La prova documentale al tempo dei *deep fakes*

di Valentina Capasso

1. Introduzione: gli effetti collaterali della nozione ampia di «documento».

In un brevissimo appunto, pubblicato nel 1924, Francesco Carnelutti notava con un certo compiacimento che, mentre finanche molti «discepoli» avevano in precedenza accolto con «sorrisi d'incredulità» la sua idea che presto anche il documento fonografico avrebbe trovato spazio nella «documentazione notarile» (1), la «cronaca» avesse finito per dargli ragione; e, dopo aver dato conto di un incidente fortuitamente filmato, con pellicola poi sequestrata dall'autorità giudiziaria che aveva avviato il procedimento per omicidio colposo, concludeva nel senso che «nel processo penale e nel processo civile, che eventualmente […] si innesti su quello o lo segua», avrebbe potuto, se non addirittura dovuto, sostituirsi «alla prova per testimoni o per presunzioni» quella «cinematografica» (2). Conclusione implicitamente quanto evidentemente fondata sulla presunta superiorità (anche in termini di fedeltà ai fatti) di tale tipo di prova documentale.

(1) F. Carnelutti, *Prova cinematografica*, in *Riv. dir. proc.,* 1924, 1, 204.
(2) *Ibid*., 105.

Ma se la nozione ampia di «documento» patrocinata da Carnelutti è ormai pacificamente accettata in dottrina, e confermata dal legislatore (3), la «fiducia [ne]lla evoluzione della tecnica», che pur a lungo ha sorretto lo studioso della materia (4), oggi vacilla: perché è quella stessa evoluzione, che pur si immaginava potesse aiutare a risolvere problemi, a crearne di nuovi.

In particolare, il riferimento è, in questa sede, ai *deep fakes*, espressione che deriva dalla crasi tra *deep learning* (tipo di *machine learning* che utilizza reti neurali artificiali per apprendere dai dati, imitando il funzionamento del cervello umano) e *fake*, *i.e.* non genuino, inattendibile.

Un *deep fake* è, nella definizione dell'art. 3(60) *AI act*, «un'immagine o un contenuto audio o video generato o manipolato dall'IA che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona». Più ampiamente, l'art. 3 *Measures for Labeling of AI-Generated Synthetic Content*, promulgate in Cina il 14 marzo 2025, include nella nozione di «*AI-generated synthetic content*», cui è riferita la successiva disciplina, ogni «*text, imag[e], audio, video, virtual scen[e], or other information that is generated or synthesized using AI technology*» (5). Tutti contenuti, questi, su-

(3) In passato, infatti, come noto, tale nozione era indebitamente circoscritta, dall'una come dall'altro, al solo scritto: v. F. Carnelutti, *La prova civile*, Milano, 1992, 167-169; per ulteriori riferimenti, v., tra gli altri, F. Zacché - G. Voena, *La prova documentale*, in G. Ubertis - G. Voena (dir.), *Trattato di procedura penale*, Milano, 2012, 7 ss.

Peraltro, se, dal 2006, l'art. 2712 c.c. menziona espressamente, oltre alle riproduzioni fotografiche, anche quelle informatiche, si è osservato che la disposizione in parola «già rappresentava una sorta di clausola generale all'interno della disciplina della prova documentale, poiché consentiva l'inserimento di nuovi mezzi di prova frutto della evoluzione della tecnica», sicché sarebbe stato verosimilmente «possibile ricondurre il documento informatico […] all'interno di questa norma anche senza l'intervento del legislatore»: S. Patti, *Delle prove. Art. 2697-2739*, in G. De Nova (a cura di), *Commentario del Codice civile e codici collegati Scialoja-Branca-Galgano,* Bologna, 2015, 482.

(4) V., a proposito del problema della paternità del documento, A. Bonafine, *L'atto processuale telematico,* Napoli, 2017, 94, richiamando ancora F. Carnelutti, *Studi sulla sottoscrizione*, in *Riv. dir. comm.* 1929, I, 509.

(5) Ma sull'evoluzione della disciplina cinese in materia (già avviatasi da qualche anno), v. F. Corona, *IA e regolamentazione: una comparazione tra approcci normativi*

scettibili non solo di diffusione più o meno ampia e lesiva — e perciò progressivamente fatti oggetto di disciplina sostanziale (6) — ma anche di essere prodotti in giudizio quali «documenti», e così divenire oggetto di apprezzamento giudiziale; mettendolo, però, in crisi.

Del problema hanno già iniziato a farsi carico la giurisprudenza e la letteratura straniera (7) e, da ultimo, quella processualpena-

per un equilibrio sostenibile, in U. Comite - A. Kostyuk (a cura di), *Sostenibilità e Intelligenza Artificiale: resilienza o panacea?*, Milano, 2025, 123 s.

(6) Principalmente, in campo penale: così, in Italia, l'art. 26 l. 23 settembre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale" ha — tra l'altro — introdotto il reato di cui all'art. 612-*quater* c.p., che sanziona l'illecita diffusione di contenuti generati o alterati a mezzo dell'IA e una nuova aggravante comune (art. 61, comma 11-*undecies*: «l'avere commesso il fatto mediante l'impiego di sistemi di intelligenza artificiale, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano costituito mezzo insidioso, ovvero quando il loro impiego abbia comunque ostacolato la pubblica o la privata difesa, ovvero aggravato le conseguenze del reato»). Analogamente, in Francia, la *loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique* (c.d. *loi SREN*) ha introdotto il reato di cui all'art. 226-8 CP, che punisce la diffusione al pubblico e la comunicazione a terzi di contenuti audiovisivi generati artificialmente che rappresentano l'immagine o la voce di una persona, senza il suo consenso, qualora la natura artificiale degli stessi non sia chiaramente evidente o non vi sia alcuna indicazione esplicita in tal senso; disposizione il cui campo di applicazione limitato è stato però criticato dalla dottrina: A. Guedj, *L'apport de la Loi SREN en matière de deepfake : une obsolescence annoncée ?,* in *Dalloz IP/IT,* 2024, 391 ss.; N. Mallet-Poujol, *Droit des communications électroniques (2e partie),* in *Légipresse,* 2025, 300 ss. Più in generale, sugli strumenti attivabili nel panorama francese, v. C. Poirson, M. Sirot, *Vademecum des moyens de droit pour lutter contre la diffusion en ligne d'hypertrucages visuels ou sonores générés par un traitement algorithmique, communément appelés deepfakes*, in *Légipresse,* 2025, 620 ss.

(7) Benché la maggioranza dei contributi stranieri (specialmente statunitensi) abbia specifico riguardo al processo penale (v., ad esempio, A. McPeak, *The Threat of Deepfakes in Litigation: Raising the Authentication Bar to Combat Falsehood,* in *Vanderbilt J. Entertainment and Technology L.,* 2021, 443 ss.; S. Kothari - S. Tibrewala, *AI's Trojan Horse: The Deepfake conundrum under the criminal justice system,* in *KALP Journal of Multidisciplinary Studies,* 2024, 45 ss.), non mancano studi di più ampio respiro, indirizzati al problema senza distinzioni di materia (v., tra gli altri, R.A. Delfino, *Deepfakes on Trial: A Call To Expand the Trial Judge's Gatekeeping Role To Protect Legal Proceedings from Technological Fakery,* in *Hastings L.J.,* 2023, 293 ss.; Id., *The Deepfake Defense—Exploring the Limits of the Law and Ethical Norms in Protecting Legal Proceedings from Lying Lawyers,* in *Ohio State L.J.,* 2024, 1067 ss.; A. Dalal - C. Gao - P.W. Grimm - M.R. Grossman - D.W. Linna Jr. - C. Pulice - V.S. Subrahmanian - J. Tunheim, *Deepfakes in Court: How Judges Can Proactively Manage Alleged AI-Generated Material in National Security Cases*, in *The University Of Chicago Legal Forum,* 2024, 75 ss.) o rivolti a spe-

listica italiana (8). Rispetto al processo civile domestico, invece, se un rinnovato interesse ha recentemente destato l'indirizzo giurisprudenziale (anche di legittimità) (9) che tende a ricondurre il trattamento processuale degli *screenshot* WhatsApp a quello delle riproduzioni meccaniche (10), mancano ancora — a quanto consta — lavori che abbiano affrontato in generale il tema del documento di cui sia sospetta(ta) la genesi o almeno manipolazione artificiale: ciò che, appunto, ci si propone di fare, muovendo dagli spunti provenienti dalla comparazione interna ed esterna; non prima di aver precisato, però, che il discorso che si andrà conducendo, pur muovendo da fonti essenzialmente focalizzate sul tema dei contenuti *AI-generated* di tipo audiovisivo, tendenzialmente rappresentativi di fatti o cose, ben può riferirsi — mutato quel poco che v'è da mutare — a quelli che riproducono dichiarazioni di tipo testuale, indipendentemente dalla circostanza che gli stessi costituiscano oggetto di documentazione altrimenti (11) o siano invece recati da un documento (dichiaratamente) nativo digitale (12).

cifiche categorie di processo civile, come il contenzioso della famiglia (v. B. Ancel, *Défis normatifs internationaux d'une justice familiale automatisée : IA-t-il danger ?,* in *Petites affiches*, 25 novembre 2025, n. 11).

(8) S. Quattrocolo, Deepfake *e fine della tipicità probatoria? Fatto, prova e giudizio penale a confronto con la realtà delle immagini sintetiche*, in *La legislazione penale*, 31 luglio 2025.

(9) V. Cass., 18 gennaio 2025, n. 1254, secondo cui «i messaggi WhatsApp conservati nella memoria di un telefono cellulare sono utilizzabili quale prova documentale e, dunque, possono essere legittimamente acquisiti mediante la mera riproduzione fotografica, con la conseguente piena utilizzabilità dei messaggi estrapolati da una 'chat' di WhatsApp mediante copia dei relativi screenshot, tenuto conto del riscontro della provenienza e attendibilità degli stessi».

(10) Da ultimo, v. S. Rusciano, *Prova documentale*, in F. Auletta - S. Rusciano, *Prova giudiziale civile,* in S. Mazzamuto, *Trattato del diritto privato. Vol. VIII. La tutela dei diritti. Tomo IV,* Torino, 2025, 106 ss.; F. Savino, *Sul valore probatorio delle e-mail e dei messaggi whatsapp nel processo civile,* in *Riv. trim. dir. proc. civ.,* 2025, 3, 751 ss.; A. Vozza, *Rilevanza probatoria degli screenshot dei messaggi WhatsApp nel processo tributario*, in *Il Fisco*, 2025, 26, 2348 ss.

(11) Per usare la terminologia di F. Carnelutti, *La prova civile*, cit., 163, quando quello audio-visivo costituisca «documento del documento» scritto.

