



Juridical Observatory on Digital Innovation  
Osservatorio Giuridico sulla Innovazione Digitale

## DIRITTO E NUOVE TECNOLOGIE\*

### Rubrica di aggiornamento dell'OGID.

*Questa rubrica di aggiornamento è curata dal Prof. Salvatore Orlando e dal Dott. Mario Mauro nell'ambito delle attività dell'OGID, Osservatorio Giuridico sulla Innovazione Digitale, costituito presso il Dipartimento di Diritto ed Economia delle Attività Produttive dell'Università di Roma "La Sapienza" (<https://web.uniroma1.it/deap/ogid-jodi.deap@uniroma1.it>).*

### SOMMARIO

1. [2025/2\(1\)SO](#) La politica di «dominio globale dell'America sull'intelligenza artificiale» per la promozione della «fioritura umana», la competitività economica e la sicurezza nazionale: l'ordine esecutivo del Presidente Trump n.14179 del 23.1.2025  *Rimuovere le barriere alla leadership americana nell'intelligenza artificiale* e la revoca dell'ordine esecutivo del Presidente Biden n. 14110 del 30.10.2023  *Sviluppo ed uso non pericoloso, sicuro e fidato dell'intelligenza artificiale* – **Salvatore Orlando**
2. [2025/2\(2\)DI](#) La futura politica europea di sovranità digitale annunciata dalla Commissione europea nella comunicazione *The AI Continent Action Plan* del 9 aprile 2025 e nel documento *An International Digital Strategy for the European Union* del 5 giugno 2025 – **Daniele Imbruglia**
3. [2025/2\(3\)MC](#) Il report di Amnesty International del febbraio 2025 sul "razzismo automatico" – **Michele Ciancimino**
4. [2025/2\(4\)TB](#) Le Q&A della Commissione europea sulla alfabetizzazione sulla IA ("AI literacy") del 7.5.2025 – **Timoteo Bucci**

\* Contributo non sottoposto a referaggio ai sensi dell'art. 2.2, lett. c), del Regolamento per la classificazione delle riviste nelle aree non bibliometriche, approvato con Delibera del Consiglio Direttivo n. 306 del 21.12.2023.

5. [2025/2\(5\)EMI](#) La proposta di regolamento COM(2025) 501 final del 21.5.2025 di modifica del GDPR per l'estensione alla (nuova) categoria delle «piccole imprese a media capitalizzazione» (*SMC enterprises*) di determinate misure di attenuazione disponibili per le PMI – **Enzo Maria Incutti**
6. [2025/2\(6\)GCr](#) L'ammonimento al rispetto della legislazione consumeristica inviato il 26.5.2025 a SHEIN dalla Commissione europea e dal Consumer Protection Cooperation Network delle autorità nazionali di vigilanza in materia di protezione dei consumatori – **Gabriele Crescente**
7. [2025/2\(7\)GD](#) Il parere dell'Avvocato Generale Kokott presso la Corte di giustizia depositato il 19.6.2025 sul ricorso contro la sentenza di condanna di oltre 4 miliardi di euro inflitta a Google e ad Alphabet nel 2022 per abuso di posizione dominante nella causa C-738/22 P (Google LLC, Alphabet Inc. contro Commissione europea) – **Giorgia Diotallevi**
8. [2025/2\(8\)BPo](#) Il JuLIA Handbook del maggio 2025 su IA e pubblica amministrazione – **Benedetto Ponti**
9. [2025/2\(9\)FDA](#) Il rapporto di AgID del 10 giugno 2025 sull'uso dell'intelligenza artificiale nelle amministrazioni centrali della PA – **Filippo D'Angelo**
10. [2025/2\(10\)MMar](#) L'ordine della Federal Trade Commission (FTC) degli Stati Uniti d'America del 28.4.2025 contro il sistema Workado che promette di individuare contenuti sintetici generati da sistemi di IA – **Mathilde Maré**
11. [2025/2\(11\)RR](#) Il documento del 7.3.2025 sui metodi per individuare i contenuti sintetici generati da sistemi di IA, predisposto dalle autorità della Repubblica Popolare Cinese – **Rachele Ranieri**
12. [2025/2\(12\)FR](#) La Parte 3 “Generative AI Training” del Report “Copyright and Artificial Intelligence”, pubblicata sul sito dello U.S. Copyright Office nella versione “pre-publication” datata maggio 2025 – **Francesca Rotolo**
13. [2025/2\(13\)EB](#) Le azioni avviate l'11.6.2025 da Disney e Universal in California (USA) contro Midjourney per violazione del copyright sui loro personaggi – **Emanuela Burgio**
14. [2025/2\(14\)MM](#) L'ordine di conservazione dei log di output impartito a Open AI il 13.5.2025 dalla corte distrettuale di New York nella causa intentata dal New York Times per violazione di copyright – **Matteo Mansi**



15. [2025/2\(15\)FG](#) Le delibere AGCOM n. 142/25/CONS del 13.6.2025 e n. 172/25/CONS del 3.7.2025 relative alla valutazione della rappresentatività degli organismi di gestione collettiva (OGC) e delle entità di gestione indipendenti (EGI) per il 2024 – **Francesco Grossi**
16. [2025/2\(16\)RA](#) I provvedimenti dell'AGCM del 11.6.2025 in materia di pratiche commerciali scorrette relativi a pratiche di “influencer marketing” realizzate da sei influencer – **Riccardo Alfonsi**
17. [2025/2\(17\)FGu](#) Il provvedimento dell'AGCM del 20.5.2025 contro Poste italiane per pratica scorretta sulle app Banco Posta e Postepay – **Francesco Gucci**
18. [2025/2\(18\)IG](#) Il provvedimento del Garante privacy italiano n. 232 del 10.4.2025 adottato nei confronti della società che gestisce il chatbot ‘Replika’ – **Ilaria Garaci**
19. [2025/2\(19\)EG](#) Il provvedimento del Garante privacy italiano n. 243 del 29.4.2025 nei confronti della Regione Lombardia in relazione ai metadati di posta elettronica e ai log di navigazione internet dei suoi dipendenti – **Elisa Grossi**
20. [2025/2\(20\)FN](#) La sentenza del TAR Lazio Sez. Prima n. 7625/2025 del 17.4.2025 di interpretazione dell'art. 52(7) Codice privacy sulla diffusione anche integrale del contenuto delle sentenze e degli altri provvedimenti giurisdizionali – **Federico Nespega**
21. [2025/2\(21\)SR](#) L'Ordinanza n. 1832/2025 della Corte di Cassazione: tutela del minore tra conflitto genitoriale e dipendenza tecnologica – **Samuele Rosa**
22. [2025/2\(22\)BG](#) I primi provvedimenti sull'uso improprio di ChatGPT nella redazione delle difese giudiziali (Trib. Firenze sez. imprese ordinanze del 14.3.2025 e del 2.5.2025) – **Beatrice Gallucci**

*Una raccolta indicizzata dei numeri della rubrica degli anni 2020-2023 è disponibile sull'[Atlante storico del diritto dei dati 2020-2023](#). Tutti i numeri della rubrica (compresi i numeri del 2024 e quelli del 2025 non ancora raccolti nell'Atlante) sono facilmente consultabili nella sezione [OGID](#) del sito web della Rivista.*



**2025/2(1)SO**

**La politica di «dominio globale dell’America sull’intelligenza artificiale» per la promozione della «fioritura umana», la competitività economica e la sicurezza nazionale: l’ordine esecutivo del Presidente Trump n.14179 del 23.1.2025 *Rimuovere le barriere alla leadership americana nell’intelligenza artificiale* e la revoca dell’ordine esecutivo del Presidente Biden n. 14110 del 30.10.2023 *Sviluppo ed uso non pericoloso, sicuro e fidato dell’intelligenza artificiale***

Con l’[Executive Order n. 14179](#) del 23 gennaio 2025 intitolato *Removing Barriers to American Leadership in Artificial Intelligence* (**EO 14179/2025** o l’**ordine di Trump**) il Presidente degli Stati Uniti d’America (gli **Stati Uniti**) Donald J. Trump ha dichiarato la nuova politica degli Stati Uniti sullo sviluppo e l’utilizzo di sistemi di intelligenza artificiale (**IA**), al contempo disponendo in merito alla revoca dell’[Executive Order n. 14110 del 30.10.2023](#) del suo predecessore Joe Biden, intitolato *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (**EO 14110/2023** o l’**ordine di Biden**).

Come già nell’ordine di Biden, anche nell’ordine di Trump (alla sezione 3) si precisa che la definizione di intelligenza artificiale contemplata nel medesimo ordine è quella contenuta nel numero 3 del paragrafo 9401 del titolo 15 dello United States Code (**U.S.C.**) “*The term «artificial intelligence» means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to— (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action*” (15 U.S.C., § 9401(3)).

Nella sezione 1 dell’ordine di Trump si dichiara, in funzione di premessa, che gli Stati Uniti sono da tempo in prima linea nell’innovazione dell’intelligenza artificiale (**IA**) guidati dalla forza dei liberi mercati, dallo spirito imprenditoriale e da istituti di ricerca all’avanguardia a livello mondiale. Si soggiunge quindi che, al fine di mantenere questa leadership, è necessario sviluppare **sistemi di IA** che siano «**liberi da bias ideologici o da agende sociali**» e che con le giuste politiche governative, è possibile consolidare la posizione degli Stati Uniti come «leader globale nell’IA e assicurare un futuro più luminoso a tutti gli americani». Si dichiara infine che, attraverso il medesimo ordine, **vengono revocate alcune politiche e direttive sull’IA** che «fungono da barriere all’innovazione americana della intelligenza artificiale, lasciando liberi gli Stati Uniti di agire decisamente al fine di mantenere la leadership globale nell’intelligenza artificiale».

Nella sezione 2 dell’ordine di Trump si definisce quindi la **politica degli Stati Uniti sull’intelligenza artificiale** nei seguenti termini: «la politica degli Stati Uniti è di **sostenere e rafforzare il dominio globale dell’America sull’IA**



**per promuovere la fioritura umana, la competitività economica e la sicurezza nazionale»** (*«It is the policy of the United States to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security»*).

Nell'ordine di Trump non vengono offerti chiarimenti sull'espressione «fioritura umana» (*human flourishing*). In alcuni programmi e corsi universitari ed in ambito scientifico, questa stessa espressione viene utilizzata con un significato tecnico per indicare determinati **stati mentali o psicofisici** di soddisfazione, felicità o eudaimonia, dei quali si istituiscono parametri e criteri di misurazione quantitativa (v. ad esempio, per l'americana Harvard <https://hfh.fas.harvard.edu/measuring-flourishing> e per l'italiana Unicampus <https://www.unicampus.it/human-flourishing-program/>).

