l'hospital» [22].

Els vídeos deien una altra cosa, i n'hi havia molts: de testimonis, de càmeres de vigilància i del mòbil del mateix Ross. La reconstrucció del New York Times va fixar la seqüència — un tret al parabrisa i dos més, a curta distància, per la finestreta de la conductora, amb el cotxe girant per allunyar-se i l'agent dret, a uns passos, fora de la trajectòria —, i un altre àngle mostrava Good, pocs minuts abans, cedint el pas als vehicles federals i fent-los senyal que passessin [22]. I un detall que val un tractat sencer: la gravació del mateix Ross se sacseja cap amunt just al moment decisiu, i el deixa fora de quadre [22]. El registre de l'estat va quedar cec exactament quan més calia; els dels ciutadans, no.

Alex Pretti: el testimoni tirotejat

Disset dies després — l'endemà d'una vaga general que havia omplert el centre de la ciutat [21] —, l'operatiu va matar Alex Pretti: trenta-set anys, infermer de cures intensives a l'hospital de veterans, ciutadà nord-americà, sense antecedents i amb permís d'armes en regla, com va confirmar el cap de la policia de Minneapolis [23]. Pretti era aquell matí una de les persones que documentaven amb el mòbil un operatiu d'ICE — la figura exacta del testimoni del capítol 109. La secretària Noem va declarar que s'havia acostat als agents «amb una pistola»; el departament hi va afegir que volia «fer el màxim dany i massacrar les forces de l'ordre» i que duia «dos carregadors i cap mena d'identificació»; el subcap de gabinet de la Casa Blanca, Stephen Miller, en va dir «terrorista domèstic» [23].

Els vídeos dels presents — múltiples angles, revisats i verificats per Reuters, la BBC, el Wall Street Journal, AP, CNN, el New York Times i The Guardian — mostren una seqüència diferent: Pretti amb el telèfon a la mà dreta; ruixat amb esprai de pebre quan mirava d'ajudar una dona que havia caigut; mitja dotzena d'agents immobilitzant-lo a terra; un agent traient-li la pistola de la funda del maluc — i, un segon després, un altre disparant-li a boca de canó una desena de trets en cinc segons, els últims quan ja jeia immòbil [23]. Cap agent no li va practicar la reanimació, i una pediatra que es va oferir va ser apartada [23]. La forense del comtat va dictaminar la mort: homicidi [23]. I els noms dels dos agents no els va fer públics el govern: els va publicar ProPublica [24].

El setge a l'evidència

La densitat va fer la seva feina. Les versions oficials no van aguantar ni una setmana: l'alcalde i el governador, després de veure els vídeos, van desmentir públicament el relat federal [23]; un jutge federal va comptar almenys noranta-sis ordres judicials violades per ICE en un mes, i un altre va constatar que la «majoria aclaparadora» dels detinguts era al país legalment [21]; i el 12 de febrer, el «tsar de la frontera» de la Casa Blanca anunciava la fi de l'operatiu en una roda de premsa on va evitar pronunciar els dos noms [21].

Però la mateixa maquinària va tancar files al voltant de la prova: l'endemà del primer tiroteig, l'FBI va revocar a l'agència d'investigació criminal de l'estat l'accés a les evidències [22]; a l'abril, el mòbil de Pretti seguia retingut, el cotxe de Good continuava precintat en un magatzem federal sense que cap investigador estatal l'hagués pogut examinar, i els noms i expedients dels agents es negaven sistemàticament [24]. Minnesota i el comtat de Hennepin van haver de presentar una demanda per obtenir unes proves que — sostenen — es retenen «per escudar els agents implicats» [24]. Mentre escrivim això, cap agent no ha estat acusat de res: l'home que va disparar contra Renée Good va estar tres dies apartat del servei i mesos

després operava en un altre estat [22], i l'única mesura disciplinària coneguda de tot l'operatiu són dos agents en permís administratiu per «declaracions falses» sobre el tercer tirotejat, un home ferit de bala a la cama [24]. La fiscal del comtat manté obertes disset investigacions penals contra un mur d'immunitats [24]. «Sembla que estiguin impedint activament que l'estat investigui», ho resumia una professora de dret [24].

El patró: Chicago, Houston

Minneapolis no és una anomalia: és el cas més ben documentat d'un patró. Tres mesos abans, a Chicago, un agent havia disparat cinc trets a Marimar Martinez, una mestra que seguia els vehicles federals tocant el clàxon per avisar els veïns — i l'acusada d'envestir-los va ser ella; la càmera corporal va acabar mostrant el vehicle dels agents girant cap al seu just després que un digués «és hora de posar-se agressius», i els missatges del mateix agent presumint-ne — «cinc trets i set forats» —; els càrrecs contra ella es van arxivar amb caràcter definitiu [25].

Aquell mateix novembre, la jutgessa federal Sara Ellis va confrontar, en un dictamen de dues-centes vint-i-tres pàgines, els informes oficials d'ús de la força amb els vídeos de les càmeres corporals que ella mateixa havia ordenat activar: el relat del govern era «senzillament no creïble», el cap de l'operatiu havia anat canviant sota jurament l'ordre dels fets — el gas llançat abans de la pedra que deia haver rebut —, i un agent havia redactat l'informe oficial d'un incident amb ChatGPT a partir d'«una frase breu sobre una trobada i diverses imatges» [25]. Convé aturar-se en aquest últim detall: en la disputa per la realitat entre el ciutadà i l'estat, el relat sintètic era l'oficial. El recompte acumulat des del gener de 2025 arriba als trenta-vuit tirotejos per agents d'immigració, amb nou morts [25]. I no s'atura: el 7 de juliol de 2026, mentre s'acabava d'escriure aquest capítol, un home de cinquanta-dos anys moria a Houston per un tret d'un agent d'ICE que al·lega — un cop més — una envestida; els agents no duien càmeres corporals, els relats sobre els moments previs es contradiuen, i la forense del comtat n'ha dictaminat l'homicidi [26].

El contrafactual: un sol testimoni, sense àncora

Ara, l'exercici que aquest llibre no es pot estalviar. Repetiu el 7 de gener amb una sola variació: no hi ha multitud. Cap càmera de vigilància apuntant al carrer, cap veïnat congregat; només algú que, espantat, ho grava d'amagat des d'una finestra — i que triga setmanes a fer-ho públic, perquè té por. Per a llavors, la versió oficial ja fa un mes que és «la veritat»: consta en declaracions, en compareixences, en boca del president. Quan el vídeo surti, el manual que aquest capítol ja ha descrit es disparà sol: «muntatge», «actors», «és IA» — i n'hi haurà prou amb un detector gratuït i un fals positiu com el que ja hem vist [9] per fabricar-ne el «desmentiment».

Contra la paraula jurada d'un estat, un fitxer sense data certa ni integritat demostrable és només això: un fitxer. Perquè el que va salvar la veritat a Minneapolis no va ser cap institució: va ser la densitat — massa càmeres, massa testimonis, massa angles per negar-los tots alhora. I la densitat és un accident: hi era perquè l'operatiu era massiu i contestat, i la comunitat, avisada i mirant. La propera Renée Good pot tenir un sol testimoni; el proper Alex Pretti, cap. I allà on no queden contrapesos — cap jutge que compti ordres violades, cap fiscal de comtat que pugui demandar, cap vaga general — la versió oficial no és que guanyi: és l'única que existeix. En un estat així, obertament dictatorial, el testimoni de la finestra no té un vídeo: té una acusació de falsificació esperant-lo.

Amb la prova d'existència, el mateix escenari canvia de física. Si el vídeo clandestí es va segellar en néixer — l'empremta, i només l'empremta, va sortir del mòbil cap a l'àncora pública, amb la data del mateix 7 de gener [20] —, el testimoni pot esperar setmanes o anys, o revelar-lo des de l'exili: la seva àncora serà sempre anterior al relat oficial, i el «això s'ha fabricat després» deixa de ser una sortida. És exactament el que no pot oferir cap registre que depengui del poder: la càmera de l'agent que s'alça al moment decisiu, el mòbil retingut, el cotxe precintat — cada buit convenient del registre oficial es fa visible quan la resta de proves porten data certa i integritat verificable. I la simetria que aquest capítol reivindica més avall val aquí en les dues direccions: el mateix segell hauria emparat un agent que digués la veritat. No demana confiar en ningú; només fa que mentir surti car, en totes direccions.

Quan la multitud hi és, la veritat pot guanyar per densitat; quan només hi ha un testimoni, tot es juga en si la seva prova va néixer segellada. I quan no hi ha ni multitud ni segell, queda l'ofici lent de refer els fets a posteriori — un ofici heroic el preu del qual, en temps i en dubte, és el que ve ara.

La forènsica de després: guanya, però tard

La reconstrucció forense independent és l'heroïna d'aquesta guerra informativa. I alhora, la demostració de quant costa arribar tard. Tres casos, en gradació.

Shireen Abu Akleh: quatre mesos per tombar una versió

Shireen Abu Akleh, corresponsal d'Al Jazeera, va morir d'un tret al cap l'11 de maig de 2022 a Jenin, amb casc i armilla de PREMSA. La primera versió oficial va apuntar a foc palestí indiscriminat. El que va venir després és la cadència exacta del desmentiment: la investigació de CNN (24 de maig) no va trobar cap combat actiu a prop i, amb testimonis i anàlisi d'àudio, va apuntar a foc israelià; AP, el New York Times i el Washington Post van publicar reconstruccions coincidents; l'Oficina de Drets Humans de l'ONU va concloure al juny que els trets venien de les forces israelianes — «diversos trets aïllats i aparentment ben apuntats» —; els Estats Units van avaluar al juliol que el més probable era foc israelià, amb una bala massa danyada per a una balística concloent; i el 5 de setembre de 2022 l'exèrcit israelià va admetre que «probablement» l'havia morta un dels seus soldats. Sense càrrecs [11]. Gairebé quatre mesos i mitja dotzena d'investigacions independents per tombar la primera versió — amb accés al terreny, en relativa calma i amb una víctima famosa. A Gaza, sense accés, aquest camí es multiplica — o es torna impossible.

Hind Rajab: 355 impactes i una trucada

Hind Rajab tenia sis anys. El 29 de gener de 2024 va quedar atrapada en un cotxe tirotejat a la ciutat de Gaza, envoltada dels cossos de la seva família, i va suplicar auxili per telèfon a la Mitja Lluna Roja Palestina; el seu cos, el de sis familiars i el dels dos sanitaris de l'ambulància que havia sortit a buscar-la van aparèixer dues setmanes després. La reconstrucció de Forensic Architecture amb l'ONG Earshot i Al Jazeera va establir que el cotxe havia rebut 355 impactes de bala; i l'anàlisi acústica de la trucada — l'interval entre el so de cada impacte i el de la boca de canó — va situar el tirador a entre 13 i 23 metres [12]. Val la pena aturar-se en què és, aquí, la prova central: l'àudio d'una trucada de mòbil. El testimoni digital espontani ja decideix investigacions internacionals; el que encara no té és una manera de néixer indiscutible.

Les fotos Caesar: una dècada fins a Coblença

I el precedent que tanca el cercle ve de Síria, d'una dictadura: un fotògraf forense de la policia militar siriana, nom en clau «Caesar», va fugir el 2013 amb unes 53.000 fotografies de morts sota tortura a les presons del règim. Autenticar-les va costar anys — peritatges de les metadades del sistema del mateix règim, que numerava dispositius i registres, i una anàlisi mèdica forense de milers d'imatges a càrrec d'experts de la Universitat de Colònia, que hi va trobar tortura i mort sistemàtiques [13]. El 13 de gener de 2022, el tribunal de Coblença, a Alemanya, jutjant per jurisdicció universal, va condemnar Anwar Raslan, excap d'interrogatoris de la Branca 251, a cadena perpètua per crims contra la humanitat — amb les fotos Caesar com a peça clau [13]. Entre el risc de mort d'un home traient discos durs d'un país en guerra i la sentència: gairebé una dècada. El coratge va salvar la prova; el sistema va trigar deu anys a poder-se'n fiar.

Tribunals que esperen, proves que no arriben

Aquesta evidència, quan arriba, ja té on anar. El Tribunal Penal Internacional va emetre el 21 de novembre de 2024 ordres de detenció contra Benjamin Netanyahu i Yoav Gallant — pel crim de guerra de la fam com a mètode de guerra i per crims contra la humanitat — i contra el comandant de Hamàs Mohammed Deif [14]; el Tribunal Internacional de Justícia, en el cas presentat per Sud-àfrica sota la Convenció del Genocidi, va dictar mesures provisionals vinculants el gener, el març i el maig de 2024 [15]; i el marc per acceptar evidència digital de fonts obertes — el Protocol de Berkeley — ja existeix (capítol 20). No falten tribunals. Falta que la prova hi arribi sencera, ràpida i indiscutible.

Perquè quan no hi arriba, passa el que va passar amb l'hospital al-Ahli. L'explosió del 17 d'octubre de 2023 — 471 morts segons el Ministeri de Salut de Gaza; entre 100 i 300 segons la intel·ligència nord-americana — va posar els millors equips forenses del món a treballar sobre els mateixos vídeos. I van divergir: AP, CNN i altres mitjans van concloure que el més probable era un coet fallit llançat des de Gaza; el New York Times va acabar dient que la causa era incerta; Human Rights Watch hi va veure el patró d'un coet propulsat però va exigir una investigació independent; Forensic Architecture va concloure que el projectil venia de la direcció d'Israel [10]. Sense accés al cràter, amb vídeos repujats i retallats, sense hora certa ni integritat verificable dels fitxers clau, la mateixa evidència va sostenir conclusions oposades — i cada bàndol es va quedar amb la seva. La forènsica no va fallar: li van faltar els fonaments. Exactament els que un segell a l'origen li hauria donat.

Segellar a l'origen: la premsa acreditada sota setge

Que una redacció pot segellar el que publica ja no és una hipòtesi. Reuters i l'Starling Lab ho van assajar el 2020 i 2021 amb «78 Days»: durant els setanta-vuit dies de la transició presidencial nord-americana — assalt al Capitoli inclòs —, més de dues-centes fotografies es van capturar amb metadades criptogràfiques i es van ancorar en cadenes públiques, amb la procedència de cada imatge verificable per qualsevol lector [18]. Si es va poder fer per a una transició política a Washington, es pot fer per a una guerra. És exactament on més cal.

El flux de t2p per a la premsa comença al dispositiu de qui dispara: l'empremta SHA-512 — calculada al mòbil, dels bytes exactes del fitxer — rep el seu segell de temps RFC 3161/eIDAS i queda ancorada a la blockchain pública; la imatge no surt del dispositiu per generar la prova [20]. La posició GPS s'hi afegeix quan és fiable. I tot plegat viatja en un paquet .asice verificable fora de línia, de la zona de conflicte a la redacció i, si cal, a la fiscalia — la mateixa cadena de custòdia que el capítol 50 aplica al socors, aplicada al testimoni [20]. És, de fet, el que el Protocol de Berkeley demanarà demà a qualsevol prova (capítol 20), generat per defecte avui.

La credencial resol l'altra meitat del problema: l'agència signa la vinculació — «aquest material és d'un col·laborador acreditat nostre» — sense publicar qui és ni on és, la divulgació selectiva del capítol 20 [20]. La redacció pot demostrar la procedència davant del lector i davant del jutge, i alhora protegir la persona. I si la maten — a Gaza no és una clàusula d'estil [1] —, el seu arxiu segellat continua provant què va veure i quan. Matar el missatger deixa de matar el missatge.

I aquí és on la doctrina d'aquest llibre es torna literal. Les credencials de contingut signades a la càmera (capítol 17) són el complement perfecte — però són metadades que viatgen amb el fitxer, i una repujada les esborra; i tot sistema de certificació té un propietari, i tot propietari té una finestreta on trucar. L'àncora en una cadena pública no en té: cap govern — tampoc el que nega les imatges — no pot despublicar una empremta ni retrodatar-la. El capítol 112 preguntava qui controla la prova; aquí la resposta decideix vides: quan l'acusat és un estat, la prova no pot dependre de cap autoritat que aquest estat pugui pressionar. La neutralitat de la cadena no és una virtut abstracta — és el requisit tècnic perquè la prova valgui contra qualsevol poder, el propi inclòs.

El testimoni amb el mòbil: la mateixa prova per a tothom

La idea que el testimoni ciutadà mereix eines de prova no és nova. WITNESS i el Guardian Project van llançar ProofMode el 2017: una aplicació gratuïta que signa i calcula l'empremta de cada foto i vídeo al moment de la captura, amb una instantània dels sensors, i en notaritza l'empremta — amb OpenTimestamps, l'ancoratge a Bitcoin que el llibre ja coneix, entre els seus sistemes de notaria [19]. I eyeWitness to Atrocities fa una cosa semblant des de 2015 per a documentadors entrenats, amb més de 20.000 ítems ja usats com a prova judicial (capítol 20). El que faltava no és la idea: és que sigui universal, per defecte, i pensada per a qui no és activista ni periodista — per a qualsevol persona que un matí es troba gravant el pitjor dia de la seva vida.

Per a aquest escenari — el pitjor — el segell ha de tenir quatre propietats, i cap és opcional.

Només l'empremta surt del mòbil. La foto no es puja enlloc per generar la prova: el dispositiu calcula l'empremta SHA-512 i és això — només això — el que rep el segell de temps i l'àncora a la blockchain pública [20]. En un control militar, en un escorcoll, no hi ha cap pujada que delati el testimoni; la imatge pot viure xifrada o en una còpia fora del dispositiu, i l'empremta ancorada espera el seu moment.

Segella ara, publica quan sigui segur. És el compromís i revelació dels capítols 45 i 46, aplicat a la supervivència: la víctima segella avui l'empremta del vídeo i el revela d'aquí a un mes, un any, o des de l'exili — i la data certa que compta és la d'avui. El negacionista que digui «això s'ha fabricat després» xoca contra una àncora anterior a la seva pròpia negació.

La prova pòstuma. Si el testimoni mor — i 263 vegades no és una hipòtesi [1] —, el segell sobreviu: qualsevol que tingui la còpia pot demostrar què existia i quan. L'arxiu de cada Bisan i de cada Motaz [8] esdevé indestructible per decapitació: es pot matar qui grava; no es pot matar el fet que allò ja estava gravat.

La simetria. Aquesta prova no distingeix bàndols: el vídeo d'un civil israelià el 7 d'octubre i el d'una família de Khan Younis sota les bombes tenen exactament la mateixa força d'ancoratge. És la prova

simètrica del capítol 109: la càmera de Darnella Frazier va valdre perquè era autèntica, no perquè fos de ningú. La tecnologia que empara el testimoni palestí empara igual l'israelià, l'ucraïnès i el sudanès — i per això, i només per això, pot aspirar a ser un estàndard global.

Queda el límit ètic, i és innegociable (capítols 49 i 50): mai biometria obligatòria per a les víctimes. La prova de vida i el vídeo-selfie són opcions per a qui vol reivindicar l'autoria — no un peatge. Qui documenta un crim no ha de pagar amb la seva identitat; i la geolocalització es revela quan el testimoni decideix, no abans (capítol 20).

La promesa i el perill

La promesa és una guerra on el vet d'accés ja no fabrica foscor, perquè cada mòbil de dins és un notari [19] [20]; on el «fake!» reflex es respon amb una empremta datada i no amb un peritatge de mesos [9]; on el proper al-Ahli es dirimeix sobre vídeos amb hora certa i integritat verificable [10]; on l'arxiu del periodista mort continua acusant [1]; i on la fiscalia del TPI rep paquets d'evidència que compleixen el Protocol de Berkeley per defecte [14] (capítol 20). La veritat continuarà costant vides; almenys, que no es pugui enterrar amb elles.

La possessió que mata — un mòbil amb un arxiu segellat pot ser una sentència en un escorcoll. El disseny ho ha d'assumir: només empremtes fora del dispositiu, contingut xifrat o fora del mòbil, revelació diferida [20]. Però cap arquitectura no elimina el risc físic del testimoni — i prometre invulnerabilitat seria mentir. El segell protegeix la prova; protegir la persona continua sent feina del dret, dels mitjans que publiquen — i responsabilitat de qui la vol callar.

L'apagada — sense xarxa no hi ha àncora: Gaza acumula almenys vint-i-tres apagades de comunicacions documentades des de l'octubre de 2023, per atacs a la fibra i per manca de combustible — la connectivitat civil convertida en mitjà i mètode de guerra, en paraules d'Access Now [16]. El segell local es genera igual i s'ancora quan torna el senyal; però llavors la cadena només prova el «no després». El remei parcial és el sandvitx temporal: incorporar a la captura un valor públic recent i impredictible — l'empremta de l'últim bloc conegut abans de l'apagada — prova el «no abans», i l'àncora posterior, el «no després». La finestra queda tancada per les dues bandes; i més val una forquilla honesta de dies que una promesa falsa d'instantaneïtat.

El GPS que menteix — a la regió, la pertorbació i la suplantació del senyal GPS són massives i estan documentades: més de 50.000 vols afectats el 2024, aplicacions civils situant usuaris a Beirut o al Caire [17]. Un sistema honest ho reconeix: quan el senyal no és fiable, la posició es degrada o s'omet — i el valor central del segell, l'hora certa i la integritat, no en depèn [20]. Una geolocalització suplantada presentada com a certa faria més mal que cap geolocalització.

El segell no santifica — la prova d'existència acredita quan existia un fitxer i que ningú no l'ha tocat: no acredita què passava fora d'enquadrament, ni impedeix segellar una escenificació el mateix dia. Qui vulgui fer teatre amb data certa, podrà. La resposta és la de sempre en aquest llibre: corroboració — més testimonis, més angles, el satèl·lit (capítol 104), la forènsica (capítol 15) — sobre una base que almenys ja no es discuteix: quins fitxers, de quan, sense retocs. El segell no substitueix el periodisme ni el peritatge: els estalvia la meitat estèril de la feina.

El registre que persegueix — el mateix rastre que empara el testimoni pot desanonimitzar-lo si es dissenya malament (capítol 20): àncores enllaçables entre si, metadades que dibuixen patrons, geolocalització per defecte. Divulgació selectiva, identificadors no correlacionables i control del testimoni sobre cada camp no són extres de luxe: són la diferència entre una eina de drets humans i una llista de deteccions a disposició del perseguidor.

És hora d'actuar

El setge a la veritat es combat abans que comenci — quan la foto neix.

Per a les agències i els mitjans: el precedent de «78 Days» ja us ha ensenyat el camí [18] — feu del segell a la captura l'estàndard de tot material de zona de conflicte, propi o de col·laborador; publiqueu la procedència verificable amb cada peça; i signeu la credencial dels vostres col·laboradors locals sense exposar-los [20]. El seu risc ja és el màxim: que almenys la seva paraula no es pugui esborrar.

Per als fotoperiodistes i col·laboradors dins la zona: segelleu-ho tot, encara que no ho publiqueu — el compromís i revelació [20] permet documentar avui i revelar quan sigueu fora; i la vostra agència o la vostra família podran provar-ho encara que vosaltres ja no hi sigueu. L'armilla de PREMSA no atura míssils; l'empremta ancorada no atura mentides — però les fa caducar.

Per a les organitzacions de drets humans i les fiscalies internacionals: exigiu i ensenyeu el segell a l'origen — les investigacions com les d'Abu Akleh, Hind Rajab o els arxius Caesar [11][12][13] haurien guanyat mesos o anys; el Protocol de Berkeley (capítol 20) ja us dona el marc per acceptar-lo; i cada taller de documentació segura en una zona de conflicte val més que deu comunicats posteriors.

Per als ciutadans i les víctimes: el vostre mòbil és un notari que no demana permís a ningú [19][20]. Segelleu el que veieu — només l'empremta surt del dispositiu; publiqueu quan sigui segur; i si trieu l'anonimat, la prova valdrà igual. Ningú no us pot exigir la identitat com a preu del dret que us creguin.

Per a les plataformes: preservar les credencials i les empremtes del material de conflicte en lloc d'esborrar-les en recomprimir (capítol 17) és la diferència entre ser el canal del testimoni o el seu triturador; i etiquetar la procedència verificada — sense censurar el que no la té — dona al lector el criteri que els detectors no li poden donar [9].

Per als governs democràtics i els organismes internacionals: si el compromís amb la premsa lliure és de debò, val també quan la guerra és vostra o d'un aliat — accés per a la premsa acreditada [6], connectivitat civil protegida [16], i reconeixement processal de la prova d'existència, perquè el testimoni de la propera guerra no depengui del coratge d'un funcionari fugint amb 53.000 fotos [13].

Al capdavall, tot aquest llibre — i aquest capítol més que cap altre — defensa una cosa antiga: que el testimoni d'una persona val, i que la seva paraula mereix poder ser creguda. La tecnologia només hi afegeix el que la força sempre li ha volgut prendre: la prova. Per tots els qui van gravar fins a l'últim segon, **time2act**.

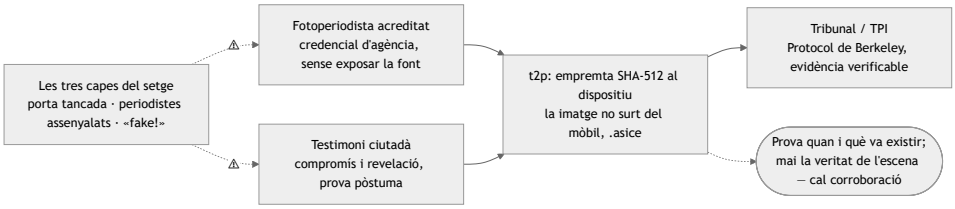


Figura 113.1 — La prova sota setge, de l'objectiu al tribunal (t2p: empremta SHA-512 al dispositiu — la imatge no surt del mòbil —, segell RFC 3161/eIDAS, àncora a la blockchain pública, paquet .asice): el fotoperiodista acreditat amb credencial d'agència sense exposar la font; el testimoni ciutadà amb compromís i revelació (segella ara, publica quan sigui segur) i prova pòstuma; les tres capes del setge (porta tancada a la premsa internacional, periodistes locals morts o assenyalats, «fake!» contra les imatges reals) i on les trenca el segell. Límits: l'apagada retarda l'àncora (sandvitx temporal «no abans / no després»); el GPS suplantat degrada la posició, no l'hora; el segell prova quan i què — mai la veritat de l'escena: la corroboració continua sent imprescindible. Fonts: CPJ; RSF; Costs of War (Brown); OHCHR; Forensic Architecture; ECCHR/Coblença; Access Now; Starling Lab/Reuters; WITNESS/Guardian Project.

---

[1] CPJ (Committee to Protect Journalists) — *Israel-Gaza War* (263 periodistes i treballadors de mitjans morts des del 7-oct-2023; 108 empresonats; 174 ferits; «l'esforç més letal i deliberat per matar i silenciar periodistes que el CPJ hagi documentat mai») i *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), projecte Costs of War — *News Graveyards: How Dangers to War Reporters Endanger the World* (Nick Turse, 1-abr-2025: més periodistes morts a Gaza que a les grans guerres del segle XX combinades — comparativa que la mateixa base de dades usada matisa; ~13 periodistes palestins morts 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 impacte ~10:00 contra la posició de la càmera de Reuters — que emetia en directe — i segon impacte ~10 min després contra rescatadors i periodistes; ≥22 morts, 5 periodistes: 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 i quatre companys, 10-ago-2025; l'alerta prèvia del CPJ i de la relatora de l'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 dona, el fill Mahmoud, la filla Sham i el net Adam de Wael al-Dahdouh) i *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 vet d'accés de la premsa internacional a Gaza: rebuig de la petició de la FPA (gen-2024, «no vested right»), nova petició (set-2024), el govern manté el vet «per raons de seguretat» malgrat l'alto el foc (gen-2026) i el Suprem ajorna de nou (28-gen-2026); més de dues dotzenes d'organitzacions informatives reclamen accés. 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 (Reporters Sense Fronteres) — *RSF files fifth complaint with ICC about Israeli war crimes against journalists in Gaza* (30-set-2025; cinc denúncies des d'oct-2023; ≥210 periodistes morts, 56 amb motius raonables de creure'ls deliberadament atacats; patró de «doble bombardeig») i *«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-set-2024, «It's Bisan From Gaza — and I'm Still Alive»; ~4 milions de seguidors; campanya de desqualificació fallida) i 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* i *Pallywood* (pic de 220.000 usos a X el nov-2023 segons BBC Verify; el cas de la «nina» publicat i retirat pel Jerusalem Post i amplificat pel compte oficial d'Israel a X; el fals positiu del detector «AI or Not» sobre una foto real; Ron Dudai: la documentació descartada amb una sola paraula, «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 — l'explosió a l'hospital al-Ahli (17-oct-2023; 471 morts segons el Ministeri de Salut de Gaza, 100-300 segons la intel·ligència dels EUA) i la divergència forense: HRW (patró consistent amb coet propulsat; cal investigació independent), CNN i AP (coet fallit des de Gaza, el més probable), NYT (causa incerta), Forensic Architecture (projectil des de la direcció d'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 — l'assassinat de Shireen Abu Akleh (11-mai-2022): conclusió de l'ONU (jun-2022: trets de les forces israelianes, «aparentment ben apuntats»), investigació de CNN (24-mai-2022) i admissió de l'exèrcit israelià (5-set-2022: «probablement» foc propi; sense càrrecs). 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-gen-2024: 355 impactes al cotxe; anàlisi acústica de la trucada: trets des de 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 — els arxius Caesar (~53.000 fotos tretes de Síria el 2013; autenticació pericial de metadades i forènsica mèdica) i la condemna de Coblença (13-gen-2022: cadena perpètua a Anwar Raslan per crims contra la humanitat). 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; crim de guerra de fam com a mètode de guerra; crims contra la humanitat; ordre també 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 Justícia — *Application of the Genocide Convention (South Africa v. Israel)*, mesures provisionals de 26-gen-2024, 28-mar-2024 i 24-mai-2024 (vinculants). 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 apagades de comunicacions des d'oct-2023, per atacs a la fibra i manca de combustible; «la connectivitat civil convertida en mitjà i mètode de guerra») i *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 — pertorbació i suplantació de GPS a la regió (2024: >50.000 vols afectats; increment ×6; aplicacions situant usuaris a Beirut o al Caire; una base aèria israeliana assenyalada com a 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→gen-2021: >200 fotos de la transició presidencial amb metadades criptogràfiques ancorades a Filecoin i Hedera; procedència verificable per qualsevol).

https://www.starlinglab.org/78days/ · https://contentauthenticity.org/blog/cai-spotlight-78-days-from-stanford-starling-lab-and-reuters ↩

[19] Guardian Project / WITNESS — *ProofMode* (des de 2017: signatura OpenPGP i empremta a la captura, instantània de sensors, notarització — amb OpenTimestamps entre els sistemes suportats; pensada per a la documentació ciutadana de drets humans). https://guardianproject.info/apps/org.witness.proofmode/ · https://blog.witness.org/2017/04/proofmode-helping-prove-human-rights-abuses-world/ ↩

[20] t2p — manual de producte (empremta SHA-512 calculada al dispositiu — només l'empremta surt del mòbil —; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; GPS forense amb degradació honesta; mode fora de línia amb ancoratge diferit; compromís i revelació; paquet .asice verificable sense connexió; certificat amb QR). Vegeu els capítols 13 i 15; el compromís i revelació, als capítols 45 i 46; la cadena de custòdia del socors, al capítol 50; la divulgació selectiva i l'evidència de crims de guerra, al capítol 20; les credencials de contingut, al capítol 17. ↩

[21] Wikipedia (EN) — *Operation Metro Surge* (4-des-2025 → feb-2026: «the largest immigration enforcement operation ever carried out» segons el DHS; milers d'agents d'ICE i CBP a Minneapolis–Saint Paul; ≥3.789 detencions, menys d'un 25 % amb antecedents; la vaga general del 23-gen-2026; el jutge Schiltz: ≥96 ordres judicials violades per ICE des de l'1-gen; el jutge Blackwell: la «majoria aclaparadora» dels detinguts, amb presència legal); NPR — *Minnesota ICE crackdown will end* (12-feb-2026: Tom Homan anuncia el final de l'operatiu — que «ha costat la vida a dos ciutadans nord-americans» — sense esmentar-ne els noms); Sahan Journal — les xifres del desplegament (més de 4.000 agents al punt àlgid), revelades per ordre 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-gen-2026, Portland Avenue, Minneapolis: l'agent d'ICE Jonathan Ross dispara tres trets — parabrisa i finestreta de la conductora — amb el vehicle girant per allunyar-se, segons la reconstrucció del New York Times; al cotxe, la parella i una criatura de sis anys; les al·legacions de Noem i de Trump; la gravació del mateix Ross, sacsejada cap amunt al moment crític; l'accés de l'agència estatal d'investigació a les proves, revocat l'endemà; Ross, tres dies apartat i reassignat fora de l'estat); The Intercept — *Video Shows ICE Agent's Fatal Shooting of Civilian in Minneapolis* (el tret a curta distància contra el vehicle que marxava; un segon àngle mostra Good cedint el pas als vehicles federals minuts abans). 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-gen-2026, Minneapolis: infermer d'UCI de l'hospital de veterans, 37 anys, permís d'armes i cap antecedent; els vídeos dels testimonis, revisats i verificats per Reuters, BBC, Wall Street Journal, AP, CNN, New York Times i The Guardian: el telèfon a la mà, l'esprai de pebre, els agents immobilitzant-lo, l'arma treta de la funda i els trets un segon després; les al·legacions del DHS — «màxim dany», «dos carregadors i cap mena d'identificació» — i de Stephen Miller; la forense del comtat de Hennepin: homicidi; els agents, identificats per ProPublica); NPR — *Videos refute DHS account of fatal shooting* (25-gen-2026: Noem — «s'havia acostat amb una pistola» — contra els vídeos: no va treure mai cap arma; filmava amb el mòbil); The Marshall Project — *How Many People Have Been Killed by ICE and Border Patrol?* (26-gen-2026: cap reanimació dels agents; una pediatra apartada; en el cas Good, tres minuts sense trucar a emergències; el desmentiment públic de l'alcalde Frey i el governador Walz després de veure els 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 comtat de Hennepin i l'agència estatal d'investigació contra els departaments de Justícia i de Seguretat Nacional, 24-mar-2026: proves retingudes «per escudar els agents implicats» — noms, armes, informes, dades GPS i declaracions de testimonis negats malgrat els requeriments formals; les disset investigacions penals de la fiscal Moriarty; l'obstacle de la clàusula de supremacia; els agents del cas Pretti, identificats per ProPublica l'1-feb); NPR — *Months after the ICE shootings in Minnesota, a federal probe remains elusive* (10-abr-2026: el mòbil de Pretti, retingut; el cotxe de Good, precintat en un magatzem de l'FBI sense examinar; investigadors estatals apartats físicament de l'escena; única mesura disciplinària de l'operatiu: dos agents en permís administratiu per «declaracions falses» en el cas del tercer tirotejat, Julio Sosa-Celis; «Sembla que estiguin impedint activament que l'estat investigui» — Rachel Moran, professora de dret). 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: cinc trets de l'agent de la Patrulla Fronterera Charles Exum; la càmera corporal mostra el vehicle dels agents girant cap al d'ella després del «it's time to get aggressive»; els missatges de l'agent — «fired 5 shots and she had 7 holes» —; els càrrecs contra Martinez i el seu codemandat, arxivats amb caràcter definitiu el 20-nov-2025) i *List of shootings by U.S. immigration agents in the second Trump administration* (el recompte acumulat: 38 tirotejos i 9 morts entre el 20-gen-2025 i el 7-jul-2026; els casos amb càrrecs contra civils retirats quan el vídeo va contradir la versió dels agents); AP (via KSAT) — *Judge's blistering opinion details use of force in Chicago-area immigration crackdown* (nov-2025: el dictamen de 223 pàgines de la jutgessa Sara Ellis — el relat del govern, «simply not credible», desmentit per les càmeres corporals que ella mateixa havia ordenat activar; les versions canviants de Bovino sobre la pedra i el gas; l'informe d'ús de la força redactat amb 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 al·lega que «va envestir un vehicle oficial» i que l'agent va disparar «en defensa pròpia»; els agents no duien càmeres corporals, segons el DHS; relats en conflicte sobre els moments previs; la forense del comtat de Harris, 9-jul: homicidi). https://www.click2houston.com/news/local/2026/07/07/heavy-law-enforcement-presence-reported-in-east-houston-neighborhood/ ↩

La dignitat de qui existeix: la «Magnifica Humanitas» i la prova d'existència

«La persona acaba reduint-se a un mitjà per obtenir resultats, a un recurs per ser usat i explotat.»