(12) In realtà, la vera differenza che corre tra tali ultimi due tipi di documenti sta, secondo la tesi che pare preferibile, nel regime di efficacia, dovendosi ritenere che solo i primi – in quanto documenti non dichiarativi — siano suscettibili di essere ricondotti alle

La precisazione non appare superflua, posto che, rispetto al tema che occupa, l'opposta possibilità — se non necessità — di condurre un discorso differenziato per i documenti del secondo tipo parrebbe suggerita non solo dalla circostanza che, come visto, l'*AI Act* (ma non la disciplina cinese) riconduce alla nozione di *deep fakes* solo contenuti audiovisivi, del resto in linea con la letteratura in materia (13), ma anche la non peregrina idea che, a mettere al riparo da alterazioni — comunque problematiche (14) — il (solo) testo in essi contenuto possa soccorrere, in via preventiva, il ricorso alla *blockchain*: questa — del resto — «[p]ur continuando a costituire l'essenza per le criptovalute, […] è oggi utilizzata in una varietà di campi» e per una pluralità di funzioni, compresa quella della «certificazione della prova di esistenza di

riproduzioni informatiche di cui all'art. 2712 c.c.; mentre i secondi, quali documenti dichiarativi, ove non sottoscritti, siano assoggettati al regime di cui all'art. 20, comma 1-*bis*, CAD); ma ciò, come si dirà *infra*, § 4, non implica anche un diverso grado di difficoltà nell'accertamento della genuinità del documento.

(13) L'apparizione "ufficiale" dei primi *deep fake*, nel 2017, è infatti comunemente individuata nell'*upload* di alcuni video pornografici da parte di un utente anonimo del sito Reddit, cui fece seguito — poco dopo — la diffusione, sulla medesima piattaforma, da parte di altro utente, di un'applicazione gratuita (*FakeApp*), che, rendendo per la prima volta possibile la creazione di *deep fakes* anche a chi non avesse competenze in materia di programmazione, ha agevolato a dismisura la diffusione di tali contenuti, in precedenza sostanzialmente confinati agli studi cinematografici: R.A. Delfino, *Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's NextTragic Act*, in *Fordham L.R.*, 2019, 893.

(14) Come rileva U. Carnevali, *Il documento informatico e la forma scritta* ad substantiam, in *Contr.*, 2025, 1, 6, «[l]e alterazioni del contenuto di un documento cartaceo lasciano inevitabilmente traccia fisica in esso e perciò sono riconoscibili. Invece i files affluiti alla memoria del computer e che costituiscono l'oggetto del documento informatico sono segnali elettronici che non sono inscindibilmente connessi con la memoria che li accoglie (salvo casi particolari: memorie ROM, ecc.) e di conseguenza il testo digitale può essere alterato senza che eventuali alterazioni siano individuabili. | In altri termini, […] mentre nel documento cartaceo il testo non può essere dissociato dal supporto materiale che lo contiene, invece il documento informatico è separabile dal supporto che lo contiene, tanto che una identica serie di dati elettronici può essere memorizzata da un supporto informatico ad un altro senza che per questo si possa distinguere un originale del documento informatico da una copia di esso. Poiché il documento informatico è la rappresentazione digitale di atti o fatti o dati, tale rappresentazione può essere stata falsificata e a tale rischio si riferisce il disconoscimento della riproduzione informatica di cui all'art. 2712 c.c. per quanto riguarda i fatti e i dati ivi rappresentati».

un documento e del suo contenuto in una certa data» (15) (c.d. notarizzazione) (16), per l'affidamento riposto nella circostanza che, una volta che il codice informatico venga inserito all'interno della stessa, «risulta estremamente difficile, se non potenzialmente impossibile, procedere ad una sua modifica» (17); ma, di là dei dubbi circa lo specifico peso probatorio di quanto ritraibile dalla catena di blocchi, la giurisprudenza straniera non conforta — allo stato — l'idea. Probabilmente, non a torto.

Invero, proprio chi, muovendo dall'indirizzo giurisprudenziale domestico, favorevole all'ammissibilità della prova atipica, ha recentemente ipotizzato, «data la natura piuttosto puntuale delle catene di blocchi, […] la possibilità che i dati della catena […]

(15) A. Sanchini, Blockchain, *metaverso e tecnologie del* web *tra tutela brevettuale e tutela dell'algoritmo,* in *Dir. ind*., 2023, 2, 141 s.

(16) Perché «sostanzialmente, come presso un Notaio, si dà ad un file sia data certa (perché […] esisteva al momento dell'operazione, se non prima ovviamente), sia prova di esistenza, essendo impossibile, appunto, *a posteriori*, costruirlo *ad hoc*»: così O. Venier, Blockchain, *NFT, Metaverso & proprietà intellettuale. Tavola Rotonda su esperienze applicative*, in *Dir. ind.,* 2023, 2, 136.

Ovviamente, ove si guardi ad effetti ulteriori, l'equivalenza non appare più così scontata; anzi, e paradossalmente, il progresso tecnologico e informatico, che pur da tempo ha indotto a ventilare la possibile esautorazione del notaio, sembra invece suscettibile di restituire centralità alla figura: come osserva R. Genghini, *La forma notarile digitale*, San Giuliano Milanese, 2022, 47, nota 39, sia pur discorrendo della funzione di accertamento della volontà negoziale (ma con considerazioni che sembrano potersi richiamare anche in relazione al valore probatorio del documento), «[c]on l'innovazione tecnologica si è avviato un processo di creazione e diffusione degli archivi pubblici (catasto, registri immobiliari, registri commerciali, anagrafi, stato civile) e dei documenti d'identità, che ha sottratto al notaio parte delle sue competenze più importanti, al punto da far correre oggi al notaio il rischio di essere percepito come un mero originatore di dati affidabili per i pubblici archivi. Invece il notaio in un mondo digitale, mediante la stipula dell'atto pubblico informatico (correttamente disegnato e gestito), è il soggetto che si può rendere garante di quella corretta percezione ed appropriazione della realtà, che l'avvento della digitalizzazione ha reso più difficile, favorendo la proliferazione dei cosiddetti "*deep fake*" e delle "*fake news*". Il notaio nel contesto digitale, ancora più che nel contesto analogico, non solo certifica l'origine delle dichiarazioni e la loro corretta riproduzione in atto, ma deve altresì garantire la corretta formazione della volontà negoziale, sin dalla fase precontrattuale e la sua trasfusione (mediante la stipula informatica) in una evidenza informatica capace di oggettivizzarsi e di divenire un oggetto sociale uguale o superiore all'atto pubblico ed alla scrittura privata cartacea».

(17) C. Attanasio, *Inadempimento dello* smart contract, *sistema rimediale e tutela effettiva,* in *Riv. dir. civ.,* 2024, 4, 719.

vengano considerati come argomenti di prova o come presunzioni semplici, proprio in virtù dei caratteri della stessa *blockchain*» (18), ha ricordato il contrario avviso espresso, ancora piuttosto recentemente, dalla giurisprudenza statunitense. In particolare, il richiamo è a *Hunichen v. Atonomi LLC* (19), che ha disconosciuto il valore probatorio della *blockchain*, peraltro osservando che «[c]*ounter-defendants fail to support the proper consideration of the blockchain evidence through judicial notice or the doctrine of incorporation-by-reference. Specifically, the court is not persuaded the blockchain evidence is necessarily complete, its contents not subject to reasonable dispute or varying interpretation, and its use not improper as a defense to otherwise cognizable*». Obiezioni che — come anticipato — non appaiono del tutto prive di fondamento: quantomeno perché, di per sé (20), «la *blockchain* consente, per ragioni di spazio, di registrare solo il codice *hash*, non il file di origine, che deve quindi essere conservato a parte, a carico e cura dell'utente» (21), sicché finisce per risultare scarsamente probante della genuinità del contenuto del documento.

2. I *deep fakes*: genesi, sviluppi e strategie (ineffettive) di contrasto.

Qualunque ne sia il contenuto, è certo che i *deep fakes* diventino ogni giorno più sofisticati e, dunque, difficili da rilevare. Mentre i primi erano fondati su una singola rete neurale[22], la maggioranza di quelli attuali si basa sulla tecnica GAN (*generative adversarial*

(18) G. Settanni, *Globalizzazione del diritto e contratti intelligenti. Interessanti spunti di approfondimento dalla giurisprudenza estera*, in *Nuova giur. civ. comm.*, 2025, 1, 237 s.

(19) No. C19-0615-RAJ-MAT, 2019 WL 7758597.

(20) Iniziano a diffondersi, tuttavia, piattaforme che integrano la tecnologia *blockchain* con lo stoccaggio in un *cloud* decentralizzato dei documenti ivi registrati, di cui — dunque — dovrebbero essere garantite anche riferibilità e autenticità originarie e immodificabilità successiva.

(21) O. Venier, Blockchain, cit.

(22) R. Pfefferkorn, *"Deepfakes" in the Courtroom*, in *B.U. Pub. Int. L.J.*, 2022, 249.

networks) (23), presentata alla comunità scientifica nel 2014 (24), e fondata sull'interazione di due sistemi: un generatore, che ha la funzione di creare nuovi contenuti (immagini, video o audio), partendo da una banca dati contenente dati autentici e tentando di produrre un contenuto che imiti strettamente gli esempi del set di addestramento; un discriminatore, cui viene sottoposto l'*output* del generatore, onde valutare la probabilità che esso sia reale o artefatto. Finché il discriminatore è in grado di identificare le immagini artefatte, il risultato non è considerato soddisfacente, e il generatore riceve un *feedback* negativo, sulla base del quale elaborare un nuovo contenuto, destinato ad essere sottoposto ancora una volta al discriminatore: l'interazione tra i due sistemi prosegue finché il discriminatore non è più in grado di stabilire se l'*output* sia reale o sintetico.

Le minime notazioni tecniche appena riportate appaiono già sufficienti alla comprensione di un dato: i due modelli "imparano" l'uno dall'altro, progressivamente perfezionandosi; il che spiega perché quella tra programmi che creano *deep fakes* e programmi atti a individuarli sia descritta in letteratura come una lotta costante, in stile gatto col topo («*any time new software is developed to detect fakes, deepfake creators can use that to their advantage in their discriminator model*») (25). Constatazione che, a propria volta, legittima i dubbi avanzati rispetto all'efficacia delle strategie preventive attualmente predisposte o predisponende, a cominciare dalla marcatura o filigranatura (c.d. *watermarking*) (26).

Invero, l'art. 50(2) e (4) *AI act* — da leggere in uno ai considerando 133 e 134 — impone ai «fornitori (27) di sistemi di IA, com-

(23) R.A. Delfino, *Deepfakes on Trial*, cit., 299.

(24) I. Goodfellow - J. Pouget-Abadie - M. Mirza - B. Xu - D. Warde-Farley -S. Ozair - A. Courville - Y. Bengio, *Generative adversarial nets*, in *Advances in Neural Information Processing Systems,* 2014, 2672 ss.