Se l'espressione dovesse ritenersi utilizzata nell'ordine di Trump per esprimere davvero un significato tecnico di questo tipo, bisognerebbe concludere che è **una politica degli Stati Uniti promuovere sistemi di IA specificamente rivolti a provocare determinati risultati sugli stati mentali o psicofisici degli esseri umani**.

Nella sezione 4 dell'ordine di Trump si prevede che certi funzionari apicali ed organi dell'amministrazione debbano sviluppare e sottoporre al Presidente, entro 180 giorni dal medesimo ordine, un piano di azione per la realizzazione della politica definita nella sezione 2.

Infine, nella sezione 5 dell'ordine di Trump si dispone in merito alla revoca dell'ordine di Biden. In particolare, è disposta una delega operativa a certe funzioni ed organi dell'amministrazione per revocare specificamente, o sospendere ove possibile, nel caso in cui la revoca non sia giuridicamente possibile, ogni atto, azione o direttiva derivata dall'EO 14110/2023.

Con quest'ultimo ordine, il Presidente Biden aveva invece fissato una politica delineata intorno all'indirizzo di uno sviluppo e di un utilizzo sicuro e responsabile dei sistemi di IA (sezione 2, punti (a), (b) e (c) EO 14110/2023), alla promozione dell'equità e dei diritti civili (*equity and civil rights*) (sezione 2, punto (d) EO 14110/2023) al rispetto delle garanzie approntate dalla legislazione consumeristica (sezione 2, punto (e) EO 14110/2023), al rispetto della privacy e delle libertà civili (*civil liberties*) (sezione 2, punto (f) EO 14110/2023), alla gestione dei relativi rischi (sezione 2, punto (g) EO 14110/2023), e ad un concetto di leadership globale degli Stati Uniti sensibilmente diversa da quella espressa nell'Ordine di Trump: *“This leadership is not measured solely by the technological advancements our country makes. Effective leadership also means pioneering those systems and safeguards needed to deploy technology responsibly —and building and promoting those safeguards with the rest of the world. My Administration will engage with international allies and partners in developing a framework to manage AI's risks, unlock AI's potential for good, and promote common approaches to shared challenges. The Federal Government will seek to promote responsible AI safety and security principles and actions with other nations, including our competitors, while leading key global conversations and collaborations to ensure that AI benefits the whole world, rather than exacerbating inequities, threatening human rights, and causing other harms”* (sezione 2, punto (h) EO 14110/2023).

<https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/>  
<https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>

## 2025/2(2)DI

**La futura politica europea di sovranità digitale annunciata dalla Commissione europea nella comunicazione *The AI Continent Action Plan* del 9 aprile 2025 e nel documento *An International Digital Strategy for the European Union* del 5 giugno 2025**

Il 9 aprile 2025 è stata pubblicata la Comunicazione COM(2025) 165 final della Commissione europea (la **Commissione**) al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, dal titolo *The AI Continent Action Plan (Comunicazione AI Continent)*. La Comunicazione *AI Continent*, come altri documenti analoghi, fa riferimento alla necessità di una intelligenza artificiale (IA) affidabile e antropocentrica, quale elemento fondamentale per la crescita economica ed altresì essenziale per il rispetto dei diritti fondamentali. Il documento illustra le diverse azioni che la Commissione ritiene essere necessarie al fine di consentire all'Unione europea di diventare leader mondiale nel settore dell'intelligenza artificiale. Oltre che necessarie per raggiungere l'obiettivo (un continente leader nel settore dell'IA), le azioni indicate sono tese anche ad assicurare la competitività, la diversità culturale e i valori democratici dell'Unione europea.

Una volta definito l'obiettivo della leadership in materia di intelligenza artificiale, la Comunicazione *AI Continent* si mostra consapevole dei punti di forza della Unione europea (mercato unico; ricerca scientifica avanzata; migliaia di start-up e diffusa competenza industriale; elevata potenza di calcolo e spazi di dati accessibili), come dei punti critici e dei ritardi. In particolare, la Comunicazione *AI Continent* sottolinea come la **dipendenza da infrastrutture installate in paesi terzi e controllate da soggetti estranei alla Unione** sia un elemento di rischio e di preoccupazione per l'industria, per il mercato e per la pubblica amministrazione. In questo discorso, reso più urgente dall'attuale scenario geopolitico, si inserisce il richiamo a garantire la competitività e la **sovranità digitale europea**.

Per raggiungere l'obiettivo della leadership, la Comunicazione *AI Continent* individua cinque pilastri.

Il primo tema riguarda l'**infrastruttura di calcolo** e la istituzione di una rete di «**fabbriche di intelligenza artificiale**».

La Comunicazione *AI Continent* richiama l'esperienza positiva del CERN come modello di struttura che promuove la collaborazione scientifica in centri avanzati e finanziati dal pubblico e da privati. Nella Comunicazione *AI Continent* si legge che la **rete comune EuroHPC di supercomputer** possa

oggi contare su 13 fabbriche di IA e in 17 Stati membri e di un investimento pluriennale di oltre 10 miliardi. La Comunicazione *AI Continent* prevede che nel corso del 2025 verrà implementato uno sportello unico che consenta l'interazione all'utenza europea con le fabbriche di IA e si procederà ad avviare le procedure per la realizzazione di **supercomputer** da inserire nelle fabbriche di IA. Al fine di consentire l'accesso ai servizi offerti dalle fabbriche di IA all'industria, alla ricerca e alle amministrazioni pubbliche saranno altresì istituite le c.d. «**antenne delle fabbriche di IA**». Per raggiungere l'obiettivo di leadership nell'IA, la Comunicazione *AI Continent* illustra poi la necessità di affiancare alle fabbriche di IA le c.d. **gigafactory**, definite come strutture su vasta scala in grado di sviluppare e addestrare modelli di IA complessi a livelli senza precedenti, con centinaia di migliaia di miliardi di parametri. L'investimento necessario alla costruzione di simili centri è significativo e la Comunicazione *AI Continent* anticipa la possibilità di una partecipazione di soggetti privati e fondi istituzionali. La realizzazione di una rete di gigafactory è essenziale per consentire la progettazione e la produzione di processori di intelligenza artificiale all'interno dell'UE e per raggiungere la sovranità nell'ambito dei semiconduttori. In seno a questa prima azione, la Comunicazione *AI Continent* prevede per la fine del 2026 la revisione del regolamento sui chip – regolamento (UE) 2023/1781 - nonché, al fine di contrastare la dipendenza da centri di dati collocati all'esterno dallo spazio europeo, l'adozione di una **proposta di atto legislativo sullo sviluppo del cloud e dell'intelligenza artificiale**. Tale nuovo atto normativo darà maggiore certezza al mercato e dovrebbe consentire quantomeno triplicare la capacità dei centri dati dell'UE entro i prossimi cinque-sette anni e portarla a un livello che soddisfi le esigenze delle imprese e delle pubbliche amministrazioni dell'UE entro il 2035.

Il secondo tema contenuto nella Comunicazione *AI Continent* richiama la necessità di consentire l'accesso, la fornitura, la messa in comune e la condivisione di **dati di alta qualità**. A tal proposito, la Comunicazione *AI Continent* anticipa che **nel corso del 2025 vi sarà la pubblicazione di una strategia per l'Unione dei dati**. Consapevole delle criticità connesse alla presenza di dati scarsamente affidabili nel processo di addestramento e di convalida di modelli di IA, tale annunciato documento intende assicurare il miglioramento dell'interoperabilità e della disponibilità di dati di alta qualità. Sempre in questo orizzonte, la Comunicazione *AI Continent* introduce la figura dei **laboratori di dati** che, istituiti all'interno delle **fabbriche di IA**, avranno il compito di riunire e organizzare i dati provenienti da altre fabbriche. Anche rispetto a questo punto, la Comunicazione *AI Continent* annuncia che vi saranno delle conseguenze sul piano normativo. In particolare, si delinea una **razionalizzazione della normativa vigente in materia di dati** per ridurre la complessità e l'onere amministrativo e garantire che le strutture di governance dei dati siano efficienti ed efficaci, sulla base di un processo inclusivo che tenga conto della normativa applicabile in materia di diritti d'autore

Il terzo punto previsto dalla Comunicazione *AI Continent* attiene allo **sviluppo di algoritmi di intelligenza artificiale e alla connessa loro adozione per usi industriali, scientifici e delle pubbliche amministrazioni**.



Nell'introdurre tale processo di accelerazione – c.d. **strategia per l'IA applicata** – la Comunicazione *AI Continent* rileva come sia necessario accelerare l'adozione dell'IA nei vari settori, sia in quelli di dove l'UE detiene una forte leadership sia in settori come l'amministrazione sanitaria, la giustizia, l'istruzione e la pubblica amministrazione. In questa politica di diffusione dell'IA, un ruolo centrale lo avranno anche i **poli europei dell'innovazione digitale**, i quali diventeranno centri per l'esperienza per l'IA. Riprendendo l'esempio discusso nella Comunicazione *AI Continent*, si può pensare ad un'impresa che intende attuare un modello di previsione del consumo energetico basato sull'IA nell'ambito di un sistema di produzione esistente e che necessita di attività specifiche per la formazione e il miglioramento del livello delle competenze del personale. I poli europei dell'innovazione digitale possono offrire tali attività di formazione e sosterranno inoltre l'impresa fornendo percorsi di formazione chiari in funzione delle esigenze dei dipendenti.

Il quarto tema coinvolge l'**alfabetizzazione** e la **formazione di talenti** nel settore dell'intelligenza artificiale. Tale obiettivo richiede una maggiore capacità di attrarre ricercatori da paesi terzi, sia un impegno a sensibilizzare l'istruzione e la pubblica amministrazione attorno alle opportunità dell'intelligenza artificiale. Centrale in questo discorso che muove dall'importanza di una maggiore educazione in tema di IA è il **sostegno a percorsi universitari specialistici nonché l'istituzione di una Accademia per le competenze in materia di IA**, ossia uno sportello unico che offrirà istruzione e formazione sulle competenze relative allo sviluppo e alla diffusione dell'IA.

La quinta azione richiamata nella Comunicazione *AI Continent* suggerisce invece di aumentare le opportunità connesse al mercato unico e al quadro normativo chiaro e tendenzialmente uniforme. In particolare, la Comunicazione *AI Continent* richiede di **modulare e graduare l'AI Act** – regolamento (UE) 2024/1689 - **in relazione alle dimensioni dei soggetti interessati**. Innanzitutto, la Comunicazione *AI Continent* informa circa lo **sportello di servizio per il regolamento sull'IA**, che costituirà un polo d'informazione centrale per il regolamento sull'IA, consentendo ai portatori di interessi di chiedere aiuto e ricevere risposte, pratiche e che aiuteranno a comprendere e rispettare il regolamento. Inoltre, la Comunicazione *AI Continent* afferma che la Commissione, a partire dagli insegnamenti tratti durante l'attuale fase di attuazione, individuerà ulteriori misure necessarie per facilitare un'applicazione agevole, snella e semplice del regolamento sull'IA, in particolare per le imprese di minori dimensioni.