— Lleó XIV, encíclica Magnifica Humanitas, §51 (2026)

El 25 de maig de 2026, al Vaticà, va passar una cosa que cap protocol no havia previst: per primera vegada en la història, un papa va presentar personalment una encíclica al món. I Lleó XIV no va comparèixer sol. Al seu costat hi seia **Chris Olah**, cofundador d'Anthropic —una de les empreses capdavanteres en intel·ligència artificial— i **ateu declarat**: criat a Toronto en una família evangèlica devota, havia deixat de creure als quinze anys [8]. El text, signat deu dies abans i titulat «Magnifica Humanitas», es va presentar al món amb una imatge tan insòlita com deliberada: un creient i un no creient, l'un al costat de l'altre, dient alhora que cada persona és única i irreemplaçable [4][6].

El papa ho va resumir amb una frase que val per a tot aquest llibre: «quin gran signe d'esperança que, amb les nostres diferències, ens puguem escoltar els uns als altres» [6]. Comencem, doncs, per aquí, i no pas per un argument de fe. La força de la idea que vertebra l'encíclica —«la dignitat que pertany a tot ésser humà pel simple fet d'existir» (§52) [1]— no rau en qui la pronuncia, sinó en el fet que la pugui subscriure igual un pontífex que un enginyer que no creu en Déu. La dignitat de qui existeix no demana cap credo: és anterior a qualsevol creença i, precisament per això, pot ser el fonament d'una tecnologia pensada per a tothom.

L'encíclica es publica exactament 135 anys després de la «Rerum Novarum» de Lleó XIII, el text fundacional de la doctrina social catòlica que va posar les bases del respecte per la dignitat del treballador [2]. Aquesta coincidència cronològica subratlla una continuïtat històrica: tal com l'antic document denunciava les condicions d'explotació industrial, la nova encíclica es dirigeix cap a un món dominat per algoritmes i dades. El seu tema central —«la custòdia de la persona humana en el temps de la intel·ligència artificial»— ressona amb la crida que la mateixa Església va fer fa més d'un segle, ara transposada al context digital [1].

Al cor del text, al paràgraf cinquanta-dos, apareix una frase que sembla una clau de volta per a tot el debat que hem conduït des del capítol 10 fins al capítol del segell (cap. 112): «la dignitat que pertany a tot ésser humà pel simple fet d'existir» (§52) [1]. No es tracta d'una declaració merament teològica; és una afirmació que pretén fonamentar moralment qualsevol tecnologia que pretengui validar la presència i la integritat d'un individu.

La pregunta que aquest capítol planteja, com a fil conductor de les seccions anteriors sobre identitat digital (cap. 47) i la crisi de la veritat provocada per les deepfakes (cap. 10), és clara: si la dignitat neix simplement d'existir, quin paper pot jugar una eina que prova l'existència —t2p— en aquest escenari? Pot aquesta tecnologia servir com a guardià de la dignitat, certificant que algú o alguna cosa existeix sense reduir-la a un simple conjunt de dades? O, per contra, podria esdevenir el «poder tecnològic amb rostre privat» que l'encíclica denuncia (§5) [1], transformant la persona en una mercaderia utilitzable per interessos econòmics i polítics?

Aquesta intersecció entre fe i ciència, entre moralitat i innovació, estableix el marc on s'haurà de valorar tant la promesa com el perill de qualsevol mecanisme que pretengui provar l'existència. La resposta determinarà si la «Magnifica Humanitas» es converteix en una brúixola ètica capaç d'impulsar un futur on la tecnologia no només reconeix, sinó també protegeix, la dignitat intrínseca de tot ésser humà.

Un creient, un ateu i la mateixa dignitat

Que el Vaticà triés Chris Olah per presentar el text al costat del papa no va ser un gest decoratiu. Olah no hi era com a creient discret convidat per cortesia, sinó com un dels enginyers que construeixen, des de dins, els models que el món tot just comença a comprendre. I la seva mirada —justament perquè ve de fora de la fe— dona a aquest capítol el to que volem que hi prevalgui: primer la humanitat, després la religió.

Les seves paraules al Vaticà podrien ser el lema d'aquest llibre. Va elogiar l'Església com a «crític informat» i va parlar de l'inici d'«una llarga col·laboració entre els qui construïm això i els qui poden veure el que nosaltres, des de dins, no veiem» [7]. En una sola frase hi cabia tota la tesi de *time2act*: qui fa la tecnologia no es pot jutjar a si mateix. Per això Olah reclamava el diàleg amb gent «no moguda pel

benefici» [7] i advertia, sense embuts, que la indústria «no es pot governar a si mateixa» [8]. És exactament la raó de ser d'una prova externa i verificable: que la veritat no depengui de la bona fe de qui la produeix.

Aquesta convergència —un papa i un ateu que afirmen el mateix— és, ella mateixa, la demostració que la dignitat de qui existeix no és una doctrina d'uns quants, sinó un mínim comú humà. Quan Lleó XIV escriu que cada persona és «única i irreemplaçable» [1], no demana que hi creguem per fe: nomena una evidència que un enginyer escèptic reconeix igual de bé. I és sobre aquest mínim universal —no sobre cap teologia particular— que una eina com la prova d'existència (t2p) pot aspirar a servir tothom. Perquè a tots, creients i no creients, ens pertoca la mateixa dignitat pel sol fet d'existir; i una tecnologia que es limiti a donar-ne testimoni, sense pretendre atorgar-la ni mesurar-la, pot ser de tots sense ser de ningú.

Cent trenta-cinc anys després de *Rerum Novarum*

Des del moment en què el papa Lleó XIII va publicar *Rerum Novarum* (1891), la doctrina social catòlica ha marcat el ritme d'una conversa mundial sobre treball, dignitat i responsabilitat col·lectiva [2]. Aquell document, nascut de les tensions de la Revolució Industrial, posava com a pedra angular la dignitat del treballador davant l'explotació. Un segle després, *Centesimus Annus* (1991) celebrava el centenari d'aquesta missió, recordant-nos que el progrés econòmic ha de ser al servei del benestar humà i no al revés [5]. El 2015, amb *Laudato Si'*, Francesc va ampliar aquest marc a la «Casa comuna», advertint del perill d'un paradigma tecnocràtic que reduïa la natura —i, per extensió, la persona— a simples recursos explotables [3].

El 2026, al maig, el papa Lleó XIV ha publicat la seva primera encíclica, *Magnifica Humanitas*, una obra que es posiciona com a continuació directa d'aquest llegat. Signada el 15 del mes i difosa al final d'aquell, per coincidència amb l'aniversari de *Rerum Novarum* [1], s'obre amb la declaració que ressona al cor de tot debat: «la dignitat que pertany a tot ésser humà pel simple fet d'existir» (segons el paràgraf corresponent) [1]. Aquesta afirmació, senzilla però profunda, estableix la base moral del projecte *time2act*: una tecnologia —la prova d'existència (t2p)— que pot validar la presència i la integritat d'una persona sense intentar assignar-li dignitat, ja intrínseca.

L'element clau de l'encíclica es troba al primer paràgraf, on el papa planteja una elecció decisiva per a la humanitat: «una elecció decisiva: aixecar una nova torre de Babel o edificar la ciutat on Déu i la humanitat habitin junts» (§1) [1]. Aquesta metàfora no és només retòrica; representa el punt d'inflexió en què les tecnologies emergents, com la intel·ligència artificial i la blockchain, poden convertir-se tant en ponts cap a una convivència més justa com en noves torres que separen i fragmenten. El risc, ja advertit al paràgraf §9 de l'encíclica, és que «la tecnologia pot guarir, connectar, educar... però també pot dividir, descartar» [1]; i encara més, que el poder tecnològic adopti un rostre privat i dominant (§5) [1].

Com hem vist en els capítols 10, 47 i 112, aquesta narrativa convergeix en una elecció moral: si la prova d'existència es desenvolupa com una eina humil, capaç només de certificar que algú existeix i és íntegre, pot servir com a bastió per a la dignitat humana sempre que no es converteixi en «el poder tecnològic de rostre privat» denunciat (§5) [1]. *Magnifica Humanitas* ens recorda que el futur depèn del nostre compromís ètic; la nostra tasca, com a lectors i creadors d'aquestes tecnologies, és escollir la «ciutat on Déu i la humanitat habitin junts», assegurant-nos que cada innovació sigui un pont cap a la dignitat i no una nova torre de Babel que ens separi.

La doctrina social davant la tècnica



Figura 114.1 — La doctrina social de l'Església davant l'economia i la tècnica: de la 'Rerum Novarum' (1891, el treball) a la 'Laudato Si'' (2015, la Casa comuna) i la 'Magnifica Humanitas' (2026, la persona en temps d'IA).

La dignitat de qui existeix

El 25 de maig del 2026 el papa Lleó XIV va presentar personalment la seva primera encíclica, *Magnifica Humanitas*, que esdevé el far moral d'aquest llibre. Al paràgraf cinquanta-dos l'encíclica afirma amb claredat i contundència: «la dignitat que pertany a tot ésser humà pel simple fet d'existir» (§52) [1]. Aquesta afirmació, arrelada en la tradició social de l'Església des de *Rerum Novarum* (1891) —esmentada per Lleó XIII com a fonament de la dignitat obrera— [2], no és una mera declaració abstracta; és el punt d'arrencada per a qualsevol tecnologia que pretengui ser responsable. La dignitat, segons l'encíclica, és prèvia i intrínseca: la persona ja la posseeix simplement per estar viva, tal com es recorda al paràgraf cinquanta: «l'home i la dona són creats a imatge i semblança del Déu trinitari» (§50) [1].

Aquesta premissa moral ressona directament amb el problema exposat al capítol 47 sobre identitat digital. Milions d'individus arreu del món encara no disposen d'una identitat legal reconeguda; la seva existència queda reduïda a un número d'arxiu o, pitjor encara, a l'absència total d'un registre oficial. En aquest context, *t2p* —la prova d'existència que hem desenvolupat— no pretén conferir dignitat; el seu paper és certificar una realitat que ja existeix però que sovint es veu negada per les estructures legals i administratives.

El risc de confondre certificació amb conferència de dignitat està advertit a l'encíclica. Al paràgraf cinquanta-un, Lleó XIV denuncia la reducció de la persona a un simple mitjà: «la persona acaba reduint-se a un mitjà per obtenir resultats, a un recurs per ser usat i explotat» (§51) [1]. Això és el perill que recorden les deepfakes descrites al capítol 10; sense una prova fiable, la identitat pot ser substituïda o esborrada per algoritmes que prioritzen l'engany sobre la transparència.

t2p, en aquest marc, actua com a escut contra aquesta erosió. Quan un sistema nega l'existència jurídica d'un individu —per exemple, una persona sense registre civil— la prova d'existència pot registrar de forma immutable que aquella veu és seva i que aquell esdeveniment ha tingut lloc. Això no només ofereix una defensa legal; és una reivindicació moral que recolza l'afirmació del papa: la dignitat ja està present, cal només reconèixer-la.

Tanmateix, l'encíclica també ens adverteix sobre el poder tecnològic privat (paràgraf cinc): «el poder tecnològic adquireix així un rostre inèdit, predominantment 'privat'» (§5) [1]. Si la prova d'existència es converteix en una eina controlada per entitats amb interessos exclusius, el seu potencial emancipador s'anul·la i es transforma en una nova forma de dominació. La nostra responsabilitat, com a creadors i usuaris, és garantir que *t2p* sigui una infraestructura oberta, transparent i sotmesa a principis de subsidiarietat (paràgraf seixanta-vuit): «allò que poden fer les persones... no ha de ser absorbit per instàncies superiors» (§68) [1].

En definitiva, la prova d'existència és una eina humil però poderosa. No atorga dignitat —aquesta ja existeix pel simple fet d'estar—, sinó que l'enforteix en proporcionar un testimoni inequívoc de la nostra presència en el món digital. Si s'utilitza amb saviesa i responsabilitat, pot ser el pont que l'encíclica descriu entre la tecnologia i la custòdia amorosa de la humanitat: una ciutat on Déu i l'home cohabiten, més que una torre de Babel que ens separa.

Que la persona no es redueixi a una dada

L'encíclica recorda amb claredat el perill que amenaça la nostra essència: «la persona acaba reduint-se a un mitjà per obtenir resultats, a un recurs per ser usat i explotat» (com hem vist al paràgraf 51)[1]. Aquesta advertència ressona especialment en l'era de les identitats digitals, on el valor d'una vida sovint es mesura en bits, tokens o puntuacions algorítmiques. Un sistema mal dissenyat pot convertir-nos en simples registres, empremtes o perfils que la tecnologia tracta com a recursos negociables, i no com a éssers amb una dignitat intrínseca.

El model de prova d'existència (t2p) pretén ser l'oposició directa a aquesta reducció. No es tracta d'una eina que assigni un valor o una puntuació moral; el seu objectiu és certificar, amb mínima intervenció, que algú existeix i ho fa sense crear un arxiu centralitzat que pugui ser explotat. La clau del disseny resideix en tres principis: **minimització de l'empremta**, **localitat del processament** i **propietat personal del segell**.

1. **Minimització de l'empremta, no del contingut.** En lloc d'emmagatzemar tota la història d'interacció o les dades biomètriques completament, el protocol genera un hash únic que representa només la presència verificable. Això es tradueix en una petita cadena de caràcters que, sense la clau privada del titular, no pot ser reconeguda com a informació personal. Aquesta reducció evita que les plataformes acumulin grans volums d'informació sensible i impedeix l'ús posterior per a finalitats comercials o de vigilància.

2. **Processament al dispositiu, no en bases centrals.** La verificació es realitza íntegrament al terminal de l'usuari: el seu telèfon intel·ligent o un dispositiu IoT autoritzat. El càlcul del hash i la signatura digital s'executen localment, sense que cap servidor extern tingui accés a les dades originals. Així, la informació no surt mai de l'entorn controlat per la persona, i el risc d'una filtració massiva es redueix dràsticament.

3. **El segell pertany al titular.** Un cop generada la prova, aquesta s'emmagatzema en una cartera digital que només el propietari pot administrar. La clau privada és única i intransferible; cap entitat externa pot revocar-la ni modificar-la sense el consentiment explícit del subjecte. Això garanteix que el segell no es converteixi en un actiu negociable, sinó en una certificació humil de la presència.

Aquests principis reflecteixen el principi de subsidiarietat assenyalat a l'encíclica (§68)[1] —«allò que poden fer les persones... no ha de ser absorbit per instàncies superiors»— i, com hem vist abans, garanteixen a cada individu el control total sobre la seva pròpia prova, protegint-la de la temptació del poder tecnològic privat descrita al paràgraf (§5)[1]. No es tracta només d'una qüestió tècnica, sinó d'un compromís ètic: la tecnologia ha de ser una eina que **custodi** i no una màquina que **exploti**.

En resum, el disseny de t2p respon a l'avís del Papa Lleó XIV, convertint-se en un pont entre la innovació i la custòdia amorosa de la humanitat. Si s'aplica amb rigor i responsabilitat, pot impedir que la persona es redueixi a una dada, mantenint viva la dignitat que li pertany pel simple fet d'existir.

El rostre privat del poder

El maig del 2026 el papa Lleó XIV va presentar personalment la seva primera encíclica, *Magnifica Humanitas*, amb una missió moral clara: «la custòdia de la persona humana en el temps de la intel·ligència artificial» [4]. Aquest moment, com hem vist, marcava un aniversari simbòlic i establia el fil conductor del nostre llibre: la dignitat intrínseca de tot ésser humà pel simple fet d'existir, tal com afirma l'encíclica (§52) «la dignitat que pertany a tot ésser humà pel simple fet d'existir» [1].

La «crítica al rostre privat del poder» es desenvolupa en diversos paràgrafs de *Magnifica Humanitas*. Primer, el document adverteix que «el poder tecnològic adquireix així un rostre inèdit, predominantment 'privat'» i que cal preguntar «qui deté avui aquest poder i cap a quins fins l'orienta» (§5) [1]. Aquesta pregunta es converteix en la pedra angular de la governança democràtica: si les infraestructures digitals —patents, algoritmes, plataformes, dades— són controlades per uns pocs actors, el risc és que la tecnologia deixi d'ésser una eina de custòdia i es transformi en una extensió del poder personalitzat. El capítol 112, dedicat a qui controla la infraestructura, ja havia mostrat com les grans plataformes defineixen condicions d'accés, regles de visibilitat, formes de relació i fins i tot oportunitats econòmiques (§71) [1]; així, el que semblava una anàlisi tècnica es revela com una continuïtat directa de la crítica papal.

Seguidament, l'encíclica subratlla que «la tècnica pren el rostre de qui la concep, la finança, la regula, la utilitza» (§9) [1]. Cada model d'aprenentatge profund és una extensió del seu creador; quan aquesta responsabilitat recau en mans privades, la persona es redueix a un simple recurs. L'avís de l'encíclica —«la persona acaba reduint-se a un mitjà per obtenir resultats, a un recurs per ser usat i explotat» (§51) [1]— ressona amb les conclusions del capítol 10 sobre la crisi de la veritat i les deepfakes; com hem vist, l'absència d'una prova fiable facilita la manipulació massiva d'imatges i veus.

En aquest context, *t2p* apareix com una resposta tècnica humil però potent: certifica que algú o alguna cosa existeix i és íntegre sense atorgar-li dignitat. La dignitat ja està garantida pel simple fet d'existir (§52); la prova només pot reforçar aquesta realitat contra l'engany. Si el mecanisme es posa al servei d'un grup reduït per consolidar poder —com una «carta de crèdit digital» que controla l'accés a serveis essencials—, es converteix en el mateix rostre privat que la doctrina condemna.

Així, la intersecció entre l'encíclica i el capítol 112 demostra que qualsevol implementació de *t2p* ha d'estar subordinada a principis de subsidiarietat (§68) i a una governança oberta que asseguri que «allò que poden fer les persones... no ha de ser absorbit per instàncies superiors» [1]. Només així la tecnologia pot

complir la seva missió de custodi, tal com el papa recorda en §15: «es tracta de custodiar amb amor aquesta magnífica humanitat... que cap màquina no podrà mai substituir». La nostra tasca és traduir aquest amor en estructures democràtiques i transparents, evitant que la innovació es converteixi en un instrument de dominació.

El destí universal dels béns digitals

El papa Lleó XIV recorda amb una claredat sorprenent que el «destí universal dels béns inclou avui «patents, algoritmes, plataformes digitals, infraestructures tecnològiques, dades»» (§67) [1]. Aquest avís moral sobre la nova geografia del poder es manté vigent: les xarxes de blockchain i els sistemes d'intel·ligència artificial configuren l'arquitectura de la confiança, i el que abans era propietat intel·lectual passa a ser una part integral del teixit social. Cada token i cada model entrenat amb dades massives es converteixen en béns col·lectius que afecten la dignitat de qui existeix.

Segons l'encíclica, la resposta ètica és el principi de subsidiarietat: «allò que poden fer les persones... no ha de ser absorbit per instàncies superiors» (§68) [1]. En termes tècnics, això implica una infraestructura de prova d'existència (t2p) totalment oberta i comuna. No pot ser un servei gestionat per una corporació que, com avisa el paràgraf §5, ha adquirit «un rostre inèdit, predominantment 'privat'» del poder tecnològic (§5) [1]. La centralització nominal —on la propietat d'un node o d'una clau es concentra en mans de pocs— no garanteix la transparència ni la rendició de comptes que la dignitat humana demana.

A la pràctica, això implica una arquitectura descentralitzada real. Les xarxes distribuïdes han de permetre que qualsevol usuari verifiqui la seva pròpia identitat i la d'altri sense dependre d'una autoritat superior. Com hem vist a les plataformes que defineixen condicions d'accés (§71) [1], el sistema t2p hauria d'establir regles obertes, auditories independents i mecanismes de governança participativa. Un model de «governança per consorci», en què les decisions sobre les actualitzacions del protocol es prenen mitjançant votació entre entitats públiques i organitzacions de la societat civil, és un marc possible per evitar la captura per part d'un sol actor.

Aquesta configuració té una doble promesa. Primer, serveix a la dignitat dels exclosos: persones que viuen en contextos de vulnerabilitat —refugiats digitals, treballadors del sector informal o víctimes de deepfakes — poden demostrar la seva existència i protegir els seus drets sense dependre d'una empresa que podria vendre les seves dades. Segon, reforça la veritat contra l'engany: una prova d'existència verificable impedeix que algú manipuli imatges o àudios per desacreditar un individu, com hem vist al capítol 10.

No obstant això, el perill persisteix. Si la infraestructura queda sota el control d'un grup privat, es converteix en «un recurs per ser usat i explotat» (§51) [1], revertint l'objectiu de custodiar amb amor aquesta magnífica humanitat (§15) [1]. Per tant, el repte no és només tecnològic sinó institucional: cal establir marcs legals que obliguin a la transparència i a la rendició de comptes, tal com la doctrina social de 'Rerum Novarum' (1891) va exigir en el seu moment per al treballador industrial [2].

En resum, el destí universal dels béns digitals ha d'alinear-se amb la subsidiarietat i la descentralització genuïna. Només així l'eina t2p pot ser una «eina humil» que certifica l'existència sense usurpar la dignitat intrínseca de qui existeix, convertint-se en el veritable pont entre la tecnologia i la moralitat que l'encíclica tant insistia a defensar.

El límit que cap màquina substitueix

Hi ha un darrer límit que aquest llibre ha de reconèixer. L'encíclica fa una crida a la responsabilitat: «la dignitat que pertany a tot ésser humà pel simple fet d'existir» (§52) i, alhora, ens recorda que aquesta dignitat no es pot delegar a cap algoritme ni a cap cadena de blocs. Aquesta doble afirmació estableix el marc moral on s'insereix la nostra proposta tecnològica —t2p.

La humilitat és el principi central que l'encíclica demana als creadors i usuaris de tecnologia. Així, «acceptar els límits i la fragilitat de la humanitat sense considerar-los un error que calgui corregir» (§12) implica reconèixer que cap sistema pot capturar la totalitat de l'ésser humà. La prova d'existència, tal com es descriu al llarg del llibre, és una eina que certifica que un fitxer existia íntegre i que una persona és qui diu ser. No pretén mesurar l'ànima, el mèrit o la virtut; no pretén substituir la confiança humana ni la cura que només pot oferir una relació directa. Això coincideix amb l'avís de Lleó XIV sobre el perill de reduir la persona a un mitjà: «la persona acaba reduint-se a un mitjà per obtenir resultats, a un recurs per ser usat i explotat» (§51) [1].

t2p es presenta com una «eina humil». La seva funció és estrictament documental: registra la integritat d'un arxiu en el moment de la seva creació i verifica que l'emissor sigui qui declara ser. Aquesta certificació pot protegir els drets dels més vulnerables —com les víctimes de deepfakes descrites al capítol 10— però no té capacitat per assignar dignitat ni determinar el valor intrínsec d'una vida, tal com afirma el Papa: «custodiar amb amor aquesta magnífica humanitat... que cap màquina no podrà mai substituir» (§15) [1].

El límit de l'eina queda clar en les seves especificacions tècniques. En el context de la identitat digital (capítol 47), t2p pot garantir que una credencial digitalitzada sigui autèntica, però no substitueix el reconeixement personal d'un intercanvi cara a cara. De manera similar, en el capítol sobre qui controla la infraestructura (capítol 112) s'insinua que la centralització del poder tecnològic —«el poder tecnològic adquireix així un rostre inèdit, predominantment «privat»» (§5)— pot convertir qualsevol eina en instrument de dominació. La nostra proposta manté la subsidiarietat proclamada per l'encíclica: «allò que poden fer les persones... no ha de ser absorbit per instàncies superiors» (§68) [1].

Així, el missatge final d'aquesta secció és una crida a la moderació. La tecnologia pot i ha de servir com a suport a la dignitat humana, però mai com a substitut del compromís moral que l'home ha de tenir amb ell mateix i amb els altres. En aquest equilibri —entre el potencial transformador de la prova d'existència i el respecte per les limitacions intrínseques de qualsevol màquina— es troba el veritable valor de *t2p*: una eina al servei de la persona, no un oracle del seu valor.

La promesa i el perill

En el paràgraf novè de *Magnifica Humanitas* el Papa Lleó XIV descriu la tecnologia com una doble cara: «la tecnologia pot guarir, connectar, educar, tenir cura de la Casa comuna; però també pot dividir, descartar» (§9) [1]. Aquesta paradoxalitat és el fil conductor del que anomenem *t2p*: una eina capaç de certificar l'existència d'una persona o d'un actiu digital amb un grau d'integritat fins ara inabastable. Si la prova d'existència es desplega com a mecanisme de transparència, pot aportar una resposta concreta a les crisis documentades anteriorment —la manipulació de la veritat i l'erosió de la identitat digital— i, com hem vist, convertir el testimoni d'una existència en un registre públic que ningú pot negar ni falsificar. Això és literalment tornar la veritat a ser verificable i donar «existència provada» a qui ha estat privatament negada.

No obstant això, el mateix poder tecnològic que dona vida a *t2p* conté un perill intrínsec. L'encíclica avisa que «el poder tecnològic adquireix així un rostre inèdit, predominantment 'privat'» (§5) [1]; i que la persona pot acabar reduint-se a un mitjà per obtenir resultats, a un recurs per ser usat i explotat. Si una entitat —pública o privada— controla l'emissió i el reconeixement d'aquests certificats, es crea una nova forma de dominació: decidir qui és «existent» i qui no ho és. En aquest escenari, la prova d'existència es converteix en un instrument de vigilància massiva, similar al que vam observar, i podria ser utilitzada per establir «censura d'existència», excloent individus o grups de la vida econòmica i social simplement perquè no disposen del certificat adequat.

L'encíclica ofereix una metàfora poderosa: «una elecció decisiva: aixecar una nova torre de Babel o edificar la ciutat on Déu i la humanitat habitin junts» (§1) [1]. Si la prova d'existència és governada per interessos privats, es construeix una Torre de Babel digital —un laberint de protocols incompatibles que fragmenta la cooperació humana. En canvi, si el seu desenvolupament segueix els principis de subsidiarietat, com hem vist, i de custòdia amorosa (§15) [1], pot sorgir una «ciutat santa» on cada certificat és testimoni d'una dignitat preexistent, no la font d'aquesta. Així, el perill no resideix en l'eina en si, sinó en la intenció i les estructures de govern que l'envolten.

El lector ha d'assumir aquest discerniment: reconèixer que *t2p* pot ser una clau per restaurar la confiança en un món saturat de deepfakes i identitats falses, però també és susceptible de reforçar les jerarquies de poder si es deixa sense supervisió. La nostra tasca —i la del llibre— és oferir no només la tecnologia, sinó el marc ètic que garanteixi que la prova d'existència serveixi per «custodiar amb amor aquesta magnífica humanitat» (§15) [1], i no per convertir-la en una nova forma de dominació. En aquest equilibri entre promesa i perill es troba el veritable valor de *t2p*: un instrument humil que certifica l'existència sense intentar atorgar dignitat, deixant aquesta última com a prerrogativa intrínseca de tot ésser humà.

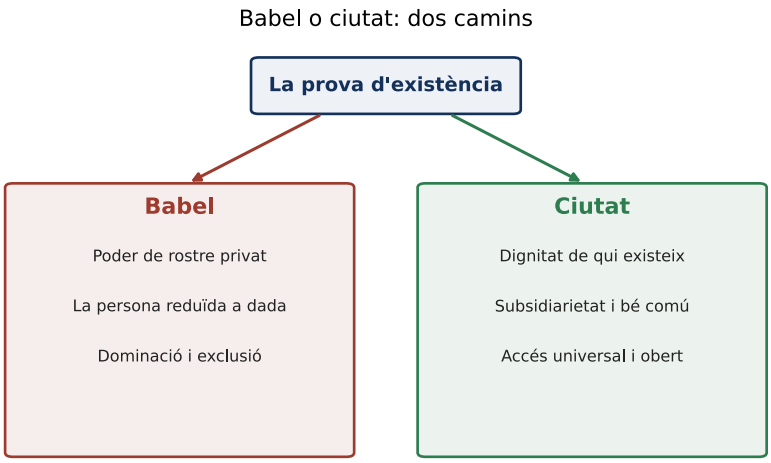


Figura 114.2 — La mateixa prova d'existència, dos camins (§1): cap a «Babel» (poder privat, reducció de la persona a dada, dominació) o cap a la «ciutat» (dignitat de qui existeix, subsidiarietat, accés universal). La diferència no és tècnica, sinó de governança i de fi.

És hora d'actuar

El magatzem de les decisions que la intel·ligència artificial ja ha pres sobre la nostra vida quotidiana s'estén com una catifa infinita, i al seu centre hi ha una crida clara: «Triem... el camí de Nehemies... transformant la diversitat en un recurs» (§10) [1]. Aquestes paraules no són només un ideal moral; són un pla d'acció que, a través dels principis ja madurats al llarg de *time2act*, pot guiar-nos cap a una era en què la tecnologia serveixi realment a la dignitat humana.

Primer principi — Prova d'existència per als exclosos. Com hem vist al capítol 47, la identitat digital es converteix en un refugi per a qui no en té, ja sigui un migrant sense documents o una comunitat marginada que viu al marge de les xarxes tradicionals. La prova d'existència (t2p) ha de ser el pont que connecti aquestes persones amb el seu reconeixement legal i social, sense que cap entitat pugui negar-les l'accés a drets fonamentals.

Segon principi — Veritat com a defensa contra les deepfakes. La crisi de la veritat descrita al capítol 10 mostra que els continguts manipulats amenacen d'anul·lar qualsevol base per a un diàleg autèntic. En aquest context, la prova d'existència actua com una empremta immutable que certifica l'origen i la integritat de les declaracions, impedint que la informació es converteixi en una mera il·lusió visual.

Tercer principi — La persona no ha de reduir-se a dada. L'encíclica recorda que «la persona acaba reduint-se a un mitjà per obtenir resultats, a un recurs per ser usat i explotat» (§51) [1]; com hem vist, la prova d'existència ha de quedar en mans de qui la posseeix, no en bases de dades centralitzades que podrien convertir-la en un objecte negociable. Cada individu ha de poder validar el seu propi estat sense dependre d'un tercer que ho controla.

Quart principi — Governança democràtica i anti-rostre privat. El perill del «poder tecnològic... amb rostre inèdit, predominantment «privat»» (§5) [1] s'ha exposat al capítol 112, on es detalla com la concentració d'infraestructura pot erigir una nova aristocràcia digital. La resposta ha de ser un model de governança oberta, amb consells representatius que reflecteixin la diversitat humana.

Cinquè principi — Infraestructura comuna i subsidiarietat. L'encíclica subratlla que «el destí universal dels béns inclou avui patents, algoritmes, plataformes digitals, infraestructures tecnològiques, dades» (§67) [1] i que el principi de subsidiarietat demana que «allò que poden fer les persones... no ha de ser absorbit per instàncies superiors» (§68) [1]; així, la infraestructura que sosté la prova d'existència ha de ser una xarxa pública, cooperativa i descentralitzada, accessible a tothom sense barreres econòmiques ni polítiques.

En resum, el camí de Nehemies ens convida a transformar la diversitat en un recurs que garanteixi identitat per als invisibles, veritat per a les societats fragmentades i autonomia per a cada persona. És aquest l'últim pas del viatge iniciat amb *Rerum Novarum* i continuat amb *Laudato Si'*; ara, al cor de la

intel·ligència artificial, ens trobem davant la decisió més crucial: **custodiar la magnífica humanitat de qui existeix —és, en l'era de la IA, time2act**.

