Visicchio A, 'Il danno alla privacy dopo il ritiro della AI Liability Directive: Art. 82 GDPR, AI Act e responsabilità per danno da prodotti difettosi' (2027) 1 EJPLT.
DOI: https://doi.org/10.57230/EJPLT271AV

EJPLT
ISSN 2704-8012



Il danno alla privacy dopo il ritiro della AI Liability Directive: Art. 82 GDPR, AI Act e responsabilità per danno da prodotti difettosi

Privacy harm after the withdrawal of the AI Liability Directive: Article 82 GDPR, AI Act and liability for damage caused by defective products

ANTONIO VISICCHIO
Professore a contratto di Diritto Privato, Ph.D.
Università Mercatorum, Roma

Abstract

Il ritiro della proposta di AI Liability Directive lascia irrisolte le difficoltà probatorie nelle azioni per danni derivanti da trattamenti di dati personali mediante sistemi di IA. Il contributo esamina l'interazione tra art. 82 GDPR, AI Act e direttiva (UE) 2024/2853. La prova può circolare tra regimi diversi, mentre onere probatorio ed effetti giuridici restano disciplinati dalla normativa applicabile alla domanda: un modello qui definito «traslazione probatoria inter-regime».

The withdrawal of the proposed AI Liability Directive leaves unresolved the evidentiary difficulties of claims for harm caused by AI-based processing of personal data. This article examines the interaction between Article 82 GDPR, the AI Act and Directive (EU) 2024/2853. It argues that evidence may circulate across regulatory regimes, while the burden of proof and legal effects remain governed by the law applicable to the claim, a model defined here as "cross-regime evidentiary translation".

© The author(s) 2026, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Keywords: Intelligenza artificiale; responsabilità civile; art. 82 GDPR; onere della prova; AI Act.

Summary: 1. Il ritiro della direttiva sulla responsabilità da intelligenza artificiale e la delimitazione del problema. – 2. Disclosure e presunzioni nella proposta ritirata. – 3. Art. 82 GDPR e pregiudizio connesso all'impiego di sistemi di IA. – 4. Dalla documentazione dell'AI Act alla prova nel giudizio risarcitorio. – 5. Responsabilità per danno da prodotti difettosi: facilitazione della prova e delimitazione del danno. – 6. Tecniche di facilitazione probatoria e limiti della traslazione inter-regime. – 7. Conclusioni.

1. Il ritiro della direttiva sulla responsabilità da intelligenza artificiale e la delimitazione del problema.

Il ritiro della proposta di direttiva sulla responsabilità da intelligenza artificiale (AILD) non ha determinato un vuoto di tutela rispetto ai danni causati o mediati da sistemi di IA, poiché la risposta risarcitoria continua a dipendere dal titolo applicabile alla fattispecie concreta. Possono così venire in rilievo la disciplina dei prodotti difettosi, le regole nazionali sulla responsabilità contrattuale o extracontrattuale e, quando il danno derivi dalla violazione delle norme sulla protezione dei dati personali, l'art. 82 GDPR[1]. Più circoscritta era, invece, la funzione assegnata alla AILD, che non avrebbe introdotto una fattispecie generale di responsabilità civile per i danni da intelligenza artificiale, ma avrebbe agevolato, in alcune azioni extracontrattuali fondate sulla colpa, l'accesso a determinate prove e l'accertamento di specifici passaggi del nesso causale[2]. Gli effetti del ritiro devono pertanto essere misurati non soltanto sul piano dei rimedi rimasti disponibili, ma anche su quello degli strumenti attraverso i quali il danneggiato può dimostrare i fatti necessari a farli valere.

Il percorso dell'indagine va perciò chiarito sin d'ora. I tre testi considerati non disciplinano lo stesso fatto né operano sul medesimo piano. L'art. 82 GDPR costituisce il titolo risarcitorio quando il pregiudizio derivi da una violazione del regolamento. L'AI Act può rendere disponibili, nei casi e nei tempi previsti,

[1] Il richiamo a più titoli di responsabilità non implica che essi concorrano necessariamente sulla stessa fattispecie. Il rimedio applicabile dipende dalla natura del fatto, dal tipo di danno e dalla disciplina violata. Art. 82 Regolamento 2016/679/UE (GDPR); direttiva 2024/2853/UE. Sulla persistente pluralità dei titoli di responsabilità dopo il ritiro della AILD, v. O. TUJJAR, G. IENTILE e F. TOPPETTI, *After the AI Liability Directive: Civil Liability for Healthcare AI and the Limits of EU Risk Regulation,* in «European Journal of Risk Regulation», 2026, First View, pp. 1-18, DOI 10.1017/err.2026.10130.

[2] La proposta lasciava quindi impregiudicate, salvo le specifiche regole probatorie introdotte, le condizioni sostanziali della responsabilità previste dagli ordinamenti nazionali. *Proposta di direttiva del Parlamento europeo e del Consiglio relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (direttiva sulla responsabilità da intelligenza artificiale)*, COM(2022) 496 final, 28 settembre 2022, artt. 1, 3 e 4.

documentazione e registrazioni utili alla prova. La PLD assume invece funzione di termine di confronto, perché mostra come il legislatore europeo possa attribuire espressamente a disclosure e presunzioni determinati effetti probatori. Il filo che collega i tre regimi è dunque la prova, non l'identità della fattispecie di responsabilità.

