



Il diritto digitale

Temi di informatica giuridica

a cura di

Monica Palmirani, Giovanni Sartor
Federico Galli, Salvatore Sapienza

Bologna
University Press

IL DIRITTO DIGITALE

Temi di informatica giuridica

a cura di
Monica Palmirani, Giovanni Sartor
Federico Galli, Salvatore Sapienza

Bologna
University Press

Title: LEGAL DESIGN AND DATA SCIENCE FOR EXPLICABLE AI IN LEGAL DOMAIN

Acronym: LEDS 4 XAIL

n. GPA: 101085576

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.



Co-funded by the
European Union



LEDS4XAIL

Fondazione Bologna University Press

Via Saragozza 10, 40123 Bologna

tel. (+39) 051 232 882

www.buonline.com

e-mail: info@buonline.com

Quest'opera è pubblicata sotto licenza Creative Commons CC BY-4.0

ISBN 979-12-5477-771-8

ISBN on line 979-12-5477-772-5

DOI 10.30682/9791254777725

Questo volume è stato realizzato a partire da un impaginato camera-ready in formato pdf fornito dai curatori

In copertina: Summit Art Creations/Shutterstock.com

Prima edizione: marzo 2026

INDICE

Introduzione	1
<i>Federico Galli, Monica Palmirani, Salvatore Sapienza, Giovanni Sartor</i>	

PARTE I – DATI

La protezione dei dati personali	11
<i>Federico Galli, Giovanni Sartor</i>	

Data Governance Act e Data Act nel quadro degli Spazi Comuni Europei dei Dati	37
<i>Salvatore Sapienza</i>	

L'uso secondario dei dati sanitari elettronici nella cornice dell'European Health Data Space	55
<i>Paola Aurucci</i>	

Open Government Data	75
<i>Monica Palmirani</i>	

Investigare i dati informatici: la <i>digital forensics</i> tra norme giuridiche, standard tecnici e innovazioni tecnologiche <i>Raffaella Brighi, Michele Ferrazzano</i>	97
--	----

PARTE II – STRUMENTI ABILITANTI

Identità e firme digitali <i>Chantal Bompreszi, Monica Palmirani</i>	121
Smart contract e blockchain <i>Chantal Bompreszi</i>	137

PARTE III – SISTEMI E PRODOTTI

La protezione dei beni informatici attraverso il diritto d'autore <i>Claudio Di Cocco</i>	161
La regolazione dell'Intelligenza Artificiale nell'UE: l'AI Act <i>Giuseppe Contissa, Marco Billi</i>	203
La decisione automatica e la sua spiegazione tra GDPR e AI Act <i>Francesca Lagioia, Giovanni Sartor</i>	221
Responsabilità e Intelligenza Artificiale <i>Chantal Bompreszi</i>	251

PARTE IV – MERCATI E SERVIZI

La regolazione dei mercati digitali: il Digital Markets Act <i>Federico Galli</i>	263
La regolazione degli intermediari di Internet: il Digital Service Act <i>Giuseppe Contissa</i>	287

La tutela del consumatore digitale <i>Federico Galli</i>	307
---	-----

PARTE V – SICUREZZA

La Cybersicurezza nella trasformazione digitale <i>Raffaella Brighi</i>	341
--	-----

Il diritto UE della Cybersicurezza: il quadro normativo <i>Pier Giorgio Chiara</i>	363
---	-----

I reati informatici e la violazione dei diritti della persona in rete <i>Francesco Di Tano</i>	391
---	-----

Il data breach e l'incidente di sicurezza <i>Juri Monducci</i>	409
---	-----

PARTE VI – ETICA DEL DIGITALE

Etica dell'Intelligenza Artificiale <i>Giorgio Bongiovanni, Claudio Novelli</i>	435
--	-----

Gli Autori	463
------------	-----

RESPONSABILITÀ E INTELLIGENZA ARTIFICIALE

Chantal Bompreszzi

Sommario: 1. Responsabilità e software. 2. L'imputazione di responsabilità e la qualificazione giuridica del software. 3. Etica dell'IA e *accountability*. 4. Le principali problematiche sollevate dalla dottrina. 5. L'approccio adottato con l'*AI ACT*. 6. Gli interventi legislativi delle istituzioni europee. 7. Il ritiro dell'AILD e il cambio di approccio del legislatore europeo.