---

[1] Lleó XIV — *Carta encíclica «Magnifica Humanitas»* (Vaticà, 15-25 de maig de 2026; sobre la custòdia de la persona humana en el temps de la intel·ligència artificial). https://www.vatican.va/content/leo-xiv/es/encyclicals/documents/20260515-magnifica-humanitas.html ↩

[2] Lleó XIII — *Rerum Novarum* (1891; origen de la doctrina social de l'Església). https://www.vatican.va/content/leo-xiii/es/encyclicals/documents/hf_l-xiii_enc_15051891_rerum-novarum.html ↩

[3] Francesc — *Laudato Si'* (2015; la Casa comuna i el paradigma tecnocràtic). https://www.vatican.va/content/francesco/es/encyclicals/documents/papa-francesco_20150524_enciclica-laudato-si.html ↩

[4] Vatican News — *Lleó XIV presenta la seva primera encíclica «Magnifica Humanitas»* (25 de maig de 2026). https://www.vaticannews.va/es/papa/news/2026-05/papa-leon-xiv-primera-enciclica-magnifica-humanitas.html ↩

[5] Joan Pau II — *Centesimus Annus* (1991; centenari 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 — *Lleó XIV presenta «Magnifica Humanitas» en persona, amb el cofundador d'Anthropic Chris Olah; «amb les nostres diferències, ens puguem escoltar els uns als altres»* (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»* (l'Església com a «informed critics»; «a long collaboration between those of us who are building this and those who can see what we, from inside, cannot»; diàleg amb gent «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* (criat evangèlic a Toronto, ateu des dels 15; la indústria «can't govern itself») (03-06-2026). https://fortune.com/2026/06/03/who-chris-olah-anthropic-cofounder-atheist-pope-leo-vatican-ai/ ↩

Bibliografia

1. AIE, *Oil 2025 — Executive summary*. https://www.iea.org/reports/oil-2025/executive-summary
2. IRENA (via 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), *funcionament i límits de l'estàndard de procedència*. https://truescreen.io/articles/c2pa-standard-history-limitations/
7. Tapscott, Don i 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* (Reglament (UE) 2024/1689). https://artificialintelligenceact.eu/article/50/
10. Comissió 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* (projecció de frau per 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 d'usuari (Solució d'Integritat de Dades)*, 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, *preus del Brent i OPEP+ (2022-2025)*. https://www.eia.gov/todayinenergy/detail.php?id=55020
17. AIE, *Oil Market Report (set. 2025) — esquist EUA*. https://www.iea.org/reports/oil-market-report-september-2025
18. BloombergNEF / AIE, *Global EV Outlook 2025 i preus de bateries*. https://www.iea.org/reports/global-ev-outlook-2025/electric-vehicle-batteries
19. AIE / CFR, *domini xinès en minerals i tecnologies netes (2024-2025)*. https://www.iea.org/commentaries/with-new-export-controls-on-critical-minerals-supply-concentration-risks-become-reality
20. Sightline / anàlisi, *exportacions netes xineses al Sud Global (2024)*. https://www.sightlineclimate.com/research/a-tour-of-chinas-electrostate
21. IPCC AR6 (via COP28 Global Stocktake), *retallades d'emissions 2030/2035*. https://www.iea.org/topics/cop28-tracking-the-energy-outcomes
22. UNFCCC / Comissió Europea, *resultats 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* (revisió). 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. Nacions Unides, *Greenwashing*. https://www.un.org/en/climatechange/science/climate-issues/greenwashing
31. (deepfakes) Blockchain Council / Europol — vegeu 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 per a la xarxa*. 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 avançat i SMR per a la demanda d'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 tokenitzats i MRV en blockchain*. https://www.rwa.io/post/renewable-energy-credits-on-blockchain-a-tokenized-approach
37. Frontiers in Blockchain (2025), *estat dels mercats de carboni 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 (especificació 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, *cost del H_2 verd 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 $25 million after video call with deepfake 'CFO'* (cas Arup). https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk · World Economic Forum. https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/
54. Deloitte — *Generative AI is expected to magnify the risk of deepfakes and other fraud in banking* (≈40 mil M$ el 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; documents judicials dels EAU: almenys 17 implicats, 400.000 $ rastrejats fins a comptes del Centennial Bank als EUA). 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* (maig 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* (metadades eliminables). https://arxiv.org/html/2604.24890v1
67. NSA/CISA — *Content Credentials: Strengthening Multimedia Integrity* (gen 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 · resum amb xifres: 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* (campanya de desinformació russa). https://www.disinfo.eu/doppelganger-hub/
83. FCC — *Proposed $6M fine for AI-deepfake Biden robocall* (2024); IPI (Eslovàquia). 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 a la captura; casos a Ucraïna). 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); Protocol 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)* i *Deepfake Defense* (2024); NATO StratCom COE. https://www.darpa.mil/research/programs/semantic-forensics
88. Comissió Europea — *About the EU Emissions Trading System* (cobertura ~40 %, 175.000 M€ recaptats, −47 % vs 2005, −62 % el 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; màxim històric 105,73 € el feb-2023). https://tradingeconomics.com/commodity/carbon
90. Comissió Europea (Taxation and Customs Union) — *Carbon Border Adjustment Mechanism (CBAM)* (fase definitiva des de l'1-gen-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, assignació gratuïta). https://icapcarbonaction.com/en/ets/eu-emissions-trading-system-eu-ets
93. Comissió Europea — *ETS2: buildings, road transport and additional sectors* (inici ajornat al 2028; acord nov-2025). https://climate.ec.europa.eu/eu-action/carbon-markets/ets2-buildings-road-transport-and-additional-sectors_en
94. EASA — *ICAO CORSIA* (emissions internacionals 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. Comissió Europea — *Monitoring, reporting and verification of EU ETS emissions* (MRR i AVR; informe verificat abans del 31 de març). 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* (fins al 90 % del volum fraudulent en alguns països). 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) i *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. Comissió Europea — *Announcement: transitional measure for the EU ETS registry system* (19-gen-2011) i OCCRP — *Germany: Six Executives Stand Trial for Emissions Fraud* (~850 M€; sis condemnats). 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. Banc Mundial — *Why data infrastructure is key for a transparent carbon market* i 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-gen-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* (rèplica). https://verra.org/verra-response-guardian-rainforest-carbon-offsets/
102. Mongabay — *Head of Verra, top carbon credit certifier, to leave in June* (dimissió de David Antonioli, 22-maig-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 crèdits en excés 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; desforestació −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 emplaçaments en 6 països; resultat disputat, rèplica arXiv 2312.06793). https://www.science.org/doi/10.1126/science.ade3535
107. Ecosystem Marketplace / Forest Trends — *State of the Voluntary Carbon Market 2024* (mercat ~2.000 M$ el 2021 → 723 M$ el 2023; volum −56 %; preu mitjà 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* i *First high-integrity CCP-labelled carbon credits* (juny 2024; ~27 M de crèdits). 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-juny-2023). https://vcmintegrity.org/launch-claims-code/
110. CarbonPlan — Danny Cullenward i Grayson Badgley, *Zombies on the blockchain* (7-abr-2022; ~28 % de crèdits zombi). https://carbonplan.org/research/toucan-crypto-offsets
111. Verra — *Verra Addresses Crypto Instruments and Tokens* (prohibició de tokenitzar crèdits retirats, 25-maig-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 obert). https://forestsnews.cifor.org/76905/blockchain-platform-offers-reforestation-efforts-access-to-carbon-finance
114. Comissió Europea — *Energy Efficiency Directive* (Directiva 2023/1791, art. 8; nous estalvis fins a l'1,9 % anual el 2028-2030; «more than doubles» cap al 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 d'energia final acreditat; subjectes obligats/delegats, verificador, coordinador). https://www.boe.es/buscar/doc.php?id=BOE-A-2023-2027
116. BOE — *Orden TED/845/2023, de 18 de julio* (catàleg de mesures estandarditzades d'eficiència energètica). 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* (resultats 2024: ~1.200 actuacions, ~2 TWh, ~500.000 t CO_2, ~230 M€; indústria 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* (objectiu acumulat d'estalvi 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, 6è període 2026-2030; 1.050 TWh cumac/any). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000052486193
120. Légifrance — *Loi n° 2025-594 du 30 juin 2025* (sancions fins al 10-12 %; fotografies *horodatées et géolocalisées* o vídeo a distància, conservades 6 anys). https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000051824277
121. DGCCRF (economie.gouv.fr) — *Rénovation énergétique : focus sur l'isolation à 1 euro* (469 establiments controlats; 56 % d'incompliment). https://www.economie.gouv.fr/dgccrf/laction-de-la-dgccrf/les-enquetes/renovation-energetique-focus-sur-lisolation-1-euro
122. Hellio / Govern francès — *Fraude aux CEE* (480 M€ de frau bloquejat el 2024, 236 M€ en CEE; taxa de control 10 %→15 %). https://www.hellio.com/actualites/reglementation/fraude-cee
123. ANSA / PordenoneToday — *Contributi per 10 milioni su certificati bianchi inesistenti* (292 projectes ficticis; 50.322 TEE; dany ~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 i l'anul·lació de títols d'eficiència energètica* (doctrina de la «formació progressiva»; cas 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 i 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 l'any, −3,7 % vs 2024; 36.330 llars noves +229 MW; comercial +176 MW; industrial +679 MW; cinquena font de generació per potència instal·lada, per davant de la nuclear; objectiu PNIEC 19 GW); UNEF — *El autoconsumo sigue avanzando, superando ya el umbral de los 8 GW* (2024: +1.182 MW, acumulat 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 — *Reial decret 244/2019, de 5 d'abril* (condicions administratives, tècniques i econòmiques de l'autoconsum; compensació simplificada d'excedents ≤100 kW, voluntària, a la factura mensual — facturació neta; autoconsum individual i col·lectiu; registre administratiu); MITECO — *Preguntas frecuentes sobre autoconsumo*; UNEF — *Real Decreto 244/2019*; Puentes de Muras — *RD 244/2019: novedades* (ampliació del radi de l'autoconsum col·lectiu fins a 5 km, plantes fins a 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 producte (certificar qualsevol fitxer per lots — només l'empremta viatja; captura de pantalla i de pàgina web amb imatge completa + codi font; escàner de documents fins a 50 pàgines; foto amb GPS forense; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; els CAE, al capítol 23; l'acta de la comunitat, al capítol 37; la factura, al capítol 34.
129. Parlament Europeu (EPRS) — Enrico Pastori i Raffaele Vergnani, *Odometer manipulation in motor vehicles in the EU* (2018; dany de 5.600-9.600 M€/any; 30-50 % en vendes transfrontereres). 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* (fins al 50 % dels cotxes transfronterers). 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€/any; sobrepreu mitjà del 26,3 %). https://www.carvertical.com/en/blog/cost-of-odometer-fraud-in-europe
132. Car-Pass (Bèlgica) — *Annual report 2022* (1.344 casos el 2022, <0,2 %; importacions 2,4 %→0,87 %). https://www.car-pass.be/en/blog/car-pass-annual-report-2022
133. MITECO — *Catálogo de fichas CAE: sector transporte* (fitxes 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* (agost 2025; 65 % menys energia; autonomia 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 ciberatacs el 2025; 92 % remots; 67 % a telemàtica/núvol). 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) i *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. Reglament (UE) 2023/1542 — *Passaport de Bateria digital* (obligatori des del 18-feb-2027 per a bateries de VE i industrials de més de 2 kWh; accés per QR). https://www.circularise.com/blogs/eu-battery-passport-regulation-requirements
139. Smart Freight Centre — *GLEC Framework v3.0 / ISO 14083:2023* (comptabilitat d'emissions del transport de mercaderies). 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. Reglament (UE) 910/2014 (eIDAS), articles 41-42 — presumpció legal d'exactitud del segell de temps qualificat. https://eur-lex.europa.eu/eli/reg/2014/910/oj
141. Susan Shaheen i Elliot Martin (UC Berkeley, Transportation Sustainability Research Center) — *Impacts of car2go: One-Way Carsharing in North America* (2016; cada vehicle compartit retira 7-11 cotxes privats; VMT i GEI a la baixa). 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; mitjana de 3,3 cotxes substituïts; rang 2,1-5,3). https://pmc.ncbi.nlm.nih.gov/articles/PMC7544607/
143. BlaBlaCar — *Sustainability Report 2024* (2,5 Mt CO_2 evitades el 2024; 92 milions de passatgers). 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 (fiscalia EDNY) — *Two charged in $40M ride-hail surge-pricing GPS spoofing scheme* (cas «Fake GPS», agost 2024). https://www.insurancejournal.com/news/east/2024/08/30/790683.htm
146. Hai Yang i 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) i *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; cap implementació a escala real fins ara). https://www.sciencedirect.com/science/article/pii/S2590198225002908
149. Next Mobility / ONSS — *Mobility budget in Belgium: ONSS figures 2024* (18.386 treballadors amb pressupost de mobilitat; 17.030 sense cotxe d'empresa). https://www.nextmobility.be/en/post/mobility-budget-belgium-onss-figures-2024/
150. Bruxelles Environnement — *Prime Bruxell'Air* (ajut de 505-1.010 €/any per donar de baixa la matrícula, vigent el 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: eliminades les indemnitzacions de 15 i 30 minuts per a AVE, Avlo, Alvia, Euromed i Intercity; nou règim 50 % a partir de 60 min i 100 % a partir de 90; devolució del 200 % en punts o 150 % en vals; justificació: liberalització i ajust a la legislació); Renfe — *Compromiso de puntualidad* i nota de premsa de l'actualització; Xataka — *el debat sobre indemnitzar des dels 15 minuts* (situació normativa oberta). 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 — *Reglament (CE) 261/2004* (compensacions de 250/400/600 € per cancel·lació i, per la doctrina Sturgeon del TJUE, gran retard ≥3 hores a l'arribada; excepció de circumstàncies extraordinàries; dret d'atenció; jurisprudència del TJUE: l'«hora d'arribada» és l'obertura de portes). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32004R0261
155. t2p — manual de producte (foto amb GPS forense — fix genuí ~50 m / ≤30 s, la ubicació simulada bloqueja la certificació; certificació en segon pla que es reprèn en recuperar cobertura — mode avió; captura de pantalla certificada; escàner de documents; projectes per agrupar l'expedient d'un viatge; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; la reclamació de serveis, al capítol 33; el rellotge del proveïdor, al capítol 59.
156. Coalition Against Insurance Fraud — *The Impact of Insurance Fraud on the U.S. Economy* (2022; 308.600 M$/any, ~933 $ per 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* (capítol Fraud) i *The impact of insurance fraud* (~10 % de la despesa en sinistres; estimació de 2013, ~13.000 M€ referits 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 reclamacions). 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 %* (Espanya, 2024). https://segurosnews.com/news/el-sector-detecto-285-407-casos-sospechosos-de-fraude-de-los-que-evito-un-637
160. Verisk (amb el National Insurance Crime Bureau) — *AI editing tools are fueling a new era of insurance fraud* (març 2026; 36 % de consumidors, Gen Z 55 %; 99 % de les asseguradores). 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 (via PetaPixel) — *Fraudsters are editing photos of damaged vehicles to claim insurance* (cas LV=; +300 % de fotos manipulades, 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* (metadades + anàlisi de nivell d'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 %; recomana prova de vida i ancoratge 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 % dels comunicats d'auto a Espanya). https://www.lineadirectaaseguradora.com/-/vii-barometro-de-fraude-al-seguro
166. OCDE / EUIPO — *Mapping Global Trade in Fakes 2025* (falsificacions: 467.000 M$ el 2021, 2,3 % de les importacions mundials; UE 4,7 %). https://www.oecd.org/en/publications/mapping-global-trade-in-fakes-2025_94d3b29f-en.html

167. Organització Mundial de la Salut — *Substandard and falsified medical products* (≥1 de cada 10 als països de renda baixa/mitjana; ~30.500 M$/any). https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products
168. OMS — *Medical Product Alert N°6/2022* (Gàmbia; xarops de Maiden Pharmaceuticals contaminats amb 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* (Índia; xarop «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 — *Reglament (UE) 2023/1115* (EUDR; coordenades de geolocalització de parcel·les; 7 matèries primeres; data de tall 31-des-2020). https://eur-lex.europa.eu/eli/reg/2023/1115/oj/eng
171. Comissió Europea (Access2Markets) — *Delay until December 2026 — implementation of the EUDR* (segona pròrroga, Reg. UE 2025/2650; aplicació 30-des-2026 / 30-juny-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 únic 2D obligatori des del 9-feb-2019). https://www.ema.europa.eu/en/human-regulatory-overview/public-health-threats/falsified-medicines-overview
173. Aura Blockchain Consortium — *About* (fundat el 2021 per LVMH, Prada i Cartier; >50 M de productes registrats). https://auraconsortium.com/about
174. WWD — *Aura Blockchain crosses 50 million products* (LVMH, Prada, OTB; setembre 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 d'agost de 2024; en vigor el 21 d'octubre de 2024; fins a 51.744 $ per infracció; prohibeix la compravenda de ressenyes, les ressenyes d'insiders sense revelació, les webs de ressenyes controlades, la supressió selectiva i els indicadors falsos d'influència 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 juliol de 2022; més de 10.000 grups; EUA, Regne Unit, Alemanya, França, Itàlia, Espanya i Japó); Marketing4eCommerce — *Amazon denuncia a los administradores de más de 10.000 grupos de Facebook* («Amazon Product Review», més de 43.000 membres; 10 $ per ressenya; més de 10.000 grups reportats a Meta des de 2020, la meitat eliminats); 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* (només 1 de cada 3 productes s'abarateix; pujades mitjanes del 13 % en les setmanes prèvies en categories com rellotges intel·ligents, càmeres i auriculars; el 43 % dels productes dispara el preu; estalvi anunciat del 23 % vs preus reals un 3 % més cars; en el 99 % dels casos el «preu anterior» no és el menor dels últims 30 dies; monitoratge des de setembre); 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. Centre Europeu del Consumidor a Espanya (Ministeri de Consum) — *España amplía la garantía legal mínima de dos a tres años* (des de l'1 de gener de 2022; transposició de les Directives (UE) 2019/770 i 2019/771; presumpció d'origen del defecte ampliada de 6 mesos a 2 anys — 1 any per a segona mà —; recanvis durant 10 anys; prescripció de 3 a 5 anys); 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 producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; acreditació sense identificació — la prova de compra viatja, la identitat mai; contingut al dispositiu i revelació voluntària). Vegeu els capítols 13 i 15; l'origen del producte, al capítol 29.
180. Digital Perito — *Estafas en Wallapop y Vinted: cómo denunciar con pruebas* (>19 milions d'usuaris actius a Wallapop a Espanya; mercat de segona mà >13.000 M€ anuals; les estafes de plataformes de segona mà com a gruix dels >412.000 fraus informàtics de 2024; +60 % de denúncies el 2025); Público — *Así operan los estafadores en plataformas de segunda mano* (tipologies: pagament fora de plataforma, triangulació/«cambiazo» aprofitant la protecció al comprador, phishing, etiquetes fraudulentes, suplantació); OKDiario / Genbeta — alertes de la Guàrdia Civil i trucs de detecció. 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. Marc civil de la compravenda entre particulars (vici ocult; absència de garantia comercial de consum). Vegeu el capítol 30 per a la garantia B2C i el capítol 36 per a l'estafa de l'anunci fals.
182. t2p — manual de producte (vídeo amb data/hora sobreimpresa; foto amb GPS forense — fix genuí ~50 m / ≤30 s, la ubicació simulada bloqueja la certificació; captura de pantalla certificada; certificar qualsevol fitxer; projectes per agrupar l'expedient d'una venda; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; el pagament enganyat, al capítol 69.
183. Direcció General de Consum (DSCA) — *Prácticas irregulares de compañías españolas de alquiler de coches* (indemnitzacions desproporcionades de 300 a 1.000 € per ratllades o desperfectes petits, carregades a la targeta del dipòsit amb quantia fixada unilateralment); CEC-España (Centre Europeu del Consumidor) — *Alquiler de vehículos: derechos y recomendaciones* (càrrecs posteriors per neteja o danys menors; revisions sense la presència del consumidor; recomanacions: tornar amb l'oficina oberta, revisar amb el personal, demanar justificant i «fer fotografies de l'interior i l'exterior com a prova»); 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 producte (vídeo amb data/hora sobreimpresa; foto amb GPS forense — fix genuí ~50 m / ≤30 s, la ubicació simulada bloqueja la certificació; escàner de documents; projectes per agrupar l'expedient d'un lloguer; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; l'inventari del pis, al capítol 36; l'estat de la cosa venuda, al capítol 31; el càrrec a la targeta, al capítol 69.
185. BOE — *Llei 10/2025, de 26 de desembre, per la qual es regulen els serveis d'atenció a la clientela* (BOE 27-12-2025; 12 mesos d'adaptació; 95 % de trucades en <3 minuts; codi identificatiu de seguiment; resposta en 15 dies — 5 per a càrrecs no autoritzats; avís 15 dies abans de renovacions automàtiques; baixa senzilla amb DNI i número de contracte; prohibició d'atenció exclusivament automatitzada); 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* (vulneració del dret de desconnexió fins a tres vegades; obstrucció a la inspecció; 20.100 € amb reducció); FACUA — *Multa a Movistar por acosar a través de una gestora de cobros a una socia por una deuda falsa* (1.741 € per línies mai contractades); 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 producte (gravació d'àudio en segon pla; captura i gravació de pantalla certificades amb verificació de l'app en primer pla; captura de pàgina web amb imatge completa + codi font; escàner de documents fins a 50 pàgines; projectes per agrupar captures per cas; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió; només empremtes a la cadena). Vegeu els capítols 13 i 15; la licitud de gravar converses pròpies, al capítol 75; la veu clonada, al capítol 68.
188. AEAT — *Sistemas Informáticos de Facturación (SIF) y VERI*FACTU *(RD 1007/2023: registre de facturació normalitzat amb empremta encadenada — cada registre conté el hash de l'anterior —, signatura electrònica i QR de verificació; modalitats «Verifactu» d'enviament immediat voluntari i conservació inalterable; FAQ oficial); Guía Fiscal* — Verifactu 2026-2027 *i Davisa* — Guía Verifactu 2026* (calendari ajornat pel RD-llei 15/2025, de 2 de desembre: 1-1-2027 societats, 1-7-2027 resta; sancions de fins a 50.000 €/exercici per a usuaris i 150.000 € per a fabricants). 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 — *Llei 3/2004, de 29 de desembre, de mesures de lluita contra la morositat en les operacions comercials* (60 dies naturals de màxim pactat entre empreses, 30 per defecte des de la recepció; interès de demora automàtic; 40 € de costos de cobrament per factura; AAPP 30 dies — Llei 15/2010); Togas — *Los intereses de demora en el primer semestre de 2025: 11,15 %* (Resolució del Tresor de 30-12-2024); PMcM / Revista Limpiezas — *Informe sobre morosidad 2025* (el 85 % de les grans companyies incompleix els terminis; AAPP a 70 dies de mitjana, +3 el 2025; sector privat 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 producte (foto amb GPS forense — fix genuí ~50 m / ≤30 s, la ubicació simulada bloqueja la certificació; certificació en segon pla que es reprèn en recuperar cobertura; escàner de documents fins a 50 pàgines en un PDF; captura de pantalla i de correu certificades; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió; només empremtes a la cadena). Vegeu els capítols 13 i 15; el comerç internacional, al capítol 54; l'auditoria, al capítol 55.
191. Banc Mundial — Laura Tuck i Wael Zakout, *7 reasons for land and property rights to be at the top of the global agenda* (~30 % de la població amb títol registrat). 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 d'adults, 23 %, inseguros sobre la seva terra/habitatge). https://www.prindex.net/news-and-stories/tenure-insecurity-on-the-rise/
193. FAO (informe SOFA, via UN News) — *Global report highlights slow progress in expanding secure land tenure* (~35 % de la terra documentada; >1.100 M temen perdre-la). https://news.un.org/en/story/2026/02/1167037
194. FBI IC3 (via National Association of Realtors) — *Online real estate fraud climbed to $275M in 2025* (12.368 víctimes). 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* (juliol 2024; 28 %; sòl sense edificar 85 %; credencials de notari falses 43 %). https://www.alta.org/news-and-publications/news/20240730-Seller-Impersonation-Fraud-Attempts-Increase-Study-Shows

196. FBI Boston (via ALTA) — *FBI Boston Issues Quit Claim Deed Fraud Warning* (abril 2025; frau immobiliari 2019-2023: 58.141 víctimes / 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 títols ancorats a Bitcoin; «ningú pot alterar la marca de temps»). https://exonum.com/story-georgia
198. Eurasianet — *Georgia authorities use blockchain technology for developing land registry* (ampliació feb-2017; Hernando de Soto, assessor). 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€/any d'estalvi). https://www.computerweekly.com/news/450421958/Sweden-trials-blockchain-for-land-registry-management
200. CoinDesk — *Blockchain land title project stalls in Honduras* (Factom; encallat per qüestions polítiques, 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 maig de 2026; Operació ISLEDA; 3 detinguts de 19-34 anys a San Fernando; destapada a Valladolid; comptes oberts amb identitats robades en falses ofertes de feina; estafa, blanqueig i organització 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* (preus-ganxo, propietaris «a l'estranger», pagaments abans 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* (termini d'un mes; interessos legals; acord de liquidació amb inventari); Ático Jurídico — *Devolución de la fianza del alquiler* (els tribunals exigeixen proves a qui reté: factures, 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 d'abril de 2025; allanament art. 202 CP i usurpació art. 245 CP per judici ràpid; desallotjament policial dins de les primeres 48 hores; supressió de l'informe de vulnerabilitat en aquesta via); 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 producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; el contingut no surt mai del dispositiu; revelació voluntària; els buits de la sèrie queden datats). Vegeu els capítols 13 i 15; per a la titularitat i el registre, el capítol 35.
206. Vecindia — *Condenado administrador de fincas por apropiación indebida* (Gijón: 1 any i mig de presó confirmats; 2.984,04 € del compte comunitari; maniobres enganyoses al llibre d'actes fent signar expresidents; rebuts d'obra i serralleria falsos per encobrir-se; descobert en canviar president i tresorer); 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 (impugnació d'acords contraris a la llei, lesius o abusius; convocatòries i actes; juntes telemàtiques habilitades per reforma recent); 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 producte (escàner de documents fins a 50 pàgines en un PDF certificat; gravació d'àudio; captura de pantalla i correu certificades; foto amb GPS forense; projectes per agrupar l'expedient d'una obra; certificar qualsevol fitxer — només l'empremta viatja; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; la propietat i el registre, al capítol 35; el lloguer, al capítol 36.
209. Atlántico — *Investigan varias estafas en reformas de viviendas en Vigo y su comarca* (almenys sis víctimes; fins a 10.000 € cadascuna; constructor que inicia obres i desapareix); Liberal de Castilla — *Un vecino de Guadalajara pierde sus ahorros ante un falso albañil de internet* (Guàrdia Civil; estafador localitzat a Madrid); Telemadrid — *Destapamos al presunto estafador de las reformas*; Allende Abogados — *Estafas en reformas* (patró: oferta digital atractiva, pressupost barat, bestreta «per a materials», desaparició; pèrdues que superen els 77.000 € en alguns 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. Marc del contracte d'obra (Codi Civil) i normativa de consum aplicable a reformes amb consumidors (pressupost previ i factura). Vegeu el capítol 34 per al cobrament del professional i el capítol 37 per a l'obra comuna.
211. t2p — manual de producte (escàner de documents fins a 50 pàgines en un PDF certificat; foto amb GPS forense — fix genuí ~50 m / ≤30 s; vídeo amb data/hora sobreimpresa; projectes per lligar pressupost, fases, evidències i pagaments; signatura amb vídeo-selfie, reptes de vida i biometria; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; la derrama, al capítol 37; la factura, al capítol 34.
212. BCG i ADDX — *Relevance of On-chain Asset Tokenization in 'Crypto Winter'* (2022; ~16,1 bilions $ el 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; cas base ~2 bilions $, rang 1-4, exclou stablecoins). https://www.mckinsey.com/industries/financial-services/our-insights/from-ripples-to-waves-the-transformational-power-of-tokenizing-assets
214. CoinDesk (informe RedStone / Gauntlet / RWA.xyz) — *Real-world asset tokenization market has grown almost fivefold in 3 years* (~24.000 M$; crèdit privat ~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* (març 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* (barres serialitzades a Brink's Londres; atestacions mensuals de KPMG). https://www.paxos.com/paxg-transparency
218. Financial Stability Board — *The Financial Stability Implications of Tokenisation* (octubre 2024; custodis i oracles com a nous punts de vulnerabilitat). https://www.fsb.org/2024/10/the-financial-stability-implications-of-tokenisation/
219. Moody's (via CoinDesk) — *Tokenized fund adoption grows but brings technology risks* (2024; fallades d'oracle, historial limitat). https://www.coindesk.com/markets/2024/01/15/tokenized-

fund-adoption-grows-but-brings-technology-risks-moodys
220. Standard Chartered i 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 verificació d'identitat com a condició). 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-des-2023; annex de 127 pàgines amb sortides 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* (gener 2026). https://news.bloomberglaw.com/ip-law/openai-must-turn-over-20-million-chatgpt-logs-judge-affirms
224. Getty Images — *Getty Images statement* (acció contra Stability AI; consentiment i llicència, gener 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 major part de les reclamacions 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 des d'agost 2024). https://copyrightalliance.org/andersen-v-stability-ai-copyright-case/
227. Karla Ortiz — *Testimony before the U.S. Senate Judiciary Committee* (12-jul-2023; «mai m'han preguntat, acreditat ni compensat»). 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 per 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; consentiment per a la «rèplica digital»). https://en.wikipedia.org/wiki/2023_SAG-AFTRA_strike
230. U.S. Copyright Office — *Copyright and Artificial Intelligence, Part 2: Copyrightability* (29-gen-2025; l'autoria humana com a fonament). https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf
231. USPTO — *America Invents Act (AIA): Frequently Asked Questions* (primer a presentar des del 16-mar-2013; «la data de la invenció és irrellevant»). https://www.uspto.gov/patents/laws/america-invents-act-aia/america-invents-act-aia-frequently-asked
232. WIPO (Organització Mundial de la Propietat Intel·lectual) — *Patents: Frequently Asked Questions* (prior art; la divulgació prèvia destrueix la novetat; el període de gràcia no és universal). https://www.wipo.int/en/web/patents/faq_patents
233. BitLaw — *What does a patent application cost?* (redacció 9.000-17.000 $; pressupostar 15.000-25.000 $ abans de la concessió). https://www.bitlaw.com/guidance/patent/what-does-a-patent-application-cost.html
234. USPTO — *Fee Schedule* (sol·licitud provisional: fixa data, 12 mesos; taxes oficials). 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?* (sense valor legal; obsoleta des del first-to-file de 2013). https://www.mclane.com/insights/know-the-law-is-the-poor-mans-patent-real/
236. Technical Disclosure Commons — *FAQ* (gratuït; data de publicació automàtica; indexat per Google Patents). https://www.tdcommons.org/faq.html
237. IP.com — *Publishing Disclosures to the Prior Art Database* (segell de temps mitjançant Surety AbsoluteProof). https://kb.ip.com/pad/knowledge-base/publishing-disclosures-to-the-prior-art-database-pad/
238. Richard Coller III i 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 Patents (EPO) — *Espacenet reaches 160 million patent documents* (abril 2025). https://agip-news.com/news.aspx?id=76074&lang=en
240. WIPO — *PATENTSCOPE* (~128 milions de documents de patent; 5,4 M de sol·licituds PCT). https://patentscope2.wipo.int/
241. CNBC — *Trump pardons Anthony Levandowski, the engineer who stole self-driving car secrets from Google* (milers de fitxers descarregats abans de marxar; Otto comprada per Uber; acord

Waymo-Uber de 2018 valorat per la premsa en ~245 M$ en accions; culpabilitat el març de 2020; 18 mesos de presó — jutge William Alsup: «the biggest trade secret crime I have ever seen»; indult total el 20-1-2021, últim dia de mandat); TechCrunch — *Former Google engineer Anthony Levandowski among list of last-minute Trump pardons*; Wikipedia — *Anthony Levandowski* (acord 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 — *Llei 1/2019, de 20 de febrer, de Secrets Empresarials* (transposició de la Directiva (UE) 2016/943; tres requisits: secret + valor empresarial + mesures raonables; abast: fórmules, processos, bases de dades, llistes de clients, algorismes, know-how; equilibri: no cobreix l'experiència i competències adquirides honestament pel treballador ni pot restringir la seva mobilitat; mesures de confidencialitat processals); 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 producte (certificar qualsevol fitxer — només l'empremta viatja, el contingut no surt mai del dispositiu; escàner de documents fins a 50 pàgines; signatura amb vídeo-selfie, reptes de vida i biometria; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice amb revelació selectiva verificable sense connexió). Vegeu els capítols 13 i 15; el prior art i la patent, al capítol 41; els registres d'un atac, al capítol 57; els alertadors, al capítol 62.
244. Spend Network / Banc Mundial — *The $13 trillion global value of public procurement* (~13-15 % del PIB; menys del 3 % en dades obertes). https://www.spendnetwork.com/13-trillion-the-global-value-of-public-procurement/
245. Banc Mundial — *The hidden $1 trillion: halting waste in public procurement* (~una quarta part malgastada; ~1 bilió $/any). 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 l'obra pública; ~6 bilions $/any cap al 2030). https://infrastructuretransparency.org/2016/02/05/this-is-why-construction-is-so-corrupt/
247. OCDE — *Guidelines for Fighting Bid Rigging in Public Procurement (2025 Update)* (la col·lusió pot encarir els contractes un 20 % o més). https://www.oecd.org/en/publications/2025/09/oecd-guidelines-for-fighting-bid-rigging-in-public-procurement-2025-update_127880ea.html
248. Transparency International — *Corruption Perceptions Index 2025* (mitjana mundial 42/100, mínim històric; Dinamarca 89, vuitè any al capdavant). https://www.transparency.org/en/news/cpi-2025-findings-insights-corruption
249. Open Contracting Partnership — *The impact of ProZorro in Ukraine* (~6.000 M$ estalviats; Dozorro, 33.000+ licitacions). https://www.open-contracting.org/impact-stories/impact-ukraine/
250. e-Estonia — *KSI Blockchain* (primer Estat amb blockchain en producció, 2012; Guardtime; només s'ancora l'empremta). https://e-estonia.com/solutions/cyber-security/ksi-blockchain/
251. World Economic Forum — *Exploring Blockchain Technology for Government Transparency to Reduce Corruption* (Colòmbia, Programa d'Alimentació Escolar, BID, 2020). https://www.weforum.org/publications/exploring-blockchain-technology-for-government-transparency-to-reduce-corruption/
252. EUR-Lex — *Reglament eIDAS (UE 910/2014), article 41* (presumpció legal d'exactitud del segell de temps qualificat). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
253. Banc Mundial — *GovTech Maturity Index* (198 economies; quatre àrees de maduresa del govern digital). https://www.worldbank.org/en/programs/govtech/gtmi
254. BOE — *Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques* (art. 21: termini general de tres mesos per resoldre i notificar; silenci administratiu amb efectes des del venciment; certificat acreditatiu del silenci expedit d'ofici en 15 dies; notificacions electròniques: 10 dies naturals des de la posada a disposició, transcorreguts els quals s'entén rebutjada); 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 acaparen cites; revenda; sistema desbordat); OKDiario — *El caos en la web de Extranjería impulsa a las mafias que cobran hasta 350 € por cita* (revenda per WhatsApp de 50 a 350 €, fins a 600 €); Parainmigrantes — *El problema de la cita previa llega al Defensor del Pueblo* (queixes constants, ≈3.000 en un any; >163.000 sol·licituds d'asil el 2023; «demores excessives»); 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 producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; contingut als sistemes de cada part, només empremtes a la cadena; traça verificable per ambdues parts). Vegeu els capítols 13 i 15; la contractació pública, al capítol 43.
257. AFAPNA — *Oposiciones 2026: sorteo de letras de tribunales y aspirantes*; OpositaTest — *Sorteo por letra del orden de actuación en oposiciones* (sorteig públic de lletres; procediments reglats posteriors; sistema «mirall» d'inversió de l'ordre 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* (sorteig davant notari segons el procediment de cada administració; possibilitat d'impugnació); 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/adjudicacionde viviendasprotegidas/ · 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 producte (empremta SHA-512; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; compromís previ per empremta — les dades personals no s'exposen —; actes ancorades i reverificables). Vegeu els capítols 13 i 15; la integritat electoral, al capítol 48.
260. Cloudflare / League of Entropy — *Distributed Randomness Beacon* (drand: balisa d'aleatorietat distribuïda i públicament verificable; membres fundadors: Cloudflare, EPFL, Kudelski Security, Protocol Labs i Universitat de Xile; valors imparcials, impredictibles i verificables a intervals fixos; criptografia de llindar; aplicacions: loteries i eleccions); PR Newswire — *The League of Entropy launches production drand network* (primera balisa pública verificable en producció); 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 servei basc de salut; denúncies sindicals a Anestèsia i Angiologia; indicis en 19 exàmens de 12 especialitats; dimissions del conseller de Salut Jon Darpón, la directora general d'Osakidetza i dos directius de RH); Deia — *Archivan la causa por las presuntas filtraciones en la OPE de Osakidetza en 2018 por falta de pruebas* (desembre de 2024: arxivament «al no existir indicios racionales de la comisión del ilícito», provisional per a dos investigats de Cirurgia Plàstica); elDiario.es — *La Justicia cierra sin culpables la investigación* i *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 producte (certificar qualsevol fitxer — només l'empremta viatja, el contingut no surt mai de la custòdia; foto amb data certa; escàner de documents; captura de publicacions oficials amb data; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell

de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; el sorteig de tribunals, al capítol 45; les credencials, al capítol 19; els alertadors, al capítol 62.