La stessa nozione di «ritiro» richiede, peraltro, una precisazione temporale. Nel febbraio 2025 la Commissione annunciò l'intenzione di non proseguire l'iniziativa, ritenendo improbabile il raggiungimento di un accordo, mentre il ritiro fu successivamente approvato nel luglio dello stesso anno e pubblicato nella Gazzetta ufficiale dell'Unione europea il 6 ottobre 2025[3]. Non si è dunque in presenza di una proposta ancora pendente, bensì di un procedimento legislativo conclusosi senza l'adozione della direttiva. Ciò che resta da verificare è, allora, in quale misura le difficoltà pratiche e probatorie cui la AILD intendeva porre rimedio trovino oggi risposta nelle discipline già vigenti.

Nel settore dei dati personali questa delimitazione acquista un rilievo particolare. Quando la violazione del GDPR cagioni un danno, l'interessato può agire per il risarcimento ai sensi dell'art. 82, mentre la nuova direttiva sulla responsabilità per danno da prodotti difettosi (Product Liability Directive, PLD), pur introducendo strumenti idonei ad agevolare la prova, circoscrive il proprio regime a categorie di danno specificamente individuate e non vi ricomprende la violazione della privacy considerata in sé[4]. Diversa è ancora la funzione dell'AI Act. Per alcuni sistemi ad alto rischio esso impone la formazione e la conservazione di documentazione e registrazioni capaci di restituire elementi sul funzionamento del sistema e sugli eventi verificatisi. Da tali obblighi non discendono, per ciò solo, né un generale diritto del danneggiato a ottenere quei materiali in giudizio né una presunzione di responsabilità civile per ogni violazione del regolamento[5].

La letteratura ha già isolato i due versanti dai quali il problema può essere osservato. Da un lato, è stata riconosciuta la capacità dell'art. 82 GDPR di offrire tutela risarcitoria anche rispetto a pregiudizi connessi all'impiego di sistemi

[3] La sequenza è rilevante perché distingue l'annuncio politico dell'intenzione di ritirare la proposta dal successivo atto formale di ritiro pubblicato nella Gazzetta ufficiale. COMMISSIONE EUROPEA, *Programma di lavoro della Commissione per il 2025,* COM (2025) 45 final, 11 febbraio 2025, Allegato IV; COMMISSIONE EUROPEA, *Withdrawal of Commission proposals*, in «Gazzetta Uff. UE», 6 ottobre 2025, serie C, C/2025/5423.

[4] La distinzione fra danno ai dati e violazione della privacy è centrale nel confronto svolto nel par. 5. La PLD tipizza le categorie di danno alle quali collega il proprio regime e, nei considerando richiamati, esclude che la violazione della privacy, in quanto tale, sia sufficiente ad attivarlo. Direttiva 2024/2853/UE, artt. 6, 9 e 10 e considerando 20 e 24.

[5] Gli obblighi richiamati sono obblighi di documentazione, registrazione o conservazione posti a carico degli operatori dell'AI Act. Non equivalgono a una regola processuale generale di esibizione in favore del soggetto che agisca per il risarcimento. Regolamento 2024/1689/UE (AI Act), testo consolidato al 27 luglio 2026, come modificato dal regolamento 2026/1744/UE, artt. 11, 12, 18, 19 e 26, par. 6.

algoritmici, purché ricorrano i presupposti della disposizione[6]. Dall'altro, è stato posto in evidenza il possibile rilievo processuale della documentazione tecnica, delle valutazioni di conformità e delle registrazioni, senza che la loro esistenza elimini l'asimmetria informativa derivante dal fatto che tali materiali rimangono frequentemente nella disponibilità degli operatori[7]. Il punto di contatto fra questi due itinerari è rappresentato dalla possibilità che un documento o una registrazione formati in adempimento degli obblighi dell'AI Act siano successivamente impiegati per dimostrare i fatti costitutivi di una distinta pretesa risarcitoria. È in questo spazio che la responsabilità civile può concorrere a precisare il significato concreto dei doveri regolatori e ad allocare i rischi prodotti dalle attività digitali[8].

L'analisi muove, dunque, da una dissociazione che deve essere preservata. Un documento o una registrazione possono essere formati o conservati perché l'AI Act lo impone e, una volta legittimamente acquisiti in un giudizio promosso ai sensi dell'art. 82 GDPR, divenire rilevanti per la prova di un fatto costitutivo della domanda. Il diverso uso processuale del medesimo documento o della medesima registrazione non consente, tuttavia, di trasferire nel giudizio risarcitorio anche presunzioni o agevolazioni probatorie proprie di altre discipline. Per questa ragione il confronto tra i tre regimi deve mantenere distinti la fattispecie regolata, l'interesse protetto, il danno risarcibile, il nesso causale e la distribuzione degli oneri probatori. Soltanto la previa delimitazione di ciascun piano consente di ricostruirne le possibili interferenze senza sovrapporli.

2. Disclosure e presunzioni nella proposta ritirata.

Il disegno della AILD era deliberatamente circoscritto e non mirava ad armonizzare in via generale la responsabilità civile per l'intelligenza artificiale. L'art. 1 limitava infatti l'intervento, nelle azioni extracontrattuali fondate sulla colpa, all'accesso a determinate prove e ad alcune regole sull'onere

[6] I due contributi sono richiamati per profili diversi: Palmerini mette in luce la possibile attrazione di alcuni danni algoritmici nell'area dell'art. 82 GDPR; Salziger ricostruisce specificamente il danno non patrimoniale e le difficoltà probatorie della disposizione nel contesto dell'IA. E. PALMERINI, *Data protection law and the regulation of artificial intelligence: a two-way discourse*, in «EJPLT», Special Issue 2025/1, spec. pp. 9-10, DOI 10.57230/EJPLTSI251EP; S. SALZIGER, *Between Data Protection and AI: Civil Liability for Non-Material Damage in Article 82 GDPR*, in «European Data Protection Law Review», 2024, IV, pp. 324-335, DOI 10.21552/edpl/2024/4/4.