(25) D.G. Capra, *Deepfakes Reach the Advisory Committee on Evidence Rules*, in *Fordham L.R.,* 2024, 2494.

(26) Per una esaustiva rassegna di rischi e strategie di contrasto, v. C. Bird - E.L. Ungless - A. Kasirzadeh, *Typology of Risks of Generative Text-to-Image Models*, in *AIES '23: Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society,* 2023, 396 ss.

(27) Secondo la definizione dell'art. 3(3) *AI Act* «fornitore» è «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema

presi i sistemi di IA per finalità generali, che generano contenuti audio, immagine, video o testuali sintetici» di «garanti[re] che gli *output* del sistema di IA siano marcati in un formato leggibile meccanicamente e rilevabili come generati o manipolati artificialmente», e ai «*deployer* (28) di un sistema di IA che genera o manipola immagini o contenuti audio o video che costituiscono un "*deep fake*"» anche di «rend[ere] noto che il contenuto è stato generato o manipolato artificialmente»; l'art. 3 *Measures for Labeling of AI-Generated Synthetic Content* richiede che ciascun *AI-generated synthetic content* sia contrassegnato da "*Explicit labels*" (29) e "*Implicit Labels*" (30), rispettivamete dettagliati negli artt. 4 e 5. Meno ampio — ma sostanzialmente convergente nelle intenzioni — l'ambito applicativo della *Proposition de loi visant à identifier les images générées par intelligence artificielle publiées sur les réseaux sociaux,* n° 675, attualmente in discussione in Francia (31), e mirante ad imporre agli utenti dei *social networks* di indicare l'origine "artificiale" dei contenuti pubblicati e alle piattaforme di predisporre strumenti tecnici atti a consentire il rilevamento di tali contenuti e verificare la conformità del *labelling* (32). Ma, com'è stato rilevato, «*these methods are far from foolproof and there is*

di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito».

(28) Ovvero, in base all'art. 3(4) *AI Act* «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale».

(29) Ovvero «*labels added to generated synthetic content or interactive scenario interfaces, which appear in forms such as text, sound, or images, and can be clearly perceived by users*».

(30) Cioè «*labels added to generated synthetic content file data by employing technical measures, which are not easily perceived or known of by users*».

(31) Ove il termine *deep fake* è tradotto con *hypertrucage*.

(32) Si noti peraltro che, già attualmente, l'art. 5 *loi* n° 2023-451 *du* 9 *juin* 2023 *visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux*, prevede che i c.d. *influencers* debbano indicare in maniera chiara e leggibile la menzione «*images retouchées*» o «*images virtuelles*» sulle foto e i video contenenti — rispettivamente — immagini reali, nelle quali siano stati modificati la *silhouette* e/o il viso dei soggetti rappresentati, o interamente generate dall'IA.

evidence that such watermarks can be removed, at least in some cases, without much difficulty. Even if all online services could prevent malicious uses and added watermarks to outputs, people with moderate technical skills can access software that would allow them to create deepfakes without watermarks. Today, publicly accessible code-repositories such as GitHub include large amounts of software source code that can be used to create fake audio clips, images, and videos. Such code repositories rarely embed watermarks. Even in the rare cases when they do, the watermarks can be easily removed by programmers» (33).

La discutibile efficacia delle misure preventive sposta evidentemente il problema sull'*assessment* successivo; il quale, tuttavia, non sembra potersi affidare al giudizio umano (e, per quanto qui rileva, ove il contenuto sia versato quale prova in giudizio, al prudente apprezzamento del giudice). Come rileva una recente analisi sintetica dei risultati di 56 studi editi, infatti, la capacità umana di rilevare *deepfakes* è sostanzialmente assimilabile al caso: nell'85% delle ricerche esaminate, invero, la percentuale di rilevazione dei falsi si è attestata, in media, intorno al 50%; e ciò, indipendentemente dalla circostanza che si trattasse di audio, immagini o testo, ove singolarmente sottoposti a valutazione (34). Certo, si dà qualche eccezione, tuttavia

(33) A. Dalal - C. Gao - P.W. Grimm - M.R. Grossman - D.W. Linna Jr. - C. Pulice - V.S. Subrahmanian - J. Tunheim, *Deepfakes in Court: How Judges Can Proactively Manage Alleged AI-Generated Material in National Security Cases*, in *The University Of Chicago Legal Forum,* 2024, 80 s. L'opinione è condivisa — v., tra gli altri, anche M. Fabbri, Sub *art. 50*, in A. Mantelero - G. Resta - G. Ricico (a cura di), *Intelligenza artificiale. Commentario*, Milano, 2025, 468 ss.; F. Romero-Moreno, *Deepfake detection in generative AI: A legal framework proposal to protect human rights,* in *Computer L. & Security R.*, 2025, n. 106162, 14 s. — e, allo stato, si direbbe anche supportata da evidenze empiriche: un recente studio, condotto esaminando i 50 principali *AI tools* che consentono di creare contenuti artificiali, mostra come solo una minima parte di essi utilizzi già la tecnica della filigranatura, e come la stessa sia nella maggioranza dei casi facilmente rimovibile (B. Rijsbosch - G. van Dijck - K. Kollnig, *Missing the Mark: Adoption of Watermarking for Generative AI Systems in Practice and Implications under the new EU AI Act*, arXiv:2503.18156).

(34) A. Diel - T. Lalgi - I.C. Schröter - K.F. MacDorman - M. Teufel - A. Bäuerle, *Human performance in detecting deepfakes: A systematic review and meta-analysis of 56 papers,* in *Computers in Human Behavior Reports,* 2024, n. 100538.

spiegabile per ragioni diverse dalla particolare abilità cognitiva umana: così, in particolare, i risultati di maggior accuratezza ricavati dagli studi di Groh et al. nel 2022 e nel 2024 sembrano potersi spiegare — il primo (35) — per l'oggetto (*video deepfake*, che, essendo multimodali, in quanto incorporano immagini, movimenti e voce, aumentano le *chance* di individuazione degli errori, poiché essi possono affettare ciascuna di tali dimensioni); il secondo (36) poiché i video esaminanti riguardavano Donald Trump e Joseph Biden, sicché la maggiore accuratezza dei risultati potrebbe ricondursi alla maggiore capacità di rilevazione delle distorsioni che si riscontra nei volti familiari rispetto a quelli che tali non sono (37).

3. Uno sguardo oltreoceano: l'obsolescenza delle *Federal Rules of Evidence*.

L'avvento dei *deep fakes* ha messo in crisi la regola cardine del giudizio di ammissibilità della prova operato dal giudice prima che la stessa potesse essere presentata alla giuria [*i.e.* la necessità che la parte che voglia valersene ne dimostri l'autenticità: *Rule* 901(a) FRE]: quest'ultimo, infatti, si è per decenni fondato sulla presunta «*innate human ability to determine what is real by trusting one's senses under the theory that "seeing is believing"*», laddove i progressivi miglioramenti della tecnologia alla base dei *deep fakes* — come visto — rendono sempre più difficile… credere ai propri occhi (o alle proprie orecchie) (38). Ciò di cui la giurisprudenza comincia ad essere avvertita, pur mostrando evidenti oscillazioni e disorientamenti: così, in una recente, esemplare de-

(35) M. Groh - Z. Epstein - C. Firestone - R.W. Picard, *Deepfake detection by human crowds, machines, and machine-informed crowds*, in *Proceedings of the National Academy of Sciences,* 2022, n. e2110013119.

(36) M. Groh - A. Sankaranarayanan - N. Singh - D.Y. Kim - A. Lippman - R. Picard, *Human detection of political speech deepfakes across transcripts, audio, and video*, in *Nature Communications,* 2024, n. 7629.

(37) A. Diel - M. Lewis, *Familiarity, orientation, and realism increase face uncanniness by sensitizing to facial distortions,* in *Journal of Vision,* 2022, n. 14.

(38) R.A. Delfino, *Deepfakes on Trial*, cit., 307.

cisione, la Corte suprema della California (39) ha sanzionato nella misura più grave (con il *dismissal with prejudice*) una richiesta di *summary judgement* fondata, secondo la Corte, su prove generate con l'IA. Dopo aver evidenziato gli "errori" rivelatori di alcune delle prove prodotte, con tanto di confronti di immagini inserite nel testo della sentenza, la Corte ha concluso affermando di restare «*suspicious of the other evidentiary submissions*», ma di non disporre di «*time, funding, or technical expertise to determine the authenticity of Plaintiffs' statements or conduct a forensic analysis of the suspect evidentiary submissions*».

Non altrettanto avveduta appare, invece, la decisione resa nel caso *USA v. Khalilian*, ove la Corte ha respinto la richiesta della difesa, di escludere una registrazione vocale dell'imputato, sul presupposto che si trattasse di un falso prodotto con l'IA, ritenendo che la testimonianza di soggetti non esperti, che avrebbero — secondo l'accusa — potuto attestare che la voce apparisse quella dell'imputato, fosse «probabilmente sufficiente per ammetterla». Un approccio più cauto trapela, invece, dalla lettura di *Wisconsin v. Rittenhouse*, ove, richiesta dall'accusa l'ammissione di un video ingrandito girato con un iPad, e opposto dalla difesa il dubbio che la funzione *pinch-to-zoom* di Apple, fondata sull'IA, fosse suscettibile di manipolare il video, la Corte ha richiesto la testimonianza di un esperto sul punto.

Se già la diversità di approcci rappresentata dalle pronunce richiamate risulta di per sé preoccupante, il tema potrebbe apparire complicato — quantomeno nel panorama statunitense — dalla tradizionale ripartizione dei ruoli tra giudice e giuria (40); sicché non stupisce rinvenire, tra le molteplici proposte

(39) *Ariel and Maridol Mendones v. Cushman & Wakefield, Inc., et al*. (9 settembre 2025).

(40) Sotto tale profilo, merita richiamare *People v. Smith*, 969 N.W.2d 548, 563 (Mich. Ct. App. 2021), *appeal denied*, 962 N.W.2d 277 (Mich. 2021): censurata la sentenza di primo grado per non aver escluso che alcuni post pubblicati su Facebook potessero essere stati in qualche modo contraffatti, la Corte d'appello ha respinto l'impugnazione, non per l'infondatezza delle censure sul punto, ma in ragione dei limiti della cognizione del giudice di seconde cure, limitata alla verifica della (in)sussistenza di un abuso di di-

dottrinali presentate come suscettibili di regolare il fenomeno (spesso, ma non sempre, orientate nel senso di una revisione normativa), quella di chi ritiene che la soluzione vada ricercata nell'attribuzione espressa al giudice, piuttosto che ai *laymen* che compongono la giuria, del compito di valutare l'autenticità della prova (41) (sostanzialmente estendendo anche alla materia che occupa il ruolo di *gatekeeper* consacrato dalla giurisprudenza *Daubert* (42), e così mutuandone il presupposto, comune ma già altrove criticato come erroneo, che il primo sia dotato di capacità epistemiche superiori a quelli di un *quivis de populo*) (43).

screzionalità da parte del giudice di primo grado; verifica che, ove negativa (com'è stata nella specie, nonostante anche il giudice d'appello abbia avuto cura di sottolineare che la conclusione raggiunta «*does not discount the possibility that evidence from social media might, in fact, be inaccurate, hacked, or faked*»), lascia riemergere il potere sovrano della giuria di determinare l'affidabilità e il peso dei post pubblicati su Facebook.