L'insieme delle varie politiche verrà perseguito da tutti i soggetti istituzionali dell'Unione nonché dai Paesi membri. La Comunicazione *AI Continent* è altresì consapevole che sia fondamentale collaborare con Paesi e istituzioni terzi.

Tale collaborazione e, più in generale, la dimensione internazionale delle politiche digitali dell'UE hanno formato oggetto del **documento dello scorso 5 giugno 2025, *An International Digital Strategy for the European Union***. Quest'ultimo testo, prodotto dalla Commissione e dall'Alto rappresentante dell'UE per gli affari esteri e la politica di sicurezza, conferma l'aspirazione

dell'Unione a porsi come leader nell'IA, rafforzando partenariati esistenti e attivandone di nuovi e individuando cinque aree prioritarie di cooperazione: **tecnologie emergenti; infrastrutture; sicurezza informatica; piattaforme online**. Come la Comunicazione *AI Continent*, anche *An International Digital Strategy for the European Union* intende rafforzare la competitività europea, la promozione della **sovranità digitale e tecnologica** e la protezione e la promozione dei suoi valori e interessi.

La cooperazione dell'UE con questi altri soggetti terzi non dovrebbe però avvenire a tutti i costi: la citata dichiarazione conferma l'impegno a definire norme e standard in base a valori comuni basati sui diritti umani.

DANIELE IMBRUGLIA

[AI Continent Action Plan](#)  
[The International Digital Strategy for the European Union](#)

### 2025/2(3)MC

#### Il report di Amnesty International del febbraio 2025 sul “razzismo automatico”

Nel suo Rapporto pubblicato nel febbraio 2025, *Automated Racism: How police data and algorithms code discrimination into policing*, Amnesty International UK affronta il fenomeno dell'uso delle tecnologie predittive da parte delle forze di polizia del Regno Unito. Il documento, frutto di un'indagine estesa svolta tra ottobre 2022 e novembre 2024, lancia un'accusa netta contro la neutralità algoritmica. Esso, infatti, denuncia come i sistemi algoritmici applicati alla prevenzione e al controllo del crimine stiano perpetuando dinamiche discriminatorie in violazione dei diritti fondamentali, rafforzando in particolare gli effetti del 'razzismo istituzionale' già radicato nel sistema di giustizia penale britannico.

L'indagine è stata svolta sulla base di molteplici richieste di accesso agli atti della polizia del Regno Unito, interviste sul campo a soggetti a rischio, ma anche ad esperti e accademici competenti in materia. Specifica il Report che diverse richieste di intervista sono state inoltrate a forze di polizia locali (Essex Police, Metropolitan Police o West Midlands Police), ma senza ricevere alcun riscontro effettivo.

Il Rapporto di Amnesty International si inserisce in un più ampio dibattito internazionale sulla liceità e legittimità dell'utilizzo dell'intelligenza artificiale e dei big data nel settore della sicurezza nazionale. Non a caso, la tematica è inquadrata sotto l'angolo visuale dei diritti umani rispetto all'ordinamento britannico e alla luce del diritto internazionale, ma sono richiamate anche esperienze proprie di altri ordinamenti (fra cui il noto sistema COMPAS) che hanno prodotto effetti altrettanto discriminatori e che sono state progressivamente abbandonate in molte giurisdizioni per effetto delle pressioni esercitate dalla società civile.

Il Rapporto prende le mosse dalla constatazione che circa tre quarti delle forze di polizia del Regno Unito impiegano strumenti di profilazione predittiva per

individuare aree considerate a rischio di criminalità, nell’ottica di prevedere dove potrebbero verificarsi dei reati, o per valutare la probabilità che specifici individui possano anche soltanto rischiare di commettere reati. Questi strumenti, che rientrano nell’ambito più ampio del cosiddetto *predictive policing*, si fondano su dataset generati a partire da dati provenienti dall’attività della stessa polizia, i quali sembrano però riflettere bias e pregiudizi discriminatori, prevalentemente razziali (secondo quanto riferito dal Rapporto), di lunga data: si evidenzia, ad esempio, che “*areas with high populations of Black and racialised people are repeatedly targeted by police and therefore crop up in those same police records*”. L’algoritmo, nutrendosi di tali dati, produce così previsioni che rafforzano e legittimano l’intensificazione della sorveglianza proprio in quelle stesse comunità già precedentemente iper-pattugliate, creando un circolo vizioso di controllo, sospetto e criminalizzazione.

Il Rapporto distingue tra due tipologie principali di sistemi predittivi: quelli a base geografica (*geographic predictive policing systems*), e quelli individuali (*individual predictive policing, profiling, and risk assessment systems*), mirati alla valutazione del rischio di recidiva o di possibile commissione di reati da parte di soggetti specifici.

Appartengono al primo gruppo i sistemi in grado di ‘predire’ se un crimine si verificherà in un dato luogo, identificare le zone ad alto rischio di reati (c.dd. “hotspot” criminali), e sono usati per gestire e coordinare le attività di pattugliamento e individuare le aree dove svolgere attività di indagine preventiva.

Nell’ambito del secondo gruppo, invece, si collocano i sistemi impiegati per valutare la probabilità o il rischio di recidiva di specifici soggetti, di cui le forze di polizia del Regno Unito talora si servono per assegnare a determinati individui una percentuale di rischio criminale, così da orientare le attività di monitoraggio dei singoli. Tali analisi predittive, peraltro, risultano essere condivise con pubbliche amministrazioni legate al settore della giustizia, ma non solo: queste valutazioni del rischio, infatti, sono anche messe a disposizione di enti previdenziali e locali, potendo così incidere negativamente sul diritto dei singoli ad accedere a prestazioni di welfare di varia natura.

Entrambe le categorie risultano profondamente problematiche dal punto di vista dei diritti umani, sia per la scarsità di trasparenza che ne accompagna l’adozione, sia per l’inadeguatezza dei meccanismi di controllo democratico e di tutela giurisdizionale.

L’approccio adottato, secondo Amnesty International, pone in essere una vera e propria “sorveglianza di massa” che non soltanto viola il principio di non discriminazione, ma mina le fondamenta dello Stato di diritto: il principio di legalità, la proporzionalità, la trasparenza, la presunzione di innocenza, il diritto a un giusto processo, la libertà di associazione e di espressione, nonché il diritto alla privacy risultano tutti compromessi. In particolare, le persone appartenenti a comunità razzializzate e residenti in aree socio-economicamente svantaggiate vengono sistematicamente profilate come “a rischio”, subendo una sorveglianza preventiva che si traduce in fermi,

controlli e potenzialmente anche in esclusioni dall'accesso a servizi essenziali come l'assistenza sociale, l'istruzione o l'impiego.

Ciò comporta, anzitutto, una compromissione della presunzione di innocenza, in virtù dell'attività di profilazione posta in essere che, nella misura in cui frutto di inferenze algoritmiche distorte, influenza, prima, l'attività di prevenzione della polizia e, poi, mette a rischio la neutralità delle conseguenti decisioni giudiziarie. Peraltro, poiché le decisioni algoritmiche di tali sistemi risultano essere spesso condivise con altri servizi pubblici, si riscontra un effetto di rinforzo dei pregiudizi discriminatori, con conseguente danno ingiustamente patito dai soggetti sottoposti a valutazione, in grado di generare effetti significativi sulle libertà fondamentali anche al di fuori del contesto penale.

L'indagine rivela come, in molti casi, le persone coinvolte non siano nemmeno consapevoli di essere state profilate né abbiano accesso ad alcun mezzo effettivo per contestare l'etichettatura ricevuta. Il principio di legalità risulta in tal modo svuotato di significato, poiché l'opacità delle procedure impedisce al cittadino di conoscere e, se del caso, di modificare la propria condotta in modo da evitare l'intervento coercitivo dello Stato. Si spiega, infatti, nel rapporto che i cittadini non sono realmente a conoscenza dell'uso di tali sistemi di polizia predittiva, non sono in grado di comprendere in che termini possono essere o essere state oggetto delle relative analisi né sanno come poter contestare tali valutazioni, compromettendo così l'effettività delle tutele.

L'analisi si arricchisce di numerosi esempi concreti tratti da forze di polizia locali che illustrano il funzionamento dei sistemi predittivi, l'uso distorto dei dati, le conseguenze discriminatorie e l'impatto devastante sulle comunità coinvolte. Amnesty International documenta inoltre le difficoltà incontrate nell'ottenere informazioni tramite richieste di accesso documentale, a riprova della mancanza di trasparenza strutturale che caratterizza l'intero comparto. In una prospettiva rimediabile, il Rapporto evidenzia l'assenza di chiari o sufficienti meccanismi di tutela collettiva avverso le ipotesi di profilazione razziale predette, in violazione degli standard internazionali, così come la ridotta efficacia dei rimedi contro il trattamento illecito dei dati personali posto in essere da detti sistemi. Vengono, quindi, tratteggiate alcune possibili tutele, più o meno soddisfattorie, azionabili dinanzi all'Independent Office for Policy Conduct, all'Information Commissioner's Office (ICO) e all'Equality and Human Rights Commission.

Sulla base di tale scenario, Amnesty International formula raccomandazioni nette: Amnesty International propone, in definitiva, l'introduzione di un divieto assoluto di utilizzo di strumenti predittivi, sia geografici che individuali, nel settore della giustizia penale.

Tale proposta, nella sostanza già avanzata da Amnesty International in sede europea nel contesto del negoziato sull'AI Act, si accompagna a richieste di maggiore trasparenza e di garanzie effettive di tutela giurisdizionale per le persone impattate da queste tecnologie: viene, quindi, evidenziata la necessità, da un lato, di prevedere meccanismi di trasparenza e di spiegazione del processo decisionale predittivo, particolarmente con riguardo alle attività di profilazione e valutazione del rischio e, dall'altro, di introdurre espresse

procedure di opposizione-contestazione avverso le decisioni adottate in forza di tali sistemi algoritmici. L'organizzazione suggerisce, inoltre, l'istituzione di un registro pubblico obbligatorio che documenti l'uso, i dati impiegati, gli algoritmi applicati e le finalità perseguite da tali strumenti.