1. Responsabilità e software

La responsabilità per danni cagionati da software è oggetto di indagine sin dagli Anni '80¹. Al pari di oggi, si indagava chi dovesse rispondere dei danni cagionati da un software. Il dibattito giuridico si è acceso particolarmente negli Anni '90, quando è diventato comune nei mercati finanziari di tutto il mondo concludere automaticamente contratti per conto delle parti ad opera dei cd "*electronic agents*" o "agenti software", programmi informatici in grado di spostarsi nella rete verso le raccolte di dati sui quali devono operare e che recano al loro interno istruzioni circa le priorità da rispettare². Questi sistemi informatici abbinavano proposte di acquisto e di vendita in base a parametri predefiniti relativi a prezzo, data e ora. In particolare, ci si è concentrati sull'imputazione delle dichiarazioni contrattuali e sulla responsabilità conseguente in caso di inadempimento, dato il maggiore grado di autonomia di questi strumenti. Il problema che si è posto con maggior forza è stato quello dell'allocazione del rischio riconducibile a un malfunzionamento dell'agente. La posizione prevalente è stata quella di considerare gli agenti come meri mezzi di trasmissione di volontà, e

¹ G. ALPA, *Responsabilità extracontrattuale ed elaboratore elettronico*, in *Dir. dell'Informazione e dell'Informatica* 1986 (II), pp. 387-393; C. ROSSELLO, *La responsabilità da inadeguato funzionamento di programmi per elaboratore elettronico: aspetti e problemi dell'esperienza nordamericana*, in G. ALPA (a cura di), *Computers e responsabilità civile*, Milano: Giuffrè 1985, pp. 87-142.

² Una definizione di "*electronic agent*" è contenuta nell'*Uniform Electronic Transactions Act*, per cui esso è «*a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual*» (sect. 2 (6)).

non come entità dotate di una soggettività giuridica³, per cui il rischio deve considerarsi accettato e sopportato dal soggetto che utilizza l'agente, sulla base dei principi di autoresponsabilità e affidamento. Questo approccio è stato adottato a livello internazionale dall'UNCITRAL, affermando che il principio di imputazione della responsabilità in capo al soggetto che si serve di un determinato software sia responsabile del medesimo anche nel caso in cui l'agente non agisca in maniera automatica ma autonoma⁴. La posizione dell'UNCITRAL ha costituito un opportuno chiarimento in materia, privilegiando l'interpretazione normativa e negando la necessità di un intervento normativo nuovo e *ad hoc*.

Questioni nuove sul tema della responsabilità si pongono, invece, laddove il software abbia una certa autonomia decisionale, ovvero quando gli output del programma siano imprevedibili per il loro carattere non deterministico e opaco, quali sono i sistemi di intelligenza artificiale.

2. L'imputazione di responsabilità e la qualificazione giuridica del software

In merito al rapporto tra intelligenza artificiale e responsabilità, il primo interrogativo posto ha riguardato la qualificazione del software come mero strumento di trasmissione di volontà piuttosto che come soggetto giuridico su cui addossare direttamente le conseguenze negative del proprio operare. Rispetto al dibattito verificatosi sul punto negli Anni '90, l'elemento di novità è rappresentato dal fatto che si è innanzi a sistemi dotati di autonomia decisionale e imprevedibilità dei risultati.

Il Parlamento europeo, con una Risoluzione del 16 febbraio 2017⁵, ha invitato la Commissione europea a valutare «l'istituzione di uno status giuridico specifico per i robot nel lungo termine, di modo che almeno i robot autonomi più sofisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il ricono-

³ Vedi il confronto tra G. FINOCCHIARO, *La conclusione del contratto telematico mediante i «software agents»: un falso problema giuridico?*, in *Contratto e Impresa*, 2002 (XVIII-II), pp. 500-509 e G. SARTOR, *Gli agenti software: nuovi soggetti del ciberdiritto?*, in *Contratto e Impresa*, 2002 (XVIII-II), pp. 465-499.