[7] Chen e Giacalone valorizzano la funzione probatoria dei materiali prodotti dai meccanismi di accountability; TUJJAR, IENTILE e TOPPETTI insistono invece sulla persistente asimmetria informativa quando gli artefatti tecnici restino nella disponibilità degli operatori. S. CHEN e M. GIACALONE, *From Accountability to Liability: How Accountability Mechanisms Shape the Non-Contractual Liability of Generative AI in the EU and China*, in «EJPLT», 2026, II, spec. pp. 14-15, DOI 10.57230/EJPLT262SCMG; O. TUJJAR, G. IENTILE e F. TOPPETTI, *op. cit.*

[8] D. DWORNICZAK, *Regulation in the Making: The Governance Effects of Civil Liability in EU Digital Regulation*, in «European Journal of Risk Regulation», 2026, First View, pp. 1-17, DOI 10.1017/err.2026.10114.

probatorio [9]. In questo quadro la «disclosure» designava, in sostanza, la possibilità di ottenere per ordine del giudice l'esibizione di prove nella disponibilità della controparte o degli altri soggetti individuati dalla proposta, mentre le condizioni della responsabilità non espressamente disciplinate sarebbero rimaste affidate al diritto nazionale [10]. Ne discendeva che la violazione di un obbligo imposto dalla regolazione dell'IA non sarebbe stata, da sola, sufficiente a fondare il diritto al risarcimento.

Sul versante dell'accesso alla prova, l'art. 3 avrebbe consentito al giudice, ricorrendone le condizioni, di ordinare l'esibizione di prove rilevanti relative a uno specifico sistema di IA ad alto rischio e detenute dal fornitore del sistema (provider) o dagli altri soggetti indicati dalla proposta. L'esibizione non avrebbe potuto assumere carattere esplorativo, poiché l'attore era tenuto a offrire elementi sufficienti a rendere plausibile la propria pretesa e l'ordine restava comunque assoggettato ai criteri di necessità e proporzionalità, oltre che alla tutela dei segreti commerciali [11]. Alla mancata esecuzione dell'ordine la proposta ricollegava, inoltre, una conseguenza tipizzata, imponendo al giudice di presumere, salvo prova contraria, la violazione del dovere di diligenza che la prova non esibit avrebbe dovuto consentire di accertare[12].

L'art. 4 interveniva, invece, sul rapporto causale tra la violazione di un dovere di diligenza e il comportamento del sistema, senza introdurre una presunzione generalizzata. Occorreva che fosse dimostrata, o presunta ai sensi dell'art. 3, la violazione di un dovere destinato a proteggere dal danno concretamente verificatosi, che risultasse ragionevolmente probabile l'incidenza di tale violazione sull'output del sistema o sulla sua mancata produzione e che il danneggiato provasse comunque la causalità tra il comportamento del sistema e il danno[13]. Restavano perciò fuori dalla presunzione tanto l'esistenza del pregiudizio quanto, in termini generali, il nesso causale, secondo una selettività dell'intervento che aveva già alimentato il dibattito circa l'effettiva capacità di disclosure e presunzioni di ridurre l'asimmetria informativa propria delle controversie sull'IA[14].

---

[9] Art. 1 proposta COM(2022) 496 final, *cit.*

[10] *Relazione alla proposta COM(2022) 496 final*, sezione «Detailed explanation of the specific provisions in the proposal», par. 1, «Subject matter and scope (Article 1)».

[11] Art. 3, parr. 1-4, proposta COM(2022) 496 final, *cit.*

[12] Art. 3, par. 5, proposta COM(2022) 496 final, *cit.*

[13] Art. 4, par. 1, proposta COM(2022) 496 final, *cit.*

[14] Il dibattito precedente al ritiro non riguardava dunque soltanto l'opportunità politica della proposta, ma anche l'effettiva capacità dei suoi strumenti di ridurre il divario informativo e le difficoltà nella prova del nesso causale. S. Li e B. Schütte, *The Proposed EU Artificial Intelligence Liability Directive: Does/Will Its Content Reflect Its Ambition?*, in «Technology and Regulation» (2024), pp. 143-151, DOI 10.26116/techreg.2024.014; G. Noto La Diega e L.C.T. Bezerra, *Can there be responsible AI without AI liability? Incentivizing generative AI safety through ex-post tort liability under the EU AI liability directive*, in «International Journal of Law and Information Technology», XXXII (2024), eaae021, DOI 10.1093/ijlit/eaae021; A. Bertolini, *Artificial Intelligence and Civil Liability – A European Perspective*, studio per il Parlamento europeo, PE 776.426, Bruxelles 2025; P. Hacker, *The European AI Liability Directives – Critique of a Half-Hearted Approach and Lessons*

Il ritiro ha fatto venir meno, quindi, soprattutto un apparato di facilitazioni probatorie riferito alle azioni comprese nell'ambito della proposta. È precisamente su questo piano che la sua portata deve essere apprezzata, perché l'esistenza astratta di un'azione risarcitoria non dice ancora se il danneggiato disponga degli strumenti necessari per esercitarla effettivamente. Assumono allora rilievo i fatti da provare, le fonti idonee a dimostrarli, la disponibilità materiale di tali fonti e l'eventuale attribuzione normativa di effetti presuntivi a determinati accadimenti. È insita in questa trama, e non in una pretesa lacuna generale di responsabilità, l'incidenza che il ritiro della AILD produce anche sulle controversie relative ai dati personali.