In conclusione, il Rapporto induce a interrogarsi criticamente sul futuro della relazione tra tecnologia, potere e giustizia. L'apparente neutralità dell'algoritmo si rivela, in realtà, profondamente ideologica e rischia di legittimare, in forme nuove e più insidiose, pratiche di controllo sociale profondamente ingiuste. Si riscontra, dunque, la sempre viva esigenza di un efficace bilanciamento fra istanze fondamentali, con riguardo, in tale contesto, alla necessità di una prevenzione della criminalità che, pur giovandosi dei benefici delle nuove tecnologie, si realizzi nel pieno rispetto della dignità umana. In gioco non è soltanto l'equilibrio tra sicurezza e libertà, ma la credibilità stessa dello Stato democratico nella tutela dei diritti fondamentali.

MICHELE CIANCIMINO

<https://www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20UK%20-%202025.pdf?VersionId=JqCcTODw37yAXyINmAY6uAzrKEWucFF7>  
<https://www.amnesty.org.uk/predictive-policing>

#### 2025/2(4)TB

#### Le Q&A della Commissione europea sulla alfabetizzazione sulla IA (“AI literacy”) del 7.5.2025

Il 7 maggio 2025 la Commissione europea (la **Commissione**) ha pubblicato una serie di domande e risposte (**Q&A**) in tema di alfabetizzazione sull'intelligenza artificiale (**AI literacy**, **AI**), al fine di fornire agli operatori indicazioni utili per conformarsi agli obblighi previsti a tal riguardo dal regolamento (UE) 2024/1689 sull'intelligenza artificiale (**AI Act**).

L'art. 4 dell'AI Act impone infatti ai fornitori e ai deployer di sistemi di AI (come ivi definiti) di assicurare che il loro “personale” nonché “qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto” sia dotato di un adeguato livello di alfabetizzazione in materia di AI, vale a dire l'insieme de “le competenze, le conoscenze e la comprensione che consentono ai fornitori, ai deployer e alle persone interessate, tenendo conto dei loro rispettivi diritti ed obblighi ai sensi [dell'AI Act] di procedere ad una diffusione informata dei sistemi di AI, nonché di acquisire consapevolezza in merito alle opportunità ed i rischi dell'AI e dei possibili danni che essa può causare (definizione di “AI literacy” di cui all'art. 3, n.56 dell'AI Act)

Nelle Q&A, la Commissione ha in primo luogo specificato che per “soggetti che utilizzano i sistemi di AI per conto di fornitori e deployer” si intendono le persone che non sono dipendenti, ma comunque operano a più ampio



raggio nella cerchia di una determinata organizzazione, come ad esempio appaltatori, fornitori di servizi o clienti.

Questi soggetti ed i dipendenti (il “personale”) dovranno essere formati in considerazione delle loro specifiche abilità, delle loro mansioni e delle caratteristiche della loro organizzazione, secondo un approccio basato sul rischio già tipico del GDPR e di altre normative di matrice europea.

Dovranno quindi aversi iniziative formative a diversi livelli di dettaglio, progettate in base al livello di esperienza e conoscenza dei destinatari. Sotto questo profilo, la Commissione precisa che soggetti con un titolo di studio o esperienza nello sviluppo di AI possono in linea di principio considerarsi alfabetizzati, ma che occorrerà una verifica caso per caso in relazione al sistema di AI di volta in volta rilevante ed alle specifiche qualifiche dei soggetti in questione.

Ancora, le iniziative di alfabetizzazione potranno essere basate sugli specifici rischi connessi ad un determinato sistema - come il rischio di c.d. “allucinazione” per ChatGPT - o sulla classificazione dei sistemi utilizzati: ad esempio, per i sistemi che si classificano tra quelli ad alto rischio, le organizzazioni dovrebbero adottare misure rinforzate per assicurare che i dipendenti siano consapevoli delle modalità di utilizzo di tali sistemi e dei rischi correlati. Su questo punto, la Commissione ha anticipato che emanerà delle Linee guida sugli obblighi di cui agli articoli da 8 a 15 e 25 dell’AI Act, che includeranno indicazioni in materia di alfabetizzazione.

Ciò premesso, le Q&A precisano che il livello di conoscenza dei dipendenti non è soggetto ad un metodo di misurazione specifico, né vi sono requisiti particolari previsti in relazione a specifici settori.

Tuttavia, indicazioni rilevanti possono essere rinvenute nelle Linee guida sulla definizione dei sistemi di AI pubblicate dalla Commissione in data 2 febbraio 2025 (su cui v. in questa Rubrica la notizia n. 3 del [numero 1/2025 \[2025/1\(3\)RA\]](#)), così come nel living repository in cui l’AI Office ha raccolto le pratiche di alfabetizzazione già attuate da una serie di stakeholder virtuosi - destinate a fungere da “fonte di ispirazione” - e che sarà continuamente aggiornato (su cui v. in questa Rubrica la notizia n. 7 del [numero 1/2025 \[2025/1\(7\)TB\]](#)). Sotto questo profilo, giova precisare che – come chiarito in più occasioni dalla Commissione - l’adozione delle pratiche censite nel living repository non può garantire di per sé sola la conformità agli obblighi di cui all’art. 4 dell’AI Act.

In ogni caso, l’AI Office non imporrà requisiti stringenti ma – al contrario – garantirà un certo margine di flessibilità, anche in considerazione della velocità di evoluzione delle tecnologie AI. Ciononostante, secondo la Commissione, in un’ottica di compliance con l’art. 4 dell’AI Act, le organizzazioni dovrebbero rispettare almeno i seguenti requisiti minimi:

- a) Assicurare una comprensione generale dell’AI nell’organizzazione;
- b) Considerare il ruolo dell’organizzazione (fornitore o deployer);
- c) Considerare il rischio dei sistemi di AI forniti o utilizzati e di quanto previsto ai fini della sua mitigazione;
- d) Pianificare azioni di alfabetizzazione sulla base delle precedenti analisi, considerando le differenze di conoscenza tecniche, le esperienze,

l'educazione e la formazione dello staff, nonché il contesto in cui i sistemi di AI vengono utilizzati ed i relativi scopi.

Per quanto concerne l'*accountability* delle organizzazioni in relazione alle iniziative di alfabetizzazione, la Commissione chiarisce che non vi è necessità di erogare certificati specifici ai destinatari delle stesse, ma che le organizzazioni possono tenere dei registri interni delle attività erogate.

Con riguardo alla coercibilità degli obblighi in questione (entrati in vigore il **2 febbraio 2025**), le Q&A specificano che le norme di supervisione ed enforcement troveranno applicazione soltanto dal **3 agosto 2026**.

Quanto al campo di applicazione territoriale, le Q&A precisano che le norme dell'AI Act – comprese quelle in materia di alfabetizzazione – si applicano ad attori pubblici e privati all'interno e al di fuori dell'UE, fintanto che il sistema è immesso sul mercato e/o utilizzato nell'UE e/o "il suo utilizzo ha un impatto sulle persone" localizzate all'interno dell'UE.

L'attività di supervisione sarà di competenza delle autorità di *market surveillance* che gli Stati membri sono chiamati a designare entro il **2 agosto 2025**. Entro tale data gli Stati membri dovranno altresì individuare le misure sanzionatorie secondo criteri di proporzionalità.

Da ultimo, le Q&A menzionano un network composto da varie *European Digital Innovation Hubs* che le piccole e medie imprese (PMI) possono contattare per ottenere supporto in materia di AI e digitalizzazione, e forniscono una serie di link per accedere a materiale formativo ed informativo in tema di alfabetizzazione in materia di AI, destinato sia ai cittadini in generale, sia a professionisti dell'educazione.

TIMOTEO BUCCI

<https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers>

### 2025/2(5)EMI

**La proposta di regolamento COM(2025) 501 final del 21.5.2025 di modifica del GDPR per l'estensione alla (nuova) categoria delle «piccole imprese a media capitalizzazione» (SMC enterprises) di determinate misure di attenuazione disponibili per le PMI**

Il 21 maggio 2025, la Commissione europea ha pubblicato un pacchetto di proposte, il c.d. pacchetto *Omnibus IV*, volto a sostenere la competitività e la crescita delle imprese europee.

Tra i vari interventi auspicati, il pacchetto contiene anche la proposta di regolamento COM(2025) 501final di modifica del GDPR e di altri regolamenti dell'Unione europea relativamente a certe misure di semplificazione disponibili per le piccole e medie imprese (la **Proposta**).

Nella relazione illustrativa della Proposta, si spiega che essa risponde al programma "Legiferare meglio" della Commissione europea (*Legiferare meglio: unire le forze per produrre leggi migliori* ([COM\(2021\) 219 final](#)) volto a sostenere la competitività delle imprese europee. Vi si legge altresì che la Proposta ha attinto, quanto alle sue motivazioni, alla relazione di Mario

Draghi del settembre 2024: [The future of European competitiveness](#), e alla relazione di Enrico Letta dell'aprile 2024: [Much more than a market](#).

In particolare, nella relazione illustrativa della Proposta si ricorda che nel citato rapporto, Mario Draghi sostiene che le normative dell'UE impongono un onere proporzionalmente più elevato per le piccole e medie imprese (PMI) e le piccole imprese a media capitalizzazione rispetto a quello imposto alle imprese più grandi. La relazione illustrativa ricorda altresì che, nel medesimo rapporto, Mario Draghi suggeriva alla Commissione europea di estendere alle piccole imprese a media capitalizzazione le misure di attenuazione esistenti per le PMI, contestualmente rilevando che l'UE non dispone di una definizione concordata di piccola impresa a media capitalizzazione e di dati statistici prontamente disponibili.

Quanto alla sopra citata relazione di Enrico Letta, nella relazione illustrativa della Proposta si ricorda che proprio in tale rapporto era stata sostenuta l'idea di operare una distinzione di trattamento giuridico tra imprese a media capitalizzazione e grandi imprese promuovendo la crescita e una partecipazione equa delle imprese a media capitalizzazione al mercato unico, consentendo così a tali imprese di contribuire al completamento del mercato unico e al suo miglior funzionamento.

La Proposta è così rivolta alle piccole e medie imprese (PMI) e mira ad introdurre la nuova categoria autonoma di “*small mid-cap enterprises*” (SMC), ovvero «piccole imprese a media capitalizzazione». L'obiettivo è quello di supportare l'innovazione tecnologica e l'occupazione attraverso un processo di semplificazione degli oneri in capo a queste tipologie di imprese. L'articolo 1 della Proposta introduce modifiche al Regolamento (UE) 2016/679 (GDPR). Nello specifico, si propone l'introduzione di due nuove definizioni all'art. 4 del GDPR: al punto 27) la nozione di “*microimpresa, piccole e medie imprese*“, ovvero le imprese disciplinate dall'art. 2 dell'allegato alla Raccomandazione 2003/361/CE della Commissione; e al punto 28) la definizione di “*piccole imprese a media capitalizzazione*“, categoria definita con una nuova raccomandazione *ad hoc* della Commissione europea, coeva alla Proposta: la [Raccomandazione \(UE\) 2025/1099](#) della Commissione del 21.5.2025, relativa alla definizione delle piccole imprese a media capitalizzazione.