⁴ United Nations, General Assembly, *Legal aspects of electronic commerce*, A/CN.9/WG.IV/WP.95, par. 71-73. «[. . .] while the expression “electronic agent” has been used for purpose of convenience, the analogy between an automated system and a sales agent was not appropriate. This, general principle of agency law (for example, principle involving limitation of liability as a result of the faulty behaviour of the agent) could not be used in connection with the operation of such systems» «[. . .] as a general principle, the person on whose behalf a computer was programmed should ultimately be responsible for any message generated by the machine».

⁵ Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_IT.html.

scimento della personalità elettronica dei robot che prendono decisioni autonome o che interagiscono in modo indipendente con terzi» (punto 59, lett. f).

Questa posizione del Parlamento europeo, volta a riconoscere specifica soggettività giuridica e personalità elettronica ai robot, è stata fortemente criticata, in quanto ritenuta una soluzione apparente⁶. Anche ammettendo, infatti, di poter conferire soggettività a una cosa (un programma informatico), è stato sollevato il problema del risarcimento del danno, poiché il robot non avrebbe un patrimonio di cui poter disporre con il quale risarcire il danno. Peraltro, anche laddove venisse costituito un patrimonio dedicato (così come da taluno suggerito), si è osservato che un patrimonio riservato al risarcimento di queste tipologie di danni si potrebbe comunque ipotizzare senza dover costruire tutta l'impalcatura della soggettività. L'attribuzione di soggettività si sostanzierebbe, cioè, in un'inutile complicazione di rapporti.

Più recentemente, la Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale⁷ ha escluso il conferimento di personalità giuridica⁸, ponendosi in antitesi rispetto alla precedente Risoluzione del 16 febbraio 2017. Sulla stessa lunghezza d'onda, l'UNCITRAL *Model Law on Automated Contracting* del 2025⁹ ha chiarito che i sistemi automatizzati sono strumenti privi di volontà propria o di personalità giuridica, e i risultati prodotti da tali sistemi devono essere attribuiti alle persone e non al sistema stesso (art. 7)¹⁰.

3. Etica dell'IA e accountability

Nel giugno 2018, la Commissione europea ha nominato cinquantadue esperti indipendenti nel *High-Level Expert Group on Artificial Intelligence (AI HLEG)*¹¹, con il compito di formulare linee guida per un'IA affidabile (*Ethics Guidelines for Trustworthy AI* dell'8 aprile 2019), basate su tre pilastri fondamentali: legalità (garantire il rispetto delle leggi e dei diritti fondamentali), etica (difendere la dignità

⁶ Vedi U. RUFFOLO, *La personalità elettronica tra "doveri" e "diritti" della macchina*, in ID. (a cura di), *XXVI Lezioni di diritto dell'intelligenza artificiale*, Torino: Giappichelli 2021, pp. 115-127; G. FINOCCHIARO, *Intelligenza artificiale e responsabilità*, in *Contratto e Impresa*, 2020 (II), pp. 713-731.

⁷ Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL)), https://www.europarl.europa.eu/doceo/document/TA-9-2020-027_6_IT.html.

⁸ Vedi il punto 7 della Risoluzione.

⁹ <https://uncitral.un.org/en/mlac>.

¹⁰ Vedi in particolare il par. 2 dell'art. 7, secondo cui «an action carried out by an automated system is attributed to the person who uses the system for that purpose».

¹¹ <https://digital-strategy.ec.europa.eu/en/news/commission-appoints-expert-group-ai-and-launches-european-ai-alliance>.

e prevenire la discriminazione) e robustezza tecnica (assicurare sicurezza e resilienza).