3. Art. 82 GDPR e pregiudizio connesso all'impiego di sistemi di IA.

L'art. 82 GDPR riconosce il diritto al risarcimento a chi abbia subito un danno materiale o immateriale causato da una violazione del regolamento, sicché l'illiceità del trattamento, isolatamente considerata, non esaurisce la fattispecie risarcitoria. La Corte di giustizia, nella sentenza Österreichische Post, ha individuato come elementi autonomi la violazione del GDPR, il danno e il nesso causale che deve collegare la violazione al danno[15], escludendo, per un verso, che il danno non patrimoniale debba superare una soglia minima di gravità e, per altro verso, che la mera violazione possa essere identificata con il danno risarcibile [16]. L'impiego dell'intelligenza artificiale può rendere più complessa la ricostruzione fattuale, soprattutto quando il funzionamento del sistema rimanga poco accessibile all'interessato, ma non altera gli elementi che devono essere accertati ai fini del risarcimento.

In questa prospettiva l'espressione «danno alla privacy» è impiegata nel contributo con funzione meramente descrittiva e non intende individuare una categoria autonoma di danno. Essa designa i pregiudizi patrimoniali o non patrimoniali dei quali sia chiesto il risarcimento in quanto causalmente riconducibili a una violazione del GDPR. La violazione della disciplina del trattamento non può, infatti, essere sovrapposta né alla lesione dell'interesse protetto né, a maggior ragione, al danno risarcibile, poiché ciascuno di tali elementi occupa un distinto segmento della fattispecie e richiede un autonomo accertamento. La varietà delle forme nelle quali il pregiudizio può manifestarsi, insieme alla persistente delicatezza della prova del danno non patrimoniale, emerge del resto con particolare nettezza nella letteratura più recente[17].

---

for the Future, in «Computer Law & Security Review», LI (2023), 105871, DOI 10.1016/j.clsr.2023.105871; M. Ziosi, J. MÖKANDER, C. NOVELLI, F. CASOLARI, M. TADDEO e L. FLORIDI, *The EU AI Liability Directive (AILD): Bridging Information Gaps*, in «European Journal of Law and Technology», XIV (2023), n. 3.

[15] C. Giust. Ue, 4.5.2023, C-300/21, Österreichische Post, ECLI:EU:C:2023:370, par. 32.

[16] *Ivi*, parr. 42 e 45-51.

[17] La formula privacy harm è impiegata nella letteratura in significati non sempre coincidenti. Nel testo viene deliberatamente usata in senso descrittivo, così da evitare che la denominazione anticipi la qualificazione

La recente sentenza Brillen Rottler conferma questa separazione dei piani, riconoscendo che l'art. 82 può trovare applicazione anche quando il danno consegua alla violazione del diritto di accesso previsto dall'art. 15 GDPR e ammettendo che la perdita di controllo sui propri dati, così come l'incertezza circa il loro trattamento, possano integrare un danno non patrimoniale. Anche in tali ipotesi il pregiudizio deve essere effettivamente dimostrato e causalmente ricondotto alla violazione dedotta. La medesima pronuncia individua, sul distinto versante dell'accesso ai dati personali, una specifica regola probatoria interna al GDPR. Ai sensi dell'art. 12, par. 5, grava infatti sul titolare l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta, secondo criteri restrittivi. La distribuzione dell'onere non è dunque uniforme neppure all'interno del regolamento, ma varia con il fatto e con la posizione giuridica dedotti[18].

L'autonomia della violazione, del danno e del nesso causale non comporta, tuttavia, che l'interessato debba dimostrare ogni circostanza interna all'organizzazione del titolare. La giurisprudenza della Corte di giustizia restituisce una distribuzione articolata degli oneri probatori. In Krankenversicherung Nordrhein la colpa del titolare è stata considerata presunta, salva la prova della non imputabilità del fatto causativo del danno. In Natsionalna agentsia za prihodite, gli artt. 5, par. 2, 24 e 32 GDPR sono stati letti nel senso che grava sul titolare la prova dell'adeguatezza delle misure di sicurezza. Questa regola non trasferisce sul titolare la prova della violazione, del danno o della causalità. Individua, invece, un fatto rispetto al quale la documentazione prodotta in adempimento dell'AI Act può concorrere all'assolvimento di un onere già posto dal regime applicabile alla domanda. La fonte probatoria può migrare. L'onere resta quello del regime di destinazione[19].

4. Dalla documentazione dell'AI Act alla prova nel giudizio risarcitorio.

L'AI Act non costruisce un regime generale di responsabilità civile, poiché disciplina principalmente la progettazione, l'immissione sul mercato, l'uso e il controllo dei sistemi di IA. In tale architettura trovano spazio anche alcune

---

del pregiudizio concretamente dedotto. S. Li, *Contract Model versus Tort Model: One View of the Privacy Harm*, in «EJPLT» (2025), Special Issue n. 1; B. SCHÜTTE e K. HAVU, *Damages liability for privacy infringements: the case law of the Court of Justice of the European Union in light of The Privacy Fallacy*, in «EJPLT» (2025), Special Issue n. 1, spec. pp. 3-5, DOI 10.57230/EJPLT251BSKH.

[18] C. Giust. UE, 19.3.2026, C-526/24, Brillen Rottler, ECLI:EU:C:2026:216, parr. 35-45 e 55-67. Sull'art. 12, par. 5, la Corte ribadisce che grava sul titolare l'onere di dimostrare il carattere eccessivo della richiesta e che l'eccezione va interpretata restrittivamente.