(41) R. Delfino, *Deepfakes on Trial*, cit., 45.

(42) Come noto, negli USA, il giudizio di ammissibilità della prova scientifica, dal 1923 parametrato unicamente sulla *general acceptance* della stessa da parte della comunità scientifica in base al c.d. *Frye test* [*Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923)], è stato rivoluzionato dalla giurisprudenza *Daubert* [*Daubert v. Merrell Dow Pharmaceuticals, Inc.,* 509 U.S. 579 (1993), in *Foro it.,* 1994, IV, 184, con nota di G. Ponzanelli, *Scienza, verità e diritto: il caso Bendectin*. V. anche, tra gli altri, M. Taruffo, *Le prove scientifiche nella recente esperienza statunitense*, *in Riv. trim. dir. proc. civ.,* 1996, 1, 219 ss.; A. Dondi, *Problemi di utilizzazione delle "conoscenze esperte" come "expert witness testimony" nell'ordinamento statunitense*, in *Riv. trim. dir. proc. civ.,* 2001, 4, 1133 ss.; V. Pironi, *Prove scientifiche e processo civile: alcune riflessioni*, in *Giusto proc. civ.,* 2013, 4, 1257 s.] che, intervenendo nel 1993, ha non solo risposto affermativamente all'interrogativo se le *medio tempore* approvate *Federal Rules of Evidence* (FRE) e, in particolare, la *rule* 702, non avessero comportato il superamento del *Frye test*, ma anche delineato quattro parametri (non strettamente cogenti) alla luce dei quali è possibile valutare la bontà dell'*expert evidence*: la *testability*; la *peer review and publication*; l'*error rate*; la *general acceptance*. Con le successive *Joiner* e *Kumho* [*General Electric Co. v. Joiner,* 522 U.S. 136 (1997) e *Kumho Tire Co. v. Carmichael*, 526 U.S. 137 (1999)], poi, la Corte ha precisato la propria giurisprudenza, con il risultato finale di estendere il ruolo di *gatekeeper* a tutte le discipline tecniche — anche non scientifiche — e non solo alla verifica del metodo, ma anche delle conclusioni dell'esperto.

(43) V., *si vis,* V. Capasso, Tractent fabrilia fabri. *Contributo all'affermazione del «diritto al consulente tecnico» nel processo civile*, Torino, 2025, sia quanto ai limiti cognitivi che il giudice incontra nella comprensione e valutazione dei fatti in quanto uomo (*ibid*., 215 ss.), sia, più specificamente quanto all'incapacità dei *lawyer-judges* di comprendere appieno il significato dei criteri del *Daubert test* (*ibid*., 228 ss.).

Anche in ragione del dibattito dottrinale, l'*Advisory Committee On Evidence Rules* si è infine fatto carico del problema, inizialmente ipotizzando di modificare la *Rule* 901 FRE (44); in particolare, l'idea originariammente coltivata era quella di prevedere, alla lett. b), che, ai fini dell'ammissibilità della prova dichiaratamente generata dall'IA, fosse necessario fornire «*additional evidence that* […] *describes the training data and software or program that was used; and* […] *shows that they produced reliable results in this instance*»; e, alla lett. c), che, «[i]*f a party challenging the authenticity of computer-generated or other electronic evidence demonstrates to the court that a jury reasonably could find that the evidence has been altered or fabricated, in whole or in part, by artificial intelligence [by an automated system], the evidence is admissible only if the proponent demonstrates to the court that it is more likely than not authentic*» (45). L'ipotesi è stata però scartata dal *Judicial Conference Committee on Rules of Practice and Procedure* (*Standing Committee*), che, il 10 giugno 2025, ha approvato — invece — l'introduzione di una nuova *Rule* 707, dedicata alla «*Machine-Generated Evidence*», e in base alla quale «[w]*hen machine-generated evidence is offered without an expert witness and would be subject to Rule 702 if testified to by a witness, the court may admit the evidence only if it satisfies the requirements of Rule 702(a)-(d). This rule does not apply to the output of simple scientific instruments*» (46).

(44) V. il Rapporto dell'8 novembre 2024, in *https://www.uscourts.gov*. Sui lavori dell'*Advisory Committe,* v. D.G. Capra, *Deepfakes Reach the Advisory Committee*, cit., 2491 ss.; sul tema v. anche S. Quattrocolo, *op. cit.*, 24 ss.

(45) Per F. Demartis, *I sistemi automatici di riconoscimento facciale nel procedimento penale. Tra possibilità di impiego e limiti ordinamentali*, Milano, 2025, 239, «[p]ur essendo apprezzabile l'intento dei compilatori, […] la proposta di emendamento [avrebbe dovuto] essere in parte ripensata, dato che il procedimento descritto, eccessivamente farraginoso, potrebbe rivelarsi scarsamente efficace al fine di rilevare le pratiche di deepfake più sofisticate. Ed infatti, la parte che intende contestare l'autenticità di una prova potrebbe incontrare notevoli difficoltà nel riuscire a dimostrare che la stessa prova, in base all'apprezzamento della giuria (organo non tecnico), sia stato oggetto di manipolazioni. I giurati, infatti — dai quali è legittimo non attendersi conoscenze approfondite in ambito informatico — potrebbero percepire come frutto di un deepfake solo i cosiddetti "falsi grossolani" e non, invece, le manipolazioni operate con tecniche più subdole».

(46) Un riepilogo dell'*iter* seguito dalla Commissione, in uno al testo della dispo-

La previsione — che non è peraltro da ritenersi ancora approvata in via definitiva, avendo la Commissione stabilito a larga maggioranza (8 a 1) di sottoporne il testo a pubblica consultazione, nel periodo tra il 15 agosto 2025 al 16 febbraio 2026 — pur astrattamente costituendo un primo passo per la regolamentazione processuale della prova *AI-generated*, ha evidentemente un ambito applicativo più ridotto rispetto alla proposta iniziale: essa, infatti, risulta applicabile nei soli casi in cui l'origine "artificiale" della prova sia riconosciuta dalla stessa parte che ne chiede l'ammissione, mentre lascia del tutto irrisolto sia il problema della disciplina applicabile ai casi di contestazione della prova asseritamente genuina, sia — per quanto qui maggiormente rileva — quello delle modalità di accertamento della stessa (non) genuinità.

4. Ritorno al panorama domestico: *deep fakes,* riproduzioni meccaniche, copie e il problema dell'*assessment*.

Né tali questioni sembrano potersi risolvere, nel contesto del processo civile domestico, facendo ricorso *sic et simpliciter* alla disciplina delle riproduzioni meccaniche — come pure si potrebbe essere indotti a fare, ulteriormente estendendo l'ambito di applicazione del noto indirizzo giurisprudenziale che vi riconduce anche documenti (quali, come ricordato sopra, i messaggi e gli *screens* Whatsapp) privi di firma (47), ovvero per i quali «non si pone tanto un problema di imputabilità [....], quanto di attendibilità della riproduzione» (48) —, e così affidando il destino (del valore) della prova al meccanismo della (non) contestazione (49).

sizione e al relativo comento, può leggersi in Committee on Rules of Practice and Procedure Judicial Conference of the United States, *Preliminary Draft. Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure, and the Federal Rules of Evidence,* agosto 2025, in *www.uscourts.gov*, 102 ss.

(47) Indirizzo comunque non incontroverso: v., sia pur sul tema più specifico dell'e-mail, F. Ricci, *L'efficacia probatoria dell'e-mail non sottoscritta*, in *Riv. trim. dir. proc. civ.,* 2021, 2, 630 s.

(48) A. Bonafine, *L'atto*, cit., 99.

(49) Sul tema v. A. Bonafine, *L'atto*, cit., 99 ss.; M. Gradi, *Le prove*, in G. Ruffini (a cura di), *Il processo telematico nel sistema del diritto processuale civile*, Milano, 2019, 534 ss.

Da un lato, infatti, lo stesso non appare indiscriminatamente applicabile a tutte le possibili ipotesi di (millantato o sospetto) *deep fake*, e, in particolare, non a quelle in cui il documento possa ricondursi al novero di quelli dichiarativi non sottoscritti (50), già in dottrina ritenuti «ontologicamente e strutturalmente differenti» dalle riproduzioni informatiche (51), e di conseguenza assoggettati alla disciplina di cui all'art. 20, comma 1-*bis*, CAD (52), che li rende sempre liberamente valutabili dal giudice (53).

(50) Come noto, documenti dichiarativi sono quelli che «costituiscono il mezzo per manifestare lo stato interno di volontà o di scienza del loro autore»; mentre non dichiarativi sono i documenti che «rappresenta[no] un fatto che non concorr[ono] a realizzare, e quindi possibilmente anche una dichiarazione, della quale tuttavia non costituisc[ono] lo strumento di realizzazione»: così F. Ricci, *op. cit.*, 633. In particolare, come sintetizza l'a. (*ibid.*, 632 s.), i documenti dichiarativi costituiscono «il risultato materiale di particolari atti di linguaggio, cioè di comportamenti simbolici consistenti nella composizione di segni evocativi impressi sul documento (tali sono le scritture), destinati ad essere completati con altri comportamenti di diversa natura e ad essere interpretati alla luce di tali contegni ulteriori e delle circostanze, che concorrono ad identificare le intenzioni del loro autore», quali, ad esempio, «la consegna o la spedizione dello scritto con le quali l'autore emette la dichiarazione resa tramite il documento, quando sono fatte in circostanze tali da manifestare o implicare la paternità del documento e della dichiarazione stessa. A tali condizioni, le vicende del documento scritto incidono non solo sulla prova, ma anche sull'esistenza stessa del fatto da provare, cioè la dichiarazione che concorrono a realizzare. Così non è nel caso delle riproduzioni meccaniche, che non servono a dare forma a stati mentali altrimenti relegati nel foro interno del soggetto, quali la sussistenza di una volontà impegnativa o dello stato di conoscenza di taluni fatti. Più in generale, le vicende di questi documenti non incidono sull'esistenza dei fatti che rappresentano, che possono provare, ma non realizzare».

(51) F. Savino, *op. cit.*, 765.

(52) *Ibid.*, 767.