Si propone, inoltre, la modifica del par. 5 dell'art. 30 GDPR in merito al registro delle attività di trattamento. La vigente disciplina prevede, a determinate condizioni, l'esenzione dall'obbligo di tenuta del registro per le imprese con meno di 250 dipendenti. La proposta, invece, mira a ampliare l'ambito applicativo dell'eccezione, estendendolo alle “imprese o organizzazioni” con meno di 750 dipendenti, salvo che il trattamento impiegato non possa generare un rischio elevato per i diritti e le libertà degli interessati *ex art. 35* GDPR.

In relazione ai codici di condotta, invece, si prevede la modifica del par. 1 dell'art. 40 del GDPR sostituito con un nuovo paragrafo che include anche le piccole imprese a media capitalizzazione. L'attuale disposizione dell'art. 40 («Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità



dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese») viene così integrata con l'estensione del suo campo applicativo alle c.d. “*small mid-cap enterprises*”.

Stessa *ratio* e stessa modalità di intervento nella modifica proposta all'art. 42 GDPR relativo ai meccanismi di certificazione della protezione dei dati. Anche in questo caso, l'attuale formulazione («Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese») è modificata dall'inserimento del riferimento alle “*small mid-cap enterprises*”.

Il 9 luglio 2025, il Comitato europeo per la protezione dei dati (EDPB) e il Garante europeo della protezione dei dati personali (EDPS) hanno pubblicato un [parere congiunto](#) sulla proposta di regolamento. Il parere si dimostra favorevole verso le misure di semplificazione proposte ma domanda attenzione su alcuni profili della riforma. In particolare, si ritiene che l'estensione dell'eccezione *ex art. 30*, interessando diversi settori disciplinati da normative tra loro interconnesse, andrebbe adeguatamente motivata, considerando in particolare che, per questa disposizione, la Proposta non utilizza le categorie di piccole e medie imprese e di piccole imprese a media capitalizzazione. Infine, nel loro parere congiunto, l'EDPB e l'EDPS chiedono di specificare nel nuovo testo dell'art. 30 GDPR di cui alla Proposta, che la parola “organizzazioni” non comprende autorità e organi pubblici.

ENZO MARIA INCUTTI

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0501>  
[https://www.edpb.europa.eu/news/news/2025/targeted-modifications-gdpr-edpb-edps-welcome-simplification-record-keeping\\_en](https://www.edpb.europa.eu/news/news/2025/targeted-modifications-gdpr-edpb-edps-welcome-simplification-record-keeping_en)

### 2025/2(6)GCr

**L'ammonimento al rispetto della legislazione consumeristica inviato il 26.5.2025 a SHEIN dalla Commissione europea e dal Consumer Protection Cooperation Network delle autorità nazionali di vigilanza in materia di protezione dei consumatori**

Il 26 maggio 2025 è stato diramato sul sito istituzionale della Commissione europea (la **Commissione**) un comunicato stampa relativo all'avvio di un'azione congiunta nei confronti della piattaforma di e-commerce SHEIN. Più nello specifico, la Consumer Protection Cooperation Network (**CPC**) - rete di cooperazione tra le Autorità nazionali competenti, istituita dal Regolamento (CE) n. 2006/2004 sulla cooperazione per la tutela dei consumatori - unitamente alla Commissione, hanno notificato a SHEIN un ammonimento formale relativo ad una serie di pratiche ritenute in violazione

della normativa europea in materia di protezione dei consumatori. In aggiunta, le Autorità procedenti hanno intimato all'operatore economico il rispetto della disciplina consumeristica europea vigente.

Occorre preliminarmente rilevare che il 26 aprile 2024 la Commissione aveva conferito a SHEIN la qualifica di Very Large Online Platform (VLOP), ai sensi del regolamento (UE) 2022/2065 (**Digital Services Act** o **DSA**), in considerazione del superamento della soglia dei 45 milioni di utenti attivi mensili, prevista dal medesimo regolamento quale criterio per la designazione delle piattaforme online di grandi dimensioni (v. in questa Rubrica, notizia n. 11 del [numero 2/2024](#) [2024/2(11)RA]).

Suddetto riconoscimento comporta l'assoggettamento ad un regime normativo maggiormente gravoso, richiedendo l'implementazione di strategie mirate a garantire la sicurezza dei fruitori dei servizi online, la responsabilizzazione degli stessi nell'ambiente digitale, nonché l'onere di procedere ad un'attenta valutazione e al contenimento dei pericoli di natura sistemica eventualmente generati dalle attività di servizio.

Nel caso di specie - nel quadro del predetto procedimento - le pratiche oggetto di contestazione riguardano, in primo luogo, la condotta fraudolenta relativa a sconti ingannevoli ossia riduzioni di prezzo non ancorate all'effettivo "*prior price*" (il prezzo precedentemente applicato).

Si osserva, invero, come la direttiva 2000/31/CE sul commercio elettronico preveda all'art. 6 lett. c) che "le offerte promozionali, come ribassi, premi od omaggi, qualora permesse dallo Stato membro in cui è stabilito il prestatore, devono essere chiaramente identificabili come tali".

Inoltre, la direttiva 98/6/CE - relativa all'indicazione dei prezzi sui prodotti di consumo - all'art. 6-*bis*, così come modificato dalla più recente direttiva (UE) 2019/2161, dispone che "Ogni annuncio di riduzione di un prezzo deve indicare il prezzo precedente applicato dal professionista per un determinato periodo di tempo prima dell'applicazione di tale riduzione", specificando poi che "per prezzo precedente si intende il prezzo più basso applicato dal professionista durante un periodo di tempo non inferiore a 30 giorni prima dell'applicazione della riduzione del prezzo".

Viepiù, la direttiva 2005/29/CE sulle pratiche commerciali sleali - nella Sezione 1) rubricata "Pratiche commerciali ingannevoli" - all'art. 7 (omissioni ingannevoli), paragrafo 4, lett. c), qualifica come attività di vendita ingannevole quella che, per la natura del prodotto, renda impossibile l'identificazione dei criteri di calcolo del prezzo, compresi i costi accessori relativi a spedizione, consegna o servizi postali ovvero qualora la determinazione preventiva di tali spese non sia ragionevolmente praticabile.

Un'ulteriore pratica oggetto di contestazione concerne la c.d. "*pressure selling*" ossia l'induzione all'acquisto tempestivo mediante l'imposizione di fittizie scadenze d'acquisto.

L'art. 8 della summenzionata direttiva 2005/29/CE, rubricato "Pratiche commerciali aggressive", tra le altre, definisce condotta aggressiva quella che "tenuto conto di tutte le caratteristiche e circostanze del caso, mediante [...] indebito condizionamento, limiti o sia idonea a limitare considerevolmente la libertà di scelta o di comportamento del consumatore medio in relazione al

prodotto e, pertanto, lo induca o sia idonea ad indurlo ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso”.

Ed ancora, all’Allegato 1) è definita “pratica commerciale sleale” la condotta del prestatore che miri a far credere, in modo ingannevole, che il prodotto potrà essere acquistato per un tempo limitato o che sarà disponibile solo a condizioni particolari, per una finestra temporale estremamente limitata, al fine di determinare una scelta d’acquisto immediata, compromettendo così il diritto del consumatore a un’adeguata valutazione dell’offerta ovvero privando quest’ultimo del tempo minimo necessario ai fini di una scelta consapevole.

Nel quadro degli accertamenti, posti in essere dalle Autorità preposte, è emersa, altresì, una prassi caratterizzata da insufficiente trasparenza informativa, consistente nella presentazione da parte di SHEIN di informazioni incomplete, fuorvianti e inesatte riguardo ai diritti di reso e di rimborso del consumatore, nonché nella mancata corretta esecuzione delle relative procedure.

Si rileva, infatti, che nella direttiva 2011/83/UE sui diritti dei consumatori nel Capo III, all’art. 6 rubricato “Obblighi di informazione per i contratti a distanza e per i contratti negoziati fuori dei locali commerciali”, lett. h), è espressamente indicato che, ove sia previsto, il professionista deve informare il consumatore sulle condizioni, i termini e le procedure per l’esercizio del diritto di recesso.

Inoltre, ai sensi del già menzionato art. 7 della Direttiva 2005/29/CE, ed in particolare della lettera e), si evidenzia che, nell’ambito di un “invito all’acquisto” – quale si configura la vendita online – riveste particolare importanza la comunicazione chiara e trasparente circa l’esistenza del diritto di recesso o di risoluzione del contratto, ove previsto dalla normativa applicabile.

Inoltre, rientrano – tra le condotte contestate all’azienda e suscettibili di incidere negativamente sui diritti dei consumatori – sia la promozione di caratteristiche presentate come peculiari del prodotto ma in realtà imposte da obblighi di legge, sia l’attribuzione ingannevole di qualità ambientali o di sostenibilità ai prodotti commercializzati.

La prima condotta è espressamente vietata dalla direttiva sulle pratiche commerciali sleali, il cui Allegato I, punto 10, qualifica come sleale la presentazione dei diritti conferiti ai consumatori dalla legge come elemento distintivo dell’offerta commerciale.

La seconda condotta – riconducibile a forme di comunicazione ambientale ingannevole e nota come greenwashing – risulta in contrasto con i principi di trasparenza e correttezza professionale ed è stata oggetto di intervento normativo da parte del legislatore europeo con l’adozione della Direttiva (UE) 2024/825, che modifica le direttive 2005/29/CE e 2011/83/UE. Tale intervento è finalizzato a garantire un elevato livello di tutela dei consumatori e dell’ambiente, promuovendo al contempo il corretto funzionamento del mercato interno e sostenendo la transizione verde.

In tale prospettiva ed al fine di promuovere modelli di consumo maggiormente sostenibili, la predetta direttiva persegue l’obiettivo di

assicurare al consumatore condizioni di scelta e di acquisto consapevoli ed informate.

A tal fine, essa interviene modificando l'art. 6 della direttiva 2005/29/CE ed inserendo tra le azioni ingannevoli del paragrafo 1) quelle pratiche commerciali che contengono informazioni false o fuorvianti in relazione alle caratteristiche ambientali o sociali del prodotto e gli aspetti relativi alla circolarità, quali la durabilità, la riparabilità o la riciclabilità.

Ulteriore profilo di criticità, segnalato dalle Autorità precedenti, riguarda il difetto di trasparenza informativa consistente nell'occultamento e nell'insufficiente accessibilità ai dati di contatto del professionista; elemento suscettibile di incidere negativamente sull'effettività dei diritti dei consumatori, in particolare in relazione alla possibilità di inoltrare reclami o richieste di chiarimenti.