Per rendere operativi questi pilastri, le Linee guida hanno definito sette requisiti: agenzia e supervisione umana; robustezza tecnica e sicurezza; privacy e governance dei dati; trasparenza; diversità, non discriminazione e equità; benessere sociale e ambientale; e responsabilità (*accountability*). Dopo un ampio periodo di sperimentazione con vari stakeholder, l'8 luglio 2020 l'AI HLEG ha pubblicato la *Assessment List for Trustworthy AI* (ALTAI)¹², uno strumento di autovalutazione che permette alle organizzazioni di confrontare i propri sistemi con i sette requisiti attraverso un questionario strutturato e una metodologia di valutazione. Entrambi i documenti sono volontari, pensati per promuovere standard etici condivisi pur senza pregiudicare il regime di responsabilità vincolante previsto dalle proposte legislative precedenti.

In particolare, per quanto qui interessa, il requisito dell'*accountability* sottolinea l'importanza di stabilire meccanismi chiari e trasparenti per garantire la responsabilità di chi sviluppa, distribuisce e utilizza i sistemi di IA. Esso richiede di mettere in atto strumenti che permettano di gestire i rischi, di monitorare e valutare le decisioni prese dall'IA, e di intervenire in caso di impatti ingiusti o dannosi. È fondamentale che i sistemi di IA siano soggetti a meccanismi di *audit*, interni ed esterni. La possibilità di condurre valutazioni e di accedere ai registri di tali valutazioni può contribuire a un'IA affidabile. In applicazioni che riguardano diritti fondamentali, inclusi sistemi critici per la sicurezza, i sistemi di IA dovrebbero poter essere sottoposti a *audit* indipendenti. Ciò non implica necessariamente che le informazioni sui modelli di business e sulla proprietà intellettuale legati al sistema di IA debbano essere sempre pubblicamente disponibili.

Inoltre, bisogna prevedere procedure di gestione del rischio, che consentano di riferire sulle azioni o decisioni che contribuiscono all'esito del sistema di IA, sia di rispondere alle conseguenze di tale esito. È fondamentale identificare, valutare, documentare e minimizzare i potenziali impatti negativi dei sistemi di IA, specialmente per coloro che sono (direttamente o indirettamente) coinvolti o colpiti. Deve essere garantita una protezione adeguata per *whistleblower*, ONG, sindacati o altri soggetti che segnalano legittimamente preoccupazioni riguardo a un sistema di IA.

Infine, in caso di eventi avversi, devono essere previsti a monte meccanismi accessibili che garantiscano un risarcimento adeguato.

¹² HIGH-LEVEL EXPERT GROUP ON AI (2020), *The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self Assessment*, <https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>.

4. Le principali problematiche sollevate dalla dottrina

Come prima anticipato¹³, il principale elemento di novità è rappresentato dal fatto che i sistemi di intelligenza artificiale sono dotati di autonomia decisionale e imprevedibilità dei risultati. In dottrina è stato dunque posto il tema del soggetto a cui attribuire la responsabilità giuridica in caso di danni cagionati dall'intelligenza artificiale. Si è in proposito indagata l'applicabilità delle norme sulla responsabilità civile e sulla responsabilità da prodotto difettoso.

Superata l'idea di attribuire una specifica soggettività giuridica ai robot, in secondo luogo, sono state evidenziate le difficoltà probatorie per il danneggiato. Da un lato, molteplici sono gli attori coinvolti (dal produttore, al fornitore, all'ideatore del programma, all'utilizzatore, etc.), per cui non è agevole identificare la causa del danno; dall'altro, la prova è ostacolata dalla maggiore autonomia di elaborazione dell'algoritmo, che sfugge al controllo del soggetto astrattamente responsabile. In generale, è stato ritenuto poco efficace tentare di applicare categorie e criteri di natura soggettiva, quali il dolo o la colpa, o la ricerca dell'errore *ex post*. Piuttosto, si è ritenuto più utile un modello fondato sulla responsabilità oggettiva e sull'allocazione *ex ante* del rischio. Principio cardine di quest'ultimo modello sarebbe l'*accountability*, che implicherebbe la preventiva responsabilizzazione del soggetto che trae vantaggio dall'uso del sistema di intelligenza artificiale e che sarebbe tenuto ad evitare il rischio adottando le misure più idonee a tale scopo, anche dandone la prova¹⁴.