Più in generale, sulla disciplina del CAD, anche in prospettiva comparata, v., da ultimo, A. Graziosi, *Brevi considerazioni sull'efficacia probatoria del documento informatico in ambito europeo*, in *Dir. aff.,* 2025, 2, 150 ss.

(53) Non è possibile operare una categorizzazione *a priori,* fondata sulla natura del mezzo (scritto, foto, audio o video) prodotto, la qualificazione come documento dichiarativo o meno dipendendo dall'oggetto della prova e dalle modalità di produzione della stessa; ad orientare nelle singole ipotesi che dovessero venire in rilievo valgono, tuttavia, i criteri indicati da F. Ricci, *op. cit.,* 635: «l'elemento dirimente per comprendere se un documento elettronico che non consista in un testo è una scrittura informatica, o è solo la rappresentazione informatica di una dichiarazione orale, dipende dall'alternativa tra il caso in cui il documento sia un mezzo per comunicare quella dichiarazione (in tal caso, esso concorre a realizzarla ed è quindi un documento dichiarativo) ovvero non lo sia (e in tal caso si limita a riprodurla ed è quindi una mera rappresentazione informatica)». L'a. richiama il testo del fu art. 1.10 Princìpi Unidroit 1994, poi divenuto art. 1.11 Princìpi Unidroit 2016, secondo cui

Dall'altro, è noto che, secondo la Cassazione, «il disconoscimento della fotografia», come, in genere, di ogni altra riproduzione meccanica (cui pure sembra potersi ricondurre buona parte degli "ordinari" *deep fakes*), «non ha gli stessi effetti del disconoscimento previsto dall'art. 215 c.p.c., comma 2, in quanto mentre questo, in mancanza di richiesta di verificazione e di esito positivo di questa, preclude l'utilizzazione della scrittura, il primo non impedisce che il giudice possa accertare la conformità all'originale anche attraverso altri mezzi di prova, comprese le presunzioni» (54); sicché, anche nei casi in cui il documento sia di tipo non dichiarativo, l'applicazione della disciplina di cui all'art. 2712 c.c. consentirebbe di ritenere il problema risolto (55) solo a metà, la necessità di procedere all'accertamento della natura non *AI-generated* del documento ponendosi quantomeno nei casi di (tempestiva) (56) contestazione (57).

« "*writing" means any mode of communication that preserves a record of the infor mation contained therein and is capable of being reproduced in tangible form*», osservando come tale definizione superi «l'idea di scritto come mera rappresentazione di parole in forma visibile per arrivare ad includere nel concetto ogni *res signata* che consenta la riproduzione e la conservazione in forma documentale di qualsiasi modalità di comunicazione, cioè di comporta menti simbolici consistenti nella composizione di segni evocativi non solo scritti, ma anche orali o mimici». Ne deriva che, «[a] tali condizioni, non solo un testo, ma anche una "registrazione sonora, visiva o audiovisiva" può essere una scrittura, e in particolare lo è allorché essa sia realizzata ed utilizzata come mezzo per comunicare, cioè per dichiarare alcunché; mentre è una mera rappresentazione della dichiarazione, ma non una scrittura, quando il documento è destinato non a comunicare alcunché, ma solo a rappresentare una dichiarazione avvenuta per altre vie (ivi compresa eventualmente la mera forma orale registrata e resa riproducibile tramite il documento)».

(54) Così Cass., 29 aprile 2022, n. 13519; ma nello stesso senso v. anche Cass., 26 agosto 2020, n. 17810; Cass., 11 gennaio 2020, n. 308; Cass., 17 luglio 2019, n. 19155; Cass., 21 febbraio 2019, n. 5141; Cass., 23 maggio 2018, n. 12737; Cass., 17 febbraio 2015, n. 3122.

(55) S'intende: esclusivamente sul piano della verità formale del processo, in disparte restando ogni considerazione sulla opportunità e attualità della soluzione normativa rispetto all'obiettivo, che eventualmente si assuma, della c.d. decisione giusta.

(56) Ovvero, come precisa Cass., 24 febbraio 2023, n. 5755, avanzata nella prima istanza o difesa successiva alla produzione, «alla luce di un principio di tempestività, che trova un'espressione generale nell'art. 157, comma 2 c.p.c. […] ed una espressione specifica praticamente identica nell'art. 215, comma 2 c.p.c.».

(57) Come già più volte accennato, stante la nozione ampia di *deep fakes* qui adottata (v. *retro*, § 1), non può escludersi che quello prodotto sia il documento di un docu-

mento; sicché pare potersi dare anche l'ipotesi che a venire in rilievo sia l'art. 2719 c.c., piuttosto che l'art. 2712 c.c.

Alla prima disposizione, in particolare, pare potersi ricondurre lo *screenshot* della scrittura "tradizionale". Uno spunto in tal senso sembrerebbe offerto da A. GRAZIOSI, *Premesse ad una teoria probatoria del documento informatico*, in *Riv. trim. dir. proc. civ.* 1998, 2, 529, che, nel commentare l'art. 6, comma 3, D.P.R. 10 novembre 1997, n. 513 (Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59), oggi abrogato, in base al quale «[l]e copie su supporto informatico di documenti, formati in origine su supporto cartaceo o, comunque, non informatico, sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata con le modalità indicate dal decreto di cui al comma 1 dell'articolo 3», e rilevato come «[l]a norma, pur essenziale, lascia[sse] assolutamente impregiudicato il problema di eventuali copie digitali non autenticate, di documenti scritti "tradizionali"», riteneva che «il problema [fosse] facilmente superabile» tramite «l'estensione a questa fattispecie dell'art. 2719 c.c. », muovendo dall'indirizzo dottrinale che già riconduceva a tale disposizione anche l'efficacia del documento inviato a mezzo fax.

Peraltro, l'applicazione dell'art. 2719 c.c. in luogo dell'art. 2712 c.c. non pare spiegare conseguenze processuali di rilievo, quantomeno rispetto al profilo che interessa. Come sottolineato recentemente da Cass., 7 ottobre 2024, n. 26200, costituisce infatti «principio consolidato, in giurisprudenza, che In tema di prova documentale il disconoscimento, ai sensi dell'art. 2719 c.c., della conformità tra una scrittura privata e la copia fotostatica, prodotta in giudizio non ha gli stessi effetti di quello della scrittura privata, previsto dall'art. 215, comma 1, n. 2, c.p.c., in quanto, mentre quest'ultimo, in mancanza di verificazione, preclude l'utilizzabilità della scrittura, la contestazione di cui all'art. 2719 c.c. non impedisce al giudice di accertare la conformità della copia all'originale anche mediante altri mezzi di prova, comprese le presunzioni»; nello stesso senso, v., tra le altre, Cass., 18 gennaio 2022, n. 1324; Cass., 8 giugno 2018, n. 14950; Cass., 11 ottobre 2017, n. 23902. È evidente, allora, che il problema dell'apprezzamento giudiziale dinanzi all'accusa di non genuinità per genesi o manipolazione artificiale si pone tal quale.

Semmai, una differenza di disciplina (ma di "invenzione" squisitamente pretoria) è rinvenibile nella circostanza, già rilevata da G. DELLA PIETRA, *L'ansia di specificazione nel processo civile: tre sintomi*, in *Riv. trim. dir. proc. civ.,* 2019, 4, 1335, che «[d]a un po' di tempo la Cassazione vuole che il disconoscimento» richiesto dall'art. 2719 c.c. «sia non solo testuale, ma anche motivato. Esige, cioè, per un verso, che la parte dichiari univocamente che sta negando la conformità all'originale di un preciso documento; per l'altro, che la contestazione sia ricca dei profili per i quali si assume che la fotocopia differisca dall'originale»; onere, questo, che non solo — come giustamente sottolinea l'a. — non risulta esigibile né alla luce del tenore letterale della norma, né del pur mutato contesto normativo in cui oggi essa si inserisce, ma che appare sostanzialmente inutile, perché facilmente aggirabile: «[s]e si vuole che al disconoscimento si accompagni l'elenco delle difformità, deve riflettersi che la parte diligente potrà fornirlo sempre: sol che si avveda che la lista può anche essere inventata» (*ibid*., 1138); e l'allegazione della creazione/manipolazione artificiale del documento si presta evidentemente benissimo allo scopo (v., infatti, subito *infra*, nel testo).

Casi che, peraltro, appaiono verosimilmente destinati a moltiplicarsi: come evidenziato ampiamente nella letteratura straniera sul tema, infatti, le criticità non attengono tanto (o, comunque solo) al rischio che sia attribuito valore probatorio ad un *fake*, quanto, piuttosto, a quello inverso, ovvero che diventi sin troppo agevole, per la parte contro la quale la prova è prodotta, inficiarne la capacità asseverativa. È questo il fenomeno del c.d. *liar's dividend* (58) (e della conseguente «*deepfake defense*») (59): quasi paradossalmente, la progressiva presa di coscienza dei rischi di manipolazione dei contenuti rende sempre più facile contestare — anche pretestuosamente — la genuinità delle prove audiovisive; sicché «[l]*'asymétrie bénéficie au menteur, ainsi que le contexte de défiance, car plus nous sommes sceptiques, plus nous sommes perméables à ses allégations, considérant qu'il faut prendre le temps de les vérifier*» (60). Ma verificarle come?

5. La necessarietà del ricorso al consulente tecnico d'ufficio (una volta di più).

Indipendentemente dal sistema processuale — e così, anche negli ordinamenti che non conoscono la scissione soggettiva del giudizio di fatto e quello di diritto, entrambi essendo affidati al giudice —, il ricorso alla prova peritale è ritenuto imprescindibile (61) a tal fine; ma deve darsi atto che la notazione è di norma

(58) L'espressione, ormai nota alla letteratura specialistica, è di R. Chesney - D.K. Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,* in *California L.R.* 2019, 1785.

(59) R. Delfino, *The Deepfake Defense*, cit.

(60) C. Deschamps, *Les professionnels de l'intelligence économique face aux nouvelles technologies de falsification*, in *Rev. int. int. econ.,* 2023, 116, nota 37.