263. Banc Mundial (ID4D) — *Global progress in identification: 3 findings from the latest data* (2025; ~800 M sense identitat oficial; >50 % són infants no registrats). 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 d'apàtrides oficials, fins a ~10 M reals; rohingyes ~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* (desembre 2024). https://www.unicef.org/press-releases/birth-registration-steadily-increases-worldwide-150-million-children-still-invisible
266. Comissió Europea — *European Digital Identity (eIDAS 2.0)* (Reg. UE 2024/1183; EUDI Wallet obligatòria a finals de 2026; divulgació selectiva). https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation
267. W3C — *Verifiable Credentials Data Model v2.0 becomes a W3C Recommendation* (15-maig-2025) i *Decentralized Identifiers (DID) v1.0* (2022). https://www.w3.org/press-releases/2025/verifiable-credentials-2-0/
268. Govern de l'Índia (Press Information Bureau) — *Aadhaar* (~1.340 milions de titulars vius; >99,9 % dels adults; >170.000 milions d'autenticacions). 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 milions de registres, 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) — recerca sobre Aadhaar i l'exclusió en programes de benestar (*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; reconeixement d'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: prohibicions i ordres de supressió* (2024-2025). https://www.biometricupdate.com/202510/colombia-orders-world-shut-down-citing-biometrics-compliance-failures
275. Wikipedia (amb BBC / Al Jazeera) — *2017 Kenyan presidential election petition* (anul·lació 4-2; CJ David Maraga; primera a l'Àfrica). https://en.wikipedia.org/wiki/2017_Kenyan_presidential_election_petition
276. The Standard (Kenya) — *Presidential petition: what scrutiny of key IEBC forms revealed* (291 formularis 34B; 56 sense trets de seguretat, 31 sense número de sèrie, 32 sense signatura). 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 observadors; correlació 0,976-0,991; ~3,6 M de vots). https://cic.nyu.edu/resources/who-really-won-the-congolese-elections/
278. Sunoo Park, Michael Specter, Neha Narula i 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; trencat en ~20 minuts). 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 (Universitat de Minnesota) — *Colorado successfully completes the nation's first risk-limiting audit* (2017; límit de risc del 9 %).

https://electionacademy.lib.umn.edu/2017/11/27/colorado-successfully-completes-nations-first-risk-limiting-audit/
283. OSCE/ODIHR — *Election Observation Handbook* (6a edició; observadors de curt i llarg termini; distingir l'aïllat del sistemàtic). https://cdn.osce.org/sites/default/files/f/documents/5/e/68439.pdf
284. The Carter Center — *Election Standards i 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 transferències; ~6 M de persones; Ucraïna: 337 M$ coordinats, ~35 M$ de solapament evitat; 159 organitzacions el 2025). https://www.wfp.org/building-blocks
288. UN Innovation Network — *How the Building Blocks blockchain network is transforming humanitarian aid* (>1 M de refugiats 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 persones; PRIMES/BIMS). https://www.unhcr.org/blogs/unhcrs-biometric-tools-in-2023/
290. Development Initiatives — *Cash and Voucher Assistance* (~10,6 mil M$ el 2022 → 9,7 mil M$ el 2023; WFP, major proveïdor). 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 noms compartits amb 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 biomètrica amb els houthis, 2019-2023). https://news.un.org/en/story/2023/12/1144417
294. GiveDirectly / The New Humanitarian — *DRC mobile-cash fraud* (~1,2 M$ desviats; ~1.900 famílies). https://www.givedirectly.org/drc-case-2023/
295. Carmela Troncoso et al. (EPFL SPRING Lab, amb el CICR) — *Janus: Safe Biometric Deduplication for Humanitarian Aid Distribution* (IEEE S&P 2024; revela només un bit, sense base biomètrica). 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* (doblet M7,2 San Felipe + M7,5 Yumare, 24-6-2026, 39 s de diferència; >3.342 morts, >16.840 ferits, >68.000 desapareguts; aeroport Simón Bolívar suspès; conflictes de distribució: subministraments retinguts a Altamira, centres d'acopi civils prohibits a Charallave i Campo Elías, distribució impedida a El Limón, accés restringit a La Guaira; resposta: >30 països, >3.600 rescatistes, >1.000 tones); 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* (context humanitari; donacions: José Andrés/World Central Kitchen 1 M$, Rosalía 2 M$ a UNICEF, Metallica 100.000 $). https://ayudaenaccion.org/blog/ayuda-humanitaria/terremotos-venezuela/
299. Departament del Tresor dels EUA — *Treasury Disrupts Corruption Network Stealing From Venezuela's Food Distribution Program (CLAP)* (25-7-2019; xarxa d'Alex Saab; Group Grand Ltd; sobrepreus); 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 caixes des de Mèxic, ~30 $/caixa de sobrepreu, ~360 M$; llet per sota d'etiquetatge — 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* (pont de Tienditas bloquejat amb cisterna i contenidors; 23-2-2019: 14 camions/280 tones, 2 camions cremats; tancament de frontera); CNN en Español — *Venezuela bloquea puente en frontera con Colombia* (6-2-2019); Infobae — *Maduro ordenó retirar los contenedores del puente Tienditas* (des. 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 Leone ~2,13 M col·lusió amb banc sobre el tipus de canvi; Guinea ~1,17 M facturació fraudulenta d'un proveïdor de despatx duaner; Libèria ~2,7 M preus inflats d'articles de socors, nòmines i incentius); 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; Grup de Monitoratge: «fins a la meitat» desviada; contractistes/milícies/personal local; família Adaani); VOA — *WFP Report says No Evidence of Food Diversion in Somalia* (negació del WFP — Josette Sheeran; auditoria pròpia sense evidència); 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€ desviats segons la Fiscalia Anticorrupció, ~10.000 donants de baixa; Anesvad: president detingut el 5-4-2007 per apropiació indeguda, denunciat pels treballadors). 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* (convergència material; donacions no sol·licitades col·lapsen pistes i magatzems); TED Ideas — *After a disaster, don't send toys or clothing — send money* (José Holguín-Veras: 50-70 % dels béns que arriben no són necessaris ni apropiats; el cas de l'avió de joguines). 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)* (dipòsits a Bríndisi, Accra, Kuala Lumpur, Ciutat de Panamà i Dubai; despatx en 48 h; estocs per a múltiples organitzacions); UNHRD — *Our Services*; World Economic Forum — *Logistics Emergency Team: 20 years* (Clúster Logístic liderat pel 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: traçabilitat de vials de vacunes del dipòsit al centre de salut); WFP Innovation Accelerator — *3 ways blockchain innovation is enhancing humanitarian work* (traçabilitat d'aliments; Building Blocks); LSE — *How Blockchain is Contributing to the Humanitarian Sector as of 2025* (pilot IFRC/AID:Tech amb la Creu Roja irlandesa i 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 producte (roda de modes; escàner de documents fins a 50 pàgines en un PDF; empremta SHA-512 calculada al dispositiu; certificació en segon pla que es reprèn en recuperar cobertura; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; GPS forense — fix genuí ~50 m / ≤30 s, la ubicació simulada bloqueja la certificació; comprovació d'integritat del dispositiu i attestation de maquinari; superposició de data/hora al vídeo; signatura amb vídeo-selfie, reptes de vida i biometria; paquet d'evidència .asice ETSI EN 319 162 verificable sense connexió; només empremtes a la cadena).

Vegeu els capítols 13 i 15; l'entrega d'efectiu i la deduplicació, al capítol 49; l'euro del donant, al capítol 73.

308. Wikipedia — *2023 Pylos migrant boat disaster* (l'Adriana; sortida de Líbia; ≈750 persones a bord; més de 600 morts; 104 supervivents; 82 cossos; versió de la guàrdia costanera); Human Rights Watch — *Greece: Disparities in Accounts of Pylos Shipwreck Underscore the Need for Human Rights Compliant Inquiry* (errors de les autoritats; al·legacions sobre el remolc). 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. Amnistia Internacional — *Greece: Trial of Pylos shipwreck survivors must not be a shield in the investigation of the alleged responsibilities of the Greek authorities* (maig de 2024; nou supervivents processats; crítica de les organitzacions de drets humans). 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 maig de 2025; capità de la ΠΠΛΣ-920 acusat de causar naufragi amb resultat de mort d'almenys 82 persones; querella en nom de 40 supervivents). 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* (reconstrucció periodística amb dades de trànsit marítim, testimonis de supervivents i material dels seus telèfons). https://gijn.org/stories/investigating-pylos-shipwreck/
312. t2p — manual de producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; només empremtes a la cadena; publicació opcional; recuperació de còpies verificables contra l'empremta). Vegeu els capítols 13 i 15; l'evidència de drets humans, al capítol 20; la posició dels vaixells, al capítol 103.
313. Wikipedia — *Border Violence Monitoring Network* (coalició de més de 12 organitzacions, fundada el 2017); Statewatch — *The 'Black Book of Pushbacks': testimonies of pushbacks affecting over 12,000 people* (desembre de 2020; 12.654 persones); Balkan Insight — *Study Reports 25,000 Violent Pushbacks at EU Borders* (edició ampliada de 2022: més de 3.000 pàgines, 4 volums). 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* (assumpte C-136/24 P, sentència de 18 de desembre de 2025; nacional sirià despullat del telèfon i retornat a Turquia amb Frontex present; adaptació de la càrrega de la prova; Frontex com a posseïdora de la documentació). 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* (cas Leigh Voysey i el testament 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 $84 trillion in wealth transfers through 2045* (2022; «gran transferència de riquesa»). https://www.cerulli.com/press-releases/cerulli-anticipates-84-trillion-in-wealth-transfers-through-2045
317. Caring.com / YouGov — *Wills and Estate Planning Study 2025* (només el 24 % dels adults té testament). https://www.caring.com/resources/wills-survey
318. Dutton Gregory / Probate Registry — *Inheritance dispute statistics* (11.362 caveats el 2024, +56 % en cinc anys). https://www.duttongregory.co.uk/site/blog/personalnews/inheritance-dispute-statistics
319. Justia — *Will contests: testamentary capacity, undue influence, forgery* (motius de nul·litat). https://www.justia.com/estate-planning/wills/will-contests/
320. CBS News — *QuadrigaCX CEO took password to his grave* (Gerald Cotten; ~137 M$ bloquejats). https://www.cbsnews.com/news/gerald-cotten-quadrigacx-ceo-took-password-to-his-grave-leaving-company-unable-to-access-137-million/
321. Chainalysis (via Decrypt) — *~3,7 milions de bitcoins perduts per sempre* (2020; ~20 % de l'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 es perd sense les claus). https://www.americanbar.org/groups/real_property_trust_estate/resources/estate-planning/digital-property/
323. Comissió Europea (Interoperable Europe) / e-Estonia — *Estonia's KSI blockchain: the Succession Registry* (primer servei estatal sobre blockchain, 2012). https://e-estonia.com/blockchain-security-control-for-government-registers/
324. eSignGlobal — *Electronic wills legislation and remote notarization* (eIDAS QES; els testaments sovint exclosos de la notarització electrònica). https://www.esignglobal.com/blog/electronic-wills-legislation-remote-notary
325. INE / Gracia Carrión (anàlisi) — *Custodia compartida supera a la materna en España (INE 2024)* (49,7 % dels divorcis amb fills, +1,3 punts; primera vegada per sobre de la custòdia materna; 12,6 % el 2010); APFS — *Separaciones y divorcios en España 2024* (82.991 divorcis, +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* (aplicació de coparentalitat de referència per a tribunals i professionals als 50 estats dels EUA, Canadà, Regne Unit, Austràlia i Nova Zelanda; missatges amb marca de temps i sense esborrat; confirmacions de lectura; calendaris amb historial; informes per a judicis; 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 pla de parentalitat com a marc comú de criança més enllà del conveni regulador). https://www.elespanol.com/mujer/relaciones/20251214/abogada-solicitar-custodia-compartida-despues-anos-necesitas-plan-parentalidad/1003744039064_0.html
328. t2p — manual de producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; registre bilateral; contingut als dispositius, només empremtes a la cadena; revelació davant del jutjat). Vegeu els capítols 13 i 15; la gravació legal de converses pròpies, al capítol 75.
329. Banc Asiàtic de Desenvolupament (ADB) — *Global trade finance gap expands to $2.5 trillion in 2022* (Trade Finance Gaps, Growth and Jobs Survey). https://www.adb.org/news/global-trade-finance-gap-expands-25-trillion-2022
330. McKinsey — *The multi-billion-dollar paper jam: unlocking trade by digitalizing documentation* (2022; estalvi de 6.500 M$ + comerç nou). 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* (penetració real del coneixement d'embarcament electrònic: 5,7 %, gener 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 anys; ~12.300 M iuans amb rebuts 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 anys, reduïts a 13,5 en apel·lació el març 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_fo
334. FINMA — *Greensill / Credit Suisse* (insolvència 2021; ~10.000 M$ en quatre fons; factures fictícies). https://www.finma.ch/en/news/2023/02/20230228-mm-greensill/
335. Maersk — *Maersk and IBM to discontinue TradeLens* (tancament del consorci, 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 jurisdiccions; inclou el Regne Unit). https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records/status
337. Clifford Chance — *UK Electronic Trade Documents Act 2023* (equivalència legal del coneixement d'embarcament electrònic). 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 documents/dia; regles UCP 600). https://iccwbo.org/news-publications/news/survey-shows-steady-rise-of-global-adoption-of-electronic-bills-of-lading/

339. Financial Times (via S&P Global) — *Wirecard auditor did not independently verify its bank balance* (EY; comptes de garantia inexistents; extractes fabricats). 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: «negligència greu»; multa de 500.000 € i prohibició de 2 anys). 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$ perduts; Arthur Andersen, ~85.000 empleats; 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 vendes fabricades). https://www.sec.gov/newsroom/press-releases/2020-319
344. PCAOB — *AS 2310, The Auditor's Use of Confirmation* (adoptada el setembre de 2023; confirmació externa directa). https://pcaobus.org/oversight/standards/auditing-standards/details/AS2310
345. Association of Certified Fraud Examiners (ACFE) — *Report to the Nations 2024* (5 % dels ingressos; frau d'estats financers, mediana de 766.000 $ per cas). https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf
346. Comissió Europea — *Corporate sustainability reporting (CSRD)* (asseguració limitada obligatòria; normes ESRS d'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* (llindar de >1.000 empleats i >450 M€; l'asseguració limitada es manté). 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 d'asseguració de sostenibilitat). https://www.iaasb.org/publications/international-standard-sustainability-assurance-5000-general-requirements-sustainability-assurance
349. Juniper Research (via PR Newswire) — *22% of online ad spend is wasted due to ad fraud in 2023* (84.000 M$ el 2023 → 172.000 M$ el 2028; mòbil 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* (desembre 2023; 36 cèntims per dòlar; ~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* (els bots, el 49,6 % del tràfic d'internet el 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 i 3ve)* (novembre 2018; 1,7 M d'ordinadors; >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 visionats/dia). 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 suplantació de dominis). 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) — recerca independent sobre el frau publicitari 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 mitjà de 14 dies el 2025; traspàs d'accés en 22 segons). https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026
360. MITRE ATT&CK — *T1070 Indicator Removal / T1070.001 Clear Windows Event Logs* (l'esborrament deixa l'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 i cadena de custòdia). https://csrc.nist.gov/pubs/sp/800/86/final
362. IBM — *Cost of a Data Breach 2025* (cost mitjà global de 4,44 M$ / 10,22 M$ als EUA; 241 dies per identificar i contenir). https://www.ibm.com/think/x-force/2025-cost-of-a-data-breach-navigating-ai
363. Comissió Europea — *NIS2 Directive (UE 2022/2555)* (notificació en 24 h / 72 h; 23 estats en procediment d'infracció). https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
364. EUR-Lex — *DORA, Reglament (UE) 2022/2554* (aplicable des del 17-gen-2025; reporting d'incidents TIC greus). 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 dies hàbils). https://www.sec.gov/newsroom/press-releases/2023-139
366. GDPR-info — *Article 33 GDPR* (notificació de bretxa de dades en 72 hores). https://gdpr-info.eu/art-33-gdpr/
367. Global News — *Hamilton cyberattack cost* (l'asseguradora denega la cobertura per MFA incomplet; 18,3 M CAD). https://globalnews.ca/news/11313018/hamilton-cyberattack-cost/
368. Richard Bejtlich (TaoSecurity) — *Mandiant global median dwell time* (dos anys consecutius de deteriorament). 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 — *Sentència de 4 de maig de 2023, assumpte C-300/21 (UI c. Österreichische Post)* (article 82 RGPD: tres condicions acumulatives — infracció, dany i relació de causalitat; la mera infracció no dona dret a indemnització; el dany immaterial és indemnitzable sense llindar mínim de gravetat; quantificació segons el dret nacional amb equivalència i efectivitat); anàlisis de Cuatrecasas, finReg360 i 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: notificació de bretxes a l'autoritat en 72 h i als afectats en cas d'alt risc; art. 82: dret a indemnització); Have I Been Pwned com a eina pública de comprovació de filtracions. Vegeu el capítol 57 per al costat de l'empresa.
373. t2p — manual de producte (captura de pantalla i de pàgina web certificades — imatge completa + codi font; gravació d'àudio de converses pròpies; certificar qualsevol fitxer; projectes per al diari d'un incident; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió; només empremtes a la cadena). Vegeu els capítols 13 i 15; el SIM-swap, al capítol 68; l'estafa amb dades filtrades, al capítol 85.
374. Wikipedia — *2024 Delta Air Lines disruption* / TechTarget — *CrowdStrike outage explained* (19-7-2024: actualització defectuosa de Falcon Sensor; ~8,5 milions de Windows; la caiguda informàtica més gran de la història; impacte en aerolínies, hospitals, bancs, emergències); CNBC — *Delta, CrowdStrike sue each other over widespread IT outage* (Delta: >7.000 vols cancel·lats en cinc dies, >1,3 M de passatgers; demanda d'octubre de 2024 per ~550 M$; demandes creuades). 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. Reglament (UE) 2022/2554 (DORA — resiliència operativa digital del sector financer: gestió del risc TIC de tercers, report d'incidents; aplicable des de l'11-1-2025) i Directiva NIS2 (obligacions ampliades de notificació d'incidents). Vegeu el capítol 57 per al context de seguretat i terminis de notificació.
376. t2p — manual de producte (certificar qualsevol fitxer — només l'empremta viatja; captura de pàgina web amb imatge completa + codi font; captura i gravació de pantalla certificades; projectes per

agrupar l'expedient d'un incident; certificació en segon pla; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; els registres d'un atac, al capítol 57; la reclamació d'assegurança, al capítol 28.

377. CNBC — *This $80 million art scam fooled experts* (galeria Knoedler; Pei-Shen Qian; <9.000 $ per 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 pigment impossible). 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 peces, ~143 M$; Shiva Chola). https://www.occrp.org/en/news/india-sentences-notorious-antiquities-trafficker-from-manhattan
380. Manhattan District Attorney's Office — *Antiquities Trafficking Unit* (~6.000 antiguitats de 29 països, >460 M$ recuperats). 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 obres). 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 països). https://www.state.gov/washington-conference-principles-on-nazi-confiscated-art
383. UNESCO — *1970 Convention against the illicit trafficking of cultural property* (~149 estats). https://www.unesco.org/en/fight-illicit-trafficking/about
384. INTERPOL — *Cultural heritage crime: the issues* (comerç il·lícit de 225 M$ a 6.000 M$/any). https://www.interpol.int/en/Crimes/Cultural-heritage-crime/The-issues-cultural-property
385. Art Loss Register — *~700.000 objectes registrats; fundat per Julian Radcliffe (1991); >100 M$ recuperats*. https://www.artloss.com/
386. CNN — *The forensic archaeologist hunting trafficked antiquities* (Christos Tsirogiannis; «els papers menteixen»). 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* (juny de 2024, amb el Congrés Jueu Mundial; ChatGPT i el fals «Holocaust per ofegament»; cites de testimonis fabricades per Bard; simplificació excessiva; recomanacions a tecnològiques i sistemes educatius); comunicat de premsa en castellà (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 febrer de 2025; imatges sintètiques de fets i personatges reals publicades sense etiqueta; alteració de la percepció històrica i desconfiança en els mitjans). 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 filtrats; token de GitLab exposat des de finals de 2022; DDoS simultani sobre la Wayback Machine); NPR — *Hackers steal information from 31 million Internet Archive users*; Hispasec — *Internet Archive sufre su segunda brecha* (més de 800.000 tiquets de suport exposats). 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 novembre de 2025; 8.941 restes localitzades i recuperades; només 70 identificades i lliurades; Mapa Integrat de Fosses: 5.848 fosses, ≈1.500 obertes; Banc Estatal d'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 producte (empremta SHA-512 a l'origen; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; manifests per lots; contingut als sistemes de cada arxiu, només empremtes a la cadena). Vegeu els capítols 13 i 15; els comunicats oficials, al capítol 86; l'evidència de crims de guerra, al capítol 20.
392. EUR-Lex — *Directiva (UE) 2019/1937 sobre la protecció dels denunciants* (confidencialitat de la identitat; canals segurs; terminis). 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* (març 2025; ~39 M€; Alemanya 34 M€; Estònia 500.000 € + 1.500 €/dia). 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* (més de 60 redaccions; servei ocult de Tor; protecció arquitectònica de la font). https://securedrop.org/overview/
395. ICIJ — *Panama Papers* (11,5 milions de documents; 2,6 TB; >350 periodistes; la font «John Doe»). https://www.icij.org/investigations/panama-papers/
396. OCCRP — *John Doe: «The Revolution Will Be Digitized»* (manifest de la font dels 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* (punts de rastreig de la impressora; sèrie 29535218; 9-maig-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 més llarga als EUA per a una font de premsa). 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* (codi d'identificació de la màquina). https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots
400. Wikipedia — *Stylometry / Adversarial stylometry* (atribució d'autoria amb un 80-95 % de precisió). https://en.wikipedia.org/wiki/Stylometry
401. Wikipedia — *Frances Haugen* (filtració de Facebook; va decidir revelar la seva identitat). 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 i Ferric Fang — *The Prevalence of Inappropriate Image Duplication in Biomedical Research Publications* (mBio, 2016; 20.621 articles, 3,8 %). https://journals.asm.org/doi/10.1128/mbio.00809-16
405. American Society for Microbiology / mBio — *Pilot d'ImageTwin* (2.627 manuscrits; 410 amb problemes d'imatge; 6 acceptacions revocades). 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* (imatges/dades tergiversades en subvencions als 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; dimissió del president). https://boardoftrustees.stanford.edu/news/board-trustees-statement-release-report-and-announcements
408. American Physical Society — *The Schön scandal* (comitè Beasley; mala conducta en 16 de 24 càrrecs). https://www.aps.org/apsnews/2022/08/september-2002-schon-scandal-report
409. Retraction Watch (Ivan Oransky i Adam Marcus) — *The new retraction record holder* (Joachim Boldt, 184 retractacions, juliol 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, Universitat d'Oxford) — *COMPare: outcome-switching en assaigs clínics* (Trials, 2019; 76,3 % de desenllaços primaris ben reportats). https://pmc.ncbi.nlm.nih.gov/articles/PMC6375128/
411. Center for Open Science (Brian Nosek) — *Registered Reports* (de 91 a més de 300 revistes; el protocol abans dels resultats). https://www.cos.io/initiatives/registered-reports
412. eLife — *Reproducibility Project: Cancer Biology* (Amgen, 11 % de 53 estudis; efectes replicats un 85 % més petits). https://elifesciences.org/articles/71601

413. Wikipedia (amb BBC / AFP / Japan Times) — *Sogen Kato* (momificat 32 anys; pensió de supervivència cobrada; ~9,5 M de iens). https://en.wikipedia.org/wiki/Sogen_Kato
414. France 24 — *Over 230,000 listed centenarians missing in Japan* (234.354 sense confirmar; 77.118 amb 120+ anys). 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) i *6,5 M de titulars de ≥112 anys sense data de defunció al 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 (via HuffPost) — *Greece stops pensions and benefits for 200,000 people* (~9.000 «centenaris»; fins a 800 M€/any d'estalvi). 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 frau, de funcionaris, segons l'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 certificats; ~11,5 M per autenticació 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 (Índia) — *Digital Exclusion: Poor, Elderly Face the Brunt of Aadhaar-Based Authentication Errors* (empremtes desgastades; pensions denegades; huella no obligatòria). 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 (operació LEAP)* (119.050 pagaments insuficients, 736 M£; >15.000 ja morts). 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* i la bona pràctica VIVESS (pensionistes espanyols a l'estranger). 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* (cas Jennifer DeStefano, Arizona; trucada del 20 de gener cap a les 16:55; filla de 15 anys en una competició; rescat d'1 milió rebaixat a 50.000 dòlars; «la voz era tan real»; testimoni posterior davant d'un subcomitè del Senat dels EUA); 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* (mecànica de l'estafa; números internacionals; impediment de contacte; rescat per transferència; recomanacions: calma, contactar per una altra via, preguntes que només la persona real sap respondre); 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 i vídeos alterats o generats amb IA com a falsa «prova de vida», sovint a partir d'imatges públiques; incoherències com tatuatges o cicatrius absents; denúncia a ic3.gov amb el material rebut); Axios — *AI-generated videos, photos used in new virtual kidnapping scams, FBI warns* (5 de desembre 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 producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; prova de vida amb repte i frescor — nonce imprevisible respost i segellat al minut; rastre voluntari amb

moments triats; cap registre central; revocabilitat). Vegeu els capítols 13, 15 i 64; la veu clonada, al capítol 68.

427. La Moncloa / Ministeri de l'Interior — *Las Fuerzas de Seguridad investigaron la desaparición de 16.147 personas en 2024* (+6 %; el 72 % dels casos esclarits en menys d'una setmana; CNDES pioner a Europa); Ministeri de l'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 denúncies; 928 alertes publicades, 132 actives; 11.461 episodis únics, mitjana de 3 denúncies en reincidents). 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 (síntesi de l'*Informe McLaren*) — *McLaren Report* (≥643 positius «desapareguts»; ADN masculí en mostres femenines). https://en.wikipedia.org/wiki/McLaren_Report
429. World Anti-Doping Agency — *Independent investigation confirms Russian state manipulation of doping control* (McLaren, Persona Independent; >1.000 atletes). 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 mostres amb marques als taps, 12 de medallistes; Part 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 mostres amb sal fisiològicament impossible). https://www.chemistryworld.com/news/anti-doping-scientists-expose-cheating-russian-athletes/2500159.article
432. Republik — *Bad bottles* (les ampolles «inviolables» Berlinger, vulnerades). https://www.republik.ch/2018/02/21/bad-bottles
433. World Anti-Doping Agency — *Athlete Biological Passport* (detecció indirecta; mòdul hematològic 2009, esteroide 2014). https://www.wada-ama.org/en/athlete-biological-passport
434. ESPN — *Pellizotti banned in landmark biological-passport ruling* (2 anys sense positiu; primer cas validat pel 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 partits; 425 persones; >15 països). 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 partits; 1.108 sospitosos; 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 anys; ~180 tenistes de >35 països; ~7 M€). https://www.washingtonpost.com/world/interactive/2023/tennis-match-fixing-itf-grigor-sargsyan/
438. U.S. Department of Justice / SDNY (via Music Business Worldwide) — *North Carolina man pleads guilty to AI-assisted music streaming fraud* (Michael Smith; decomís 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 comptes-bot; 661.440 reproduccions/dia; els correus). 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 l'activitat; estimació de part). 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* (anunciat nov-2023; vigent 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 $424 million in unmatched royalties* (la «caixa negra»). https://www.billboard.com/pro/mechanical-licensing-collective-receives-over-424-million-unmatched-royalties-streaming-services/
443. IFPI — *Global Music Report 2026* (31.700 M$; 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 entrades; >31 M$ en sancions). 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 revenedors, 6.345 comptes, 246.407 entrades; «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 peticions; ~12 M d'«entitats» amb 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 denúncies, 48,8 M$ de pèrdues). https://www.ic3.gov/AnnualReport/Reports
449. NPR — *The AI deepfake Biden robocall and the FCC* (Nou Hampshire; Steve Kramer; multa de 6 M$). https://www.npr.org/2024/05/23/nx-s1-4977582/fcc-ai-deepfake-robocall-biden-new-hampshire-political-operative
450. Federal Communications Commission — *FCC makes AI-generated voices in robocalls illegal* (Declaratory Ruling, febrer de 2024). https://www.fcc.gov/document/fcc-makes-ai-generated-voices-robocalls-illegal
451. Federal Communications Commission — *FCC settles Lingo Telecom robocall investigation* (1 M$; STIR/SHAKEN + conèixer el client i el proveïdor). https://www.fcc.gov/document/fcc-settles-lingo-telecom-robocall-investigation
452. TransNexus — *SHAKEN statistics, April 2025* (només el 42,5 % de trucades firmades; la bretxa no-IP). https://transnexus.com/blog/2025/shaken-statistics-april/
453. Cifas — *Fraudscape 2025* (+1.055 % de SIM-swaps no autoritzats al Regne Unit). 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 criptomonedes). 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 l'origen humà de la veu al punt de creació). 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 xarxa). 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 frau de veu sintètica conegut). http://thenextweb.com/news/fraudsters-deepfake-ceos-voice-to-trick-manager-into-transferring-243000
458. Payment Systems Regulator (Regne Unit) — *APP fraud reimbursement protections* (règim obligatori des del 7-10-2024, primer del món; particulars, microempreses i entitats benèfiques; Faster Payments i CHAPS; límit 85.000 £ — rebaixat de 415.000 per alinear-lo amb l'FSCS; cost compartit 50/50 entre proveïdor emissor i receptor; reemborsament en 5 dies hàbils o fins a 35 amb investigació; substitueix el codi voluntari CRM); anàlisis de Freshfields, A&O Shearman i 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, transposada a Espanya pel RDL 19/2018): en operacions de pagament no autoritzades, devolució per part del proveïdor llevat de frau o negligència greu del client; càrrega de la prova de l'autenticació correcta sobre el proveïdor; autenticació reforçada (SCA); reforma europea dels pagaments (PSD3/PSR) en tramitació.
460. t2p — manual de producte (gravació d'àudio de converses pròpies; captura de pantalla i de pàgina web certificades — imatge completa + codi font; certificar qualsevol fitxer per lots; projectes per a l'expedient d'un incident; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice

verificable sense connexió; només empremtes a la cadena). Vegeu els capítols 13 i 15; la veu clonada i la SIM, al capítol 68; el CFO suplantat, al capítol 87; la caixa negra personal, al capítol 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 peces; >70 % rastrejades a la Xina; 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 peces falses). https://www.gao.gov/products/gao-12-375
463. Center for Public Integrity — *Counterfeit chips plague Pentagon weapons systems* (VisionTech; l'abrillantador als xips; McCloskey, 38 mesos). 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 blanc; defectes del 27 %). https://www.airandspaceforces.com/c-27jandc-130jpartslinkedtocounterfeitmills/
465. Semiconductor Industry Association — *Winning the battle against counterfeit semiconductor products* (>7.500 M$/any; ~11.000 llocs de treball). https://www.semiconductors.org/resources/winning-the-battle-against-counterfeit-semiconductor-products/
466. ERAI — *2024 Annual Report* (1.055 peces sospitoses; el màxim des de 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 mesos; submarí nuclear, sistema de míssils). 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* (laboratoris acreditats ISO/IEC 17025). https://www.sae.org/standards/content/as6171/7/
469. CALCE (University of Maryland) — *Counterfeit electronics detection and avoidance* (un xip reciclat pot semblar idèntic a l'autèntic). https://calce.umd.edu/counterfeit-electronics-detection-and-avoidance
470. Defense Microelectronics Activity (DMEA) — *Trusted Foundry / Trusted IC* (proveïdors de confiança amb pedigrí controlat; 2003, amb la NSA). https://www.dmea.osd.mil/TrustedIC.aspx
471. Wikipedia — *XZ Utils backdoor* (CVE-2024-3094; CVSS 10,0; Andres Freund, enginyer de Microsoft i desenvolupador de PostgreSQL, investigant ~500 ms de latència extra a SSH; report a Openwall el 28-29 de març de 2024; campanya d'enginyeria social de «Jia Tan» amb comptes falsos pressionant el mantenidor; codi ocult a build-to-host.m4 i fitxers de test binaris dins dels tarballs — invisible a la revisió del repositori; potencial superior a SolarWinds; caçat abans del desplegament massiu); 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 setembre de 2025; primer cuc autoreplicant a npm; >500 paquets; @ctrl/tinycolor amb >2,2 milions de descàrregues setmanals; paquets de CrowdStrike; collita de credencials AWS/GCP/Azure amb TruffleHog; persistència via GitHub Actions; propagació amb els drets de publicació dels mantenidors); CISA — *Widespread Supply Chain Compromise Impacting npm Ecosystem* (alerta del 23 de setembre de 2025); StepSecurity — *Shai-Hulud: Self-Replicating Worm Compromises 500+ NPM Packages*; Datadog — *The Shai-Hulud 2.0 npm worm* (segona onada, novembre). 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* (registre públic append-only; >101 milions d'entrades de >33.000 projectes: Kubernetes, CPython, Istio, urllib3; mètode de signatura per defecte per a Kubernetes, npm, Maven i PyPI; atestacions de procedència a npm i PyPI); OpenSSF / Trail of Bits — *Catching malicious package releases using a transparency log* (desembre de 2025; monitorització de Rekor per detectar publicacions fraudulentes amb credencials

robades). 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 — *Reglament (UE) 2024/2847, de 23 d'octubre de 2024* (Cyber Resilience Act: requisits horitzontals de ciberseguretat per a productes amb elements digitals; en vigor el desembre de 2024; obligacions de notificació des de l'11 de setembre de 2026; aplicació plena l'11 de desembre de 2027; seguretat durant tot el cicle 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 producte (empremta SHA-512; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; empremtes de versions i manifests per lots; ancoratge neutral i transversal, complementari als registres de transparència sectorials). Vegeu els capítols 13 i 15; el pedigrí del maquinari, al capítol 70; els registres inesborrables, al capítol 57.
476. Agnew et al. (PLOS ONE) — *Estimating the worldwide extent of illegal fishing* (11-26 milions de tones; 10.000-23.500 M$/any). https://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0004570
477. Oceana — *Oceana study reveals seafood fraud nationwide* (33 % mal etiquetat; «red snapper» 87 %). https://oceana.org/reports/oceana-study-reveals-seafood-fraud-nationwide/
478. Global Fishing Watch / Nature — *Satellite mapping reveals extensive industrial activity at sea* (~75 % de vaixells sense rastreig públic). https://globalfishingwatch.org/press-release/new-research-harnesses-ai-and-satellite-imagery-to-reveal-the-expanding-footprint-of-human-activity-at-sea/
479. Comissió Europea — *Illegal fishing (IUU): catch certificates i CATCH* (Reg. (CE) 1005/2008; CATCH obligatori des del 10-gen-2026). https://oceans-and-fisheries.ec.europa.eu/fisheries/rules/illegal-fishing_en
480. Global Witness — *The ITSCI Laundromat* (fins al 80-90 % de mineral «net» procedent de fonts il·lícites). https://www.globalwitness.org/en/campaigns/natural-resource-governance/itsci-laundromat/
481. Kimberley Process / World Diamond Council — *The Kimberley Process fact sheet* (de ~15 % als anys 90 a <1 %; ~99 % de la producció). https://www.worlddiamondcouncil.org/wp-content/uploads/2022/02/The-Kimberley-Process-Fact-Sheet.pdf
482. Environmental Justice Foundation — *Thailand's Seafood Slaves* (esclavitud a bord; l'illa de Benjina). https://ejfoundation.org/reports/thailands-seafood-slaves
483. Science Advances (Park et al.) — *Illuminating Dark Fishing Fleets in North Korea* (>900 vaixells; >164.000 t; >440 M$). https://www.science.org/doi/10.1126/sciadv.abb1197
484. Ledger Insights — *Everledger bankruptcy* (el risc de centralitzar la traçabilitat de diamants 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 per a un grup armat). https://www.theafricareport.com/375904/drc-rwanda-rubaya-coltan-mine-at-the-heart-of-m23-financing/
486. ProPublica / NPR (Justin Elliott i 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 $187 million* (família Reynolds; <3 % als pacients). https://www.ftc.gov/news-events/news/press-releases/2015/05/ftc-all-50-states-dc-charge-four-cancer-charities-bilking-over-187-million-consumers
488. FBI Internet Crime Complaint Center — *PSA: charity and disaster-relief fraud* (2024; ~96 M$; la IA augmenta la legitimitat aparent). https://www.ic3.gov/PSA/2025/PSA250116
489. New York Attorney General (Letitia James) — *Pennies for Charity 2025* (els captadors es queden el 25 %; <50 % en la meitat de campanyes). 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 conferències; directius destituïts el març de 2016). https://www.cbsnews.com/news/cbs-news-investigates-wounded-warrior-project-spending/