Sulla disciplina in materia di responsabilità da prodotto difettoso, gli aspetti più problematici sinora sollevati riguardo all'adequatezza della Direttiva vigente¹⁵ rispetto al digitale interessano¹⁶: l'accostabilità dei sistemi di IA alla nozione di "prodotto"¹⁷; le difficoltà probatorie, per il danneggiato, relative alla difettosità del prodotto e al nesso di causalità tra difetto e danno; l'esclusione di responsabilità del produttore per difetti sopravvenuti, di cui all'art. 120, 2° co., Cod. Cons., che mal si concilierebbe con il carattere dinamico dei *device* in questione, a discapito dei soggetti danneggiati¹⁸; il danno cagionato da dispositivi di

¹³ Vedi *supra* il par. 2.

¹⁴ G. FINOCCHIARO, *Intelligenza artificiale e responsabilità*, cit.

¹⁵ Direttiva 85/374/CEE del Consiglio del 25 luglio 1985 relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati Membri in materia di responsabilità per danno da prodotti difettosi, OJ L 210, 7.8.1985, pp. 29–33.

¹⁶ Sul rapporto tra IA e disciplina in materia di responsabilità da prodotti difettosi, si veda, *ex multis*, A. AMIDEI, *Responsabilità da prodotto e intelligenza artificiale*, in U. RUFFOLO (a cura di), *XXVI Lezioni di diritto dell'intelligenza artificiale*, Torino: Giappichelli 2021, pp. 149–162.

¹⁷ La discussione trae origine dalle perplessità circa l'applicabilità della disciplina al software.

¹⁸ Il produttore potrebbe esimersi da responsabilità in tutti i casi in cui difetti si dovessero manifestare successivamente, per effetto dell'autoapprendimento del dispositivo.

per sé non difettosi ma potenzialmente lesivi per effetto dell'interazione con altri¹⁹.

5. L'approccio adottato con l'AI ACT

L'approccio *ex ante*, basato sulla preventiva valutazione del rischio e su relativi obblighi di conformità preventiva è quello adottato dal Regolamento (UE) 2024/1689 sull'Intelligenza artificiale (d'ora in avanti, *AI ACT*)²⁰. L'*AI ACT*, infatti, classifica i sistemi di IA in pratiche proibite, applicazioni ad alto rischio²¹, applicazioni a rischio limitato e minimo. I sistemi ad alto rischio sono soggetti a obblighi vincolanti *ex ante*, come valutazioni di conformità, analisi dell'impatto sui diritti fondamentali, documentazione tecnica e monitoraggio post-commercializzazione, mentre le applicazioni a rischio limitato devono rispettare solo requisiti di trasparenza.

L'approccio anzidetto risulta evidente in particolare dal considerando 79, il quale esplicita che «è opportuno che una specifica persona fisica o giuridica, definita come il fornitore, si assuma la responsabilità dell'immissione sul mercato o della messa in servizio di un sistema di IA ad alto rischio, a prescindere dal fatto che tale persona fisica o giuridica sia la persona che ha progettato o sviluppato il sistema». In altri termini, il soggetto che trae maggiore vantaggio dal sistema di IA deve essere anche quello che deve adottare tutte le misure necessarie per evitarlo o almeno attenuarlo, le quali nel Regolamento si sostanziano nell'assoggettamento a specifici obblighi²².

D'altro canto, tranne la previsione di sanzioni amministrative, l'*AI Act* non contiene disposizioni armonizzate sulla responsabilità civile, demandando la riforma della responsabilità a un'iniziativa legislativa separata²³.

¹⁹ Si pensi all'*Internet of Things*. Qui la nozione di prodotto è sfumata, essendo l'attività di questi strumenti accostabile anche a quella di servizio.

²⁰ Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) GU L 1689 del 12.7.2024, pp. 1-144. La recente Proposta di Omnibus Digitale sull'IA (COM(2025) 836 final del 19 novembre 2025) prevede di intervenire sull'*AI Act* con misure di semplificazione mirate.

²¹ Sul rapporto tra sistemi ad alto rischio e responsabilità, vedi C. BOMPRESZI, S. SAPIENZA, *Algorithmic Justice e la classificazione di rischio nella Proposta AI Act*, in M. PALMIRANI, S. SAPIENZA (a cura di), *La trasformazione digitale della giustizia nel dialogo tra discipline*, Milano: Giuffrè 2022, pp. 65-114.