(61) Ad esempio, in Spagna, muovendo dall'art. 382 LEC — che, posta l'ammissibilità, quale mezzi di prova, di riproduzioni di «*palabras, imágenes y sonidos captados mediante instrumentos de filmación, grabación y otros semejantes*», ciascuna parte è facultata a produrre qualunque altro mezzo di prova, perizia compresa, onde, secondo i casi, corroborare o smentire il valore probatorio (e quindi, *in primis*, l'autenticità) della riproduzione stessa —, parte della dottrina, dinanzi alla diffusione dei *deep fakes*, è giunta a ritenere che, quantomeno per l'allegante, la facoltà si trasformi in un onere; ma, mentre a tale prospettazione si oppone il rilievo che costi e tempi di realizzazione della prova peritale stragiudi-

espressa senza interrogarsi (e quindi, *a fortiori*, prendere posizione) in ordine all'esistenza di un vero e proprio dovere del giudice di disporla — ove ciò sia in suo potere — o ammetterla (nei casi in cui la produzione della stessa resti affidata alle parti) (62). Ma, se si è già altrove tentato di dimostrare l'esistenza di un siffatto dovere con riferimento alla generalità dei casi in cui la controversia richieda l'impiego di conoscenze e/o competenze che travalicano quelle dell'uomo medio (63), e se, alla luce di quanto sin qui

ziale, ai fini dell'ammissibilità della riproduzione, rischiano di compromettere l'effettività della tutela (così R.B. Moreno, *Deepfakes en el procedimiento probatorio*, in *Revista Vasca de Derecho Procesal y Arbitraje,* 2023, 252), è evidente che l'obiezione assume meno pregnanza nella diversa prospettiva, che in questa sede si assume (v. *infra*, nel testo), del dovere del giudice di disporre una c.t.u. (che, pur potenzialmente determinando un allungamento dei tempi e un incremento dei costi, rimarrebbe solo eventuale, perché subordinata alla contestazione della parte contro la quale la riproduzione venga prodotta).

Nella dottrina francese, v. E. Daoud - I. Volson-Derabours, *La détection des preuves manipulées : la preuve pénale à l'épreuve de l'intelligence artificielle*, in *AJ pénal,* 2025, 387, che osservano che «*la multiplication des données numériques et leur traçabilité*», ha profondamente innovato la prova penale, da un lato mostrando la tendenza «à la fiabiliser, voire à l›objectiver», ma dall'altro rendendola «*dépendante d'une expertise complexe qui est susceptible de démunir les acteurs classiques de la chaîne judiciaire. La preuve numérique est avant tout technique : elle repose sur la maîtrise d'outils informatiques souvent sophistiqués. Ces preuves se présentent ainsi sous des formes extrêmement variées et exigent, la plupart du temps, des compétences spécifiques pour les comprendre, les analyser et, de fait, les critiquer*».

Anche R. Vazquez Llorente, *Deepfakes In The Dock: Preparing International Justice for Generative AI,* in *TheSciTechLawyer,* Winter 2024, 32, conclude nel senso della necessità ultima di un investimento nel capitale umano, in termini di incremento del tasso di expertise dei giudici, quanto di ricorso agli esperti.

(62) Così, ad esempio, se M.G. Losano, Scripta volant: *la volatilizzazione dei documenti nell'era digitale*, in *Dir. informaz. inf.* 2020, 1, 17, già qualche anno fa discorreva di «volatilizzazione dei documenti nell'era digitale», osservando che «la *Computer forensics* esige approfondite conoscenze tecniche in costante aggiornamento, e che quindi in questo campo lo scambio di idee tra l'informatico e il giurista è particolarmente difficile. In particolare il giurista non ha le conoscenze di base per affrontare questo confronto, e deve perciò delegarlo a un perito» (*ibid*., 35), non pare che il «deve» esprima una presa di posizione dell'a. circa la specifica posizione soggettiva del giudice.

Il problema è invece prospettato, ma risolto tendenzialmente per la negativa, da S. Quattrocolo, *op. cit.,* 17, per la quale sarebbe «[d]ifficile immaginare un vero e proprio obbligo per il giudice di disporre perizia» (ma la stessa a. dà conto delle opinioni dissonanti in dottrina, già alla stregua del dato normativo attuale, anche *per differentiam* rispetto a quello del Codice del 1930: v. anche *infra*, nota 65).

(63) V. Capasso, Tractent, cit., 292 ss.

osservato, tale condizione appare certamente ricorrere nella materia *de qua*, a conclusioni analoghe è giunto chi, avendo riguardo al processo penale italiano e discorrendo dei risultati generati dai sistemi automatici di riconoscimento facciale — ritenuti non autosufficienti, «vuoi perché all'operatore viene mostrato un elenco di possibili corrispondenze, tra le quali […] è possibile che vi sia il soggetto corrispondente a quello la cui immagine è stata sottoposta a raffronto, vuoi perché i sistemi *de quibus*, molto spesso, incorrono in errore e allora è indispensabile una verifica operata da un soggetto qualificato e tali caratteristiche possono attribuirsi soltanto al perito, il quale è altresì chiamato a verificare che non siano intervenute interruzioni della catena di custodia o», per quanto maggiormente interessa in questa sede rilevare, «altre forme di "adulterazione" del dato» (64) —, ha concluso (65) nel senso della «obbligatorietà della perizia» (66), individuando l'oggetto del necessario «controllo "tecnico"», anzitutto, nell'accertamento di eventuali «interruzioni della catena di custodia o altre forme di manipolazione, quali potrebbero essere, ad esempio, l'aggiunta o la sostituzione delle immagini facciali ritratte con quelle di altri soggetti per il tramite di programmi di video editing o di foto-ritocco».

E nello stesso senso sembra muoversi — seppur, ancora una volta, considerando il problema esclusivamente dal punto di vista del processo penale — la *ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility*

(64) F. Demartis, *I sistemi*, cit., 231 s.

(65) Anche traendo dalle discussioni generali maturate intorno all'evoluzione dell'art. 220 c.p.p., con conclusioni sostanzialmente convergenti con quelle che si è già avuto modo di sostenere altrove: V. Capasso, Tractent, cit., 275 ss., testo e nota 291.

(66) F. Demartis, *I sistemi*, cit., 236; v. anche *ibid*., 279 ss., ove l'a. ribadisce e precisa il pensiero, in ultimo sottolineando che, «data la complessità degli accertamenti richiesti, le cui competenze travalicano l'ambito del sapere tipicamente giuridico e sconfinano nella sfera della "scienza" e della tecnica, va da sé che l'interprete non potrà essere il giudice, che — pur definito da un noto brocardo latino come *peritus peritorum* — non possiede certamente le competenze necessarie per poter comprendere il funzionamento dei sistemi automatici di riconoscimento facciale. E, proprio per tale ragione, riteniamo imprescindibile l'accertamento da parte di un perito».

of Evidence and Electronic Evidence in Criminal Proceedings (67). L'art. 7 della Proposta, rubricato «*Admissibility of electronic evidence*», prevede, al comma 3, il dovere degli Stati membri di garantire, attraverso norme nazionali, che l'utilizzabilità di prove elettroniche nel processo penale sia subordinata alla previa dimostrazione della loro genuinità. Dimostrazione che si presume richiedere competenze esperte: sicché il comma 4 impone agli Stati membri di consentire il coinvolgimento di esperti informatici su richiesta dell'indagato o dell'imputato (68).

Certo, possono prevedersi le obiezioni: ed anzi, a quelle, classiche, che derivano dalla ritrosia del giurista innanzi alla sostanziale (seppur non formale) delega della funzione decisoria al c.t.u., sembrerebbe facile aggiungerne, in questo caso, una ulteriore. Stante la già ricordata incapacità umana di riconoscere un *deep fake*, è, infatti, evidente che lo stesso consulente finirebbe inevitabilmente per doversi avvalere di strumenti di IA nello

(67) Approvata dall'*ELI Council* il 23 febbraio 2023 e dall'*ELI Membership* il 4 maggio dello stesso anno.

(68) Questo il testo originale: «*(1) Member States shall provide that electronic evidence is used in criminal proceedings only if it is ensured that:*

(a) the evidence at the time of its use corresponds to the state in which it was obtained;

(b) the evidence at the time of its use corresponds to the full extent to the evidence at the time it was obtained;

(c) the evidence was sufficiently protected against falsification and manipulation in the period between its obtention and its use.

(2) Sufficient protection within the meaning of paragraph 1(c) shall in any event require that each access to the electronic evidence is adequately logged and that the storage medium is adequately protected against external interference.

(3) Member States shall ensure that electronic evidence is only used in criminal proceedings if there is sufficient evidence that it is not the result of manipulation or forgery prior to the time of production.

(4) The defendant has the right to access the full extent of the evidence, and to the report prepared by qualified IT experts, to challenge the chain of custody, the results of the analysis or its interpretation, and also to challenge the conclusions in the expert opinion. Member States shall ensure that qualified IT experts are involved, upon the request of the suspect or accused, in the assessment of the standards established in paragraphs 1 to 3.

(5) Member States shall consider granting the defendant the right to request the use of machine-learning technology or predictive coding when the full review or the keyword search of documents is not appropriate for an accurate assessment of the evidence».

svolgimento dell'incarico; ciò che riproporrebbe il noto problema della c.d. *black box* (69). Il giudice si troverebbe così espropriato del giudizio di genuinità della prova, in ultimo affidato (nemmeno al suo ausiliario, ma) alla macchina.

6. Verso una riserva di scienza… o forse di IA?

Il rischio effettivamente esiste, ma pare doversi ridimensionare.

Per farlo, occorre muovere dal rilievo — comune a buona parte degli studiosi, di qualunque nazionalità (70) — che quello posto dai *deep fakes* non costituisce un problema del tutto nuovo: non solo perché la contraffazione, ad esempio, di immagini risale a ben prima dell'avvento dell'IA (71), ma anche, e prima ancora, perché, se è vero che i *deep fakes* determinano astrattamente due ordini di rischi — uno «neutro», relativo al possibile «ingresso accidentale, e non proditorio, nel processo, di elementi informativi che non rappresentano fatti veritieri», e uno «estremo, ovvero l'eventualità che elementi informativi digitali siano appositamente generati […] per dimostrare nel processo fatti non accaduti o non veritieri» —, è già stato osservato che il primo si pone pure (pare il caso di aggiungere: da sempre) innanzi al «teste inatten-

(69) Così, anche F. Demartis, *op. loc. ult. cit.*, che pure sostiene la necessarietà della perizia, sottolinea che «[i]l problema […] è che neppure il perito, allo stato, sarà in grado di comprenderne l'effettivo funzionamento, posto che i software di riconoscimento facciale sono equiparabili ad una sorta di *black box* inespugnabile, di cui restano ignote sia le variabili prese in considerazione in fase di programmazione dell'algoritmo sia le forme di "ragionamento" da questo seguito per esprimere il giudizio di corrispondenza oppure di non corrispondenza tra i volti. | Se, infatti, il perito è chiamato a verificare la validità di una teoria scientifica, nell'attuale scenario ciò non risulta possibile dato che i sistemi automatici di riconoscimento facciale — non superando il noto *Daubert test* — non possono essere equiparati ad una prova scientifica».

(70) Oltre ai riferimenti riportati nelle note successive, v. R.B. Moreno, *Deepfakes*, cit., 251.