491. GuideStar, Charity Navigator i BBB Wise Giving Alliance — *The Overhead Myth* (2013; l'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 i 5.500 $ per 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 $ per recaptar 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 filantropia com a «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* (context del frau). 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 danys punitius; 33 % de responsabilitat). 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 instantània de col·lisió a +3 min; la imatge NAND; el perit 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; frenat d'emergència desactivat). https://www.ntsb.gov/investigations/Pages/HWY18MH010.aspx
499. California DMV — *Statement on Cruise LLC suspension* (24-oct-2023; el metratge de l'arrossegament, omès). 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* (supervivència; ≥88 paràmetres). 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 hores). 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-xoc 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* (els registres de geofencing contradiuen l'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* (els 4 minuts decisius, fora de la caixa). 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)* (les mateixes dades, causes oposades). 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 setembre de 2025; migració Telefónica → UTE Vodafone+Securitas; dades anteriors al 20 de març de 2024 inaccessibles; memòria de la Fiscalia General de l'Estat; ≈4.500 polseres actives). 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 setembre de 2025; «nombroses absolucions i sobreseïments provisionals»). 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 (agències) — *Redondo aborda en el Senado la gestión de pulseras para maltratadores tras ser reprobada en el Congreso* (setembre de 2025; disculpes a les víctimes; possibles penalitzacions al contractista). 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 d'octubre de 2025). https://www.hayderecho.com/2025/10/08/pulseras-antimaltrato-analisis-juridico-politico/

511. Tribunal Constitucional — *STC 114/1984, de 29 de novembre* (gravar una conversa pròpia no vulnera l'art. 18.3 CE; admissible com a prova documental; límit de l'esfera íntima; origen laboral del cas). 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 gravacions de participants); 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 (advocats) — *¿Es delito grabar una conversación sin consentimiento?* (art. 197.1 CP: presó d'1 a 4 anys i multa de 12 a 24 mesos; difusió: 2 a 5 anys); 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* (clons convincents amb 3-5 minuts d'àudio; alguns sistemes amb 30 segons; anàlisi d'espectrogrames i prosòdia). https://digitalperito.es/glosario/clonacion-voz/
515. Economist & Jurist — *La prueba sintética en el proceso judicial: retos probatorios de los deepfakes* (impugnar desplaça la càrrega; el TS exigeix impugnació tècnica, no genèrica; criteris d'admissió reforçats); 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 condemnes fermes, 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* (sèrie 2009-2024); ANAVID — *¿De dónde sale la cifra del 0,01 %?* (matís metodològic: només falsedat acreditada amb dol). 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?* (criteris AEPD: gravació limitada a l'incident, ~20 segons abans i després, preferible sense so; vàlida com a prova per interès legítim i 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: Llei 58/2019, prohibit fins i tot portar-la; Alemanya: admissió limitada a l'incident; França: CNIL, conductor responsable del tractament). https://www.tododashcam.es/pages/blog-legislacion-dashcams-espana
520. AlertCops (Secretaria d'Estat de Seguretat, Ministeri de l'Interior) — *AlertCops incorpora un botón SOS* (5 pulsacions en menys de 6 segons; ubicació + 10 segons d'àudio a les FCSE; codi AVDG per a víctimes de violència de gènere). 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 intents de frau anuals; ≈2.000 M€; 6 de cada 100 lesions; accidents simulats: 3,2 % dels declarats, 18 % del cost investigat; Procediment Operatiu 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 juliol de 2025; set accidents simulats en vuit mesos). 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 producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; el contingut no surt mai del dispositiu; revelació voluntària). Vegeu els capítols 13 i 15.

524. TechCrunch — *23andMe confirms hackers stole ancestry data on 6.9 million users* (2023; les llistes segmentades per origen ètnic). 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 i Shai Carmi (Science) — *Identity inference of genomic data using long-range familial searches* (2018; el 2 % de la població basta). https://www.science.org/doi/10.1126/science.aau4832
526. CNBC — *23andMe bankruptcy: selling and deleting DNA* (2025; +526 % de trànsit; ~1,9 M de sol·licituds d'esborrament). 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* (coalició de 28 fiscals generals). 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$; tancament 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 (Regne Unit) — *ICO fines 23andMe £2.31 million* (155.592 residents britànics; la sanció castiga la custòdia). 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* (l'ADN el va pujar 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 per defecte; només ~14 % van optar per participar). https://www.legalgenealogist.com/2019/05/19/gedmatch-reverses-course/
532. National Human Genome Research Institute — *GINA: Genetic Information Nondiscrimination Act (2008)* (no cobreix vida, invalidesa ni cures de llarga durada). 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; pujar el teu ADN no fa «públic» el dels teus parents). https://www.sciencedirect.com/science/article/pii/S0267364925000019
534. Fortune — *Tesla lawyers argue recordings of Musk touting Autopilot could be deepfakes* (Huang contra Tesla; jutgessa 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 càrrega traslladada a la fiscalia; 20 minuts per a un pèrit d'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; jutge 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* (l'agent Pinheiro; el búfer de 30 segons sense so). 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* (només el 42 % de 79 homicidis; «no existeix» fals en 1 de cada 5). https://www.propublica.org/article/how-police-undermined-promise-body-cameras
539. Robert Chesney i Danielle Keats Citron — *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security* (107 California Law Review 1753, 2019; el «dividend del mentider»). 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: proposta de Regla 707 (prova generada per màquina) i 901(c)* (comentari fins al 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 còpies digitals). 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* (àudio editat després de la trucada per inserir amenaces). 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* (Anglaterra i Gal·les; 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; jutge 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* (controls d'auditoria obligatoris; integritat de l'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 amb segell de temps; un canvi no pot ocultar el registre 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; només ~25 % amb polítiques de copiar-enganxar). 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; gairebé la meitat de la despesa al nivell màxim de severitat). 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 als historials). 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 accessos; la primera condemna de presó per una violació 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; accés del pacient a la seva informació de salut). 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 i Adam Wright (Applied Clinical Informatics) — *Identifying a Clinical Informatics or EHR Expert Witness* (2023; el log és prova que cal 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* (desembre de 2023; 3.226 casos sospitosos a LAION-5B; recomanació de deprecar els models). 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* (agost de 2024; 2.236 enllaços eliminats). https://laion.ai/blog/relaion-5b/
556. JFrog Security Research — *Data Scientists Targeted by Malicious Hugging Face ML Models with Silent Backdoor* (2024; tècnica *nullifAI*, abús de *pickle*, porta del darrere). 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* (març 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* (documentació tècnica Annex XI; resum del contingut d'entrenament; sancions de fins a 15 M€ o 3 %). https://artificialintelligenceact.eu/article/53/
559. Comissió Europea — *General-Purpose AI Models in the AI Act: Questions & Answers* (plantilla del resum d'entrenament; aplicació des del 2 d'agost de 2025; marcatge de l'art. 50 des del 2 d'agost 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, models i configuracions amb procedència; des de 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: més de 100.000 milions de continguts marcats segons Google I/O 2026 (maig de 2026); credencials de contingut). 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. Consell 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, febrer de 2024: el chatbot va inventar una política de tarifa de dol; 812 $ canadencs de compensació sobre 1.630,36 pagats; «Air Canada no va tenir la cura raonable de garantir que el seu chatbot fos exacte»; «és responsable de tota la informació del seu web — tant li fa que vingui d'una pàgina estàtica o d'un chatbot»); Forbes — *What Air Canada Lost In 'Remarkable' Lying AI Chatbot Case* (l'al·legació que el chatbot era «una entitat 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* (credencials tokenitzades d'abast limitat per a agents; servidor MCP; un token de 200 $ no pot autoritzar 500 $); Mastercard — *Agent Pay* (anunciat el 29-4-2025: Agentic Tokens que lliguen credencial, agent, àmbit de comerços i política de consentiment; «Agent Pay for Machines», juny de 2026); Google AP2 (setembre de 2025, 60+ socis: Intent Mandate + Cart Mandate signats com a credencials verificables); Eco/Paz — guies del comerç agèntic 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 producte (certificar qualsevol fitxer — el mandat i els registres, només l'empremta viatja; captura de pàgina web amb imatge completa + codi font; signatura amb vídeo-selfie, dos reptes de vida aleatoris i verificació biomètrica del dispositiu; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; la procedència dels models, al capítol 79; els agents del sector públic, al capítol 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'* (maig de 2024; anàlisi forense de la Universitat Estatal d'Arizona: més semblant que el 98 % de les actrius). 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* (consentiment informat; descripció específica de l'ús; consentiment nou per a la reutilització). 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 l'1 de juliol de 2024; la veu al dret de publicitat; responsabilitat de les eines d'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)* (dret federal sobre la rèplica digital; versió revisada de 2026, aprovada

per la Comissió Judicial del Senat el 18 de juny de 2026). https://www.judiciary.senate.gov/no-fakes-act

576. World Economic Forum — *Deepfake legislation: Denmark takes action* (presentada el juny de 2025; dret de tipus copyright sobre cara, cos i veu; retirada i compensació; excepcions de paròdia; en tràmit parlamentari, entrada en vigor prevista a mitjan 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'* (maig de 2024). https://variety.com/2024/digital/news/scarlett-johansson-responds-shocked-angered-openai-chatgpt-her-1236011135/
578. SAG-AFTRA — *Digital Replicas 101* (tipologia i drets de consentiment de l'intèrpret). 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 — *Llei núm. 2024-120, de 19 de febrer de 2024, per garantir el respecte del dret a la imatge dels infants* (modificació de l'art. 371-1 del Codi civil: l'autoritat parental inclou la protecció de la vida privada i del dret a la imatge del menor; protecció exercida en comú pels dos progenitors, associant-hi l'infant segons edat i maduresa; delegació judicial de l'exercici del dret d'imatge en cas d'atemptat greu a la dignitat o la integritat moral); DAJ/economie.gouv.fr — *Respect du droit à l'image des enfants: les apports de la loi* (context: un infant apareix de mitjana en 1.300 fotografies en línia abans dels 13 anys; riscos: usurpació, xantatge, ciberassetjament); 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. Marc espanyol (LO 1/1982 sobre l'honor, la intimitat i la pròpia imatge; LO 1/1996 de protecció jurídica del menor; intervenció del Ministeri Fiscal; doctrina judicial que exigeix l'acord de tots dos progenitors per publicar imatges dels fills). Vegeu el capítol 81 per al dret d'imatge general i el capítol 53 per als registres de coparentalitat.
584. t2p — manual de producte (escàner de documents; captura de pantalla i correu certificades; certificar qualsevol fitxer — només l'empremta viatja, el contingut no surt mai del dispositiu; signatura amb vídeo-selfie; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; la coparentalitat, al capítol 53; la difusió íntima, al capítol 83.
585. Euronews — *The Almendralejo case: when AI deepfakes are used to undress teenagers* (setembre de 2023; testimoni d'una mare; víctimes de 12-14 anys). 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* (juliol de 2024; 15 menors condemnats; 20 delictes de material d'abús infantil i 20 contra la integritat moral). https://www.scottishlegal.com/articles/spain-court-punishes-schoolboys-for-spreading-ai-deepfakes-of-girls
587. Wikipedia — *Taylor Swift deepfake pornography controversy* (gener de 2024; una publicació vista més de 47 milions de vegades; X bloqueja les cerques del seu nom). https://en.wikipedia.org/wiki/Taylor_Swift_deepfake_pornography_controversy
588. Congress.gov / The White House — *TAKE IT DOWN Act* (S.146; signada el 19 de maig de 2025; retirada en 48 h; compliment a plataformes aplicat per la FTC des del 19 de maig de 2026; primera condemna penal l'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 juny de 2024; tipifica el material íntim manipulat; ordres de retirada i preservació de proves). 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; més del 90 % del contingut deepfake és pornogràfic, gairebé tot contra dones).

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* (empremta generada al dispositiu; la imatge no surt mai; més de 500.000 imatges protegides; socis 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* (anàlisi del mecanisme d'avís i retirada). https://www.skadden.com/insights/publications/2025/06/take-it-down-act
593. RAINN — *TAKE IT DOWN Act* (perspectiva de les víctimes de violència 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 (Itàlia) — *Italy unanimously passes anti-cyberbullying law* (maig 2017; Llei 71/2017; Carolina Picchio, 14 anys, 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 desembre de 2022; 46 %; insults 32 %, rumors 22 %, amenaces 10 %). https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/
597. OMS-Europa i estudi HBSC — *One in six school-aged children experiences cyberbullying* (27 de març de 2024; 16 %; 44 països; ≈280.000 joves). https://www.who.int/europe/news/item/27-03-2024-one-in-six-school-aged-children-experiences-cyberbullying--finds-new-who-europe-study
598. Fundació ANAR i Fundació Mutua Madrileña — *VIII Informe de Prevenció de l'Assetjament Escolar* (2025; 12,3 % vs 9,4 %; 14,2 % amb IA; 91,7 % del mateix centre; 17.562 alumnes). 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* (juny de 2024; adolescents 50 %; 36 % salt al món físic). https://www.adl.org/resources/report/online-hate-and-harassment-american-experience-2024
600. CBS News / ITV News — *Molly Russell inquest* (30 de setembre 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, març de 2024; rèplica 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; gener-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 % odi; +70 % «m'agrada»; activitat coordinada sense reduir). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11819532/
604. Comissió Europea — *Guidelines on the protection of minors under the Digital Services Act* (14 de juliol de 2025; ciberassetjament, verificació d'edat; riscos sistèmics = discurs d'odi il·legal). https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors
605. La Moncloa — *Avantprojecte de Llei Orgànica per a la protecció de les persones menors d'edat als entorns digitals* (Consell de Ministres, 4 de juny de 2024; «allunyament en línia»; verificació d'edat). https://www.lamoncloa.gob.es/consejodeministros/resumenes/Paginas/2024/040624-rueda-de-prensa-ministros.aspx
606. Codi Penal (Espanya) — arts. 510 (delicte d'odi; presó 1-4 anys) i 172 ter (assetjament/stalking; agreujat per l'edat 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* (deures en vigor el 25 de juliol de 2025; bullying i contingut d'odi; multes fins al 10 % de la facturació mundial). https://www.gov.uk/government/collections/online-safety-act
608. eSafety Commissioner (Austràlia) — *Social media age restrictions* (Act 2024; menors de 16 des del 10 de desembre de 2025; primer país). https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions
609. t2p — manual de producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice). Vegeu els capítols 13 i 15.

610. INCIBE / Infobae — *El teléfono de tu hijo no se dañó: la estafa en WhatsApp que pide dinero para una emergencia* (8 de maig de 2025; mecànica del «hola mamà», variants, recomanacions de verificació); Policia Nacional (alerta) — OKDiario; València News — *Així funciona l'estafa del «fill en apuros» per SMS i 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 $7.75B to cybercrime in 2025 — a 59% jump* (201.266 denúncies de majors de 60; 4.900 M$ el 2024, +43 %; >3.100 denúncies sènior amb IA i >352 M$; >5 M$ en estafes d'angoixa amb veu clonada); PPC Land — *AI-linked fraud costs Americans $893 million* (22.364 denúncies d'IA el 2025). https://www.housingwire.com/articles/fbi-seniors-cybercrime-2025/ · https://ppc.land/ai-linked-fraud-costs-americans-893-million-fbi-reports-for-2025/
612. FBI / IC3 — *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud* (PSA-241203, 3 de desembre de 2024; clonació de veu en estafes d'angoixa i suplantació de familiars). https://www.ic3.gov/PSA/2024/PSA241203
613. Factchequeado — *Qué son las estafas de romance y cómo identificarlas* (FTC: ≈60.000 denúncies i 1.200 M$ el 2024; la franja 65-74 amb les pèrdues més altes); 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* (crim de Morata de Tajuña, 2023: tres germans grans assassinats; estafa de fins a 263.000 €). https://es.wikipedia.org/wiki/Estafa_rom%C3%A1ntica
615. Ministeri de l'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 febrer de 2022; «Les Fossoyeurs» de Victor Castanet; Orpea ≈260.000 residents; racionament; investigacions penals per maltractament, malversació i infraccions laborals; denúncies per homicidi involuntari); infoLibre — *El último escándalo de Orpea* (injecció estatal de 605 M€ per una participació majoritària). 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 € i indemnització de 3.000 € confirmades per l'Audiència Provincial de Madrid; càmera de les filles avalada com a prova). 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?* (sospita fundada de delicte greu; càmera temporal i enfocada; triple judici de proporcionalitat). 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 — *Llei 8/2021, de 2 de juny, per la qual es reforma la legislació civil i processal per al suport a les persones amb discapacitat en l'exercici de la seva capacitat jurídica* (suport, no substitució; mesures voluntàries davant notari; aptitud per testar; rendició de comptes; 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 producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; prova de vida amb repte; contingut mai fora del dispositiu; revelació voluntària). Vegeu els capítols 13, 15 i 64.
621. Atlantic Council — *Russian War Report: Hacked news program and deepfake video spread false Zelenskyy claims* (16 de març de 2022; pirateig del teletip i el web d'Ukraine 24; deepfake de rendició; desmentit amb selfie de «provocació 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* (juliol de 2025; veu clonada del secretari d'Estat a Signal; cable del Departament d'Estat del 3 de juliol). 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; reemissió no verificada de Channel 14 d'un deepfake de Yoav Gallant; tall en directe i 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* (febrer de 2024; deepfake d'inversions fraudulentes; patró en diversos bancs centrals). https://www.romania-insider.com/bnr-mugur-isarescu-deepfake-february-2024
625. Wikipedia — *2018 Hawaii false missile alert* (13 de gener de 2018; falsa alerta WEA de míssil balístic; correcció de 38 minuts; error genuí). https://en.wikipedia.org/wiki/2018_Hawaii_false_missile_alert
626. FEMA — *Integrated Public Alert & Warning System (IPAWS)* (alertes oficials signades digitalment per l'autoritat emissora i autenticades per IPAWS-OPEN; línia base d'autenticació a l'emissió). 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 maig de 2026; deepfake del PM Lawrence Wong, el president Tharman i representants de la MAS; pèrdua de 4,9 M$ SGD per 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* (setembre de 2025; alertes oficials falses, el «dividend del mentider» i l'autenticació de les comunicacions d'emergència). 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 confirmat com a víctima; HK$200M/US$25,6M; 15 transferències; declaració 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 novembre de 2024; recomana verificació en viu i MFA resistent 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 maig de 2025; veu/text generats per IA; verificació fora de banda i frases pactades). 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* (juliol de 2024; clonació de veu desbaratada amb 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* (maig de 2024; WhatsApp fals, Teams, veu clonada i imatges de YouTube; intent fracassat; advertència 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* (març de 2025; un director financer autoritza 499.000 $ en una trucada de Zoom amb tots els participants deepfake). https://www.tookitaki.com/blog/deepfake-ceo-scam-singapore-2025
635. Nacha — *FBI's IC3 Finds Almost $8.5 Billion Lost to Business Email Compromise in Last Three Years* (~3.000 M$/any; ~8.500 M$ en tres anys; base del frau de pagament). 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* (anàlisi tècnica del patró d'atac amb videotrucada multiparticipant emprat 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* (febrer de 2025; anàlisi del cas Arup i de les fallades de control; argument de la verificació fora de banda). https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/
638. 9to5Mac (sobre el reportatge de WIRED) — *Latest romance scam tactic uses two phones with face-swap app* (abr-2024: els «Yahoo Boys» i el face-swap en temps real dins de videotrucades — dos mòbils en suports i anell de llum, o portàtil amb webcam; presumeixen dels muntatges a Telegram i

els venen; Rachel Tobac: les apps han millorat dramàticament en un any). https://9to5mac.com/2024/04/18/romance-scam-face-swap/

639. iProov — *Threat Intelligence Report 2025: Remote Identity Under Attack* (atacs de càmera virtual nativa +2.665 %; face swaps +300 % respecte del 2023, dirigits contra sistemes amb protocols de detecció de vida; ~24.000 usuaris venent tecnologies d'atac com a servei; la conversió d'imatge a vídeo com a vector nou; 127 eines de face-swap, 91 càmeres virtuals i 10 emuladors catalogats). 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 (via FutureCIO) — *Deepfakes to render identity verification and authentication solutions inefficient* (predicció de feb-2024: el 2026, el 30 % de les empreses ja no consideraran fiables aïlladament les solucions de verificació d'identitat i autenticació, pels deepfakes contra la biometria facial; atacs d'injecció +200 % el 2023; els estàndards de detecció d'atacs de presentació no cobreixen la injecció digital; Akif Khan: combinar PAD, IAD i inspecció d'imatge). 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 i dades personals robades per optar a feines remotes de TI, programació, bases de dades i programari — algunes amb accés a dades de clients i sistemes corporatius; senyals: llavis i so desincronitzats, tos o esternuts que no quadren amb la imatge). https://www.ic3.gov/PSA/2022/psa220628
642. Decrypt — *People Are Using Basic AI to Bypass KYC — But Should You?* (feb-2024: OnlyFake, carnets i passaports falsos generats «amb xarxes neuronals» per 15 $ — EUA, Itàlia, Xina, Rússia, Argentina, Txèquia, Canadà —; 404 Media va superar-hi el KYC de l'exchange OKX, que usa el verificador extern Jumio; usuaris els feien servir per obrir comptes bancaris i desbloquejar comptes 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 autors, amb investigadors del MIT, d'OpenAI i de Microsoft: credencials digitals per demostrar que ets una persona real — no una IA — sense revelar cap dada personal; emissió presencial o institucional; verificació criptogràfica; «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. Comissió Europea / Corbado — el Reglament (UE) 2024/1183 d'identitat digital europea: els estats membres han d'oferir una cartera EUDI a ciutadans, residents i empreses (termini: desembre de 2026); menys d'un terç dels estats compleixen avui el llistó de preparació (observatori 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 producte (signatura amb vídeo-selfie: «la signatura més forta de l'app» — la càmera frontal grava mentre signes, parpelleig i dos reptes de vida aleatoris (girar el cap, somriure, inclinar-lo) en menys de 60 segons, verificació biomètrica del dispositiu obligatòria amb PIN com a alternativa, signatura manuscrita, 2 crèdits i dues transaccions; certificat dedicat amb el document, la signatura, l'evidència en vídeo i les dues transaccions; només una persona a l'enquadrament; certificat amb SHA-512, segell RFC 3161/eIDAS, àncora a la blockchain pública, QR i verificació forense amb integritat del dispositiu i attestation de maquinari; paquet .asice ETSI verificable fora de línia sense confiar en el fabricant; els fitxers romanen al dispositiu — només l'empremta viatja; la prova de vida confirma «una persona real i present» en signar). Vegeu els capítols 13 i 15; la suplantació de directius i la regla «sense segell, no hi ha pagament», al capítol 87; qui contractes en remot, al capítol 91; el compromís i revelació, als capítols 45 i 46; la persona única de la participació, al capítol 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; caiguda de ~368 a ~346 $; ~15.000 M$ esborrats; disculpa de l'empresa i compte @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; piulada piratejada d'AP; Dow –143,5 punts; >136.000 M$ esborrats en segons; reacció algorísmica i d'alta freqüència). 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; identitats robades d'assessors FINRA;

inflació del 1.175 %; caiguda del 94 % en un dia; acusació del DOJ el set. 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 conseller delegat Sundararaman Ramamurthy; incidents recurrents gener-abril; promesa d'accions legals). 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 gen. 2024; avís explícit sobre vídeos *deepfake* de consellers delegats per «manipular el preu d'una acció»). https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-alerts/artificial-intelligence-fraud
651. PRNEWS — *Hoax Releases Hit Newswire Services* (comunicat fals Walmart-Litecoin via GlobeNewswire; Litecoin +30 %; angle d'autenticació dels teletips). https://www.prnewsonline.com/hoax-releases-hit-newswire-services/
652. Sidley Austin — *SEC Enforcement FY2025 Results Signal Shift in Priorities* (456 accions; 17.900 M$ ordenats; ajustat 1.400 M$ + 1.300 M$; prioritat a la manipulació de mercat i el frau de revelació). 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* (difusió d'informació falsa o enganyosa i de rumors a través dels mitjans i internet com a manipulació de mercat). https://lexparency.org/eu/32014R0596/ART_12/
654. FINRA — *Artificial Intelligence (AI) and Investment Fraud* (versió de la FINRA de l'avís; llenguatge sobre vídeos *deepfake* de consellers delegats i notícies falses per moure el preu d'una acció). 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 d'octubre de 2021; 11,9 milions de documents, 2,94 TB, 14 proveïdors, 29.000+ titulars reals, 35 líders i 330+ polítics). https://www.icij.org/investigations/pandora-papers/about-pandora-papers-investigation/
657. Wikipedia — *Panama Papers* (3 d'abril de 2016; 11,5 milions de documents de Mossack Fonseca, 214.488 entitats, 150 investigacions a 79 països, tancament el 2018). https://en.wikipedia.org/wiki/Panama_Papers
658. Transparency International — *Panama Papers: 10 years on* (~1.360 M USD recuperats; reformes CTA, registres UE, ROE; «l'arquitectura del secret offshore roman 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 març de 2025; exoneració de societats domèstiques; població coberta < 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* (estimació original de 32 M de societats obligades; 6,5 M presentades el novembre 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* (sentència del TJUE de 22 de novembre de 2022; invalidació de l'accés públic; marc d'interès legítim). 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 Frankfurt operativa des de l'1 de juliol de 2025; AMLR (UE) 2024/1624 aplicable el 10 de juliol de 2027; registres 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; verificació d'identitat d'administradors i PSC; 100.400 societats afectades, 10.200+ sol·licituds rebutjades). 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 desembre de 2025; tribunal de més rang a confirmar la constitucionalitat de la CTA). https://us.transparency.org/news/unanimous-eleventh-circuit-decision-upholds-the-corporate-transparency-act/

665. FATF — *Beneficial Ownership* (Recomanació 24 revisada el 2022 i guia de 2023; informació adequada, exacta i actualitzada; enfocament multidimensional). https://www.fatf-gafi.org/en/topics/beneficial-ownership.html
666. Open Ownership — *Verification of beneficial ownership data: Overview* (les dades autodeclarades necessiten verificació: conformitat, contrastos creuats, evidència de suport). 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; relat en primera persona: foto d'estoc retocada amb IA, quatre entrevistes en vídeo, detecció EDR del 15 de juliol de 2024, granja de portàtils 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 gener de 2025; canvi de cara amb IA a les entrevistes, gir cap a l'extorsió, recomanacions de verificació d'identitat). https://www.ic3.gov/PSA/2025/PSA250123
669. US DOJ (USAO-DC) — *Arizona Woman Sentenced in $17M IT Worker Fraud Scheme for North Korea* (24 de juliol de 2025; Christina Chapman, 102 mesos, 309 empreses, 68 identitats robades, 17 M$, granja de portàtils, 49 portàtils enviats a l'estranger). 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 novembre de 2025; més de 136 empreses víctimes, més de 18 identitats compromeses, més de 2,2 M$ de beneficis). 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* (previsió del 25 % per al 2028; admissió del 6 % de suplantació a l'entrevista, enquesta a 3.000 candidats). 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 gener de 2026; First Advantage 69 % dels líders del Regne Unit; Checkr 23 % de frau d'identitat; 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* (àudio IA en ~1 de cada 106 reunions; ~1.300 % interanual; veus sintètiques al 0,33 % de les trucades al Q4 de 2024). https://www.pindrop.com/article/growing-trend-of-deepfakes-in-interviews/
674. NIST — *SP 800-63-4 Digital Identity Guidelines* (final, juliol de 2025; nivells de garantia IAL1/2/3 i taxonomia de verificació Remot/Presencial × Atès/No Atès). https://pages.nist.gov/800-63-4/sp800-63.html
675. FBI — *Fraudulent Remote IT Workers from DPRK* (cerca/recomanacions; ús d'identitats robades, ordinadors intermediaris i IA, amb mitigacions per als ocupadors). 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* (credencials verificables i verificació contínua de la identitat d'*onboarding*; context de solució adjacent). https://techcommunity.microsoft.com/blog/microsoft-security-blog/fake-employees-real-threat-decentralized-identity-to-combat-deepfake-hiring/4479864
677. Fiscalia General de Nova 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 Parlament Europeu i del Consell, de 23 d'octubre de 2024, relativa a la millora de les condicions laborals en el treball en plataformes* (en vigor el 2 de desembre de 2024; transposició fins al 2 de desembre de 2026; presumpció de laboralitat per fets de direcció i control amb càrrega de la prova sobre la plataforma; prohibició de dades sensibles en decisions automatitzades; transparència, supervisió humana i intervenció humana en decisions importants); 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 — *Llei 12/2021, de 28 de setembre* («Ley Rider»: presumpció de laboralitat en el repartiment mitjançant gestió algorítmica; dret del comitè d'empresa a ser informat dels paràmetres, regles i instruccions dels algorismes que afecten les condicions de treball; règim en vigor des de l'agost 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 a Barcelona; ≈200 M€ en quotes i multes; 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; provisions de Delivery Hero de 440-770 M€; impacte ≈100 M€ a l'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 sentències; Ola ha d'explicar la lògica de la decisió totalment automatitzada, art. 22 RGPD); Worker Info Exchange — *Uber ordered to pay €584,000 for failure to comply with court order in robo-firing case* (més 4.000 €/dia); 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 producte (empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; contingut al dispositiu, revelació voluntària; els buits de la sèrie queden datats). Vegeu els capítols 13 i 15; la procedència dels models d'IA, al capítol 79.
683. Ministeri de Treball / premsa especialitzada — *Registre horari digital obligatori: la reforma en tràmit* (tramitació urgent aprovada pel Consell de Ministres el 30-9-2025, desacoblada de la reducció de jornada; objectiu d'aprovació durant el 2026, sense data d'entrada en vigor publicada; requisits del projecte: registres electrònics traçables i immutables, segellat de temps, registre de pauses, accés remot i en temps real per a la Inspecció de Treball, historial de modificacions amb autoria i data); EPA/INE — més del 40 % de les hores extres no es remuneren; RD-llei 8/2019 — registre diari de jornada obligatori. 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. Marc laboral general (papereta del judici social; actes de la Inspecció de Treball; paper dels delegats). Vegeu el capítol 92 per al treball de plataforma i el capítol 102 per a la cadena de subministrament laboral.
685. t2p — manual de producte (foto amb GPS forense — fix genuí ~50 m / ≤30 s, la ubicació simulada bloqueja la certificació; captura de pantalla i correu certificades; certificar qualsevol fitxer — només l'empremta viatja; certificació en segon pla; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; les converses pròpies i l'assetjament, al capítol 75.
686. The Dial — *Faulty Construction* (judicis pel terratrèmol de Turquia; Isias Grand Hotel; condemnes de 18 anys el desembre de 2024; 75.000 edificis amnistiats; uns 13 milions d'edificis 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* (juliol de 2023; amnisties, no aplicació dels codis i fallades de qualitat del formigó). 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* (investigació federal oficial; 98 morts; inici per fallada de punxonament de la llosa de la piscina; formigó més feble que el codi). 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 treballadors imputats; 384 informes falsificats; manipulació de dates i substitució de provetes; Albert Leung 2,5 anys el juny 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* (febrer de 2010; Testwell/Kancharla; Freedom Tower certificada a 12.000 PSI però d'uns 9.000 PSI; 7 a 21 anys). 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* (Gènova, 14 d'agost de 2018; 43 morts; 59 acusats; documents d'inspecció «clarament falsos»; autovigilància via Spea; acord de 30 M€ el 2023). https://en.wikipedia.org/wiki/Ponte_Morandi_collapse
692. Seton UK — *Understanding the Golden Thread: Building Safety Act 2022* (registre digital traçable i amb control de versions per a edificis d'alt risc, 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* (Reglament de Productes de Construcció revisat; en vigor el 7 de gener de 2025; Passaport Digital de Producte obligatori per al marcatge CE des del 8 de gener 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* (febrer de 2025; treball experimental complet, modelització en curs, presentació tècnica el juny 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* (gestió de la informació amb BIM i registre as-built / bessó digital al llarg del cicle 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 peces; frau de 39,3 M£; ARC falsificats; condemna de 4 anys i 8 mesos; descobriment per 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* (pàgina 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 documents falsificats, 52 referències del CFM56, 68 motors, àleps 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* (traçabilitat segons 14 CFR Part 21/43, Form 8130-3, report amb Form 8120-11). https://www.faa.gov/aircraft/safety/programs/sups
700. EASA — *Suspected Unapproved Parts* (base de dades i definicions de la UE; casos d'EASA Form 1 falsificats; marc dels SIB). https://www.easa.europa.eu/en/domains/aircraft-products/suspected-unapproved-parts
701. EASA — *Safety Information Bulletin SIB 2023-05* (butlletí sobre les peces sospitoses d'AOG Technics i accions de quarantena/reemplaçament recomanades). 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 recomanacions, 9 d'octubre de 2024; digitalitzar 8130-3/Form 1; traçabilitat; acreditació de proveïdors). 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 peces falsificades o no aprovades arriben als avions cada any, ~2 % de 26 milions; mercat de més 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* (desembre de 2025; 2,45 milions de vehicles sospitosos; +14 % interanual; ~3.300 $ de pèrdua mitjana). 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* (acords 2016-2017; sanció civil de 1.450 milions de dòlars; fons de mitigació; ~590.000 vehicles als EUA; descripció del dispositiu de desactivació). https://www.epa.gov/enforcement/volkswagen-clean-air-act-civil-settlement
706. Wikipedia — *Volkswagen emissions scandal* (NOx fins a 40 vegades el límit; ~11 milions de cotxes; ~33.000 milions de dòlars de cost total; cronologia 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 gener de 2024; la sanció civil més alta sota la Clean