²² D. CHIAPPINI, *Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell'Artificial Intelligence Act dell'Unione europea*, in *Rivista Italiana di Informatica e Diritto*, 2022 (II), pp. 95-108.

²³ European Parliament, *Artificial Intelligence and Civil Liability – A European perspective*, Luglio 2025, p. 20, [https://www.europarl.europa.eu/thinktank/en/document/IUST_STU\(2025\)77642](https://www.europarl.europa.eu/thinktank/en/document/IUST_STU(2025)77642).

6. Gli interventi legislativi delle istituzioni europee

Il primo intervento in tal senso delle istituzioni europee si rinviene nella succitata Risoluzione del 20 ottobre 2020²⁴, la quale, nel delineare una Proposta di Regolamento, ha optato per un modello di allocazione del rischio sul soggetto più vicino allo stesso (l'operatore) e che trae il maggior vantaggio dal sistema di IA. Secondo un approccio basato sull'*accountability*, questi è tenuto ad adottare le misure idonee ad evitarlo e a fornire la prova liberatoria. Nella Proposta di Regolamento allegata alla Risoluzione si distingue, poi, tra sistemi ad alto rischio, per cui si configura una responsabilità di tipo oggettivo, e altri sistemi di IA, assoggettati ad un regime di responsabilità per colpa (presunta, con onere della prova sull'operatore).

Più di recente, questa Proposta è stata superata dalla Commissione europea, la quale nel 2022 ha adottato una Proposta di Direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (d'ora in avanti, AILD), avente l'obiettivo di contribuire a ridurre gli ostacoli giuridici che le vittime debbono affrontare per poter ottenere il risarcimento di danni subiti per opera di sistemi di IA, in parte succitati²⁵. La Proposta ha introdotto infatti, limitatamente a regimi di responsabilità per colpa, una presunzione di causalità da far valere, a certe condizioni, circa il rapporto tra la colpa del convenuto e il comportamento del sistema di IA; inoltre, è stato previsto in favore del danneggiato un diritto di accesso alle prove da parte di aziende e fornitori nei casi di coinvolgimento di sistemi ad alto rischio.

Nel medesimo anno, la Commissione europea, contestualmente all'AILD, ha adottato altresì una Proposta di revisione della Direttiva sulla responsabilità per danno da prodotti difettosi²⁶ (d'ora in avanti, PLD); anche in tale contesto, viene alleggerito l'onere della prova per il danneggiato in ipotesi nuove, come quella di danni prodotti da sistemi di IA, con estensione di responsabilità per prodotti divenuti difettosi a causa di aggiornamenti (o mancati dovuti adeguamenti) dei software necessari a preservarne la sicurezza, e vengono imposte *disclosure of evidence* ai fabbricanti²⁷. La Proposta è stata approvata dando luogo al-

²⁴ Vedi *supra* par. 2.

²⁵ European Commission, Proposal for a Directive on adapting non contractual civil liability rules to artificial intelligence, https://ec.europa.eu/info/files/proposal-directive-adapting-non-contractual-civil-liability-rules-artificial-intelligence_en.

²⁶ European Commission, Proposal for a Directive of the European Parliament and of the Council on liability for defective products, https://single-market-economy.ec.europa.eu/document/3193da9a-cecb-44ad-9a9c-7b6b23220bcd_en

²⁷ https://ec.europa.eu/commission/presscorner/detail/it/ip_22_5807.