Difetto di trasparenza informativa in evidente contrasto con l'art. 6, Capo III, lett. b) e c) della direttiva 2011/83 (UE), il quale impone al prestatore - prima che il consumatore si impegni in un contratto a distanza, concluso fuori dai locali commerciali o da una corrispondente offerta - di fornire a quest'ultimo, in maniera chiara e comprensibile, le informazioni relative all'identità del professionista, come ad esempio la sua denominazione sociale e l'indirizzo della sede presso cui il professionista ha stabilito la sua attività unitamente al numero di telefono, fax e email - qualora disponibili - affinché il consumatore possa avere un accesso agevole ai canali di contatto ed una comunicazione funzionale e diretta con il professionista.

In aggiunta, la rete CPC ha indirizzato a SHEIN una richiesta formale di chiarimenti ai fini di accertare il rispetto, da parte dell'azienda, delle prescrizioni ulteriori previste dal diritto dell'Unione in materia di salvaguardia dei diritti dei consumatori, tra le quali rientra, ad esempio, l'obbligo di assicurare che qualsiasi forma di valutazione del prodotto, ivi incluse recensioni e classifiche, sia comunicata al consumatore in modo attendibile e non manipolato.

È, altresì, in corso - da parte delle Autorità competenti - una verifica volta ad accertare, da un lato, l'osservanza, da parte dell'operatore economico, degli obblighi informativi concernenti le modalità di ripartizione delle responsabilità contrattuali tra SHEIN e i venditori terzi e, dall'altro, l'eventuale inapplicabilità, nei casi in cui il venditore terzo non rivesta la qualifica di professionista, delle tutele previste dalla normativa vigente a tutela dei consumatori.

Occorre, infine, evidenziare che, a seguito dell'ammonimento formale, è stato assegnato a SHEIN un termine di un mese per pronunciarsi in merito ai rilievi opposti e per fornire alla rete CPC delle soluzioni coerenti e funzionali al superamento delle sopra descritte criticità.

Sulla base delle eventuali osservazioni trasmesse da SHEIN, la rete CPC potrà avviare un'interlocuzione con l'operatore economico, prevedendosi, comunque in caso di mancata risposta nei termini indicati, che le Autorità competenti possano valutare l'adozione di misure esecutive per assicurare il rispetto della disciplina consumeristica o comunque comminare sanzioni pecuniarie determinate in misura proporzionale al fatturato annuo realizzato da SHEIN negli Stati membri dell'Unione europea interessati.



Assumerà peculiare rilievo, ove resa conoscibile, la replica trasmessa da SHEIN, quale indice di valutazione della posizione assunta dall'operatore economico nei confronti delle criticità rilevate, sia essa connotata in chiave difensiva ovvero dalla volontà di conformazione agli obblighi normativi imposti.

GABRIELE CRESCENTE

[https://ec.europa.eu/commission/presscorner/detail/en/ip\\_25\\_1331](https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1331)

### 2025/2(7)GD

**Il parere dell'Avvocato Generale Kokott presso la Corte di giustizia depositato il 19.6.2025 sul ricorso contro la sentenza di condanna di oltre 4 miliardi di euro inflitta a Google e ad Alphabet nel 2022 per abuso di posizione dominante nella causa C-738/22 P (Google LLC, Alphabet Inc. contro Commissione europea)**

Il 19 giugno 2025 l'Avvocato Generale Kokott presso la Corte di giustizia dell'Unione Europea (**CGUE** o la **Corte**) ha depositato le proprie conclusioni nell'ambito del giudizio promosso da Google LLC (**Google**) e Alphabet Inc. (**Alphabet**) contro la sentenza relativa alla condanna di oltre 4 miliardi di euro inflitta alle medesime società dalla Commissione europea (la **Commissione**) (causa C 738/22 P; Google LLC, Alphabet Inc. contro Commissione europea).

Il caso risale al 2018, quando Google finì nel mirino della Commissione per abuso di posizione dominante.

In particolare, con decisione del 18 luglio 2018 la Commissione ha inflitto a Google un'ammenda di circa 4,343 miliardi di euro, di cui circa 1,9 miliardi di euro in solido con Alphabet.

Secondo la Commissione, Google ha abusato della sua posizione dominante in tre mercati rilevanti (i.e., il mercato della ricerca generica su Internet, il mercato sistemi operativi per dispositivi mobili e il mercato della vendita di app per Android), imponendo restrizioni contrattuali anticoncorrenziali ai produttori di dispositivi mobili e agli operatori di reti mobili sin dal 1° gennaio 2011.

Nello specifico, la Commissione ha rilevato che:

1. i produttori potevano ottenere una licenza per Play Store, l'App Store di Google, solo se preinstallavano l'applicazione di ricerca generale Google Search e il browser Chrome (il c.d. "pacchetto");
2. per ottenere una licenza per Play Store e per Google Search, i produttori dovevano impegnarsi a non vendere dispositivi con versioni del sistema operativo Android non approvate da Google (c.d. "anti-frammentazione" – Anti-Fragmentation Agreement);
3. Google vincolava la partecipazione dei produttori e degli operatori di rete agli introiti pubblicitari alla condizione che non preinstallassero un altro servizio di ricerca generale su un portafoglio determinato di dispositivi ("ripartizione dei ricavi" – Revenue Share Agreement); in altri termini,

Google concedeva significativi incentivi finanziari a quei grandi produttori di dispositivi e operatori di reti mobili che fossero disposti a pre-installare in esclusiva l'applicazione Google search sull'intera gamma dei loro dispositivi Android (tale pratica rientra nella categoria di violazioni dell'art. 102 TFUE generalmente definite come "sconti fidelizzanti").

Secondo la Commissione, con tutte queste restrizioni, Google perseguiva l'obiettivo di proteggere e di rafforzare la sua posizione dominante in materia di servizi di ricerca generale e, di conseguenza, anche i suoi introiti derivanti da annunci pubblicitari collegati a tali ricerche. Considerato il loro obiettivo comune e la loro interdipendenza, la Commissione ha qualificato tali restrizioni come infrazione unica e continuata.

Google ha contestato la decisione della Commissione dinanzi al Tribunale dell'Unione europea, con un successo limitato: con sentenza del 14 settembre 2022 il Tribunale UE ha annullato la decisione unicamente per quanto riguarda il regime di ripartizione dei ricavi e ha ridotto l'ammenda a 4,125 miliardi di euro, di cui circa 1,520 miliardi di euro in solido con Alphabet.

Google ha quindi impugnato la sentenza del Tribunale UE dinanzi alla CGUE.

Nelle conclusioni presentate dall'Avvocato Generale Juliane Kokott lo scorso 19 giugno viene proposto alla CGUE di respingere l'impugnazione di Google e di confermare integralmente la sentenza del Tribunale UE.

L'Avvocato Generale afferma, da un lato, che la valutazione dei fatti e degli elementi di prova da parte del Tribunale non può essere contestata dinanzi alla CGUE (infatti, le sentenze del Tribunale UE possono essere impuginate limitatamente a questioni di diritto) e dall'altro, che gli argomenti giuridici invocati da Google sono inoperanti.

Per quanto riguarda, in particolare, il pacchetto di Play Store, Google Search e Chrome, contrariamente a quanto sostiene Google, il Tribunale non doveva esigere che la Commissione, per dimostrare l'esistenza di un abuso, analizzasse la situazione concorrenziale in assenza del comportamento censurato (analisi cosiddetta contro-fattuale).

Inoltre, il Tribunale non era tenuto ad esaminare, oltre alla capacità del pacchetto di restringere la concorrenza, se tale comportamento fosse idoneo a escludere concorrenti di Google altrettanto efficienti. Infatti, secondo l'Avvocato Generale, non sarebbe realistico, nel caso di specie, confrontare la situazione di Google con quella di un ipotetico concorrente altrettanto efficiente. Google deteneva una posizione dominante in diversi mercati dell'ecosistema Android e beneficiava quindi di effetti di rete che le consentivano di fare in modo che gli utenti utilizzassero Google Search. In tal modo, Google aveva accesso a dati che le consentivano a sua volta di migliorare i suoi servizi. Nessun ipotetico concorrente avrebbe potuto trovarsi in una situazione del genere.

A parere dell'Avvocato Generale Kokott, il Tribunale ha altresì correttamente ritenuto che nonostante l'annullamento della decisione della Commissione per quanto riguarda la ripartizione dei ricavi, sussistesse ancora un'infrazione unica e continuata. Independentemente da tale annullamento parziale, esisteva una strategia complessiva volta ad incrementare lo sviluppo di Internet sui dispositivi mobili, preservando al contempo il modello economico di Google,

il quale si basava essenzialmente sui redditi che essa ricavava dall'utilizzo del suo servizio di ricerca generale.

Infine, secondo l'Avvocato Generale, il Tribunale non ha neppure commesso errori nel ricalcolare l'importo dell'ammenda.

Com'è noto, le conclusioni dell'Avvocato Generale non vincolano la CGUE, ma rappresentano un parere autorevole che la Corte può tenere in considerazione nel prendere la sua decisione finale. L'Avvocato Generale svolge un ruolo indipendente, fornendo una soluzione giuridica alla Corte, ma la decisione finale spetta esclusivamente ai giudici della Corte. Qualora la CGUE dovesse ritenere la causa matura per essere decisa, si pronuncerà definitivamente sulla controversia; in caso contrario, la Corte rinvierà la causa al Tribunale UE, che sarà vincolato alla decisione resa dalla CGUE.

A questo punto non resta che attendere la sentenza della CGUE, attesa nei prossimi mesi.

GIORGIA DIOTALLEVI

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=301366&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=2317604>

## 2025/2(8)BPo

### Il JuLIA Handbook del maggio 2025 su IA e pubblica amministrazione

Il “*JuLIA Handbook. AI and Public Administration: The (legal) limits of algorithmic governance*” del maggio 2025 è frutto di un serie di esperienze di collaborazione e di formazione in campo giudiziario, promosse nell'ambito del *Justice Programme* dell'Unione Europea. Si presenta come un manuale, pensato per istruire alcune specifiche categorie di destinatari, in particolare giudici, avvocati e consulenti legali, sugli elementi da prendere in considerazione per valutare l'impatto sui diritti fondamentali derivanti dall'impiego di soluzioni che integrano l'intelligenza artificiale nell'esercizio della funzione amministrativa.