[19] Le pronunce riguardano segmenti diversi dell'onere probatorio. C. Giust. UE, 21.12.2023, C-667/21, Krankenversicherung Nordrhein, ECLI:EU:C:2023:1022, parr. 90-103; C. Giust. UE, 14.12.2023, C-340/21, Natsionalna agentsia za prihodite, ECLI:EU:C:2023:986, spec. parr. 52-57, sul principio di accountability e sull'onere del titolare di provare l'adeguatezza delle misure di sicurezza ex art. 32 GDPR.

posizioni individuali, tra le quali il diritto di reclamo previsto dall'art. 85 e, nei casi delimitati dall'art. 86, il diritto a una spiegazione. Il diritto alla spiegazione riguarda la persona interessata da una decisione del deployer basata sull'output di un sistema ad alto rischio dell'allegato III, con esclusione dei sistemi di cui al punto 2, quando la decisione produca effetti giuridici o incida in modo analogo significativamente e sia ritenuta pregiudizievole per salute, sicurezza o diritti fondamentali. La disposizione opera inoltre soltanto nei limiti in cui il medesimo diritto non sia già previsto dal diritto dell'Unione[20].

Il rapporto con il GDPR non è, pertanto, di semplice sovrapposizione. L'art. 15, par. 1, lett. h, assicura informazioni significative sulla logica del processo decisionale automatizzato richiamato dall'art. 22 e, dopo Dun & Bradstreet Austria, comprende un effettivo diritto alla spiegazione. L'art. 86 AI Act può invece conservare uno spazio autonomo soprattutto quando l'output del sistema ad alto rischio concorra in modo significativo a una decisione nella quale sussista un intervento umano effettivo, senza che ricorrano necessariamente i presupposti dell'art. 22 GDPR. Il confine tra l'ambito dell'art. 86 AI Act e quello dell'art. 22 GDPR non è però formale. SCHUFA mostra che un passaggio umano a valle non basta a sottrarre il procedimento all'art. 22 quando il risultato automatizzato svolga un ruolo determinante. La qualificazione del processo decisionale dipende dunque dal suo funzionamento concreto e può rendere la medesima informazione raggiungibile attraverso vie normative differenti. Una volta acquisita, la spiegazione può concorrere alla prova nel giudizio risarcitorio, ma non sostituisce la documentazione tecnica o i logs quando occorra ricostruire ciò che il sistema abbia effettivamente registrato o come abbia operato[21].

Per i sistemi qualificati come «ad alto rischio» l'AI Act prevede, tra l'altro, la predisposizione di documentazione tecnica e la registrazione automatica degli eventi. Il provider, ossia il soggetto che sviluppa o fa sviluppare il sistema e lo immette sul mercato o lo mette in servizio a proprio nome, è tenuto a conservare determinati documenti e, quando ne abbia il controllo, le registrazioni, mentre specifici obblighi di conservazione dei logs possono gravare anche sul deployer[22]. La portata di tali prescrizioni deve però essere letta alla luce del calendario applicativo risultante dalle modifiche introdotte

[20] Per l'art. 3 AI Act, il deployer è il soggetto che usa un sistema di IA sotto la propria autorità, salvo l'uso personale non professionale. Sull'ambito e sulla residualità del diritto alla spiegazione, art. 86, parr. 1-3, regolamento 2024/1689/UE.

[21] C. Giust. UE, 27.2.2025, C-203/22, Dun & Bradstreet Austria, ECLI:EU:C:2025:117, parr. 57-58; C. Giust. UE, 7.12.2023, C-634/21, SCHUFA Holding (Scoring), ECLI:EU:C:2023:957, parr. 48-50.

[22] Il calendario applicativo è essenziale per evitare di descrivere come già operativi obblighi che, per le categorie di sistemi qui considerate, diverranno applicabili nelle date indicate. Resta distinto il problema processuale dell'accesso del danneggiato ai materiali conservati. Artt. 11, 12, 18 e 19 regolamento 2024/1689/UE, cit.; art. 26, par. 6, per le registrazioni sotto il controllo del deployer. Sul calendario applicativo, v. art. 113, 3° co., lett. c, regolamento 2024/1689/UE, nel testo risultante dal regolamento 2026/1744/UE.

dal regolamento 2026/1744/UE, in forza del quale gli obblighi qui considerati troveranno applicazione dal 2 dicembre 2027 per una parte dei sistemi ad alto rischio e dal 2 agosto 2028 per l'altra parte individuata dalla disciplina. Fino a tali date l'analisi conserva dunque carattere prospettico. Resta, in ogni caso, una distinzione essenziale tra il dovere dell'operatore di formare o conservare il materiale e il diritto del danneggiato di ottenerlo nel processo. L'art. 18, ad esempio, impone che la documentazione sia tenuta a disposizione delle autorità competenti, ma da tale obbligo non può ricavarsi, senza un'ulteriore base normativa, un generale diritto di esibizione in favore di chi agisca ai sensi dell'art. 82 GDPR.

La possibile rilevanza processuale della documentazione tecnica, delle valutazioni di conformità e dei registri di audit è già stata posta in evidenza da Chen e Giacalone, secondo i quali non conformità o incoerenze possono costituire prova *prima facie* della violazione di un obbligo normativo[23]. La formula coglie il valore inferenziale di tali materiali, ma richiede una delimitazione. Se «*prima facie*» descrive soltanto la loro idoneità a sostenere l'accertamento della violazione, la conclusione è compatibile con le regole ordinarie del giudizio. Non persuade, invece, il passaggio da tale idoneità a un effetto tipizzato che, per la sola provenienza del materiale dall'AI Act, alleggerisca o inverta l'onere della prova. Un simile effetto richiede una base normativa nel regime di destinazione. Restano distinti la formazione o conservazione del materiale, la sua acquisizione processuale, il valore probatorio e, quando il materiale sia nella disponibilità del provider o del deployer, il problema dell'accesso[24].