la Direttiva (UE) 2024/2853 (d'ora in avanti, *PLD Revised*, o *PLDr*)²⁸, la quale amplia la definizione di “prodotto” includendo anche prodotti digitali e software, e allarga il campo dei danni risarcibili, come quelli psicologici e ai dati (ad esempio, distruzione o danneggiamento). Inoltre, la *PLDr* chiarisce come valutare se un prodotto è difettoso, considerando anche aspetti come la capacità di apprendere o evolversi dopo l'acquisto (molto rilevante per l'intelligenza artificiale), l'interazione con altri dispositivi connessi e la conformità agli standard di cybersecurity. Un'altra novità importante è che i tribunali possono presumere che un prodotto sia difettoso o che il danno sia causato da un difetto, soprattutto se la prova risulta difficile a causa della complessità tecnica o scientifica. I produttori, inoltre, sono ora responsabili anche per i danni causati da vulnerabilità di cybersecurity, aumentando così i rischi di responsabilità in caso di attacchi informatici. La direttiva impone anche regole più stringenti per le piattaforme online. Gli Stati membri dell'UE hanno tempo fino al 9 dicembre 2026 per recepirla nelle leggi nazionali, e le nuove regole si applicheranno ai prodotti immessi sul mercato o messi in servizio dopo quella data. In sostanza, questa direttiva mira a rafforzare la protezione dei consumatori, adattando le norme alle nuove tecnologie e all'economia digitale, anche se questo comporterà sfide per le aziende, che dovranno aggiornare le proprie pratiche e affrontare maggiori rischi di responsabilità, specialmente in settori come quello farmaceutico e dei dispositivi medici, dove le tecnologie IA sono sempre più presenti.

7. Il ritiro dell'AILD e il cambio di approccio del legislatore europeo

La AILD, proposta nel 2022, avrebbe dovuto integrare i regimi nazionali con strumenti procedurali armonizzati, ma si è rivelata tecnicamente complessa, scarsamente efficiente e con applicabilità incerta. L'eccessivo affidamento sulle presunzioni e la difficoltà di coordinamento con i diversi sistemi nazionali ne hanno minato l'efficacia. La Commissione, nel 2025, ha annunciato l'intenzione di ritirare la proposta²⁹.

Quest'ultimo atto della Commissione europea ha di fatto confermato un cambio di approccio³⁰. Nel 2017, infatti, il Parlamento europeo individuava nella responsabilità civile il fulcro della governance giuridica dell'IA, proponendo

²⁸ Direttiva (UE) 2024/2853 del Parlamento europeo e del Consiglio del 23 ottobre 2024 sulla responsabilità per danno da prodotti difettosi, che abroga la Direttiva 85/374/CEE del Consiglio, GU L 2853 del 18.11.2024, pp. 1-22.

²⁹ https://commission.europa.eu/strategy-and-policy/strategy-documents/commission-work-programme/com-missionwork-programme-2025_en. Vedi Annex IV (List of intended withdrawals).

³⁰ Chiamato “*the great reversal*”. Vedi European Parliament, *Artificial Intelligence and Civil Liability*, cit.

un regime di responsabilità oggettiva per gli operatori di sistemi autonomi, affiancato da obblighi assicurativi e da un fondo di compensazione. Dal 2021, con l'avvento della Commissione von der Leyen, l'attenzione si è spostata su un approccio "*ex ante*", incentrato sull'*AI Act*, basato su valutazioni di rischio e obblighi di conformità preventiva, relegando la responsabilità civile a strumento secondario. La gerarchia per cui il principio di legge vincolante (*hard-law*) prevale sulla governance basata su norme non vincolanti (*soft-law*), è stata di fatto invertita, posponendo a data da destinarsi una riforma della responsabilità civile specifica per l'IA.

Indipendentemente dall'approccio scelto, e dalle diversità di opinioni circa la strategia migliore da intraprendere, occorre un'azione unitaria e uniforme dell'UE, che scongiuri i rischi derivanti dalla frammentazione normativa dei singoli Stati membri. In proposito, l'Italia ha già approvato la Legge 23 settembre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", in cui si affida al Governo la delega a adottare, entro dodici mesi dall'entrata in vigore della norma, uno o più decreti legislativi con riferimento anche ai casi di responsabilità civile (art. 24, co. 1)). In quest'ultimo caso, è prescritto che il Governo debba prevedere strumenti di tutela del danneggiato, anche attraverso una specifica regolamentazione dei criteri di ripartizione dell'onere della prova, tenuto conto della classificazione dei sistemi di intelligenza artificiale e dei relativi obblighi come individuati dall'*AI ACT* (art. 24, co. 5, lett. d)).