Sul piano metodologico, l'analisi risente (il che non costituisce un limite, anzi) del tipo di approccio che ha caratterizzato il progetto di formazione e collaborazione da cui trae origine, basato essenzialmente sullo scambio e la circolazione di esperienze (in particolare, nell'ambito della tutela giurisdizionale dei diritti), e la costituzione di “comunità di pratica” destinate a svilupparsi, a crescere e a consolidarsi nel tempo, così da assicurare una circolazione di saperi, approcci e attitudini. Pertanto, fermo restando che il manuale è corredato (anche) da una sintetica ricostruzione del quadro normativo applicabile (sia sul piano UE, che sul piano nazionale, quando opportuno), la parte più cospicua (ed interessante) del manuale poggia sull'analisi di una serie davvero molto ampia (per numero di casi analizzati e di paesi dell'Unione coperti) e articolata di studi di caso. Detta analisi consiste nella illustrazione di una specifica soluzione di AI per l'esercizio di attività amministrative, sviluppata tendenzialmente a livello nazionale, regionale o

comunale, e nella evidenziazione degli impatti e delle ricadute sulla tutela dei diritti (dei destinatari dell'azione amministrativa, e dei consociati più in generale), a partire dagli elementi che emergono dall'analisi del contenzioso maturato in sede giurisdizionale, e che ha per oggetto tale specifica soluzione di AI. In base a questa casistica, sono selezionati ed evidenziati i diversi punti di attenzione di cui i destinatari del manuale dovrebbero tenere conto, in prospettiva, nel valutare l'impatto di sistemi di AI impiegati nel settore delle pubbliche amministrazioni.

Sul piano della struttura, un elemento che contraddistingue il manuale è la scelta (felice) di distinguere tra loro tre fasi (successive) in cui si articola il processo di adozione di una soluzione di AI da porre al servizio dell'esercizio di una funzione amministrativa. In particolare, tali fasi sono identificate rispettivamente nell' "*algorithmic design*" (la progettazione), nella fase di "*organisational implemetation/embedding*" (la fase di inserimento ed integrazione della soluzione nel quadro delle funzioni esercitate dall'amministrazione) e nella fase del "*public decision-making using AI systems*" (la fase di effettivo impiego della soluzione). Pertanto, il manuale si compone complessivamente di 5 capitoli. Un primo dedicato alla identificazione della nozione di intelligenza artificiale (con un essenziale ma tutto sommato efficace sunto delle nozioni di base in materia), e alla perimetrazione di cosa si intenda per "pubblica amministrazione". La nozione adottata è ampia, ed include la programmazione, l'adozione e l'attuazione degli indirizzi legislativi e delle *policy* governative. In particolare, il manuale si concentra su casi di *Public service provision*; su esempi di *Enforcement of laws and government policies*; nonché sui sistemi di *Internal management*. I capitoli dal secondo al quarto sono quindi dedicati all'analisi delle tre fasi di adozione di soluzioni di AI, mentre il capitolo quinto è dedicato alle conclusioni.

In tutti e tre i capitoli centrali ricorrono alcuni elementi comuni: l'evidenziazione (in apertura) dei rischi cui sono esposti i diritti fondamentali con specifico riferimento alla fase presa in considerazione; la descrizione delle specifiche caratteristiche della fase analizzata, e dei problemi e delle sfide che questa pone (sotto molteplici aspetti: attori coinvolti, fattori rilevanti; requisiti infrastrutturali e organizzativi, profili di *governance*, competenze professionali e formazione, per citare i principali); la ricostruzione del framework normativo rilevante per quella specifica fase di sviluppo della soluzione di AI. Altri elementi, invece, risultano caratteristici dell'analisi di specifiche fasi. Ad esempio, un'attenta disamina dei diversi problemi connessi alla individuazione (o alla efficace distribuzione) dei profili di *liability* connessi all'implementazioni di sistemi di AI nell'ambito del settore pubblico è presente nel capitolo relativo alla progettazione del sistema (cfr. par. 2.6) e in quello relativo all'*embedding* (cfr. par. 3.6). In questo secondo, poi, sono esplorati anche i mezzi specifici di tutela nei confronti delle scelte di organizzative effettuate dall'amministrazione (*injuncions* e *judicial review of administrative acts*), il cui esperimento ha consentito anche l'emersione di alcuni "principi" di cd. *legalità algoritmica* (quali: la trasparenza dell'algoritmo, la necessaria revisione umana, il monitoraggio continuo) che trovano corrispondenza in molteplici casistiche

giurisprudenziali nazionali. Infine, va segnalato che ciascuno dei capitoli centrali (2, 3 e 4) – in linea con le finalità del manuale (quella, cioè, di fornire informazioni pratiche e casi di studio reali per aiutarli a mitigare potenziali conflitti con i diritti fondamentali durante lo sviluppo di sistemi di IA) – si chiude con un riassunto delle questioni più critiche che gli enti pubblici dovrebbero prendere in considerazione durante la fase specifica fase di adozione degli algoritmi analizzata. Gli snodi critici sono declinati in forma interrogativa, a delineare il nucleo essenziale di una *check list*, modellata sugli elementi caratteristici di ciascuna fase. Tali quesiti sono poi ripresi e riassembleati in modo sistematico alla fine del manuale, nel capitolo 5.

Come detto, uno degli elementi di maggiore interesse di questo documento è la varietà e la ricchezza dei casi di studio che sono oggetto di analisi, e da cui sono estratte le indicazioni ed i punti di attenzione segnalati agli utenti del manuale.

Nel merito, preme qui segnalare quantomeno tre aspetti che emergono da questa analisi.

In primo luogo, proprio l'approccio analitico adottato, basato sulla casistica giurisprudenziale, porta con sé un effetto di selezione *temporale* dei parametri normativi più rilevanti. Infatti, sebbene l'ordinamento dell'Unione abbia intrapreso convintamente la strada di una (ampia) disciplina legislativa *ad hoc* destinata a regolare alcuni aspetti fondamentali dello sviluppo e dell'implementazione (anche nel settore pubblico) dei sistemi di Intelligenza Artificiale (il cd. AI Act), tale approccio è ancora lontano dal trovare una ricaduta concreta sul piano della tutela giurisdizionale (il quadro normativo infatti è troppo recente, e per la verità ancora in fase di completamento); pertanto, la casistica nel manuale è figlia degli elementi più consolidati (e più risalenti) del framework normativo, tanto europeo quanto nazionale (se e quando rilevante).

Anche al netto di questa considerazione (e veniamo al secondo aspetto), da questa casistica emerge la assoluta centralità acquisita dalla disciplina a tutela dei dati personali (sia quella di natura convenzionale – a partire dalla Convenzione del consiglio d'Europa – sia quella di natura secondaria, con il GDPR saldamente al centro del sistema) ai fini della definizione del quadro di principi, regole, istituti idonei innanzitutto ad evidenziare gli impatti delle soluzioni di AI (adottati anche nell'ambito del settore pubblico) sui diritti fondamentali (a cominciare dal diritto alla privacy, all'autodeterminazione informativa, alla tutela dei dati personali, ma con una decisa proiezione anche al di fuori di questi ambiti: dal diritto a non essere discriminati al diritto ad una buona amministrazione, e così via).

Anche alla luce di ciò, infine, vale forse la pena di sottolineare un aspetto problematico che emerge con sufficiente nitore dagli elementi di analisi presentati nel manuale (e siamo al terzo elemento). Per un verso, già nella descrizione (teorica) dei caratteri propri dell'AI (con specifico riferimento alle tecniche di calcolo del *deep learning* e della *generative AI*, cfr. par. 1.2.1) è evidenziato come questi sistemi di calcolo si caratterizzano “*for their opacity and poor explainability*”. Per altro, tali limiti trovano puntuale e frequente riscontro nella casistica analizzata dal manuale: una quantità di soluzioni di AI adottate nei più disparati settori dell'amministrazione

pubblica, e in una varietà di contesti nazionali diversi, sono state giudicate come incompatibili (o comunque inadeguate) proprio in ragione della scarsa trasparenza, della impossibilità di ricostruire i criteri decisionali (o di classificazione), con (grave) pregiudizio dei diritti dei destinatari dell'azione amministrativa. E così, è frequente la raccomandazione, ripetutamente formulata con riferimento alle diverse fasi di adozione dei sistemi di AI, di adottare soluzioni organizzative, operative e di *governance* adeguate rispetto all'esigenza di trasparenza (dell'algoritmo e dei processi decisionali che questo incorpora), di comprensibilità di tali percorsi decisionali (al fine di poterli effettivamente contestare, in sede di revisione da parte dell'operatore umano) e di monitoraggio e *controllo* preventivi, *in itinere* ed *ex post*, degli impatti prodotti dall'adozione di queste soluzioni. E tuttavia, non è chiaro come questa esigenza possa essere effettivamente soddisfatta, tenuto conto che il tema della cd. *explainability* dei sistemi di intelligenza artificiale è tutt'altro che risolto (anzi). Insomma, il manuale sotto questo profilo fornisce chiari elementi (quantitativi e qualitativi) circa l'esistenza di un problema, ma non sembra anche offrire o indicare adeguate soluzioni (se non quella di avere contezza del problema, e di rivolgersi a esperti – tendenzialmente esterni al settore pubblico – professionalmente qualificati e convenientemente attrezzati per assistere gli enti pubblici nelle tre fasi in cui si articola l'adozione di un sistema di AI). V'è da aggiungere che lo stesso manuale ammette di rappresentare un *work in progress*, destinato a crescere e ad arricchirsi in funzione dell'ulteriore collaborazione e scambio all'interno delle diverse reti e "comunità di pratica" che lo alimentano. Niente esclude che – anche tenuto conto del *bias* temporale già segnalato – in successive edizioni alcune indicazioni pratiche su come dare concreta soddisfazione alle esigenze di trasparenza possano essere integrate nel manuale (anche in seguito alla piena esplicazione degli effetti dell'AI Act).

Si è detto, per chiudere, che uno dei meriti del *JuLIA Handbook* consiste nella analisi articolata delle diverse fasi in cui si dispiega il processo di adozione di un sistema di AI nell'ambito di un servizio pubblico, di una funzione pubblica, di un sistema gestionale in uso all'amministrazione. In particolare, va sottolineato che l'operazione che consiste nel dare separato rilievo alla prima fase (quella di *progettazione*), come pure alla seconda (quella dell'*embedding*), risulta particolarmente meritevole, dal momento che va a coprire uno spazio scarsamente "coperto", sia in dottrina che sul piano della letteratura grigia, nel quale le amministrazioni pubbliche si trovano spesso ad operare "al buio", afflitte da una ormai strutturale asimmetria rispetto agli sviluppatori e ai fornitori delle soluzioni di AI, gravate da vincoli finanziari stringenti, e pertanto spesso unicamente interessate a trovare soluzioni per "risparmiare" (efficienza operativa). Il manuale, sotto questo profilo, adotta un approccio particolarmente lodevole, nella misura in cui suggerisce che l'adozione dell'AI non è sempre la soluzione più adeguata (nemmeno ai soli fini dell'efficienza operativa), e che i risvolti di cui occorre tenere conto sono molteplici, e vanno ben al di là dei soli profili finanziari, e deve coinvolgere – in primo luogo – la considerazione dei diritti e delle libertà fondamentali dei destinatari del servizio. Ribadito ciò, va anche osservato che l'articolazione dell'analisi nelle tre fasi presta il fianco (forse inevitabilmente)



ad alcune ridondanze, sia sul fronte analitico (non è sempre facile distinguere in modo netto una fase dall'altra), sia sul piano delle raccomandazioni. L'auspicio che ci permettiamo di suggerire agli autori, per le edizioni che seguiranno, è quello curare i raccordi tra le analisi delle fasi del processo di adozione delle soluzioni di AI, così da evitare ripetizioni (ove opportuno e possibile), al fine di ottimizzare la leggibilità e la coerenza interna di un testo che, tuttavia, costituisce già un punto di riferimento davvero importante per chi voglia documentarsi nell'ambito di un settore "di nicchia", ma decisivo, come quello dell'AI del settore pubblico.