(71) T. Mhyand, *Once the jury sees it, the jury can't unsee it: the challenge trial judges face when authenticating video evidence in the age of deepfakes*, in *Wiedener L.R.*, 2023, 186 ss., che ricorda come il fenomeno delle immagini ritoccate risalga a ben prima dell'avvento dell'IA (v., infatti, già G.L. Paul, *The "Authenticity Crisis" in Real Evidence,* in *Prac. Litig.*, Nov. 2004, 45 ss.).

dibile», che, «convint[o] dell'infallibilità dei propri ricordi, […] riport[a] fatti o circostanze non vere»; mentre il secondo non si distingue, in principio, da quello derivante dalla «dichiarazione menzognera del teste falso, che proditoriamente dichiara di aver visto l'imputato nel luogo in cui è avvenuto il fatto, ben sapendolo da tutt'altra parte» (72). Né l'*assessment* dell'attendibilità delle dichiarazioni del teste risulta operazione agevole.

(72) S. QUATTROCOLO, *op. cit.*, 8 s.

Non nuovo risulta pure il diverso, ma ancillare, problema segnalato dall'a. (*ibid.*, 9, testo e nota 26), che sottolinea che «nessuno strumento offerto soltanto dai sensi o dall'esperienza umana è in grado di individuar[e i *deep fakes*] e isolarli, neutralizzandone, soprattutto quando si tratti di elementi audio-video, l'estremo impatto evocativo che, nonostante l'eventuale inutilizzabilità, a seguito di verifica di artificiosità, potrebbe comunque influenzare inconsciamente il processo decisionale del giudice»; né risulta all'uopo sufficiente la disciplina dell'inutilizzabilità, poiché mentre «la specifica natura di questa invalidità […] impedisce al giudice di fare riferimento in motivazione alla prova inutilizzabile», risulta impossibile «escludere che questa abbia inconsciamente influenzato il processo decisionale dell'autorità giurisdizionale», stante «il forte impatto che può essere esercitato sull'inconscio umano da un'immagine che non si ha alcun motivo di sospettare di non genuinità».

Come si è altrove sottolineato — richiamando gli studi empirici di S.J.D. LANDSMAN - R.F. RAKOS, *A Preliminary Inquiry into the Effect of Potentially Biasing Information on Judges and Jurors in Civil Litigation*, in *Behavioral Sciences and the Law,* 1994, 113 ss., e A.J. WISTRICH - C. GUTHRIE - J.J. RACHLINSKI, *Can Judges Ignore Inadmissible Information. The Difficulty of Deliberately Disregarding*, in *Un. Penn. L.R.,* 2005, 1251 ss. — è pressoché impossibile (tanto per l'uomo comune, come rappresentato dal giurato medio, tanto per il giudice giurista) ignorare un'informazione ricevuta, anche se poi affermata inammissibile: V. CAPASSO, Tractent, cit., 224 s. E ciò vale, evidentemente da sempre, per tutti i documenti, che, come noto, nel processo civile domestico sono soggetti ad un vaglio di ammissibilità solo successivo (G. TARZIA, *Problemi del contraddittorio nell'istruzione probatoria civile*, in *Riv. dir. proc.,* 1982, II, 638; G.F. RICCI, *Le prove atipiche*, Milano, 1999, 150; T.M. PEZZANI, *Il regime convenzionale delle prove*, Milano, 2009, 267), e dunque sono una volta che il giudice sia già stato esposto alla conoscenza del loro contenuto.

Deve, tuttavia, riconoscersi — ferma restando la nozione ampia di *deep fakes* qui ritenuta, come comprensiva di contenuti anche testuali — che la forza evocativa di foto, audio e video risulta particolarmente impattante: studi psicologici dimostrano come la produzione di una prova *AI generated/manipulated* sia suscettibile di influenzare altri aspetti del procedimento, finanche incidendo sul contenuto delle dichiarazioni dei testimoni (che potrebbero essere indotti a "far proprie" esperienze in realtà mai vissute: B. GRATHWOHL, *Preserving Truth on the Prairie: Navigating Deepfake Challenges to Self-Authenticating Evidence in North Dakota Courts,* in *North Dakota L.R.,* 2024, 663; K.A. WADE - S.L. GREEN - R.A. NASH, *Can Fabricated Evidence Induce False Eyewitness Testimony?,* in *Applied Cognitive Psych.*, 2010, 899 s.; D.B. WRIGHT - E.F. LOFTUS - M. HALL, *Now You See It; No You Don't: Inhibiting Recall and Recognition of Scenes,* ivi, 2001, 471).

In quest'ottica, può comprendersi perché in dottrina, una volta preso atto della sostanziale incapacità del giudice non solo di avvedersi della natura *AI generated* di un documento, ma anche — e prima — di accertare la veridicità o meno delle affermazioni di un testimone e di comprendere realmente i contenuti degli elaborati peritali ("classici") eventualmente commissionati, si sia recentemente giunti alla cupa conclusione che, in generale, la verifica dell'attendibilità (*lato sensu*) della prova sfugga *in toto* alle capacità di apprezzamento del giudice (73); per poi derivarne, con particolare riferimento al tema dei *deep fakes*, che, riducendosi in ultimo ogni verifica — anche quando affidata all'esperto — in un giudizio dell'IA sull'IA (lo stesso perito dovendosi — come detto — necessariamente avvalere di *tools* per analizzare i contenuti di genesi asseritamente artificiale), la necessità di abbandonare ogni pretesa di soluzione giudiziale, e "rifugiarsi" nella giustizia consensuale (74).

Ma se, come detto, la considerazione globale del tema della valutazione della veridicità prova si comprende, e se della tesi appena riportata si condividono senz'altro le premesse, la conclusione non solo non convince — nella misura in cui sembra doversi ritenere che quella per la giustizia consensuale debba costituire una scelta (anche incentivata, ma comunque) delle parti, e non la conseguenza del "fallimento" della giustizia statale e/o dell'elaborazione teorica —, ma neppure appare necessitata, esistendo quantomeno un'alternativa che, pur verosimilmente poco attraente dall'angolo visuale del giurista, sembra poter rinvenire, quantomeno nel nostro ordinamento, un addentellato finanche co-

(73) Per J. Nieva-Fenoll, *Il disorientamento come regola di riforma del processo civile*, in *Riv. trim. dir. proc. civ.*, 2025, 1, 90 s., «[l]e prove non possono essere valutate dal giudice. Nessun giudice può scoprire le bugie attraverso i gesti, inoltre sia le parti che i testimoni sono molto spesso preparati dagli avvocati prima di essere interrogati. Ciò esclude che il controinterrogatorio contribuisca a un corretto accertamento della verità. Le prove peritali non possono essere realmente comprese e valutate dai giudici, in quanto non sono esperti. Infine, le prove documentali possono attualmente essere vittime di *deepfakes* non rilevabili. | In queste condizioni, ogni attività probatoria può essere inutile. Forse lo è sempre stata, in qualche misura».

(74) J. Nieva-Fenoll, *La prueba de los deepfakes pornográficos: I.A. sobre I.A.*, in *Diario La Ley*, 30 maggio 2024, n. 10516.

stituzionale: si allude alla c.d. «riserva di scienza», forse in questo settore da declinarsi come «riserva di IA».

Nella sua versione originale, l'espressione è stata elaborata con riferimento precipuo alla materia medico-sanitaria, onde sintetizzare il principio secondo cui, ove sorga la necessità di operare valutazioni tecnico-scientifiche, «il legislatore, l'amministrazione o il giudice s[arebbero] tenuti ad attingerle presso fonti qualificate (o rinviarle *tout court* a soggetti qualificati)», non potendo, invece, «contare meramente sull'esercizio delle rispettive forme di discrezionalità» (75). Principio ricavato dall'osservazione della giurisprudenza costituzionale, che pur non ha sempre militato in questo senso.

Così, se Corte cost., 17 novembre 1982, n. 188 — richiesta da ben 35 ordinanze di rimessione di verificare la legittimità costituzionale dell'art. 76 del d.P.R. 12 febbraio 1965, n. 162, tra l'altro, in relazione all'art. 3 Cost., nella misura in cui assoggettava ad identica sanzione due fattispecie di adulterazione del vino (dai rimettenti ritenute) di ben diversa gravità — ha degradato tale ultimo rilievo ad opinione meramente soggettiva, non provata né adeguatamente motivata, giungendo quindi ad escludere «che il legislatore delegato, il quale dispone di organi tecnici altamente qualificati e con il compito istituzionale della raccolta ed elaborazione di tutti gli elementi utili, abbia optato per l'equivalenza sul piano penale dei due fatti, senza la previa ponderazione dei disparati profili che interessano la materia, quali quello industriale, merceologico, tecnico, sanitario, tributario, etc.», con quella che è parsa «[u]na sorta di professione di fede — e di chiusura del discorso — senza il beneficio della prova contraria» (76), ben diverso è il corso della giurisprudenza costituzionale inauguratosi dai primi anni 2000.

(75) D. Servetti, *Riserva di scienza e tutela della salute. L'incidenza delle valutazioni tecnico-scienti-fiche di ambito sanitario sulle attività legislativa e giurisdizionale*, Pisa, 2019, 2.

(76) P. Veronesi, *La Corte costituzionale e la scienza: alcune tendenze e punti fermi*, in *BioLaw Journal,* 2024, 2, 130.

Anzitutto, Corte cost., 26 giugno 2002, n. 282, nell'accogliere la questione di legittimità costituzionale sollevata *ex* art. 32 Cost. avverso una legge regionale che aveva sospeso alcune terapie senza fondare su alcun previo «autonomo accertamento […] circa gli effetti delle pratiche terapeutiche considerate», ha affermato che «[s]alvo che entrino in gioco altri diritti o doveri costituzionali, non è, di norma, il legislatore a poter stabilire direttamente e specificamente quali siano le pratiche terapeutiche ammesse, con quali limiti e a quali condizioni. Poiché la pratica dell'arte medica si fonda sulle acquisizioni scientifiche e sperimentali, che sono in continua evoluzione, la regola di fondo in questa materia è costituita dalla autonomia e dalla responsabilità del medico che, sempre con il consenso del paziente, opera le scelte professionali basandosi sullo stato delle conoscenze a disposizione». In linea generale, infatti, «un intervento sul merito delle scelte terapeutiche in relazione alla loro appropriatezza non potrebbe nascere da valutazioni di pura discrezionalità politica dello stesso legislatore, bensì dovrebbe prevedere l'elaborazione di indirizzi fondati sulla verifica dello stato delle conoscenze scientifiche e delle evidenze sperimentali acquisite, tramite istituzioni e organismi — di norma nazionali o sovranazionali — a ciò deputati, dato l'"essenziale rilievo" che, a questi fini, rivestono "gli organi tecnico-scientifici"».