È proprio la possibilità che il medesimo documento o la medesima registrazione assumano una funzione probatoria in un diverso regime a giustificare la nozione di «traslazione probatoria inter-regime». Una registrazione formata o conservata in adempimento dell'AI Act può essere acquisita in un giudizio fondato sul GDPR e impiegata per dimostrare un fatto rilevante ai fini della domanda risarcitoria. L'espressione non designa una nuova categoria di prova. Serve a distinguere l'obbligo normativo che impone la formazione o la conservazione del materiale, le condizioni alle quali esso può essere acquisito e utilizzato, l'allocazione dell'onere relativo al fatto da provare e l'effetto che il giudice può attribuirgli.

La traslazione richiede, anzitutto, che il documento o la registrazione possano essere acquisiti secondo le regole applicabili e, una volta entrati nel processo, si riferiscano a un fatto rilevante per la domanda ex art. 82, quale la violazione dedotta, il danno, il nesso causale o una circostanza utile a valutarne

[23] S. Chen e M. Giacalone, *From Accountability to Liability…*, cit., pp. 14-15, ove si ritiene che non conformità o incoerenze della documentazione possano costituire prova *prima facie* della violazione di un obbligo normativo.

[24] Tujjar, Ientile e Toppetti, *op. cit.*

l'imputabilità. Il passaggio da un regime all'altro non modifica, però, chi sia tenuto a provare quel fatto. Quando il GDPR pone già un determinato onere sul titolare, il materiale acquisito in adempimento dell'AI Act può servire ad assolverlo o a valutarne l'adempimento. Quando l'onere resta sull'attore, il materiale può facilitarne la prova senza invertirlo. A ciò si aggiungono gli eventuali limiti oggettivi o soggettivi di utilizzazione posti dal regime d'origine e, infine, l'idoneità dimostrativa del materiale acquisito, che deve essere commisurata al fatto concretamente da provare.

La necessità di una base normativa espressa riguarda l'effetto probatorio tipizzato, non l'esistenza del potere del giudice di valutare le prove e il contegno processuale secondo il diritto del foro. Tale potere preesiste alla disciplina europea e non richiede che un altro regime gli attribuisca una specifica presunzione. Restano invece affidate alle regole processuali applicabili le condizioni del suo esercizio, come la disponibilità del documento o della registrazione, le richieste formulate, l'eventuale ordine giudiziale, le ragioni della mancata produzione e i requisiti delle inferenze ammesse. La mancata produzione di logs che avrebbero dovuto essere conservati può quindi assumere rilievo secondo le regole processuali applicabili. Il solo fatto che quei logs derivino da obblighi previsti dall'AI Act non consente, tuttavia, di ricavarne una presunzione legale o un'inversione dell'onere non previste dal regime di destinazione.

La portata del criterio emerge considerando l'impiego di un sistema di IA ad alto rischio nella selezione di candidati a un posto di lavoro, quando il sistema tratti dati personali. I logs possono indicare quale versione del sistema abbia elaborato i dati e quale output sia stato prodotto, mentre la documentazione tecnica può descrivere configurazione, finalità e misure di controllo. Se tali materiali, una volta acquisiti, restituiscono un funzionamento diverso da quello documentato, il giudice può valorizzare la contraddizione attraverso gli strumenti probatori del foro. Se, invece, i logs non vengono prodotti, la mancata produzione può rilevare alle condizioni previste dal diritto processuale applicabile. In nessuno dei due casi, tuttavia, il fatto che i materiali siano stati formati o conservati in adempimento dell'AI Act determina automaticamente una presunzione legale di violazione, danno o causalità.

5. Responsabilità per danno da prodotti difettosi: facilitazione della prova e delimitazione del danno.

La nuova direttiva sulla responsabilità per danno da prodotti difettosi (PLD) offre un termine di confronto particolarmente significativo, perché mostra come il legislatore europeo, quando intenda agevolare l'accertamento dei fatti, possa attribuire espressamente a determinati strumenti un preciso effetto probatorio. La nozione di prodotto comprende anche il software e consente a

un sistema di IA di ricadere nella disciplina della responsabilità da prodotto, mentre il provider può assumere, ricorrendone i presupposti, la posizione di fabbricante[25]. Il nuovo regime si applica ai prodotti immessi sul mercato o messi in servizio dopo l'8 dicembre 2026, restando quelli anteriori assoggettati alla disciplina previgente[26].

L'art. 9 interviene sull'accesso alle prove, imponendo agli Stati membri di assicurare che, quando l'attore abbia presentato fatti ed elementi sufficienti a rendere plausibile la domanda, il convenuto possa essere obbligato a esibire le prove rilevanti nella propria disponibilità, entro i limiti di necessità e proporzionalità [27]. L'art. 10 disciplina invece l'effetto probatorio di fatti specificamente individuati, muovendo dalla regola secondo cui il danneggiato è tenuto a provare difetto, danno e nesso causale, ma affiancandovi presunzioni relative in ipotesi tipizzate. Vi rientrano la mancata esibizione delle prove, la violazione di determinati requisiti obbligatori di sicurezza e, a condizioni rigorose, le eccessive difficoltà probatorie derivanti dalla complessità tecnica o scientifica[28].

La maggiore incisività di tali facilitazioni non comporta, tuttavia, che esse si estendano a ogni forma di pregiudizio. L'art. 6 della PLD ricomprende la morte e le lesioni personali, alcuni danni alle cose e la distruzione o corruzione di dati non utilizzati per finalità professionali[29], mantenendo distinto il danno arrecato ai dati dalla violazione delle norme sulla protezione dei dati personali. I considerando 20 e 24 chiariscono, infatti, che le violazioni della privacy e la discriminazione non fanno sorgere, in quanto tali, la responsabilità prevista dalla direttiva[30], senza pregiudicare i diritti che il danneggiato possa esercitare in forza del GDPR o di altre discipline[31].