Air Act; 630.000+ camions RAM; 325 M$ en remeis; condicions de la revisió). https://www.epa.gov/newsreleases/united-states-and-california-announce-diesel-engine-manufacturer-cummins-inc-agrees

708. EPA — *Summary of Criminal Prosecutions: Berkshire Power* (esbiaix intencionat del CEMS, 2009-2011; ajust fraudulent retirat abans de les auditories; multa penal de 2,75 M$ a BPC; ~7,25 M$ en total el març 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* (prop de 120 Mt de metà fòssil el 2023; UNFCCC ~50 % més baix; OGMP 2.0 ~95 % més baix; esdeveniments de fuga per satèl·lit +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* (emissions mesurades >4 vegades les estimacions de l'EPA; taxa de pèrdua de l'1,6 %, vuit vegades l'objectiu del 0,2 %; 30+ vols cobrint ~70 % de la producció terrestre dels EUA). 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 $241.5M Settlement with Marathon Oil* (11 de juliol de 2024; 64,5 M$ de sanció civil, la més alta a una font fixa; ~90 instal·lacions; ~110.000 tones de COV/metà retallades). 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; definició legal del dispositiu de desactivació; sentència prèvia de desembre de 2020 sobre el reconeixement del cicle de prova). 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* (full informatiu PDF; 58 milions de tones de metà evitades 2024-2038; reducció del ~80 %; Programa de superemissors). 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. Comissió Europea — *New EU Methane Regulation to reduce emissions from fossil fuels* (Reglament (UE) 2024/1787; MRV a escala de font amb verificació de tercers; alerta ràpida de superemissors per satèl·lit; equivalència MRV per als importadors des del 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* (sentència del TJUE de 24 de juny de 2021; extraccions il·legals no computades al Pla Hidrològic 2015-2021; queixes des del 2009); Greenpeace — *Doñana, agua sin ley* (pous, basses i canonades; hivernacles de fresses; desforestacions). 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 — *Llei 19/2022, de 30 de setembre, per al reconeixement de personalitat jurídica a la llacuna del Mar Menor i la seva conca* (primer ecosistema d'Europa; drets a existir, evolucionar, protecció, conservació i restauració; ILP amb 639.826 signatures); Araoz & Rueda — *El TC reconoce la personalidad jurídica del Mar Menor*; BOE — *Reial Decret 90/2025* (comitè de representants: 13 membres, 7 de la societat 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)* (més de 100 països; sensors ciutadans de baix cost); AireCiudadano — xarxa oberta de monitors de partícules amb mapa i API; SciStarter/CanAirIO — sensors oberts 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* (inspecció municipal amb sonòmetre homologat i calibrat; actes amb presumpció de veracitat i ple valor probatori; límits interiors orientatius 35-45 dB dia / 25-30 dB nit); COITTA — *La importancia de la prueba pericial acústica*; Defensor del Pueblo — *Comprobaciones ante las denuncias de ruidos molestos* (habilitar mitjans per comprovar les denúncies). 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 producte (empremta SHA-512 a l'origen — sensor o dispositiu —; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; sèries per lots en temps real; buits datats; contingut al dispositiu i revelació voluntària). Vegeu els capítols 13 i 15; el sensor industrial, al capítol 96; el testimoni orbital, al capítol 104.
720. EUR-Lex — *Sustainability rules for batteries and waste batteries (Regulation (EU) 2023/1542 summary)* (passaport des de 2027 via QR i identificador únic; objectius de contingut reciclat des del 18 d'agost de 2031: Co 16 %, Pb 85 %, Li 6 %, Ni 6 %; accés duaner al registre). 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)* (percentatges de 2031 —Co 16/Pb 85/Li 6/Ni 6— i de 2036 —Co 26/Pb 85/Li 12/Ni 15—, les afirmacions falsificables que el passaport transporta). https://digiprodpass.com/blogs/eu-battery-regulation-recycled-content-targets
722. Minespider — *EU Battery Due Diligence Obligations postponed* (diligència deguda ajornada del 18 ago 2025 al 18 ago 2027 via Reglament (UE) 2025/1561 «stop-the-clock»; guia ampliada fins al 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; cinc anys de desenvolupament amb Circulor; ~10 $/vehicle per 15 anys; QR al muntant de la porta; traça materials, contingut reciclat i petjada de carboni). 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* (més de 20.000 milions de punts de dades a 150 milions de cel·les; ~52 % dels fabricants mundials de cel·les; 15 anys de monitoratge d'estat de salut). https://spectrum.ieee.org/volvo-ex90-battery-passport
725. Global Battery Alliance — *World's First Battery Passport Proof of Concept* (Davos, 18 gen 2023; Audi/BASF/CATL/Glencore/Tesla/VW; les dades «no han estat plenament verificades i s'han complementat parcialment amb estimacions raonables»). https://www.globalbattery.org/press-releases/global-battery-alliance-launches-world%E2%80%99s-first-battery-passport-proof-of-concept/
726. Comissió Europea (Green Forum) — *Implementing the Ecodesign for Sustainable Products Regulation (ESPR)* (ESPR en vigor el 18 jul 2024; el passaport digital de producte com a eina horitzontal; pla de treball 2025-2030 adoptat 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* (anàlisi jurídica que distingeix el pilot de bateries del desplegament horitzontal de l'ESPR; calendari d'actes delegats). https://www.hoganlovells.com/en/publications/digital-product-passports-in-the-eu-comprehensive-expansion
728. CIRPASS — *Standardisation gaps and roadmap (v1.2, July 2024)* (model de dades del DPP, identificadors únics, portadors de dades i llacunes d'estandardització del JTC 24 — l'arquitectura on s'endolla el segell). https://cirpassproject.eu/wp-content/uploads/2024/07/CIRPASS-standardisation-gaps-and-roadmap-V1.2.pdf
729. DOUE/BOE — *Reglament (UE) 2024/1157, d'11 d'abril de 2024, relatiu als trasllats de residus* (deroga el Reglament 1013/2006; aplicable de manera general des del 21 de maig de 2026; exportacions de tots els residus plàstics a tercers països subjectes a notificació i autorització prèvies per escrit; prohibició d'exportar residus per a valorització a països no OCDE; tramitació electrònica); RETEMA — *Nuevo Reglamento de traslados de residuos*; Residuos Profesional — *Análisis del Reglamento (UE) 2024/1157* (context: Turquia va rebre el 39 % de les exportacions europees de residus — 12,4 milions de tones, dades 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. Marc general de residus (documents d'identificació i seguiment dels trasllats; responsabilitat ampliada del productor; jerarquia de residus). Vegeu el capítol 98 per al passaport digital de producte i el capítol 96 per a les emissions.

731. t2p — manual de producte (foto amb GPS forense — fix genuí ~50 m / ≤30 s, la ubicació simulada bloqueja la certificació; vídeo amb data/hora sobreimpresa; escàner de documents fins a 50 pàgines; certificar qualsevol fitxer per lots — només l'empremta viatja; captura de pàgina web amb imatge completa + codi font; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; el passaport de producte, al capítol 98; la ciència ciutadana, al capítol 97.
732. Agrodigital — *El cuaderno digital de explotación será obligatorio a partir del 1 de enero de 2028* (CUE voluntari des de l'1-1-2024; ajornaments; obligatori des de l'1-1-2028 per a explotacions >30 ha de cultius, >5 ha de regadiu o >0,1 ha d'hivernacle; registre electrònic de tractaments fitosanitaris obligatori des de l'1-1-2027 — paper fins al 31-12-2026); FEGA/Agronews — aclariments d'entrada en vigor; Govern d'Aragó — *Cuaderno digital (CUE)* (contingut: actuacions fitosanitàries, fertilització, regs i altres pràctiques). 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 seguiment per monitoratge (imatges Sentinel/Copernicus sobre les parcel·les declarades al SIGPAC; requeriments de fotografies georeferenciades a l'agricultor quan el sistema no pot concloure). Marc general del FEGA i de la Comissió Europea. Vegeu el capítol 104 per a la integritat del testimoni orbital.
734. t2p — manual de producte (foto amb GPS forense — fix genuí ~50 m / ≤30 s, la ubicació simulada bloqueja la certificació; certificació en segon pla — el camp sense cobertura; certificar qualsevol fitxer per lots; escàner de documents; projectes per a l'expedient d'una campanya; empremta SHA-512 al dispositiu; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; certificat PDF amb QR; paquet .asice verificable sense connexió). Vegeu els capítols 13 i 15; el satèl·lit, al capítol 104; els aliments, al capítol 101; els residus, al capítol 99.
735. Europol — *EUR 91 million worth of counterfeit and substandard food seized in Europe-wide operation* (Operació OPSON XIII; 22.000 t d'aliments, 91 M€, 11 xarxes; Itàlia: verge extra i clorofil·la; Espanya: oli i tonyina). 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* (Operació OPSON XIV; 95 M€, 11.566 t, 631 denunciats, 13 grups de crim organitzat, 31 països). 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 $1 million in fake olive oil* (11 de juliol de 2024; escorcoll dels Carabinieri a la Pulla, 42 t de fals verge extra, 623 L de clorofil·la, 7 acusats, etiquetes i segells falsos). https://www.cnn.com/2024/07/11/europe/italy-olive-oil-seizure-scli-intl/
738. Food Safety News — *Spanish and Italian investigators uncover olive oil fraud* (desembre de 2023; Operació Omegabad: 260.000 L comissats, 11 detencions, lampante venut com a verge extra, Ciudad Real/Sicília/Toscana, 91.000 € en efectiu). https://www.foodsafetynews.com/2023/12/spanish-and-italian-investigators-uncover-olive-oil-fraud/
739. Comissió Europea (DG SANTE) — *EU coordinated action on honey ('From the Hives')* (mostres 2021-2022; 46 % de 320 partides sospitoses d'adulteració amb xarop de sucre; metodologia i països participants). https://food.ec.europa.eu/food-safety/eu-agri-food-fraud-network/eu-coordinated-actions/honey-2021-2022_en
740. FoodNavigator — *Geographical Indications worth a mouth-watering €75 billion, study finds* (valor de les IG de la UE: 74.800 M€ el 2017; prima de preu d'unes 2 vegades per als productes protegits). https://www.foodnavigator.com/Article/2020/04/22/Geographical-Indications-worth-a-mouth-watering-75-billion-study/
741. Comissió Europea — *EU Agri-Food Fraud Network: reports and publications* (el frau afecta ~1 % de la indústria i costa 10.000-40.000 M$/any; 758 sospites el 2023, +26 %; carn, mel i oli al capdamunt). 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 maig de 2024; marc únic de DOP/IGP/IG i ETG; protecció com a ingredient i en línia). 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* (judici de 2019; Poujol (Spanghero) 2 anys + 100.000 € de multa, Fasen 2 anys + prohibició permanent; Comigel, 500+ t cap a 13 països). https://www.foodsafetynews.com/2019/04/four-sentenced-in-france-for-roles-in-horse-meat-scandal/
744. FDA — *Economically Motivated Adulteration (Food Fraud)* (definició d'EMA, p. ex. oli barat venut com a 100 % oli d'oliva; deure de controls preventius 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; estat de l'art en segellat/ancoratge de la procedència de l'oli i en autenticació 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 milions de persones en treball forçat el 2021; 17,3 milions a l'economia privada; els migrants tripliquen el risc). 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$236 billion* (març de 2024; +37 % des de 2014; 84.000 milions a Europa i l'Àsia Central). https://www.ilo.org/resource/news/annual-profits-forced-labour-amount-us-236-billion-ilo-report-finds
748. Miller & Chevalier — *UFLPA Enforcement 2024 Year in Review* (16.755 enviaments i 3.690 M$ retinguts; 1.340 M$ el 2024; 48 % d'entrades denegades; +1.600 % a l'automòbil; *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* (marques, subcomponent, cronologia desembre 2023 – mitjan gener 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* (febrer de 2024; VW, BMW, Mercedes, GM i la cadena de l'alumini). https://www.hrw.org/report/2024/02/01/asleep-wheel/car-companies-complicity-forced-labor-china
751. Comissió Europea — *Corporate Sustainability Due Diligence (CSDDD)* (Directiva 2024/1760, en vigor el 25 de juliol de 2024; transposició fins al 26 de juliol de 2028, aplicació des del 26 de juliol de 2029 després de l'Òmnibus). 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* (desembre de 2024; en vigor el 13 de desembre de 2024, aplicació el 14 de desembre de 2027; model d'investigació sense presumpció geogràfica). 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* (aplicació a empreses de 1.000 empleats des de l'1 de gener de 2024; multes fins al 2 % de la facturació mundial; 486 auditories el 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 morts, BSCI; Ali Enterprises, més de 250 morts, SA8000; totes dues havien passat la inspecció). 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* (novembre de 2022; treballadors aleccionats, dobles llibres, nòmines falses, nens amagats). 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 salari mínim legal és el 31 % d'un salari digne a l'Índia, el 37 % a la Xina i Bangladesh, el 33 % a Cambodja, el 13 % a 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 a Ormuz durant la guerra Israel-Iran de 2025; vaixells sobre terra i centrals nuclears; atribució d'Humphreys a l'Iran; ~20 % del petroli mundial per l'estret). 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* (revelació de Windward, 29 d'abril de 2026; VLCC amb números IMO; escales falses a 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 vaixells van falsejar l'AIS abans de ser sancionats, gener 2024-juliol 2025; escales falses a 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+ vaixells afectats el 2T 2025, vuit vegades més que el 1T; punts calents regionals). 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 març de 2026: 1.100+ vaixells en 24 h, 21+ nuclis; fixacions falses a Barakah i Al Hamra; Ormuz un terç avall). 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* (mida de la flota; ~17 % de la flota petroliera mundial; 9.400 M$ d'ingressos extra el 2024; pes creixent de la bandera russa). 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 — *Consell de la UE (Consilium)* (18 de desembre de 2025: el total de la UE arriba a 444+ vaixells; prohibicions d'accés a port i de serveis). 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 — *Consell de la UE (Consilium)* (18 de juliol de 2025: sostre del cru rebaixat de 60 a 47,60 $ amb mecanisme dinàmic 15 % per sota del mercat). 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* (desembre de 2024; acció de l'OFAC sota l'E.O. 13902 citant el MS ENOLA «apagant l'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* (petroler Eagle S de bandera de les Illes Cook, 25 de desembre de 2024, dany al cable submarí del Bàltic; dimensió d'amenaça 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* (blanqueig d'identitat, frau del número IMO, encaixada AIS i mecànica de l'spoofing de posició). 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 d'abril de 2022; nou imatges de Maxar del 18/19/31 de març; cossos al carrer Iablónska; fossa comuna de 14 metres). 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 recollida intensiva de Maxar; ús del *New York Times* el 4 d'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* (mètode guanyador d'un Pulitzer; imatge de Planet i tessel·les censurades; 268 camps nous i 428 emplaçaments sospitosos). https://www.buzzfeednews.com/article/alison_killing/satellite-images-investigation-xinjiang-detention-camps
771. *Deepfake Geography: Detecting AI-Generated Satellite Images* (arXiv 2511.17766, novembre de 2025; ViT 95,11 % enfront de CNN 87,02 % sobre més de 130.000 imatges; artefactes GAN enfront de difusió). 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 i Biessmann; imatge sintètica fotorealista d'instal·lacions incloses centrals nuclears; control d'armament). https://arxiv.org/abs/2404.07754
773. Comissió Europea — *Observer: How Galileo OSNMA helps counter GNSS spoofing* (OSNMA operatiu el 24 de juliol de 2025; primera autenticació mundial del senyal del Servei Obert d'un GNSS via signatures criptogràfiques 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 $700 million program to help AI make sense of satellite images* (contracte d'etiquetatge Sequoia de fins a 708 M$ en 7 anys, 2024; alimenta la visió per computador

Maven; el contracte de dades més gran de l'agència). 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 Integritat, Procedència i Confiança, abril de 2025; defineix integritat/procedència/confiança, però sense signatura criptogràfica ni cadena de blocs). 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 d'octubre de 2024; ES-Alert a les 20:11 i 21:03; en nivell 2 la petició correspon a la comunitat autònoma). 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 convocat a les 15:00, reunit a les 17:00; proposta d'alerta massiva passades les 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 d'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 morts en total: 229 a la província de València, 7 a Castella-la Manxa, 1 a Màlaga; més de 2.600 ferits; 11.242 habitatges; ≈141.000 vehicles; 800 km de carreteres). 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 novembre de 2024; correus de la CHJ de les 13:42, 15:04, 16:13 i 18:43; cabals de les 17:00 i les 18:00; 2.282 m³/s a les 18:55; l'estació d'aforament, destruïda per l'aigua cap a les 19:00, segons el comunicat de la CHJ del 4 de novembre). 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 febrer 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 novembre 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* (instrucció oberta el 10 de març de 2025; Jutjat d'Instrucció núm. 3 de Catarroja, jutgessa 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 març de 2026; el TSJ rebutja investigar 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 d'octubre de 2025); El Español — *La jueza requiere a À Punt «todas las grabaciones de imagen y sonido» de la reunión del Cecopi* (els vídeos, d'una productora contractada per la secretaria d'Emergències; se'n demanen els originals per fixar l'hora exacta de cadascun). 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 d'octubre de 2025; falsa acta municipal de «més de 220 cadàvers»; documents falsos amb més de 800 víctimes; cap víctima mortal al pàrquing). 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 novembre 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 com a principal facilitador); elDiario.es — *Los bulos y falsedades sobre la DANA de València* (interferència en les tasques d'emergència). 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 novembre de 2025; 210.106 indemnitzacions). 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 març de 2026; 212.237 sinistres pagats; 251.249 expedients; el 99,3 % tramitats; cost total estimat ≈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 fins al 19 d'agost; Ourense ≈150.000 ha; Uña de Quintana ≈40.000 ha; A Rúa >38.000 ha; Molezuelas de la Carballeda, més de 700 evacuats; 500 militars addicionals de la UME sobre més 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 vintena de grans incendis en dues setmanes, més de 300.000 ha; la pitjor temporada en més de 30 anys). https://www.vallfirest.com/noticias/oleada-incendios-forestales-2025
794. Centre de Lauegi d'Aran (Conselh Generau d'Aran) — *Butlletí de perill d'allaus i cartografia ATES* (butlletí diari; «la informació no substitueix la formació, l'experiència i el bon judici»). https://lauegi.conselharan.org/ates/?lang=en
795. ICGC — *Butlletí de Perill d'Allaus (BPA)* (Pirineu català); AEMET — *Boletín de peligro de aludes* (resta de massissos). 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 (Espanya) — *Public Warning System / ES-Alert* (art. 110 de la Directiva (UE) 2018/1972, transposat per la Llei 11/2022 General de Telecomunicacions; sistema operatiu des del juny de 2022 i a disposició dels 112 autonòmics des del 2023; tecnologia *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; Llei 40/2015; nexe causal; l'atestat de la Guàrdia Civil com a prova central; silenci administratiu de 6 mesos). https://www.administracionpublica.com/responsabilidad-patrimonial-por-danos-por-el-estado-de-la-calzada/
798. t2p — manual de producte (empremta SHA-512 al dispositiu o a l'origen de la dada; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice). Vegeu els capítols 13 i 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 (Taiwan, 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), introducció i cap. 3 («possibilist, not Pollyanna»; la procedència «alone will not solve the problem»).
806. Beth Simone Noveck — *Reboot* (2026), cap. 3 (assaig coreà sobre alfabetització mediàtica i deepfakes).
807. IPI / VSquare / HKS Misinformation Review — *el deepfake d'àudio Šimečka–Tódová a Eslovàquia* (28-09-2023; moratòria de 48 hores; forat de la política d'àudio de Meta; el debat sobre la influència real en el resultat). 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 ; i *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»; auditories externes).
812. Govern de Califòrnia — *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 (codi obert: els cinc elements; registre de consultes i entrenaments).
815. Beth Simone Noveck — *Reboot* (2026), introducció i cap. 6 («accountability in name only»; la IA com a objecte).
816. Senat Federal del Brasil — *Portal e-Cidadania / Llei Joca* (2024-2025) https://www12.senado.leg.br/ecidadania/ ; i *Reboot* (Noveck, 2026), cap. 7.
817. Audrey Tang i E. Glen Weyl — *Plurality: The Future of Collaborative Technology and Democracy* (2024) ; i *Reboot* (2026), cap. 7.
818. Beth Simone Noveck — *Reboot* (2026), cap. 3 (APIs personals).
819. Beth Simone Noveck — *Reboot* (2026), cap. 7 (escala, acció, institucionalització; «participation without integration»).
820. time2act — capítol 13 (t2p: signatura amb vídeo-selfie i prova de vida al dispositiu) ; T2P-Manual (v1.0, 2026).
821. Beth Simone Noveck — *Reboot* (2026), cap. 3 (enquesta Univ. de Madrid: 51% substituirien polítics per IA).
822. NPR — *Pulitzer Board Recognizes Darnella Frazier For Recording George Floyd's Murder* (11 de juny de 2021; menció especial; citació literal del jurat). 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 anys en gravar; el vídeo com a prova al judici 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»* (cas «Rodea el Congreso»; l'atestat inicial només recollia insults). 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'* (absolució; el tribunal no veu delicte tot i l'absència de proves de l'agressió). 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 l'eficàcia probatòria de l'atestat). 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 juliol de 2024; art. 36.23; el TC anul·la el terme «no autoritzat»; reforma pactada: risc «constatable» i motivat).

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 març de 2025; multes del conjunt de la llei). 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. Amnistia Internacional Espanya — *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 territori amb 800 càmeres; 5.000 agents formats; autorització per a 7.000 i 1.500 més; reglament en actualització). 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 càmeres més previstes; peticions de generalització). 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 model AB3; extensió gradual; previst per a la Guàrdia Civil; objectiu: protegir ciutadania i agents). 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* (agost de 2024; foto d'un membre de l'equip, sense manipular; periodistes d'AP a la pista; 15.000 assistents). 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* (verificació). https://www.univision.com/noticias/fotografias-eventos-campana-kamala-harris-no-ia-como-afirman-trump-y-redes
835. t2p — manual de producte (empremta SHA-512 al dispositiu, per segments durant la gravació; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS complementari; contenidor .asice; cadena d'empremtes contínua per a càmeres corporals; publicació opcional). Vegeu els capítols 13 i 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. (síntesi de modelització climàtica-econòmica) Earth.org. https://earth.org/have-economists-been-underestimating-the-cost-of-climate-change/
839. Orrick — *TAKE IT DOWN Act becomes law*; DEFIANCE Act (Senat, gen-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 — *Estat de descentralització dels L2 d'Ethereum (seqüenciadors)* (2026). https://l2beat.com/scaling/summary — i MEV Watch, *blocs amb 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 — *Accions contra data brokers (X-Mode/Outlogic) i 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 — i 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 — *Expansió d'Eurodac (edat 12→6; accés policial), Pacte de Migració 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 — *Guia d'estil (STYLE.md): «la promesa i el perill»; «res de tecno-utopia sense evidència»*.
851. CPJ (Committee to Protect Journalists) — *Israel-Gaza War* (263 periodistes i treballadors de mitjans morts des del 7-oct-2023; 108 empresonats; 174 ferits; «l'esforç més letal i deliberat per matar i silenciar periodistes que el CPJ hagi documentat mai») i *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), projecte Costs of War — *News Graveyards: How Dangers to War Reporters Endanger the World* (Nick Turse, 1-abr-2025: més periodistes morts a Gaza que a les grans guerres del segle XX combinades — comparativa que la mateixa base de dades usada matisa; ~13 periodistes palestins morts 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 impacte ~10:00 contra la posició de la càmera de Reuters — que emetia en directe — i segon impacte ~10 min després contra rescatadors i periodistes; ≥22 morts, 5 periodistes: 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 i quatre companys, 10-ago-2025; l'alerta prèvia del CPJ i de la relatora de l'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 dona, el fill Mahmoud, la filla Sham i el net Adam de Wael al-Dahdouh) i *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 vet d'accés de la premsa internacional a Gaza: rebuig de la petició de la FPA (gen-2024, «no vested right»), nova petició (set-2024), el govern manté el vet «per raons de seguretat» malgrat l'alto el foc (gen-2026) i el Suprem ajorna de nou (28-gen-2026); més de dues dotzenes d'organitzacions informatives reclamen accés. 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 (Reporters Sense Fronteres) — *RSF files fifth complaint with ICC about Israeli war crimes against journalists in Gaza* (30-set-2025; cinc denúncies des d'oct-2023; ≥210 periodistes morts, 56 amb motius raonables de creure'ls deliberadament atacats; patró de «doble bombardeig») i *«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-set-2024, «It's Bisan From Gaza — and I'm Still Alive»; ~4 milions de seguidors; campanya de desqualificació fallida) i 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* i *Pallywood* (pic de 220.000 usos a X el nov-2023 segons BBC Verify; el cas de la «nina» publicat i retirat pel Jerusalem Post i amplificat pel compte oficial d'Israel a X; el fals positiu del detector «AI or Not» sobre una foto real; Ron Dudai: la documentació descartada amb una sola paraula, «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 — l'explosió a l'hospital al-Ahli (17-oct-2023; 471 morts segons el Ministeri de Salut de Gaza, 100-300 segons la intel·ligència dels EUA) i la divergència forense: HRW (patró consistent amb coet propulsat; cal investigació independent), CNN i AP (coet fallit des de Gaza, el més probable), NYT (causa incerta), Forensic Architecture (projectil des de la direcció d'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 — l'assassinat de Shireen Abu Akleh (11-mai-2022): conclusió de l'ONU (jun-2022: trets de les forces israelianes, «aparentment ben apuntats»), investigació de CNN (24-mai-2022) i admissió de l'exèrcit israelià (5-set-2022: «probablement» foc propi; sense càrrecs). 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-gen-2024: 355 impactes al cotxe; anàlisi acústica de la trucada: trets des de 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 — els arxius Caesar (~53.000 fotos tretes de Síria el 2013; autenticació pericial de metadades i forènsica mèdica) i la condemna de Coblença (13-gen-2022: cadena perpètua a Anwar Raslan per crims contra la humanitat). 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; crim de guerra de fam com a mètode de guerra; crims contra la humanitat; ordre també 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 Justícia — *Application of the Genocide Convention (South Africa v. Israel)*, mesures provisionals de 26-gen-2024, 28-mar-2024 i 24-mai-2024 (vinculants). 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 apagades de comunicacions des d'oct-2023, per atacs a la fibra i manca de combustible; «la connectivitat civil convertida en mitjà i mètode de guerra») i *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 — pertorbació i suplantació de GPS a la regió (2024: >50.000 vols afectats; increment ×6; aplicacions situant usuaris a Beirut o al Caire; una base aèria israeliana assenyalada com a 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→gen-2021: >200 fotos de la transició presidencial amb metadades criptogràfiques ancorades a Filecoin i Hedera; procedència verificable per qualsevol). https://www.starlinglab.org/78days/ · https://contentauthenticity.org/blog/cai-spotlight-78-days-from-stanford-starling-lab-and-reuters
869. Guardian Project / WITNESS — *ProofMode* (des de 2017: signatura OpenPGP i empremta a la captura, instantània de sensors, notarització — amb OpenTimestamps entre els sistemes suportats; pensada per a la documentació ciutadana de drets humans). https://guardianproject.info/apps/org.witness.proofmode/ · https://blog.witness.org/2017/04/proofmode-helping-prove-human-rights-abuses-world/
870. t2p — manual de producte (empremta SHA-512 calculada al dispositiu — només l'empremta surt del mòbil —; ancoratge de l'empremta a la blockchain pública; segell de temps RFC 3161/eIDAS

complementari; GPS forense amb degradació honesta; mode fora de línia amb ancoratge diferit; compromís i revelació; paquet .asice verificable sense connexió; certificat amb QR). Vegeu els capítols 13 i 15; el compromís i revelació, als capítols 45 i 46; la cadena de custòdia del socors, al capítol 50; la divulgació selectiva i l'evidència de crims de guerra, al capítol 20; les credencials de contingut, al capítol 17.

871. Wikipedia (EN) — *Operation Metro Surge* (4-des-2025 → feb-2026: «the largest immigration enforcement operation ever carried out» segons el DHS; milers d'agents d'ICE i CBP a Minneapolis–Saint Paul; ≥3.789 detencions, menys d'un 25 % amb antecedents; la vaga general del 23-gen-2026; el jutge Schiltz: ≥96 ordres judicials violades per ICE des de l'1-gen; el jutge Blackwell: la «majoria aclaparadora» dels detinguts, amb presència legal); NPR — *Minnesota ICE crackdown will end* (12-feb-2026: Tom Homan anuncia el final de l'operatiu — que «ha costat la vida a dos ciutadans nord-americans» — sense esmentar-ne els noms); Sahan Journal — les xifres del desplegament (més de 4.000 agents al punt àlgid), revelades per ordre 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-gen-2026, Portland Avenue, Minneapolis: l'agent d'ICE Jonathan Ross dispara tres trets — parabrisa i finestreta de la conductora — amb el vehicle girant per allunyar-se, segons la reconstrucció del New York Times; al cotxe, la parella i una criatura de sis anys; les al·legacions de Noem i de Trump; la gravació del mateix Ross, sacsejada cap amunt al moment crític; l'accés de l'agència estatal d'investigació a les proves, revocat l'endemà; Ross, tres dies apartat i reassignat fora de l'estat); The Intercept — *Video Shows ICE Agent's Fatal Shooting of Civilian in Minneapolis* (el tret a curta distància contra el vehicle que marxava; un segon àngle mostra Good cedint el pas als vehicles federals minuts abans). 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-gen-2026, Minneapolis: infermer d'UCI de l'hospital de veterans, 37 anys, permís d'armes i cap antecedent; els vídeos dels testimonis, revisats i verificats per Reuters, BBC, Wall Street Journal, AP, CNN, New York Times i The Guardian: el telèfon a la mà, l'esprai de pebre, els agents immobilitzant-lo, l'arma treta de la funda i els trets un segon després; les al·legacions del DHS — «màxim dany», «dos carregadors i cap mena d'identificació» — i de Stephen Miller; la forense del comtat de Hennepin: homicidi; els agents, identificats per ProPublica); NPR — *Videos refute DHS account of fatal shooting* (25-gen-2026: Noem — «s'havia acostat amb una pistola» — contra els vídeos: no va treure mai cap arma; filmava amb el mòbil); The Marshall Project — *How Many People Have Been Killed by ICE and Border Patrol?* (26-gen-2026: cap reanimació dels agents; una pediatra apartada; en el cas Good, tres minuts sense trucar a emergències; el desmentiment públic de l'alcalde Frey i el governador Walz després de veure els 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 comtat de Hennepin i l'agència estatal d'investigació contra els departaments de Justícia i de Seguretat Nacional, 24-mar-2026: proves retingudes «per escudar els agents implicats» — noms, armes, informes, dades GPS i declaracions de testimonis negats malgrat els requeriments formals; les disset investigacions penals de la fiscal Moriarty; l'obstacle de la clàusula de supremacia; els agents del cas Pretti, identificats per ProPublica l'1-feb); NPR — *Months after the ICE shootings in Minnesota, a federal probe remains elusive* (10-abr-2026: el mòbil de Pretti, retingut; el cotxe de Good, precintat en un magatzem de l'FBI sense examinar; investigadors estatals apartats físicament de l'escena; única mesura disciplinària de l'operatiu: dos agents en permís administratiu per «declaracions falses» en el cas del tercer tirotejat, Julio Sosa-Celis; «Sembla que estiguin impedint activament que l'estat investigui» — Rachel Moran, professora de dret). 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: cinc trets de l'agent de la Patrulla Fronterera Charles Exum; la càmera corporal mostra el vehicle dels agents girant cap al d'ella després del «it's time to get aggressive»; els missatges de l'agent — «fired 5 shots and she had 7 holes» —; els càrrecs contra Martinez i el seu codemandat, arxivats amb caràcter definitiu el 20-nov-2025) i *List of shootings by U.S. immigration agents in the second Trump administration* (el

recompte acumulat: 38 tirotejos i 9 morts entre el 20-gen-2025 i el 7-jul-2026; els casos amb càrrecs contra civils retirats quan el vídeo va contradir la versió dels agents); AP (via KSAT) — *Judge's blistering opinion details use of force in Chicago-area immigration crackdown* (nov-2025: el dictamen de 223 pàgines de la jutgessa Sara Ellis — el relat del govern, «simply not credible», desmentit per les càmeres corporals que ella mateixa havia ordenat activar; les versions canviants de Bovino sobre la pedra i el gas; l'informe d'ús de la força redactat amb 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 al·lega que «va envestir un vehicle oficial» i que l'agent va disparar «en defensa pròpia»; els agents no duien càmeres corporals, segons el DHS; relats en conflicte sobre els moments previs; la forense del comtat de Harris, 9-jul: homicidi). https://www.click2houston.com/news/local/2026/07/07/heavy-law-enforcement-presence-reported-in-east-houston-neighborhood/
877. Lleó XIV — *Carta encíclica «Magnifica Humanitas»* (Vaticà, 15-25 de maig de 2026; sobre la custòdia de la persona humana en el temps de la intel·ligència artificial). https://www.vatican.va/content/leo-xiv/es/encyclicals/documents/20260515-magnifica-humanitas.html
878. Lleó XIII — *Rerum Novarum* (1891; origen de la doctrina social de l'Església). https://www.vatican.va/content/leo-xiii/es/encyclicals/documents/hf_l-xiii_enc_15051891_rerum-novarum.html
879. Francesc — *Laudato Si'* (2015; la Casa comuna i el paradigma tecnocràtic). https://www.vatican.va/content/francesco/es/encyclicals/documents/papa-francesco_20150524_enciclica-laudato-si.html
880. Vatican News — *Lleó XIV presenta la seva primera encíclica «Magnifica Humanitas»* (25 de maig de 2026). https://www.vaticannews.va/es/papa/news/2026-05/papa-leon-xiv-primera-enciclica-magnifica-humanitas.html
881. Joan Pau II — *Centesimus Annus* (1991; centenari 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 — *Lleó XIV presenta «Magnifica Humanitas» en persona, amb el cofundador d'Anthropic Chris Olah; «amb les nostres diferències, ens puguem escoltar els uns als altres»* (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»* (l'Església com a «informed critics»; «a long collaboration between those of us who are building this and those who can see what we, from inside, cannot»; diàleg amb gent «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* (criat evangèlic a Toronto, ateu des dels 15; la indústria «can't govern itself») (03-06-2026). https://fortune.com/2026/06/03/who-chris-olah-anthropic-cofounder-atheist-pope-leo-vatican-ai/

Índex de figures

- Figura 0.1 — Línia de temps 2004 → 2026: les fites d'energia, clima, IA i blockchain que emmarquen aquest llibre.
- Figura 0.2 — Del «pic d'oferta» al «pic de demanda»: la projecció de Roberts (2004) davant la trajectòria observada.
- Figura 1.1 — De la confiança centralitzada a la distribuïda: el viatge d'un fet, de la captura a la verificació que qualsevol pot refer.
- Figura 2.1 — El món encara funciona amb combustibles fòssils (~86,7 % del subministrament primari el 2024), però les renovables ja lideren el creixement.
- Figura 3.1 — El preu del Brent: del xoc de 2022 (~130 $) a l'estabilització cap als ~67 $ el 2025.
- Figura 4.1 — El cost de l'electricitat solar va caure prop d'un 90 % entre el 2010 i el 2024: la transformació de preu més ràpida de la història de l'energia.
- Figura 4.2 — Les vendes de vehicles elèctrics superen els 17 milions el 2024 i ja són més d'un de cada cinc cotxes nous.
- Figura 5.1 — La Xina domina la fabricació de la transició: del 60 % dels aerogeneradors al ~91 % del refinament de terres rares.
- Figura 6.1 — L'escalfament global ha superat per primera vegada els +1,5 °C en un any natural (2024).
- Figura 7.1 — La millora de l'eficiència (~1 % el 2024) va molt per sota del ritme necessari per duplicar-la cap al 2030.
- Figura 8.1 — Malgrat la retòrica verda, el 81% de la inversió de les energètiques estatals del G20 encara va a combustibles fòssils (2024).
- Figura 9.1 — El consum elèctric dels centres de dades es duplica cap al 2030 (~950 TWh), impulsat per la IA.
- Figura 10.1 — Les deepfakes es multipliquen: de ~500.000 (2023) a 8 milions (2025), camí del 90% del contingut en línia el 2026.
- Figura 11.1 — La IA orquestra renovables, emmagatzematge, resposta de la demanda i nou nuclear en una xarxa resilient.
- Figura 12.1 — Productor i consumidor intercanvien energia i certificats directament; la blockchain aporta confiança sense intermediari.
- Figura 13.1 — Del hash a la verificació descentralitzada: ningú ha de confiar en ningú; només en les matemàtiques.
- Figura 13.2 — C2PA demostra «qui i quan» en origen; l'ancoratge en blockchain demostra «això existia i no s'ha alterat».
- Figura 13.3 — El flux de t2p: capturar, segellar l'empremta a la blockchain pública i poder verificar-ho fins i tot sense connexió ni intermediaris.
- Figura 14.1 — L'hidrogen verd (€4-7/kg) encara és molt més car que el gris o el blau: el repte no és tècnic, sinó de cost i demanda.
- Figura 15.1 — La precisió dels detectors cau en el món real a mesura que milloren els generadors; una àncora de procedència no es degrada amb el temps.
- Figura 16.1 — En el frau per deepfake, la confiança es trenca en la identitat i la instrucció; una prova d'existència ancorada a l'origen hi posa un punt de verificació independent.
- Figura 17.1 — Quan una imatge es repuja, les metadades C2PA poden desaparèixer; el hash ancorat a la cadena pública continua demostrant que l'original existia, inalterat.
- Figura 18.1 — Si es calcula el hash de la imatge en el moment de l'adquisició i s'ancora amb segell de temps, qualsevol manipulació posterior (un tumor injectat o esborrat) es detecta a l'instant.
- Figura 19.1 — L'emissor firma i ancora el hash de la credencial; el titular la presenta; qualsevol verificador en comprova l'autenticitat i la integritat sense intermediaris.
- Figura 20.1 — Captura amb hash a l'origen → metadades i geolocalització → ancoratge immutable → prova admissible: la cadena que converteix un testimoni digital en evidència.
- Figura 21.1 — El preu del dret d'emissió europeu (EUA) va escalar fins a un màxim de 105,73 € el febrer de 2023 i es movia al voltant dels 80 € a mitjan 2026; en paral·lel, el CBAM va entrar en fase definitiva l'1 de gener de 2026, amb un primer certificat fixat en 75,36 €/t. Fonts: Trading Economics; Comissió Europea; S&P Global.
- Figura 22.1 — Al llarg de la vida d'un crèdit —disseny i línia base, implementació al camp, MRV, emissió, venda i tokenització opcional— el frau s'infiltra sobretot en la línia base inflada i en l'evidència de camp manipulable. La prova d'existència ancora les baules d'evidència (foto, mesura,

informe) però no corregeix una metodologia defectuosa. Fonts: The Guardian; Verra; CarbonPlan; ICVCM.