Ancor più significativi gli interventi costituzionali sulla legge 19 febbraio 2004, n. 40, in materia di fecondazione assistita. In particolare, Corte cost., 8 maggio 2009, n. 151 ha censurato il divieto di creare un numero di embrioni superiore a quello strettamente necessario «ad un unico e contemporaneo impianto, comunque non superiore a tre», sul rilievo che tale previsione, combinata con quella prevedente l'obbligo di impiantare contestualmente tutti gli embrioni prodotti, avrebbe obbligato il medico ad effettuare interventi ritenuti potenzialmente dannosi per la donna e per il feto dalla letteratura medica; e, nel dichiarare la previsione incostituzionale, ha richiamato i «limiti che alla discrezionalità legislativa pongono le acquisizioni scientifiche e sperimentali, che sono in continua evoluzione e sulle quali si fon-

da l'arte medica». Ancora, Corte cost., 10 giugno 2014, n. 162, nel dichiarare incostituzionale il divieto assoluto di fecondazione eterologa originariamente previsto dalla medesima legge, ha osservato che «la nozione di patologia, anche psichica, la sua incidenza sul diritto alla salute e l'esistenza di pratiche terapeutiche idonee a tutelarlo vanno accertate alla luce delle valutazioni riservate alla scienza medica, ferma la necessità di verificare che la relativa scelta non si ponga in contrasto con interessi di pari rango».

Ovviamente, visto l'oggetto del giudizio di legittimità costituzionale, la riserva di scienza costituisce un limite anzitutto per il legislatore, la cui discrezionalità deve allora — a date condizioni — «arrestarsi» (77); ma, posto che, come si evince dalla stessa definizione di riserva di scienza su riportata, chi si è dedicato *ex professo* al tema ne ha già tratto conseguenze analoghe anche per l'amministrazione e la giurisdizione, vi è un argomento ulteriore, e maggiormente familiare alla dottrina processualcivilistica, che conferma la bontà dell'estensione: è noto, infatti, che la stessa Corte costituzionale abbia già affermato, in almeno un'occasione, che il giudice, quand'anche svincolato dalla legge su autorizzazione della legge stessa (com'era il caso per il giudice di pace chiamato a pronunciarsi secondo equità necessaria), soffre comunque degli stessi limiti che si impongono al legislatore (78). E allora, se finanche la discrezionalità legislativa deve assoggettarsi ad un test di «ragionevolezza scientifica» (79), lo stesso non può non valere per il giudice.

(77) C. Casonato, *La scienza come parametro interposto di costituzionalità*, in *Rivista AIC*, 2016, 2, 6 ss.

(78) Corte cost. 6 luglio 2004, n. 206, in *Foro it*., 2007, 5, I, 1365, con nota di P.C. Ruggieri, *Il giudizio di equità necessario, i principî informatori della materia e l'appello avverso le sentenze pronunciate dal giudice di pace a norma dell'art. 113, 2° comma, c.p.c.*; in *Giust. civ.,* 2004, 11, I, 2537 ss., con nota di R. Giordano, *Giudice di pace e giudizio di equità necessario: un effettivo ritorno al passato?*; in *Corr. giur.,* 2005, 4, 497 ss., con nota di L. Zanuttigh, *Lo scandalo dell'equità «a canone inverso»*.

(79) Sull'evoluzione del concetto e il significato dell'espressione, S. Penasa, *La legge della scienza: nuovi paradigmi di disciplina dell'attività medico-scientifica. Uno studio comparato in materia di procreazione medicalmente assistita*, Napoli, 2015, *passim*; più di recente, tra gli altri, D. Zanoni, *Razionalità scientifica e ragionevolezza giuridica a confronto in materia di trattamenti sanitari obbligatori*, in *Costituzionalismo.it,* 2020, 1, 140 ss.

Ciò posto, va pure osservato che la nozione ha già mostrato una vocazione espansiva, venendo ormai frequentemente richiamata (dalla dottrina italiana, per evidente familiarità col concetto, ma non solo) ([80]) anche in tema di *climate change*, ove pare ormai dimostrato (anche se non sempre espressamente riconosciuto) il superamento dei criteri *Daubert* (che pure erano stati evocati da chi aveva, a torto, previsto una rapida "fine" del fenomeno della contenzioso climatico ([81]), esattamente come sono oggi richiamati quali ostativi all'utilizzo di *AI tools* volti a "smascherare" i *deep fakes*) ([82]), in favore della (sola) *general acceptance* ([83]), quale sostanzialmente "certificata" dall'IPCC (*Intergovernmental Panel on Climate Change*) ([84]).

([80]) L'espressione ha, infatti, già travalicato i confini nazionali: così, la nota decisione della Corte costituzionale tedesca nel caso *Neubauer* (*BVerfG*, 24 marzo 2021) è stata letta appunto come ispirata alla riserva di scienza: cfr. G. Palombino, *La dimensión constitucional del cambio climático en la sentencia del tribunal constitucional alemán de 24 de marzo de 2021*, in *Revista Española de Derecho Constitucional,* 2024, 347.

([81]) A. Hasani, *Forecasting the End of Climate Change Litigation: Why Expert Testimony Based on Climate Models Should Not Be Admissible*, in *Mississippi College L.R.,* 2013, 83 ss.

([82]) F. Romero-Moreno, *Deepfake detection in generative AI,* cit., 9.

([83]) Ciò che si è già altrove ritenuto essere auspicabile in generale: V. Capasso, Tractent, cit., 229 ss.

([84]) E il fenomeno, in questo caso, non è puramente domestico, i legislatori di un cospicuo numero di Stati avendo sostanzialmente operato un riconoscimento/recepimento automatico dei dati forniti dall'IPCC. Invero, se già l'art. 1 UNFCCC rinvia alla scienza e l'art. 3 pone «una causalità materiale affidata alle evidenze scientifiche e, cioè, all'identificazione da parte della scienza dei rischi di danni gravi o irreversibili che devono essere scongiurati, cui si aggiunge l'analisi del rapporto costi-benefici a livello mondiale» (M.F. Cavalcanti, *Fonti del diritto e cambiamento climatico: il ruolo dei dati tecnico-scientifici nella giustizia climatica in Europa,* in *DPCE online,* 2023, speciale n. 2, 331), l'art. 13, comma 7, dell'Accordo di Parigi del 2015, impegna gli Stati ratificanti a «forni[re] a intervalli regolari», tra l'altro, «un inventario nazionale delle emissioni antropogeniche di gas a effetto serra suddivise per fonti e delle eliminazioni suddivise per pozzi, redatto ricorrendo alle migliori metodologie riconosciute dal gruppo intergovernativo sui cambiamenti climatici e accettate dalla conferenza delle Parti che funge da riunione delle Parti del presente accordo». D'altro canto, la stessa Commissione europea, nel delineare la strategia europea volta allo sviluppo di un'economia sostenibile [cfr. Comunicazione della Commissione Europea, *Un pianeta pulito per tutti. Visione strategica europea a lungo termine per un'economia prospera, moderna, competitiva e climaticamente neutra*, Bruxelles, 28 novembre 2018, COM(2018) 773 *final*] evoca a più riprese gli studi dell'IPCC, e sottolinea di aver «nella preparazione della […] strategia unionale di riduzione

In sostanza, quindi, si danno già settori nei quali il giudice è tenuto ad affidarsi senz'altro ai risultati di una scienza che non comprende (e che neppure è capace, per sua stessa natura, di dare assicurazioni circa la propria correttezza); non sembra, allora, inverosimile ipotizzare che a tanto si giunga anche con riferimento al tema che occupa, tenuto conto — tra l'altro — del progressivo coagularsi degli sforzi degli Stati nel finanziare la ricerca sul contrasto ai *deep fakes*, al dichiarato scopo di fornire strumenti utilizzabili (anche) nell'amministrazione della giustizia ([85]). Perché se l'errore di valutazione è sempre (stato) dietro l'angolo, l'intero sistema si regge — e si è sempre retto — sulla "fede" riposta in qualcosa (legge, scienza, tecnica) o qualcuno (legislatore, giudice, consulente): ma se la Consulta stessa ha ritenuto che quella ordinariamente (quanto convenzionalmente) riposta nel legislatore receda innanzi a ciò che quest'ultimo non può comprendere, imponendogli di "affidarsi" a propria volta, non si vede ragione per non predicare altrettanto per il giudice.

a lungo termine delle emissioni di gas a effetto serra, […] tenuto conto della solida base scientifica su cui [essi] poggia[no]».

([85]) Il Dipartimento della difesa USA ha stipulato un contratto biennale con la *start-up* Hive AI, che produce modelli di rilevazione dei *deep fakes*: M. Heikkilä, *The US Department of Defense is investing in deepfake detection,* in *www.technologyreview.com*, 5 dicembre 2024; in Francia, nel 2022 è avviato, sotto l'egida dell'Agenzia nazionale per la ricerca, projet APATE (*A Prototype deepfake Assessment Toolbox for forensic Experts*), che mira a fornire una toolbox di strumenti di rilevazione dei *deepfakes*, al duplice fine di delineare indicatori oggettivi di manipolazione che consentano di verificare l'autenticità di un contenuto audiovisivo e restituire i risultati della ricerca agli operatori della giustizia in un «format compréhensible et juridiquement opposable»; il tutto, nella consapevolezza che, a fronte delle continue evoluzioni tecnologiche, si rende necessario lo sviluppo di unna vera e propria «*science de l'authentification numérique*» al servizio della giustizia (*in primis* — ma, si direbbe, non esclusivamente — penale): E. Daoud - I. Volson-Derabours, *op. cit*.

Anche a livello unionale iniziano a muoversi i primi passi nella medesima direzione: dal 2025 è attivo il progetto DETECTOR, finanziato dal programma Horizon, che vede coinvolti ricercatori in materia di IA, autorità di contrasto, scienziati forensi, studiosi di diritto e di etica, al fine di sviluppare strumenti specializzati di rilevazione delle manipolazioni dei media, creare dataset completi, approfondire la ricerca sullo scambio transfrontaliero di prove digitali e promuovere la formazione di esperti forensi nei media digitali e nell'IA (il progetto è consultabile nella piattaforma *cordis.europa.eu*).

ABSTRACT: Il contributo affronta il problema dei *deepfakes* nel processo civile, nella convinzione che il fenomeno, sebbene apparentemente non ancora postosi innanzi alle Corti domestiche, vi giungerà presto. Lo testimonia l'esperienza straniera, dalla quale appare utile e opportuno muovere, stante sia la globalità del tema, sia, e soprattutto, la tendenziale convergenza di conclusioni in punto di necessarietà dell'intermediazione di un esperto al fine di valutare la genuinità della prova. Di qui, il profilarsi di un nuovo campo applicativo della c.d. "riserva di scienza".

ABSTRACT: *The paper addresses the issue of deepfakes in civil proceedings, in the belief that, although this phenomenon has not yet come before domestic courts, it will soon do so. This is supported by foreign countries experience, which serves as a useful and appropriate starting point, given both the global nature of the issue and, above all, the general convergence of views on the need for expert intervention to assess evidence authenticity. Hence, the emergence of a new field of application of the so-called "reserve of science".*