La distinzione diviene evidente se si considera uno stesso archivio digitale. La sua distruzione provocata da un prodotto difettoso può integrare il danno ai dati rilevante ai sensi della PLD, mentre la comunicazione illecita a terzi o la perdita di controllo sulle informazioni personali che derivino dal trattamento richiedono una qualificazione alla luce della disciplina sulla protezione dei dati,

[25] Art. 4, n. 1, direttiva 2024/2853/UE; considerando 13.

[26] Considerando 63 e artt. 2, par. 1, 21 e 22 direttiva 2024/2853/UE; rettifica alla direttiva 2024/2853/UE, in «Gazzetta Uff. UE», 7.5.2026, serie L, 2026/90364.

[27] La disposizione configura un meccanismo di esibizione giudiziale subordinato alla previa plausibilità della domanda e ai limiti di necessità e proporzionalità. Non attribuisce quindi un diritto indiscriminato di accesso a tutta la documentazione del produttore. Art. 9 direttiva 2024/2853/UE.

[28] Le presunzioni dell'art. 10 sono tipizzate e relative. Proprio questa scelta legislativa espressa rende improprio trasferirne gli effetti, per analogia, a una domanda fondata su un diverso regime di responsabilità. Art. 10, parr. 1-5, direttiva 2024/2853/UE.

[29] Art. 6 direttiva 2024/2853/UE.

[30] La direttiva separa così il deterioramento o la perdita del dato come bene digitale dagli illeciti che incidono sulla riservatezza, sul controllo delle informazioni personali o su altri interessi protetti dalla disciplina dei dati personali. Considerando 20 e 24 direttiva 2024/2853/UE.

[31] Art. 2, par. 4, lett. a, direttiva 2024/2853/UE.

anzitutto del GDPR. L'identità dell'evento tecnologico non elimina, dunque, l'autonomia delle fattispecie alle quali le diverse discipline ricollegano i propri effetti. Il rapporto tra GDPR e PLD è stato già esaminato, ad esempio, con riguardo alla corruzione di dati provocata da consulenti automatizzati nel settore assicurativo[32]. Anche questo confronto mostra che «danno ai dati» e «danno alla privacy» rinviano a piani che non possono essere trattati come equivalenti.

6. Tecniche di facilitazione probatoria e limiti della traslazione inter-regime.

Il confronto consente di cogliere una asimmetria tra ampiezza della tutela sostanziale e facilitazione probatoria. L'art. 82 GDPR protegge, ricorrendone i presupposti, danni patrimoniali e non patrimoniali derivanti dalla violazione del regolamento, senza riprodurre l'apparato di disclosure e presunzioni progettato dalla AILD. La PLD introduce invece facilitazioni più incisive entro un catalogo di danni che non assume la violazione della privacy, in quanto tale, come categoria autonoma. L'ampiezza del rimedio e il favore probatorio non procedono dunque necessariamente insieme[33].

L'art. 10 PLD rende visibile il limite oltre il quale gli effetti probatori non possono essere trasposti. Il legislatore collega a fatti specificamente individuati presunzioni relative di difettosità o di causalità. Un raccordo analogo non è previsto dall'art. 82 GDPR per la violazione degli obblighi dell'AI Act. La documentazione formata o conservata in adempimento dell'AI Act può quindi essere acquisita e valutata secondo le regole applicabili, ma la PLD non offre un fondamento analogico per introdurre nel giudizio ex art. 82 una presunzione legale che il legislatore non ha previsto[34].

Un termine di raffronto ancora più specifico sul piano dell'asimmetria probatoria è offerto dalla direttiva 2014/104/UE sul risarcimento del danno antitrust. Essa disciplina la disclosure giudiziale secondo criteri di proporzionalità e protezione delle informazioni riservate, prevede limiti all'utilizzazione di determinate prove e, all'art. 8, par. 2, include tra le sanzioni per l'inosservanza di un ordine di esibizione o la distruzione delle prove la possibilità di trarre conclusioni sfavorevoli. Questa previsione rende evidente che una conseguenza processuale tipizzata, collegata a presupposti determinati, richiede una scelta normativa espressa. Il potere del giudice di

---

[32] S. Skalski e P. Tereszkiewicz, *Robo-Advisors as Product in the Insurance Sector: Considerations Regarding Enforceability*, in *Remedies to Digital Vulnerability in European Private Law*, a cura di C. Crea e M. Infantino, cham, Springer, 2025, pp. 363-384, DOI 10.1007/978-3-032-19720-7_19 [pubblicato online il 1° luglio 2026; citazione editoriale: 2025].

[33] S. Li e K. Heine, *Developing a harm-based approach to understand digital vulnerability in the era of AI: a perspective of the European Union*, in «Computer Law & Security Review», LX (2026), 106266, DOI 10.1016/j.clsr.2026.106266.

[34] Art. 10, par. 2, lett. b, direttiva 2024/2853/UE.

valutare il comportamento delle parti e i fatti secondari emersi nel processo opera invece secondo il diritto processuale applicabile. L'effetto normativo tipizzato non si trasferisce da un regime all'altro, mentre il fatto processuale può essere apprezzato secondo le regole del giudizio di destinazione[35].

Si potrebbe obiettare che, dopo il ritiro della AILD, il principio di effettività imponga di compensare per via interpretativa la perdita delle facilitazioni probatorie progettate dalla proposta. L'obiezione non persuade. Il principio limita l'autonomia processuale degli Stati membri quando le regole interne rendano praticamente impossibile o eccessivamente difficile l'esercizio dei diritti dell'Unione e può orientare l'impiego degli strumenti processuali nazionali già disponibili. Non genera, però, una presunzione armonizzata né una nuova inversione dell'onere della prova. Anche qui la traslazione impone di distinguere disponibilità della prova, accesso processuale ed effetto probatorio[36].