- Figura 23.1 — Del catàleg de mesures a l'emissió del certificat: l'actuació es captura com a evidència (foto abans/després, comptador, factura), es verifica i es converteix en CAE (1 CAE = 1 kWh). La prova d'existència s'insereix en el moment de capturar l'evidència —SHA-512, GPS forense, segell RFC 3161, prova de vida i contenidor .asice—, just on la llei francesa ja exigeix fotografies datades i geolocalitzades. Fonts: BOE (RD 36/2023); Légifrance (Llei 2025-594); Funcas.
- Figura 24.1 — L'autoconsum amb prova d'existència (t2p: empremta SHA-512 al dispositiu, RFC 3161/eIDAS, blockchain pública, .asice): la lectura pròpia de l'inversor i el comptador segellada per lots encadenats, la factura amb compensació contrastada, l'acta de la comunitat energètica (coeficients, altes i baixes amb data certa) i el contracte/PPA congelat el dia de signar. Context: 9,3 GW d'autoconsum a Espanya (UNEF) — cinquena font per potència; RD 244/2019 (compensació simplificada mensual ≤100 kW; col·lectiu fins a 5 km). Límits: la lectura pròpia contrasta el comptador fiscal, no el substitueix; calibratge primer; només empremtes a la cadena (la corba de consum és intimitat). Fonts: UNEF; BOE (RD 244/2019).
- Figura 25.1 — La lectura d'un sensor (odòmetre, bus CAN, GPS, sessió de càrrega OCPP) es resumeix en una empremta SHA-512 al dispositiu, s'hi lliguen el GPS forense i un segell de temps RFC 3161/eIDAS amb presumpció legal, s'ancora a la blockchain pública i s'empaqueta en un contenidor .asice verificable fora de línia, llest per emetre un CAE (fitxes TRA010-TRA050), un crèdit de carboni o un informe CSRD. Caixa comparativa: sense segell, fins al 30-50 % dels odòmetres transfronterers estan manipulats; amb un registre segellat (model Car-Pass), menys del 0,2 %. Fonts: Parlament Europeu (EPRS); Car-Pass; MITECO.
- Figura 26.1 — El nombre de cotxes privats que retira del carrer un sol vehicle compartit varia enormement segons la ciutat i la metodologia: de 3,3 de mitjana a l'estudi europeu de SHARE NOW fins als 7-11 de l'estudi de car2go a Nord-amèrica, amb escenaris encara més alts en algunes ciutats. La xifra de divulgació «un per deu» és comercial, no consensuada. La lliçó: cap número únic; sempre un rang amb la seva font. Fonts: UC Berkeley TSRC (Shaheen i Martin, 2016); Transportation Research Part A (2020).
- Figura 27.1 — El retard amb prova d'existència (segellat amb t2p — capítol 13): l'arribada amb GPS forense en obrir-se les portes (la definició del TJUE), el panell i l'estat del vol congelats, l'expedient del viatge (bitllet, embarcament, despeses d'atenció) i la simetria del transportista (registres d'operació ancorats; la circumstància extraordinària segellada quan passa). Context: Reglament (CE) 261/2004 (250/400/600 €; Sturgeon ≥3 h); Renfe 1-7-2024: dels 15/30 min als 60/90 (50 %/100 %). Límits: el jutge decideix l'extraordinari; documentar el viatge propi, mai tercers. Fonts: EUR-Lex; Renfe/Newtral.
- Figura 28.1 — Percentatge de consumidors disposats a alterar digitalment la imatge o el document d'un sinistre, encara que infringeixi les normes de l'asseguradora: un 36 % de mitjana, però fins al 55 % entre la generació Z. La predisposició cau amb l'edat. És el rostre del frau d'imatge per IA que el 99 % de les asseguradores ja ha vist. Font: Verisk amb el National Insurance Crime Bureau (2026).
- Figura 29.1 — En el punt d'origen (parcel·la, collita, fàbrica) es captura una foto georeferenciada que se segella amb GPS forense, segell de temps eIDAS i empremta SHA-512, i s'empaqueta en un contenidor .asice verificable fora de línia. Aquesta capa de prova de l'acte d'origen es combina amb la serialització (codi 2D del FMD), la declaració de diligència deguda del EUDR o el passaport digital d'Aura, fins a la verificació final a la duana o a l'estant. Fonts: EUDR (UE 2023/1115); EMA; Aura Blockchain Consortium.
- Figura 30.1 — La capa d'informació del consumidor amb prova d'existència: la ressenya amb compra acreditada i anònima (el justificant segellat al dispositiu; el mercat negre de ressenyes es queda sense matèria primera), la sèrie de preus amb data certa (la regla del menor preu dels 30 dies esdevé verificable) i el rellotge de la garantia (compra, unboxing i avisos segellats activen i acrediten els 3 anys legals). Límits: el segell no jutja la sinceritat ni la qualitat; l'acreditació de compra mai no pot identificar el comprador. Fonts: FTC (norma 2024); Amazon vs. grups de Facebook; OCU (Black Friday); CEC/Consum (garantia de 3 anys).
- Figura 31.1 — La segona mà entre particulars amb prova d'existència (segellat amb t2p — capítol 13): l'article filmat abans d'enviar (data/hora sobreimpresa + GPS forense), el precintat en pla seqüència, l'obertura simètrica del comprador i l'expedient de la disputa (anunci capturat, xat, pagament, seguiment). Simetria total: desarma el paquet fals I el «cambiazo». Context: >19 M d'usuaris a Wallapop; >13.000 M€/any; les estafes de segona mà, gruix dels >412.000 fraus informàtics del

2024 (+60 % de denúncies el 2025). Límits: proporcionalitat segons valor; el vici ocult el valora el pèrit; mai gravar tercers. Fonts: Guàrdia Civil/premsa especialitzada.

- Figura 32.1 — El lloguer de coses amb prova d'existència (segellat amb t2p — capítol 13): la volta d'agafada filmada (data/hora sobreimpresa + GPS forense del pàrquing), la volta de tornada — decisiva en devolucions fora d'hores —, el contracte i la franquícia segellats, i l'expedient contra el càrrec tardà. Simetria: la inspecció bilateral protegeix l'empresa honesta del client que nega el cop; extensible al lloguer de maquinària B2B. Context: pràctiques irregulars documentades (càrrecs de 300-1.000 € fixats unilateralment; revisions sense el client); el CEC ja recomana fotos — hi faltava la data certa. Límits: ús normal vs dany i preus, cosa del contracte i el jutge. Fonts: Consumo/DSCA; CEC-España.
- Figura 33.1 — El client davant la companyia amb prova d'existència (segellat amb t2p — capítol 13): la baixa segellada (gravació de la trucada pròpia, captura certificada del formulari), el contracte i les seves versions (captura web amb codi font), la promesa verbal gravada i l'expedient .asice exportable a consum. La Llei 10/2025 dona els drets (3 minuts, codi de seguiment, 15/5 dies, baixa simple); la data certa els fa exigibles — i acredita la companyia diligent. Límits: converses pròpies, proporcionalitat amb el teleoperador, la reclamació formal continua sent imprescindible. Fonts: BOE (Llei 10/2025); FACUA (multes Vodafone/Movistar/Telefónica).
- Figura 34.1 — El rellotge del cobrament amb prova d'existència (segellat amb t2p — capítol 13): l'albarà fotografiat amb GPS forense al lliurament, la factura amb doble data certa (emissió i enviament), el còmput automàtic de la Llei 3/2004 (30/60 dies; interès de demora 11,15 % + 40 €) i l'expedient .asice per al monitori. Context: VeriFactu (RD 1007/2023, ajornat a 2027 pel RD-llei 15/2025) ja imposa registres de facturació amb hash encadenat i QR — l'Estat construeix mitja prova d'existència; t2p hi afegeix la capa oposable entre privats. Límits: el segell no cobra factures ni valora la feina; VeriFactu protegeix Hisenda, no el creditor. Fonts: AEAT; BOE; PMcM 2025 (85 % de grans incomplidores; AAPP a 70 dies).
- Figura 35.1 — L'estat de l'habitatge (lloguer) o un document (escriptura, contracte) es captura i se segella al dispositiu amb SHA-512, GPS forense, segell de temps eIDAS i prova de vida, s'ancora a la blockchain pública i s'empaqueta en un contenidor .asice verificable fora de línia, llest per al registre, el notari, el tribunal o l'altra part. La prova d'existència aporta evidència amb data certa, no el títol legal (que crea el registre). Barra de context: ~70 % de la població mundial sense títol registrat; ~1.100 M de persones insegures sobre la seva propietat; Geòrgia, ~1,5 M de títols ancorats. Fonts: Banc Mundial; Prindex; Exonum/Bitfury.
- Figura 36.1 — El cicle del lloguer amb prova d'existència: l'anunci acreditat (titularitat + segell, contra l'estafa del pis inexistent), l'inventari d'entrada segellat bilateralment, els avisos i reparacions amb data certa durant el contracte, la cronologia de possessió (contracte i rebuts del llogater; proves d'estat periòdiques del propietari; via ràpida LO 1/2025) i l'inventari de sortida que liquida la fiança sense guerra. Només les empremtes SHA-512 s'ancoren a la blockchain pública (RFC 3161/eIDAS, .asice); les imatges de la llar no surten mai dels dispositius. Fonts: Guàrdia Civil (Op. ISLEDA); Idealista/Maldita; LO 1/2025.
- Figura 37.1 — La comunitat de propietaris amb prova d'existència (segellat amb t2p — capítol 13): la convocatòria amb data certa d'enviament, l'acta segellada el mateix dia (llibre d'actes com a cadena de versions ancorades), la derrama traçable (pressupostos, acord, factures, certificacions en un projecte) i la comunicació fefaent entre veïns i administrador. Simetria: protegeix el veí que impugna i l'administrador honest. Límits: acords de junta per gravar, publicació només per empremta (dades personals), i cap segell no resol el fons de les disputes (LPH). Fonts: condemna de Gijón (art. 253 CP); Llei de Propietat Horitzontal.
- Figura 38.1 — La reforma amb prova d'existència (segellat amb t2p — capítol 13): el pressupost i les seves versions segellats el dia de pactar-se, l'estat inicial fotografiat amb GPS forense (la prova que l'obra esborra), les fases amb fites — pagar contra fets documentats — i la recepció signada amb vídeo-selfie de les dues parts. Simetria: protegeix la família de l'estafa de la bestreta i el professional honest del client que no vol pagar. Context: investigacions de la Guàrdia Civil (Vigo: ≥6 víctimes de fins a 10.000 €; pèrdues >77.000 € en algun cas). Límits: la qualitat la valoren els pèrits; proporcionalitat; no pagar per davant dels fets. Fonts: premsa/Guàrdia Civil; normativa de consum.
- Figura 39.1 — Les dues projeccions de referència per al mercat de RWA tokenitzats el 2030 difereixen unes vuit vegades: l'escenari prudent de McKinsey (~2 bilions de dòlars, rang 1-4) i l'optimista de BCG/ADDX (~16,1 bilions); el punt de partida real era d'uns 24.000 milions a mitjan 2025. La distància depèn, en el fons, de quanta «escombraria» s'admeti: del buit entre el token i la prova del seu respatller —el problema de l'oracle— que la prova d'existència ajuda a tancar. Fonts: McKinsey (2024); BCG/ADDX (2022); CoinDesk/RWA.xyz (2025).

- Figura 40.1 — En el moment de crear (t0), l'obra se segella amb empremta SHA-512 al dispositiu, àncora a la blockchain pública, segell de temps eIDAS, GPS i prova de vida: data certa de què, quan, on i qui. En publicar-la (t1), les credencials C2PA poden esborrar-se en pujar-la a les xarxes; quan un model la ingereix o algú la copia (t2), el contenidor .asice encara demostra que el fitxer existia intacte a t0, abans de t2. La prova d'existència demostra precedència, no originalitat. Fonts: C2PA; U.S. Copyright Office; casos NYT, Getty, Andersen.
- Figura 41.1 — L'inventor segella el document de divulgació amb empremta SHA-512, àncora a la blockchain pública i segell de temps eIDAS (data certa, integritat i autoria), per un cost marginal davant dels 15.000-25.000 dòlars d'una patent. Si a més el publica (Technical Disclosure Commons, IP.com, web), es converteix en prior art indexat per Espacenet o Google Patents; quan arriba la sol·licitud d'un rival, l'examinador hi troba la divulgació datada i la rebutja per falta de novetat. El segell prova data i contingut, no la patentabilitat —que decideix l'examinador. Fonts: USPTO; WIPO; Technical Disclosure Commons.
- Figura 42.1 — El secret empresarial amb prova d'existència (t2p: empremta SHA-512 al dispositiu — el contingut no surt mai —, RFC 3161/eIDAS, blockchain pública, .asice): el dipòsit segellat (possessió + perímetre + mesura raonable del tercer requisit de la Llei 1/2019), la cronologia del know-how versió a versió, l'acta de sortida de l'empleat i el NDA amb perímetre per empremta i signatura amb vídeo-selfie. Simetria: la cadena de dates de l'acusat innocent prova el desenvolupament independent. Mirall del capítol 41: la patent protegeix publicant; el secret, ocultant — i per això només la prova que no revela el pot defensar. Fonts: cas Waymo/Uber/Levandowski; Llei 1/2019.
- Figura 43.1 — Cada pas del diner públic —l'oferta o el plec, l'adjudicació registrada i l'obra entregada (foto amb GPS i data)— es resumeix en una empremta SHA-512, s'ancora a la blockchain pública i rep un segell de temps RFC 3161/eIDAS, amb prova de vida en l'obra; tot s'empaqueta en un contenidor .asice que un ciutadà o un auditor pot verificar de manera independent i fora de línia. Context: contractació pública mundial ≈13 bilions de dòlars l'any; entre el 10 % i el 30 % de l'obra pública es perd per corrupció i mala gestió. La prova d'existència demostra integritat, moment, lloc i persona —no l'honestedat de la decisió ni la qualitat de l'obra. Fonts: Banc Mundial; CoST; OCDE; eIDAS art. 41.
- Figura 44.1 — La relació ciutadà-Administració amb prova d'existència (empremta SHA-512 al dispositiu, segell de temps RFC 3161/eIDAS, blockchain pública, .asice): la presentació amb contingut segellat (què i quan), el rellotge del silenci administratiu amb venciments datats (Llei 39/2015: 3 mesos; certificat en 15 dies), la notificació amb traça neutral (els 10 dies auditables per ambdues parts) i la disponibilitat de cites auditable (contra el mercat negre de la cita prèvia). Simetria: la mateixa traça acredita la diligència de l'Administració. Límits: no crea cites ni resol expedients; cap perfil ciutadà central. Fonts: Llei 39/2015; Defensor del Pueblo (cites d'estrangeria).
- Figura 45.1 — El sorteig que ningú no pot carregar, en dues meitats: el compromís previ (llista de participants i regla d'adjudicació segellades amb t2p — empremta SHA-512, RFC 3161/eIDAS, blockchain pública — i publicades per empremta ABANS del sorteig) i l'atzar públic verificable (balisa drand de la League of Entropy: valors imparcials, impredictibles i verificables, generats per criptografia de llindar entre operadors independents). Resultat: adjudicació recomputable per qualsevol — resultat = regla(llista, atzar). Límits: el sorteig net no cura l'escassetat; el ritual públic i el notari es reforcen, no se substitueixen. Fonts: sortejos d'oposicions i d'habitatge protegit; drand/League of Entropy.
- Figura 46.1 — La prova segellada abans (t2p: empremta SHA-512 — només l'empremta s'ancora, el contingut no surt de la custòdia —, RFC 3161/eIDAS, blockchain pública, .asice): l'examen certificat abans de la convocatòria amb accessos registrats, la plantilla de correcció compromesa abans de l'examen (les anul·lacions, transparents i datades), el full de respostes de l'opositor datat en sortir, i l'expedient d'impugnació verificable. Simetria: el tribunal net pot provar que no va tocar res — el cas Osakidetza (19 exàmens amb indicis de filtració, dimissions, vuit anys i arxivament per falta de proves) resolt en dies, en qualsevol direcció. Patró: el compromís previ del capítol 45, aplicat al contingut. Fonts: Redacción Médica; Deia; elDiario.es.
- Figura 47.1 — Una persona sense papers genera un gest de prova de vida («sóc jo, estic viu»); al dispositiu se'n calcula l'empremta SHA-512 amb GPS forense i segell de temps eIDAS («aquí, ara»), s'ancora a la blockchain pública i pot acompanyar una credencial verificable W3C; el titular guarda la prova al seu dispositiu i la comparteix amb divulgació selectiva, en un contenidor .asice verificable fora de línia. Escala del repte: ~800 M sense identitat, ~4,4 M (fins a 10 M) apàtrides, 150 M d'infants no registrats. Fonts: Banc Mundial ID4D; UNHCR; UNICEF; W3C.

- Figura 48.1 — A la mesa, l'acta es fotografia i se segella amb empremta SHA-512, segell de temps eIDAS, GPS forense i prova de vida del funcionari, en un contenidor .asice ancorat a la blockchain pública; si la xifra s'altera en trànsit cap al centre d'escrutini, l'empremta no coincideix i el delata. El que la prova d'existència NO fa: no és vot per internet, no és vot en blockchain, i no demostra que el recompte sigui veritable —això s'audita sobre el paper (RLA). Fonts: Tribunal Suprem de Kenya (2017); Rivest et al. (2021); Philip Stark.
- Figura 49.1 — Al punt de lliurament, un rebut d'entrega (beneficiari anònim, import, lloc, hora) se segella amb empremta SHA-512, segell de temps eIDAS i GPS forense, en un contenidor .asice verificable fora de línia; la prova de vida al dispositiu confirma una persona viva sense escàner central; i la desduplicació a l'estil Janus revela només un bit («ja registrat» o «nou»), sense crear cap base biomètrica. Impacte real: a Ucraïna es van evitar ~35 M$ d'ajuda duplicada. Límit: no prova què passa amb l'efectiu un cop cobrat (Iemen, Congo). Fonts: WFP; EPFL/CICR (Janus); Human Rights Watch.
- Figura 50.1 — La cadena de custòdia del socors amb prova d'existència (t2p: empremta SHA-512 al dispositiu, segell RFC 3161/eIDAS, blockchain pública, .asice): el manifest segellat a l'origen (escàner de fins a 50 pàgines), les actes de duana i magatzem amb GPS forense (fix genuí ~50 m / ≤30 s; la ubicació simulada bloqueja la certificació), el comboi amb captures represes en recuperar cobertura, i la recepció signada amb vídeo-selfie i reptes de vida — exportable com a paquet .asice verificable sense connexió per l'auditor del donant. Límits: el segell no acredita la qualitat del contingut, no aixeca bloquejos i mai no fitxa les víctimes. Fonts: IFRC (frau Ebola autodivulgat); ONU/WFP (Somàlia 2010); OFAC (xarxa CLAP); terratrèmol de Veneçuela 2026.
- Figura 51.1 — Tres cronologies ancorades que es contrasten (empremta SHA-512 al dispositiu, segell de temps RFC 3161/eIDAS, blockchain pública, .asice): el rastre segellat de qui fuig (sobreviu a la confiscació del telèfon; TJUE C-136/24 P), la documentació dels observadors (testimonis amb data certa; Black Book of Pushbacks) i els registres ancorats de les autoritats (bitàcoles i posicions; el cas Pylos). La regla d'or: l'evidència ancorada suma credibilitat; la seva absència mai no resta. Límits: cap registre de persones, seguretat física primer, i el segell no decideix l'asil ni la política migratòria. Fonts: HRW/Amnistia (Pylos); RSA (imputació de 17 guardacostes); BVMN; TJUE C-136/24 P.
- Figura 52.1 — Tres entrades convergeixen en un testament incontestable: el document, l'empremta SHA-512 del qual s'ancora a la blockchain pública (integritat); la prova de vida en vídeo, que lliga identitat, presència i voluntat (contra la influència indeguda i la falsificació); i el segell de temps eIDAS amb GPS, que fixa quina és la versió definitiva (contra «existeix un testament posterior»). El resultat és un .asice verificable fora de línia. Límit: no substitueix testimonis, notari ni homologació, i la capacitat la decideix el jutge o el metge. Fonts: Cerulli Associates; e-Estonia/Guardtime; cas Voysey.
- Figura 53.1 — La logística coparental amb prova d'existència (empremta SHA-512 al dispositiu, segell de temps RFC 3161/eIDAS, blockchain pública, .asice), sempre bilateral i acordada: la comunicació amb data certa, el lliurament acreditat des dels dos dispositius (mai càmeres ni menors fotografiats), les despeses amb justificants ancorats i el pla de parentalitat versionat. El nord: l'interès superior del menor; el registre és escut, no arma. Límits: no decideix custòdies, no mesura la criança, i en situacions de violència la prioritat són els canals especialitzats. Fonts: INE (custòdia compartida 49,7 %, 2024); OurFamilyWizard (tribunals de 50 estats); pla de parentalitat.
- Figura 54.1 — L'exportador emet un coneixement d'embarcament que se segella amb empremta SHA-512, segell de temps RFC 3161/eIDAS i GPS, ancorat a la blockchain pública (.asice). El banc A el finança i el marca com a pignorat. Quan un defraudador presenta el «mateix» document al banc B, l'empremta coincideix i consta com ja pignorat: la segona financiació es bloqueja. Límit: el segell no prova que la mercaderia existeixi físicament al magatzem (el «metall fantasma» de Qingdao). Context: bretxa de finançament del comerç de 2,5 bilions de dòlars; coneixement d'embarcament electrònic real, només el 5,7 %. Fonts: Banc Asiàtic de Desenvolupament; ICC; cas Qingdao.
- Figura 55.1 — En el model tradicional vulnerable, l'extracte bancari passa pel client (Wirecard) abans d'arribar a l'auditor: és el punt on s'hi cola la falsificació. Amb t2p, la confirmació bancària, el llibre major o la factura se segellen en origen —empremta SHA-512, segell de temps eIDAS, GPS, ancoratge a la blockchain pública— i l'auditor verifica una cadena de custòdia inalterable (.asice). Límit: el segell no fa veritable una dada fabricada des de la font (Wirecard, Luckin, Enron). Context: Wirecard, 1.900 M€ inexistents; frau d'estats financers, mediana de 766.000 $ per cas. Fonts: Financial Times; PCAOB; ACFE.
- Figura 56.1 — De cada dòlar que un anunciant posa a la compra programàtica, només 36 cèntims arriben al consumidor: 29 es perden en costos de transacció i 35 en «pèrdua de productivitat mediàtica» (webs escombraria i inventari de baixa qualitat). El frau publicitari digital va costar

84.000 milions de dòlars el 2023 —un 22 % de la inversió en línia— i els bots ja són la meitat del trànsit d'internet. Fonts: ANA (2023); Juniper Research; Imperva.

- Figura 57.1 — Els esdeveniments del sistema (inclòs l'Event ID 1102, «s'ha esborrat el registre») es reenvien en temps real fora del sistema atacat; els lots de registres es resumeixen en una arrel de Merkle que se segella amb empremta SHA-512 i segell de temps RFC 3161/eIDAS i s'ancora a la blockchain pública, encadenant cada arrel amb l'anterior (només s'hi pot afegir). Qualsevol alteració posterior trenca l'empremta i delata l'atacant. Límit: l'ancoratge no impedeix la bretxa; només protegeix el que s'ha registrat i reenviat a temps. Context: dwell time mitjà de 14 dies el 2025; cost mitjà d'una bretxa, 4,44 M$. Fonts: MITRE ATT&CK; Mandiant M-Trends; NIST SP 800-86.
- Figura 58.1 — La bretxa vista des del ciutadà, amb prova d'existència (segellat amb t2p — capítol 13): la notificació capturada (o la seva absència, datada), el certificat de presència a la filtració (captura web amb codi font), el diari del dany (phishing, trucades, intents — cada peça segellada al moment) i la reclamació .asice. Fonament: TJUE C-300/21 — dany moral indemnitzable sense llindar, però amb infracció + dany + causalitat PROVATS. Simetria: l'empresa diligent acredita la seva notificació. Límits: la valoració és del jutge; correlació ≠ causalitat; el diari queda al dispositiu. Fonts: TJUE; RGPD art. 82.
- Figura 59.1 — La caiguda documentada amb prova d'existència (segellat amb t2p — capítol 13): la sonda independent amb cadena de registres segellats (el rellotge del client), la pàgina d'estat del proveïdor congelada amb codi font, l'impacte de negoci documentat (gravació de pantalla, mètriques per empremta) i la reclamació .asice — per als crèdits del SLA, l'asseguradora i els reports DORA/NIS2. Simetria: el proveïdor que ancora la seva disponibilitat en fa el seu argument comercial. Límits: la sonda acredita quan no responia, no la causa; metodologia primer; cap segell no substitueix la redundància. Fonts: CrowdStrike 19-7-2024 (8,5 M de Windows; Delta ~550 M$).
- Figura 60.1 — En una excavació legal (esquerra), la peça es fotografia in situ amb coordenades GPS i segell de temps eIDAS abans de moure-la: la procedència queda documentada des del segon zero i s'ancora a la blockchain pública (.asice). En l'espoli (dreta), la «procedència» en paper comença anys després de la troballa i és fàcil de fabricar —com el Shiva Chola venut a Austràlia per 5,6 M$ amb papers falsos. Límit: el segell prova integritat, data, lloc i persona, però NO autentica l'objecte (una foto segellada d'una falsificació continua sent una falsificació). Context: comerç il·lícit d'antiguitats de 225 M$ a 6.000 M$/any. Fonts: INTERPOL; fiscalia de Manhattan; Art Loss Register.
- Figura 61.1 — Quatre fronts d'una mateixa defensa (empremta SHA-512, segell de temps RFC 3161/eIDAS, ancoratge a la blockchain pública, .asice): els manifests ancorats dels arxius i hemeroteques (edicions silencioses detectables), els testimonis de supervivents segellats en vida (prioritat temporal contra la fabricació), els expedients d'exhumació amb cadena de custòdia ancorada (Llei 14/2022, Banc Estatal d'ADN) i l'horitzó pre-IA de les col·leccions fotogràfiques (el cànon verificable contra la història sintètica). Límits: el segell no fa crítica de fonts ni congela la interpretació; pluralitat d'arxius, mai un «arxiu únic de la veritat». Fonts: UNESCO/CJM; Maldita.es; Internet Archive (bretxa 2024); Llei 14/2022.
- Figura 62.1 — El denunciant calcula l'empremta SHA-512 del document al seu dispositiu i l'ancora a la blockchain pública amb segell de temps eIDAS: es prova QUÈ i QUAN, no QUI. La capa que delataria —identitat, GPS, prova de vida, metadades, IP— s'omet deliberadament: el que protegeix és el que no se segella. Amb una prova de coneixement zero, el periodista o el tribunal verifiquen que el document és autèntic i anterior a una data, sense conèixer la font. Límit: la cadena no bloqueja els punts de rastreig de la impressora (cas Winner), l'estilometria ni les metadades de xarxa. Fonts: ICIJ (Panama Papers); EFF; Freedom of the Press Foundation.
- Figura 63.1 — Al llarg de la vida d'un experiment, el frau pot entrar al disseny (canvi de variables: COMPare va trobar que només el 76,3 % dels desenllaços primaris es reportaven bé), a la mostra (fabricació en origen, com Stapel), a la captura del fitxer cru o a l'edició de la figura (duplicació de bandes: Bik va trobar-ne en el 3,8 % de 20.621 articles). El segell en l'adquisició —empremta SHA-512 + segell eIDAS— cobreix el pre-registre del protocol i la captura de la dada crua, i fa detectable qualsevol edició posterior; però no demostra que la dada fabricada en origen sigui veritat. Fonts: COMPare (Oxford); Bik et al. (mBio 2016); ASM/ImageTwin.
- Figura 64.1 — Cada cicle d'atestació parteix d'un repte fresc del dia (nonce); el pensionista fa el gest de vivacitat al dispositiu; es calcula localment l'empremta SHA-512 de {vivacitat + repte + GPS + hora}, s'ancora a la blockchain pública amb segell eIDAS i es tanca en un .asice verificable fora de línia. El repte irrepetible impedeix reutilitzar gravacions antigues: el mort no pot respondre al repte d'avui. La cara no surt mai del dispositiu; a la cadena només hi viatja una empremta. Cost de no saber qui segueix viu: Japó, 234.354 centenaris sense confirmar; els EUA, 327 M$ a difunts; Sud-àfrica, 140 M de rands a 75.000 morts. Fonts: France 24; SSA OIG; SASSA/Moneyweb.

- Figura 65.1 — La prova de vida en l'era del deepfake: contra el segrest virtual amb veu clonada i la «prova de vida» fabricada amb IA (alerta FBI/IC3 2025), el protocol de tres peces — repte imprevisible, frescor del moment i segell t2p (empremta SHA-512 al dispositiu, RFC 3161/eIDAS, blockchain pública, .asice). Aplicacions: el protocol familiar, la negociació amb datació, l'últim punt del mapa voluntari i la tornada verificable (CNDES: 132 alertes actives el 2025). Límits: el segell acredita frescor, no llibertat; voluntari o res; mai un substitut de la policia i els negociadors. Fonts: CNN (cas DeStefano); FBI/IC3; Ministeri de l'Interior/CNDES.
- Figura 66.1 — La vida d'una mostra antidopatge passa per cinc nodes: obtenció i firma de l'atleta, precinte de les ampolles A i B, transport, recepció al laboratori i anàlisi. A Sotxi, el frau va entrar al node del laboratori (el «forat de ratolí» per on el servei secret intercanviava l'orina de nit). El segell de t2p —GPS forense, segell eIDAS i empremta del número de kit ancorats a la blockchain pública— fa que aquell intercanvi deixi una discontinuïtat temporal i geogràfica detectable. L'evidència forense que va delatar el frau malgrat les ampolles «inviolables»: 44 taps amb marques de manipulació (12 de medallistes), 8 mostres amb sal impossible, 2 amb ADN masculí, ≥643 positius «desapareguts». Límit: el segell no demostra què hi havia a l'ampolla abans de precintar-la. Fonts: Informe McLaren; CNN; Chemistry World.
- Figura 67.1 — La música en streaming reparteix un fons de suma fixa: el 2025, més de 22.000 milions de dòlars (IFPI). Cada escolta falsa no inventa diners nous; roba la seva part als artistes amb públic real. L'estimació de la indústria xifra la fuga per frau en uns 2.000 milions de dòlars l'any — almenys un 10 % de l'activitat (Beatdapp). El cas Smith: 661.440 escoltes-bot al dia, a mig cèntim, durant set anys. Amb prova de vida, les escoltes sense humà no entren al repartiment i el fons torna als artistes reals. Fonts: IFPI Global Music Report 2026; Beatdapp; acusació de la fiscalia de Nova York.
- Figura 68.1 — La capa de xarxa (STIR/SHAKEN) autentica el número d'origen —«des de quin número truca?»—, però només el 42,5 % de les trucades arriben firmades (abril de 2025), perquè qualsevol tram no-IP trenca la firma. La capa d'extrem (t2p: prova de vida + SHA-512 + segell eIDAS + GPS) autentica l'origen humà i el moment de l'acte —«qui, què i quan, de debò?». Són complementàries. Context: 52.800 milions de robocalls als EUA el 2024; 48,8 M$ robats per SIM-swap (FBI, 2023). Fonts: TransNexus; FCC; FBI IC3.
- Figura 69.1 — El frau del pagament «autoritzat» amb prova d'existència (segellat amb t2p — capítol 13): l'engany documentat (trucada pròpia gravada, SMS i xats capturats), la sessió capturada (la pantalla amb l'avís — o sense), la reclamació datada (terminis) i la simetria del banc diligent (avisos i friccions ancorats per lots; l'alta del compte receptor verificada). Context: Regne Unit, primer reemborsament obligatori del món (7-10-2024; £85.000; 50/50 emissor-receptor; 5/35 dies); PSD2: en operacions no autoritzades, la càrrega de la prova és del banc. Límits: la negligència greu la valora el jutge; la prevenció primer. Fonts: PSR; PSD2/RDL 19/2018.
- Figura 70.1 — Cada esdeveniment de custòdia d'un component de grau defensa —marcatge pel fabricant original, recepció al distribuïdor, «origen» declarat pel broker, informe d'assaig AS6171, acceptació del contractista, instal·lació— es pot segellar amb empremta SHA-512, segell eIDAS, GPS forense i prova de vida, ancorats a la blockchain pública. El punt cec (en vermell): la substitució física de la peça *després* de l'assaig, que el segell no detecta sense un ancoratge al silici (ADN, empremta física no clonable). Context: ~80 % dels xips falsos són reciclats o remarcats; la GAO va comprar 16 peces militars en línia i les 16 eren falses; un sol broker en va introduir 84.000. Fonts: Senat dels EUA (2012); GAO; IHS/ERAI.
- Figura 71.1 — La cadena de subministrament del programari amb prova d'existència: cada versió publicada s'ancora (empremta SHA-512 del tarball, segell de temps RFC 3161/eIDAS, blockchain pública, .asice) i es contrasta amb el codi font (la discrepància de xz-utils, detectable); la cadena de publicació vigilada als registres de transparència (Sigstore/Rekor: >101 milions d'entrades — prova d'existència en producció) dispara l'alarma davant de publicacions amb claus robades (el cuc Shai-Hulud); l'inventari (SBOM) segellat per versió fa la resposta a incidents una consulta (Reglament (UE) 2024/2847). Límits: el segell acredita origen i integritat, no bondat del codi; els mantenidors necessiten eines gratuïtes i finançament. Fonts: CVE-2024-3094; CISA (Shai-Hulud); Sigstore/Rekor; CRA.
- Figura 72.1 — El frau i l'opacitat per vertical: tres de cada quatre vaixells pesquers industrials no emeten senyal públic de posició (75 %, Global Fishing Watch); un terç del marisc dels EUA està mal etiquetat —fins al 87 % del «pargo vermell» (Oceana); una revisió global de més de trenta països troba un 36 % de mal etiquetatge; i fins al 90 % del mineral «etiquetat net» en dues zones del Kivu del Sud procedia de fonts il·lícites (Global Witness). t2p segella l'origen en el punt d'extracció, abans

de la barreja o el canvi d'etiqueta; el que el segell NO valida és l'espècie ni la legalitat de la zona. Fonts: Global Fishing Watch; Oceana; Global Witness.

- Figura 73.1 — El recorregut d'un dòlar donat, amb les seves fuites reals: el captador professional se'n queda 25 cèntims de mitjana (fiscalia de Nova York, 2024), i en la meitat de les campanyes l'entitat rep menys de la meitat; en el frau Reynolds, menys de 3 cèntims arribaven al pacient; en el projecte de Haití, un 40 % es perdia en overhead. Com a contrapunt, una ONG eficaç evita una mort per uns 3.000-5.500 dòlars (GiveWell). t2p segella tres nodes —la promesa restringida, cada desemborsament i l'evidència d'impacte (GPS + hora + prova de vida)—, convertint el «confia en l'informe» en evidència auditable. Límit: no jutja si la mètrica declarada és honesta ni l'eficàcia del programa. Fonts: fiscalia de Nova York; FTC; ProPublica; GiveWell.
- Figura 74.1 — Els registradors (la caixa negra d'avió amb més de 88 paràmetres i ara fins a 25 h de veu; el registrador del cotxe amb els 20 s previs al xoc; el registre de vol d'un dron) capturen la dada. t2p no millora la captura: en l'instant en què el registrador tanca un esdeveniment, en calcula l'empremta SHA-512 al dispositiu i l'ancora a la blockchain pública amb segell eIDAS, de manera que negar la dada (Tesla), retallar-la (Cruise) o alterar-la deixa una empremta que no quadra. Límit: el segell no corregeix una dada errònia, no resol la disputa pericial sobre la causa (EgyptAir 990), i no rebleix el que el sensor no va gravar (Jeju Air, on la gravació es va tallar 4 minuts abans). Fonts: NTSB; California DMV; cas Benavides contra Tesla.
- Figura 75.1 — La caixa negra personal: l'àudio d'una conversa pròpia (STC 114/1984), el clip de la dashcam (límits AEPD) o la foto datada es xifren i NO surten mai del dispositiu; només l'empremta SHA-512 amb segell de temps RFC 3161/eIDAS s'ancora a la blockchain pública (.asice). La revelació és decisió del titular, davant del jutge. Dues sortides simètriques: la víctima que prova el dany i l'innocent que prova la coartada. Límits: no acredita la veritat del contingut, no legalitza la gravació d'altri (art. 197 CP), exigeix revocabilitat i cap registre central. Fonts: STC 114/1984; Fiscalia General de l'Estat (Cometa; denúncies falses 0,0082 %); AEPD; UNESPA.
- Figura 76.1 — Dues veritats de la dada genètica. A l'esquerra, l'efecte familiar: n'hi ha prou que el 2 % d'una població estigui en una base de dades per reidentificar gairebé qualsevol persona a través d'un parent llunyà, i prop del 60 % dels d'ascendència europea ja són identificables encara que mai no s'hagin fet un test (Erlich et al., 2018). A la dreta, l'efecte multiplicador de la bretxa: l'atac a 14.000 comptes (el 0,1 %) va exposar 6,9 milions d'usuaris a través de la funció que connecta parents. t2p pot segellar l'acte de consentiment —què, quan i on—, però no pot tornar la privacitat a una dada irrevocable que també és de la teva família. Fonts: Science (Erlich et al.); TechCrunch; fiscalia de Nova York.
- Figura 77.1 — La prova digital pateix dos atacs oposats. A l'esquerra, el fals que enganya: un àudio o vídeo fabricat amb IA presentat com a autèntic (com l'àudio editat d'un cas de família britànic). A la dreta, el dividend del mentider: una gravació autèntica negada com a «deepfake» per eludir la responsabilitat (com en el litigi Huang contra Tesla, on es va al·legar que els vídeos de Musk «podrien ser deepfakes»). La mateixa defensa val per a tots dos: segellar el fitxer en el segon de la gravació amb empremta SHA-512, segell eIDAS i GPS (compatible amb la regla 902(14): el hash autoautentica còpies). Límit: el segell prova integritat i moment, no la veritat de l'escena —una càmera segellada que grava un muntatge certifica el muntatge. Fonts: Chesney i Citron (2019); ProPublica; casos Tesla i Baltimore.
- Figura 78.1 — Una nota clínica vista en dos carrils. A dalt, la versió impresa: un sol punt, «02:03 — nota de medicació, Dr. X». A baix, el rastre d'auditoria real amb segell de t2p: l'esdeveniment de creació declarat a les 02:03 però amb l'empremta ancorada a la blockchain pública a les 08:11 —un desfàs de sis hores—, fet des d'una estació no clínica (GPS forense fora de l'àrea de cures), amb una modificació posterior retrodatada que no pot ocultar la informació anterior (21 CFR 11.10(e)). El papel mostra un punt; el segell mostra la història. Límit: el segell prova qui i quan, no la veritat clínica del que s'hi va escriure. Fonts: HIPAA i FDA (controls d'auditoria); cas Prieto contra Rush; anàlisi forense d'historials.
- Figura 79.1 — El cicle de vida d'un model en quatre baules: dades d'entrenament → entrenament → pesos + AI-BOM (targeta de model, informe d'avaluació) → desplegament. t2p ancora l'empremta SHA-512 dels pesos i del manifest a la blockchain pública, amb segell RFC 3161/eIDAS complementari (.asice). Dos punts de risc: dades il·legals o opaques a l'origen (LAION-5B) i pesos manipulats entre el laboratori i l'usuari (porta del darrere *nullifAI* via *pickle*), que la comprovació d'empremta detecta. Límit: el segell prova què es va declarar i quan, i que els pesos són els avaluats; no prova que la declaració sigui certa ni que el model sigui segur. Fonts: Stanford Internet Observatory (LAION-5B); JFrog (models maliciosos); Reglament europeu d'IA, art. 53 i 50; CycloneDX ML-BOM.

- Figura 80.1 — El mandat verificable per a agents d'IA amb prova d'existència (segellat amb t2p — capítol 13): el mandat segellat abans d'activar (pressupost, àmbits, vetos), el registre d'accions ancorat per lots encadenats, la captura certificada de l'oferta que l'agent va veure (imatge + codi font) i l'autorització forta amb vídeo-selfie per sobre del llindar. Context: la indústria ja construeix mandats signats (Visa Intelligent Commerce, Mastercard Agent Pay, Google AP2 — Intent/Cart Mandate com a credencials verificables); la capa que falta és la neutral entre usuari, plataforma i comerç. Precedent: Moffatt v. Air Canada (2024) — qui desplega l'agent respon. Fonts: tribunal de la Colúmbia Britànica; Visa/Mastercard/Google AP2.
- Figura 81.1 — Dues vies. A dalt: la persona crea, amb prova de vida, una concessió de consentiment acotada (quins usos, per a qui, fins quan) lligada a una referència biomètrica (empremta SHA-512; la cara no surt del dispositiu), ancorada a la blockchain pública, amb segell eIDAS complementari (.asice); una rèplica legítima en porta un punter verificable, i la revocació queda datada. A baix: un anunci deepfake sense cap concessió segellada —l'absència mateixa demostra la falta de consentiment. Límit: el segell prova si es va consentir, de qui i quan; no detecta el deepfake ni n'impedeix la creació, i no jutja si el consentiment va ser lliure. Fonts: cas Tom Hanks; cas Johansson–OpenAI; acord SAG-AFTRA; ELVIS Act; reforma danesa.
- Figura 82.1 — La imatge del menor amb prova d'existència (segellat amb t2p — capítol 13) — es documenten les decisions dels ADULTS, mai el menor: l'autorització escolar precisa i segellada (usos, canals, durada), el desacord entre progenitors datat, la petició de retirada amb resposta o silenci datats, i l'empremta de la publicació per al futur (el fill gran podrà acreditar què es va publicar d'ell, sense que cap contingut viatgi). Context: un infant apareix en ~1.300 fotos en línia abans dels 13 anys; Llei francesa 2024-120 (dret a la imatge dins l'autoritat parental, exercit en comú; delegació judicial en casos greus). Límits: l'interès superior del menor el fixa el jutge; proporcionalitat; la prudència primer. Fonts: Légifrance; DAJ.
- Figura 83.1 — La víctima o l'entitat de suport calcula al dispositiu l'empremta SHA-512 del contingut (la imatge no surt del telèfon) i hi afegeix on i quan s'ha trobat; l'empremta del conjunt s'ancora a la blockchain pública, amb segell eIDAS complementari (.asice). Dos resultats: a l'esquerra, la retirada demostrable a totes les plataformes (model StopNCII, amb rebut segellat de les 48 hores); a la dreta, evidència datada i admissible per al tribunal (com a Almendralejo). Límit: el segell no retira la imatge, no impedeix crear-la ni detecta el deepfake; mai un registre d'imatges, només empremtes. Fonts: cas Almendralejo; cas Taylor Swift; TAKE IT DOWN Act; Directiva (UE) 2024/1385; StopNCII.org.
- Figura 84.1 — La víctima, la família o el centre educatiu calcula al dispositiu l'empremta SHA-512 del contingut d'odi (el contingut no surt del telèfon) i hi afegeix on i quan s'ha trobat i la sol·licitud de retirada; l'empremta del conjunt s'ancora a la blockchain pública, amb segell eIDAS complementari (.asice). Tres sortides: l'expedient escolar, la denúncia penal (arts. 510 i 172 ter) i el notice-and-action de la plataforma (DSA/UK OSA), amb rebut segellat. Límit: el segell no retira el post, no impedeix crear odi ni el detecta; mai un registre del contingut ni una eina de desanonimització, només empremtes al dispositiu. Fonts: cas Picchio; Molly Russell; ANAR; StopNCII.
- Figura 85.1 — Tres escuts per a la gent gran amb una sola lògica (empremta SHA-512 al dispositiu, segell de temps RFC 3161/eIDAS, ancoratge a la blockchain pública, .asice): la verificació familiar contra la veu clonada (repte + prova de vida segellada), la cura acreditada (registres de residència ancorats; càmera només dins de la doctrina de proporcionalitat del TS) i la voluntat amb data certa (Llei 8/2021: suport, no substitució). Límits: cap registre central de veus, revocabilitat, i el control sempre en mans de la persona gran. Fonts: INCIBE; FBI/IC3; elDiario.es (El Escorial); Llei 8/2021.
- Figura 86.1 — L'òrgan emissor (oficina de premsa, centre d'operacions, banc central) calcula al dispositiu l'empremta SHA-512 de la declaració oficial —vídeo, comunicat, decisió o alerta— sense que el fitxer surti; per a declaracions en directe del principal hi afegeix prova de vida i GPS forense. L'empremta del conjunt s'ancora a la blockchain pública, amb segell RFC 3161/eIDAS complementari (.asice), i se'n publica el handle de verificació (QR/URL) al canal oficial. Dos resultats: a l'esquerra, verificació pública en segons per part de periodistes i ciutadans; a la dreta, el desmentiment d'una falsificació (teletip piratejat, reemissió no verificada) contra l'original segellat. Límit: el segell prova origen, hora, autor i integritat, no que el contingut sigui cert, legal ni assenyat; no atura un deepfake mai comparat ni protegeix l'emissor de ser piratejat. Fonts: cas Ukraine 24/Zelenski; imatge falsa del Pentàgon; cas Rubio; cas Channel 14/Gallant; alerta de Hawaii de 2018; article 50 del Reglament d'IA; IPAWS; CSI Content Credentials NSA/CISA.
- Figura 87.1 — El directiu genuí captura la instrucció de pagament al dispositiu (text signat, factura en PDF o vídeo amb prova de vida i GPS forense), en calcula l'empremta SHA-512 sense que surti

del dispositiu, i l'ancora a la blockchain pública, amb un segell de temps RFC 3161/eIDAS complementari (.asice). La tresoreria verifica el segell contra l'àncora pública: si quadra, paga; si falta, atura —la instrucció «urgent» sense segell és, per disseny, una bandera vermella (mode de fallada d'Arup). Límit: el segell prova l'acte d'autoritzar, no que la instrucció sigui legítima; no atura un directiu coaccionat ni una clau robada, ni recupera fons ja transferits. Fonts: cas Arup; alerta FinCEN FIN-2024-Alert004; FBI/IC3 PSA250515; eIDAS art. 41-42.

- Figura 88.1 — La identitat en directe amb prova d'existència (t2p: vídeo-selfie amb reptes de vida aleatoris — parpellejar, girar, somriure, inclinar — en <60 s, biometria o PIN del dispositiu, empremta SHA-512, segell RFC 3161/eIDAS, àncora a la blockchain pública, certificat amb l'evidència en vídeo i attestation de maquinari, paquet .asice verificable fora de línia): a l'esquerra, el handshake de la reunió (full de la reunió com a document-repte signat per cada participant abans d'obrir micròfons; comparació de la cara segellada amb la de pantalla; la pregunta a contracorrent com a capa extra); a la dreta, l'alta com a humà (el formulari d'alta signat amb vídeo-selfie: pseudònim-però-humà, la plataforma verifica sense custodiar biometria; identitat civil via cartera EUDI quan cal). Context: face-swap en temps real comercialitzat (Yahoo Boys), +2.665 % d'atacs de càmera virtual nativa i +300 % de face swaps contra sistemes amb liveness (iProov 2025), 30 % de desconfiança empresarial prevista (Gartner). Límits: els reptes gestuals són un llistó, no una muralla — capes i cost asimètric (el frau que signa queda notariat); la comparació de cares és del receptor, mai de l'app. Fonts: WIRED/9to5Mac; iProov; Gartner; FBI IC3; Decrypt; arXiv/MIT; CE (EUDI).
- Figura 89.1 — L'emissor (o el seu agent o teletip) segella la revelació sensible al preu en el moment d'emetre-la: empremta SHA-512 al dispositiu → blockchain pública, amb segell de temps RFC 3161/eIDAS complementari (.asice), amb GPS forense i prova de vida si hi ha un directiu filmant. L'empremta es publica al costat del compte oficial; qualsevol periodista, borsa, regulador o canal algorísmic confirma en mil·lisegons si una piulada o comunicat «d'última hora» coincideix amb el genuí (Lilly, Pentàgon-Bloomberg, BSE, Ostin) o és l'impostor. Límit: el segell prova qui ho va emetre i quan, no que la revelació sigui veritat; un comunicat de pump-and-dump segellat continua sent fals, i la manipulació continua sent feina de la SEC/ESMA/FINRA i les borses. Fonts: cas Eli Lilly; imatge falsa del Pentàgon; Hack Crash de 2013; cas Ostin Technology; avís SEC/FINRA/NASAA; MAR art. 12.
- Figura 90.1 — El titular real, l'administrador o el proveïdor de serveis societaris presenta la declaració i la seva evidència (registre d'accionistes, escriptura de fideïcomís, identitat, prova de vida amb GPS forense al terreny); es calcula l'empremta SHA-512 al dispositiu —els documents no surten — i s'ancora l'empremta a la blockchain pública, amb segell RFC 3161/eIDAS complementari (.asice). El rebut complementa els registres (FinCEN BOI · AMLR/AMLA · Companies House · GAFI R.24): prova qui va declarar què i quan, i fa detectable la retrodatació. Límit: el segell no prova que la persona declarada sigui el titular real últim; no travessa cadenes de societats pantalla ni detecta un testaferro. Fonts: Papers de Pandora (ICIJ); Papers de Panamà; Transparency International; FinCEN; CJUE C-37/20 i C-601/20; GAFI R.24; Open Ownership.
- Figura 91.1 — La contractació remota segellada en tres baules: entrevista en vídeo amb prova de vida → verificació d'identitat (document + selfie) → atestació d'*onboarding* lligada a qui rep el portàtil. A cada moment es calcula l'empremta SHA-512 al dispositiu (la biometria no surt), amb segell RFC 3161/eIDAS, GPS forense i ancoratge a la blockchain pública (.asice). Resultat: una cadena de no-repudi que demostra que el mateix humà verificat hi era als tres punts. Límit: el segell no prova que la persona sigui honesta, que la identitat no sigui robada ni que no sigui un nacional sancionat; complementa, no substitueix, el cribratge d'antecedents, de sancions i la detecció de deepfakes. Fonts: cas KnowBe4; cas Chapman (DOJ); FBI/IC3 I-012325-PSA; NIST SP 800-63-4; Pindrop.
- Figura 92.1 — La relació laboral de plataforma amb prova d'existència: el treballador segella el seu diari laboral (hores, encàrrecs, instruccions, captures de condicions) al seu dispositiu; la plataforma ancora el registre de decisions algorítmiques i la revisió humana (art. 22 RGPD; Directiva (UE) 2024/2831); el comitè rep els paràmetres de l'algorisme amb versionat segellat (Ley Rider). Tres sortides: la presumpció de laboralitat provada amb fets datats, la desactivació auditable i la inspecció que no comença de zero. Límits: el segell no decideix la laboralitat ni substitueix la negociació col·lectiva; el diari és del treballador, mai un filtre reputacional. Fonts: DOUE (Dir. 2024/2831); BOE (Llei 12/2021); elDiario.es (cas Glovo); Worker Info Exchange (Drivers v. Uber/Ola).
- Figura 93.1 — La jornada amb prova d'existència (segellat amb t2p — capítol 13): el diari laboral del treballador (fitxatge, hores, torns — al seu dispositiu, només empremtes a la cadena), el fitxatge amb GPS forense (el moment, mai el seguiment), el quadrant i l'ordre capturats amb data certa, i el registre oficial de l'empresa certificat per lots encadenats — demostrablement íntegre davant

d'Inspecció i jutjat. Context: la reforma del registre horari digital (tramitació urgent des del 30-9-2025) exigirà immutabilitat, traça i accés remot de la Inspecció; >40 % de les hores extres no es paguen (EPA). Límits: el conveni i el jutge decideixen el fons; proporcionalitat sempre. Fonts: EPA/INE; projecte de registre horari digital.

- Figura 94.1 — Tres fites irreversibles d'una obra: inspecció prèvia al formigonat (armadura, encofrat, recobriment), assaig de proveta als 28 dies, i plànols as-built + informe geotècnic a la signatura. A cada fita, t2p calcula l'empremta SHA-512, hi afegeix GPS forense i prova de vida si hi ha captura de camp, segella amb RFC 3161/eIDAS i ancora a la blockchain pública (.asice); el contenidor flueix cap al fil daurat (BSA 2022) i el model BIM (ISO 19650) i s'aparella amb el Passaport Digital de Producte (Reglament UE 2024/3110). Punts de risc que la datació independent fa demostrables: canviar la data de l'ordinador (Hong Kong–Zhuhai–Macau) i escriure el valor de l'especificació (Testwell). Límit: el segell prova que un registre existia, qui el va fer i quan, no que l'edifici sigui segur ni que el material compleixi. Fonts: terratrèmols de Turquia 2023 (Isias Grand Hotel); NIST (Champlain Towers South); ICAC (pont HZMB); Testwell; pont Morandi; Building Safety Act 2022; Reglament (UE) 2024/3110.
- Figura 95.1 — Un esdeveniment de manteniment crea un registre (EASA Form 1 / FAA 8130-3, entrada de quadern, lectura de comptaquilòmetres). El tècnic en calcula l'empremta SHA-512 al dispositiu (el fitxer no surt), hi afegeix GPS forense i prova de vida si hi ha captura de camp, i l'empremta del conjunt s'ancora a la blockchain pública, amb segell RFC 3161/eIDAS complementari (.asice). Qualsevol part posterior —recepció de mercaderies, CAMO, regulador, comprador— verifica de manera independent qui ho va declarar i quan. Límit: el segell prova l'origen, el temps, l'autor i la integritat del document; no prova que la peça sigui genuïna, nova o aeronavegable, ni que el quilometratge sigui cert — escombraries a l'entrada, escombraries a la cadena. Fonts: cas AOG Technics (SFO); demanda de CFM International; estimacions FAA de peces no aprovades; CARFAX i Parlament Europeu sobre comptaquilòmetres; Aviation Supply Chain Integrity Coalition.
- Figura 96.1 — La cadena d'una dada d'emissions en quatre baules: captura al sensor (CEMS, analitzador de metà, banc de proves, vol de dron/satèl·lit) → adquisició → informe regulador → auditoria. t2p calcula al dispositiu l'empremta SHA-512 de la lectura bruta, hi afegeix segell de temps RFC 3161/eIDAS i, en camp, GPS forense, i l'ancora a la blockchain pública (.asice); l'auditor confronta la xifra presentada amb la captura segellada. Dos punts de risc: el banc de proves trucat (dispositiu de desactivació VW/Cummins) i el sensor esbiaixat al voltant de les auditories (CEMS de Berkshire), que el segell NO detecta. Límit: el segell prova origen, temps, autor i integritat de la mesura; no prova que la mesura sigui certa al punt de captura, ni quantifica emissions ni jutja el compliment. Fonts: EPA (VW, Cummins, Berkshire, Marathon, norma de metà); AIE; MethaneSAT; TJUE (finestra tèrmica).
- Figura 97.1 — La ciència ciutadana amb prova d'existència: el sensor del balcó, la foto de l'abocament i el diari del soroll s'ancoren en origen (empremta SHA-512, segell de temps RFC 3161/eIDAS, blockchain pública, .asice) i esdevenen cronologies amb integritat acreditada que activen la inspecció oficial (acta amb sonòmetre homologat, amb presumpció de veracitat), orienten el pèrit i donen memòria a la veu legal dels ecosistemes (Mar Menor, Llei 19/2022). Límits: el segell no acredita el calibratge ni substitueix l'acta oficial; es documenten fets, no persones. Fonts: TJUE (Doñana, 2021); BOE (Llei 19/2022); Sensor.Community; Defensor del Pueblo.
- Figura 98.1 — El cicle de vida d'una bateria en quatre baules: materials i mina → fabricació → ús i estat de salut → segona vida / reciclatge. Cada baula genera un artefacte probatori (certificat de reciclat, informe de petjada de carboni de l'organisme notificat, exportació del BMS, acta de desmuntatge); t2p en calcula l'empremta SHA-512 al dispositiu i l'ancora a la blockchain pública, amb segell RFC 3161/eIDAS complementari (.asice), amb GPS forense i prova de vida en captura de camp. El QR del passaport enllaça l'afirmació amb l'artefacte segellat, verificable fora de línia per duanes, auditors i compradors de segona mà. Límit: el segell prova origen, data, autor i integritat de l'artefacte; no prova que el contingut reciclat sigui real, que l'estat de salut no s'hagi maquillat ni que la bateria sigui segura. Fonts: Volvo EX90 / Circulor; Global Battery Alliance; Reglament (UE) 2023/1542; ESPR (UE) 2024/1781.
- Figura 99.1 — La cadena del residu amb prova d'existència (segellat amb t2p — capítol 13): el contenidor amb lloc i hora a cada canvi de mans (GPS forense; precintat filmat amb data sobreimpresa), el balanç de massa segellat per lots encadenats (entrades vs sortides datades), el certificat de tractament final ancorat i l'afirmació verda congelada (captura web amb codi font). Context: Reglament (UE) 2024/1157, aplicable des del 21-5-2026 — notificació prèvia per a tot residu plàstic exportat, prohibició cap a països no OCDE; Turquia rebia el 39 % de les exportacions

europees (12,4 Mt). Límits: la traça acredita custòdia, no qualitat de tractament; primer reduir i reutilitzar. Fonts: DOUE/BOE; RETEMA.

- Figura 100.1 — El camp amb prova d'existència (segellat amb t2p — capítol 13): l'entrada del quadern segellada al moment i al camp (GPS forense), la foto georeferenciada que el monitoratge demana — amb data certa neutral —, la sèrie de campanya com a defensa contra el satèl·lit que s'equivoca (la simetria del capítol 104, mirada des de baix) i l'expedient de l'ajuda en .asice. Context: PAC vigilada per Sentinel/Copernicus; quadern digital (CUE) voluntari des de 2024, fitosanitaris electrònics des de l'1-1-2027, CUE obligatori l'1-1-2028 (>30 ha). Límits: complementa el quadern oficial, no el substitueix; la bretxa digital del camp exigeix cooperatives i tècnics com a aliats. Fonts: FEGA/normativa CUE; PAC 2023-2027.
- Figura 101.1 — El productor captura la prova de camp geoetiquetada amb prova de vida i GPS forense (olivar, rusc, línia d'envasat) i en calcula l'empremta SHA-512 al dispositiu; en paral·lel, l'organisme de control i el laboratori segellen el certificat, l'informe analític, el número de lot i l'etiqueta DOP/IGP. L'empremta de tot plegat s'ancora a la blockchain pública, amb segell RFC 3161/eIDAS complementari (.asice), lligat a un identificador de lot. Qualsevol inspector, duana o tribunal ho verifica fora de línia: existència, autor, data i integritat. Límit: el segell prova el paper i l'acte de camp, no que l'oli sigui verge extra ni que la mel no estigui tallada —això ho diu el laboratori (NMR/IRMS/ADN/pol·len). Fonts: OPSON XIII i XIV (Europol); cas Pulla; Operació Omegabad; «From the Hives»; Reg. (UE) 2024/1143.
- Figura 102.1 — Dues fonts de prova: el treballador, el sindicat o l'auditor de camp capturen al dispositiu una imatge o un testimoni del taller (empremta SHA-512 que no surt del telèfon, GPS forense, prova de vida); la marca segella la declaració del proveïdor i el registre de diligència deguda. L'empremta de tot plegat s'ancora a la blockchain pública, amb segell de temps RFC 3161/eIDAS complementari (.asice). Resultats: testimoni del treballador més difícil de desestimar com a deepfake, i expedient datat per a la CBP, la BAFA o l'autoritat de la UE. Límit: el segell prova l'acte, el lloc i la data; no prova que les condicions siguin bones, que la declaració sigui veraç ni que el testimoni fos lliure. Fonts: cas Volkswagen/CBP; OIT; Miller & Chevalier (UFLPA); HRW (auditories i automòbil); ECCHR (certificats).
- Figura 103.1 — En prendre una fixació, una unitat de bord o un inspector de l'estat del port captura el registre de navegació (GNSS + hora, IMO/MMSI, calat, trama AIS) i en calcula l'empremta SHA-512 al dispositiu; l'empremta del conjunt s'ancora a la blockchain pública, amb segell RFC 3161/eIDAS complementari (.asice), amb GPS forense i prova de vida quan hi ha inspecció física. Dos resultats: a l'esquerra, un llibre major de posició i identitat no repudiable; a la dreta, l'absència de segell esdevé una bandera vermella per al cribratge de l'OFAC/UE. Límit: el segell certifica que el dispositiu va registrar aquesta fixació en aquest instant, no que el senyal GNSS fos genuí; un senyal falsejat ancora una posició falsa. Fonts: cas Windward (esquema de 800 M$); Kpler (261 vaixells); GPSPATRON (10.000+ vaixells); Scientific American (Ormuz); OFAC (MS ENOLA).
- Figura 104.1 — La cadena de l'observació de la Terra en dues baules de segellat. A l'origen, l'operador (Maxar, Planet, Copernicus) calcula l'empremta SHA-512 de l'escena crua/L1 més les metadades a l'ingest de l'estació de terra; l'empremta s'ancora a la blockchain pública, amb segell RFC 3161/eIDAS complementari (.asice). A l'altre extrem, l'analista o periodista OSINT torna a segellar el retall, l'anotació i les coordenades, amb GPS forense i prova de vida. Punts de risc: imatge forjada amb GAN/difusió (Stable Diffusion, StyleGAN2) i interferència del GNSS, que la signatura de Galileo OSNMA i els detectors de Vision Transformer mitiguen però no eliminen. Límit: el segell prova origen, hora, autor i integritat bit a bit; no prova que l'escena sigui observació autèntica ni que la interpretació sigui correcta. Fonts: cas Bucha (Maxar); Bo Zhao (geografia deepfake); Xinjiang (BuzzFeed); arXiv 2511.17766; Galileo OSNMA; OGC IPT.
- Figura 105.1 — La dada d'emergència se segella en origen: la lectura del sensor (SAIH/Poio), l'acta i el vídeo de l'òrgan de coordinació (CECOPI), l'alerta (ES-Alert), l'ordre d'evacuació i la foto de danys del ciutadà reben l'empremta SHA-512 al dispositiu o a la font, l'ancoratge de l'empremta a la blockchain pública i el segell de temps RFC 3161/eIDAS complementari (.asice). Tres sortides: la instrucció judicial (cronologia no repudiable), la reclamació a l'asseguradora i al Consorci, i l'auditoria pública i periodística. Límit: el segell no prediu, no avisa i no salva; només fa la veritat indestructible. Fonts: Maldita.es; CHJ/SAIH; Consorci de Compensació d'Assegurances; Lauegi.
- Figura 106.1 — Davant la cursa sovint perduda de la detecció, l'ancoratge neutral demostra que una cosa autèntica va existir i no s'ha alterat.
- Figura 107.1 — La decisió d'IA pública deixa un registre citat que, ancorat amb prova d'existència, esdevé una auditoria independent i no-repudiable.

- Figura 108.1 — La prova de personalitat es pot fer al dispositiu, sense bases biomètriques centralitzades: una persona, una veu, sense vigilància.
- Figura 109.1 — La prova simètrica al carrer: el vídeo del manifestant i la càmera corporal de l'agent se segellen en captura, per segments (empremta SHA-512 al dispositiu, segell de temps RFC 3161/eIDAS, ancoratge a la blockchain pública, .asice), sense publicar res ni identificar ningú. Al jutjat, les dues cadenes es fusionen en una línia de temps verificable; qualsevol tall o supressió es detecta. Límits: el segell no acredita el context fora de pla, no valora la proporcionalitat i exigeix revocabilitat, publicació voluntària i zero reconeixement facial. Fonts: Pulitzer/Frazier; elDiario.es («Rodea el Congreso»); SME/USPAC (Axon Body 3); Telemundo/Univision (Detroit).
- Figura 110.1 — Com més puja la temperatura, més cau l'economia: el cost de no actuar es dispara amb cada dècim de grau.
- Figura 111.1 — Cada actor —govern, empresa i ciutadania— té accions concretes a curt, mitjà i llarg termini.
- Figura 112.1 — El segell i la cadena: qui controla la prova, i qui hi queda atrapat. Els riscos que el capítol desgrana — la neutralitat que no existeix, el consentiment cristal·litzat, la plusvàlua de la prova, el dret a l'oblit eliminat, els algoritmes inapel·lables i l'autocensura del registre permanent — i els contrapesos que reclama: només-empremta per defecte, revelació selectiva, governança democràtica de la infraestructura i el dret a no segellar.
- Figura 113.1 — La prova sota setge, de l'objectiu al tribunal (t2p: empremta SHA-512 al dispositiu — la imatge no surt del mòbil —, segell RFC 3161/eIDAS, àncora a la blockchain pública, paquet .asice): el fotoperiodista acreditat amb credencial d'agència sense exposar la font; el testimoni ciutadà amb compromís i revelació (segella ara, publica quan sigui segur) i prova pòstuma; les tres capes del setge (porta tancada a la premsa internacional, periodistes locals morts o assenyalats, «fake!» contra les imatges reals) i on les trenca el segell. Límits: l'apagada retarda l'àncora (sandvitx temporal «no abans / no després»); el GPS suplantat degrada la posició, no l'hora; el segell prova quan i què — mai la veritat de l'escena: la corroboració continua sent imprescindible. Fonts: CPJ; RSF; Costs of War (Brown); OHCHR; Forensic Architecture; ECCHR/Coblença; Access Now; Starling Lab/Reuters; WITNESS/Guardian Project.
- Figura 114.1 — La doctrina social de l'Església davant l'economia i la tècnica: de la 'Rerum Novarum' (1891, el treball) a la 'Laudato Si'' (2015, la Casa comuna) i la 'Magnifica Humanitas' (2026, la persona en temps d'IA).
- Figura 114.2 — La mateixa prova d'existència, dos camins (§1): cap a «Babel» (poder privat, reducció de la persona a dada, dominació) o cap a la «ciutat» (dignitat de qui existeix, subsidiarietat, accés universal). La diferència no és tècnica, sinó de governança i de fi.

Glossari

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)