Il criterio della traslazione consente anche di affrontare il possibile riuso, in una controversia ex art. 82 GDPR, di una prova ottenuta attraverso l'esibizione prevista dall'art. 9 PLD. Non basta chiedersi se il materiale sia astrattamente rilevante. Occorre verificare il titolo dell'acquisizione, gli eventuali limiti oggettivi e soggettivi all'utilizzo posti dal regime d'origine, la riutilizzabilità secondo il processo del foro, l'allocazione dell'onere relativo al fatto da dimostrare e, soltanto infine, il valore probatorio nel giudizio di destinazione. La direttiva 2014/104 mostra che il diritto dell'Unione può imporre limiti persino soggettivi all'uso di determinate prove, riservandole a chi le abbia ottenute e ai suoi aventi causa. La traslazione non presuppone quindi la libera circolazione della prova tra procedimenti. Il criterio rende invece espliciti i passaggi che devono essere verificati prima di attribuire alla prova un effetto nel nuovo giudizio[37].

[35] Direttiva 2014/104/UE (azioni risarcitorie antitrust), artt. 5-8 e 17, parr. 1-2, spec. art. 8, par. 2, e considerando 33. L'art. 8, par. 2, include tra le sanzioni disponibili per specifiche violazioni processuali la possibilità di trarre conclusioni sfavorevoli; l'art. 17 distingue il potere di stima del danno dalla presunzione relativa del danno nei cartelli.

[36] Il principio di effettività opera insieme al principio di equivalenza entro l'autonomia processuale degli Stati membri. Nel testo interessa il solo profilo per cui una regola nazionale non può rendere praticamente impossibile o eccessivamente difficile l'esercizio di un diritto attribuito dall'ordinamento dell'Unione. C. Giust. CE, 16.12.1976, 33/76, Rewe-Zentralfinanz, ECLI:EU:C:1976:188; C. Giust. CE, 16.12.1976, 45/76, Comet, ECLI:EU:C:1976:191; C. Giust. CE, 14.12.1995, C-312/93, Peterbroeck, ECLI:EU:C:1995:437, parr. 12-14.

[37] Direttiva 2014/104/UE, art. 7, spec. par. 3: le prove ottenute esclusivamente mediante accesso al fascicolo di un'autorità garante della concorrenza, fuori dalle categorie dei parr. 1 e 2, possono essere utilizzate nell'azione risarcitoria soltanto da chi le abbia ottenute o dai suoi aventi causa. Il richiamo vale come termine di confronto circa la possibilità che il regime d'origine apponga limiti soggettivi all'utilizzazione della prova.

7. Conclusioni.

Il ritiro della AI Liability Directive non ha lasciato privi di tutela i danni connessi all'intelligenza artificiale, ma ha eliminato dal quadro europeo una proposta che avrebbe agevolato, per determinate azioni extracontrattuali fondate sulla colpa, l'accesso alle prove e l'accertamento di alcuni passaggi causali. Quando il pregiudizio derivi dal trattamento di dati personali, l'art. 82 GDPR continua a fornire il titolo risarcitorio, mentre la distribuzione degli oneri probatori resta quella risultante dal GDPR e dalla giurisprudenza della Corte di giustizia.

L'AI Act può assumere un rilievo concreto perché, nei casi e nei tempi previsti, impone la formazione o la conservazione di documentazione e registrazioni capaci di concorrere alla ricostruzione dell'accaduto. Ciò non attribuisce però, per sé solo, un generale diritto processuale di accesso né una presunzione di responsabilità. La PLD e, sul diverso terreno dell'asimmetria probatoria, la direttiva 2014/104 mostrano invece come il legislatore europeo possa tipizzare disclosure, limiti d'uso, presunzioni e conseguenze processuali, attribuendo espressamente a tali strumenti effetti determinati.

Il criterio della traslazione probatoria inter-regime esprime il risultato dell'indagine. Quando documenti, registrazioni o spiegazioni formati o ottenuti nell'ambito di un regime sono invocati in un procedimento governato da un altro regime, occorre verificare, in sequenza, la ragione normativa per cui il materiale è stato formato, conservato o ottenuto, le condizioni della sua acquisizione e i limiti alla sua utilizzazione, chi sopporti l'onere relativo al fatto da dimostrare e quale effetto il giudice possa attribuirgli nel procedimento di destinazione. La fonte probatoria può migrare. L'onere resta quello del regime di destinazione. Il giudice può attribuire al materiale soltanto gli effetti probatori consentiti dalle regole del procedimento di destinazione. In tal modo documenti, logs o spiegazioni possono sostenere la ricostruzione fattuale e le inferenze consentite senza trascinare con sé presunzioni o inversioni dell'onere proprie di un diverso apparato normativo.

Resta una questione di politica del diritto. La complessità tecnologica può produrre difficoltà probatorie analoghe in controversie fondate su titoli differenti, mentre soltanto alcune di tali controversie beneficiano di strumenti europei di facilitazione. Un'eventuale disciplina più generale dovrebbe però confrontarsi con le ragioni che sconsigliano un'ulteriore armonizzazione della responsabilità civile. Il lascito del ritiro della AILD risiede, in definitiva, nella diversa capacità dei singoli regimi di consentire al danneggiato di procurarsi le prove e dimostrare la propria domanda[38].

[38] S. Li e M. Faure, *Does the EU Need an Artificial Intelligence Liability Directive? Insights from the Economics of Federalism*, in *Revue économique*, 2025, I, 115-139, DOI 10.3917/reco.761.0115.