BENEDETTO PONTI

[https://www.julia-project.eu/sites/default/files/2025-05/Final%20Handbook\\_%20AI%20and%20Public%20Administration\\_%20The%20%28legal%29%20limits%20of%20algorithmic%20governance.docx.pdf](https://www.julia-project.eu/sites/default/files/2025-05/Final%20Handbook_%20AI%20and%20Public%20Administration_%20The%20%28legal%29%20limits%20of%20algorithmic%20governance.docx.pdf)

### 2025/2(9)FDA

#### Il rapporto di AgID del 10 giugno 2025 sull'uso dell'intelligenza artificiale nelle amministrazioni centrali della PA

Il 10 giugno 2025 l'Agenzia per l'Italia Digitale (**AgID**) ha pubblicato i risultati della prima indagine sull'uso dell'intelligenza artificiale (**IA**) nelle amministrazioni centrali della pubblica amministrazione (il **Rapporto**). Il censimento, incluso tra le azioni del piano triennale per l'informatica nella pubblica amministrazione 2024–2026, si è svolto mediante questionario tra il 25 settembre e il 10 ottobre 2024 e ha riguardato 108 autorità pubbliche impegnate nel settore economico e finanziario (pp. 2-3 del Rapporto).

Il Rapporto mette in luce che il 42% dei progetti esaminati (in totale 120 di durata biennale) intende migliorare l'efficienza operativa degli enti interpellati; il 24% vuole potenziare la capacità di gestione e analisi dei dati; il 18% mira a incrementare l'accesso ai servizi da parte dell'utenza (p. 4 del Rapporto). Evidenzia che tra le soluzioni tecniche prescelte dai vari enti prevalgono quelle basate sul Machine Learning e sulla Intelligenza Artificiale Generativa (p. 7 del Rapporto); ma in questo ultimo caso ri-scontra una «limitata attenzione da parte delle amministrazioni agli standard di qualità dei dati, elemento che potrebbe compromettere l'affidabilità e l'efficacia delle soluzioni di Intelligenza Artificiale» (p. 10 del Rapporto).

Sul piano delle modalità di approvvigionamento dei sistemi di IA, il Rapporto nota come larga parte delle procedure di acquisto analizzate discenda da accordi quadro, convenzioni Consip, mercato elettronico delle pubbliche amministrazioni e sistemi dinamici di acquisizione; tuttavia constatata la carenza di «strumenti di procurement specificamente strutturati per l'Intelligenza Artificiale» col «rischio di acquisire soluzioni non pienamente aderenti alle esigenze specifiche delle amministrazioni» (p. 11 del Rapporto). Pur non mancando all'interno delle amministrazioni coinvolte nell'indagine figure professionali capaci di gestire efficacemente i sistemi di IA, il rapporto

segnala una forte dipendenza da soggetti esterni, principalmente da società d'ingegneria: il che «solleva interrogativi rispetto alla capacità delle amministrazioni di adeguare i profili professionali interni alle esigenze progettuali, o di formare risorse in linea con gli obiettivi di sviluppo e gestione delle soluzioni IA» (p. 13 del Rapporto). Inoltre il Rapporto sottolinea la mancanza, in quasi tutti i progetti, di specifici indicatori di risultato che possano misurarne il «potenziale di diffusione» (p. 15 del Rapporto).

Ecco allora che il Rapporto suggerisce a tutte le amministrazioni – non solo a quelle interpellate – di seguire alcuni accorgimenti quali nell'ordine: adottare, ove possibile, soluzioni progettuali avanzate e sostenibili; rafforzare la qualità e la gestione dei dati; innovare le modalità di acquisto dei sistemi di IA con gare dedicate e pianificate nel lungo periodo; reclutare personale tecnico specializzato, introducendo apposite figure professionali come l'AI Officer o il Data Steward (p. 20 del Rapporto).

FILIPPO D'ANGELO

[https://www.agid.gov.it/sites/agid/files/2025-06/AGID\\_Ricognizione\\_Progetti\\_AI\\_Rapporto\\_2025\\_V\\_2\\_2\\_10giu25.pdf](https://www.agid.gov.it/sites/agid/files/2025-06/AGID_Ricognizione_Progetti_AI_Rapporto_2025_V_2_2_10giu25.pdf)

## 2025/2(10)MMar

### L'ordine della Federal Trade Commission (FTC) degli Stati Uniti d'America del 28.4.2025 contro il sistema Workado che promette di individuare contenuti sintetici generati da sistemi di IA

Il 28 aprile 2025, la Federal Trade Commission degli Stati Uniti d'America (FTC o la **Commissione**) ha emesso un pre-ordine nei confronti di Workado LLC (**Workado** o la **Società**), responsabile dell'omonimo sistema (il **Provvedimento**), contestando l'assenza di prove a supporto del claim a sentire il quale il medesimo sistema sarebbe in grado di individuare i contenuti sintetici generati da sistemi di intelligenza artificiale (**IA**) con un grado di accuratezza del 98%. Il provvedimento della FTC è particolarmente rilevante in quanto segna una delle prime posizioni della Commissione nei confronti di un sistema di IA, individuando in particolare un caso di cosiddetto *AI washing*. Tale pratica consiste nel deformare l'uso effettivo dell'IA rispetto ai prodotti o servizi offerti da un'azienda.

Nel caso in questione, il Provvedimento è stato emesso dalla FTC nei confronti di Workado per lo sviluppo del suo rilevatore di testo basato sull'IA. Workado commercializza un servizio usato dai consumatori per determinare se contenuti pubblicati online siano stati scritti da un essere umano, oppure creati tramite l'intelligenza artificiale. In particolare, la Società afferma che il suo rilevatore sarebbe in grado di classificare il testo come «creato dall'uomo», oppure «generato dall'IA» con una precisione pari o superiore al 98% nei confronti di vari tipi di testi, provenienti da IA generativa (ChatGPT, GPT4, Claude e Bard).

Ciononostante, in seguito ad un'indagine interna, la FTC ha rilevato che il modello di intelligenza artificiale utilizzato da Workado, e alla base del suo

*AI Content Detector*, sarebbe stato addestrato esclusivamente per classificare i contenuti accademici e non per tutti i contenuti di diverso genere. Test indipendenti avrebbero dimostrato che il tasso di accuratezza del sistema sarebbe solamente del 53%, e non del 98%, come sostenuto dall'azienda. Di riflesso, la FTC ha riconosciuto la violazione della quinta sezione del *Federal Trade Commission Act* in materia di pratiche ingannevoli in quanto «l'affermazione del 98% era falsa, fuorviante o infondata».

In merito alle violazioni riscontrate, la FTC ha raggiunto un accordo con la Società. La Commissione ha annunciato, tramite il suo Direttore dell'Ufficio per la tutela dei consumatori, che «i consumatori si fidavano dell'AI Content Detector di Workado per capire se dietro un testo ci fosse un'intelligenza artificiale, ma il prodotto non ha funzionato meglio del lancio di una moneta. Affermazioni fuorvianti sull'intelligenza artificiale compromettono la concorrenza, rendendo più difficile per i fornitori legittimi di prodotti basati sull'intelligenza artificiale raggiungere i consumatori».

Nell'accordo tra FTC e Workado con durata ventennale, che verrà pubblicato sul *Federal Register* al fine di ricevere commenti pubblici, la Società non ha riconosciuto né negato espressamente le accuse contestate, pur addivenendo a un accordo dalla natura implicitamente confessoria. In particolare, nell'accordo vi sono disposizioni volte ad impedire che l'azienda ponga in essere azioni o pratiche simili in futuro. Nello specifico, il Provvedimento riguarda i prodotti finalizzati alla rilevazione di contenuti, testi, immagini e video che vengono generati oppure alterati dall'intelligenza artificiale.

Più nel dettaglio, il Provvedimento contiene otto disposizioni elaborate dalla FTC nei confronti di Workado. La prima disposizione vieta all'azienda di rilasciare dichiarazioni riguardanti l'efficienza di qualsiasi prodotto citato nel provvedimento, a meno che tali dichiarazioni siano formulate in modo non fuorviante e Workado abbia prove (scientifiche o non) attendibili e competenti, nonché sufficienti per la loro quantità, qualità e tempestività, a supporto di quanto affermato. La seconda disposizione impone a Workado di conservare qualsiasi prova su cui si basano le proprie dichiarazioni riguardanti i prodotti ricompresi nell'ordine della FTC; la terza disposizione richiede all'azienda di notificare i propri consumatori circa l'accordo raggiunto con la FTC. La quarta disposizione prevede che Workado, entro 10 giorni dalla data di entrata in vigore del provvedimento, presenti alla Commissione una conferma di ricezione dello stesso, nonché distribuisca l'ordine ai suoi dirigenti, ai funzionari e ad alcuni dipendenti e agenti ed ottenga da loro le relative ricevute firmate. La quinta disposizione impone che l'azienda rediga periodicamente report per la FTC circa l'attività effettuata, mentre la sesta disposizione pone in capo a Workado l'obbligo di conservare report riguardanti la propria attività. La settima disposizione pone in capo all'azienda ulteriori obblighi circa la compilazione di questi report. Infine, l'ultima disposizione specifica le date di validità del provvedimento, inclusa la clausola che prevede che, salvo eccezioni, esso cesserà di essere efficace dopo 20 anni.

In conclusione, il Provvedimento affronta una questione controversa in materia di intelligenza artificiale e di accuratezza dei sistemi di rilevamento basati sull'IA. La vicenda analizzata è un chiaro esempio delle tematiche

legate all'utilizzo dell'IA e del potenziale impatto che queste possano avere nei confronti del consumatore. Non sorprenderebbe dunque che la FTC o altre autorità possano trattare di questioni simili in futuro, al fine di tutelare il consumatore e verificare la veridicità di quanto affermato dalle aziende circa l'accuratezza e funzionalità dei loro sistemi basati su IA.

MATHILDE MARÈ

<https://www.ftc.gov/news-events/news/press-releases/2025/04/ftc-order-requires-workado-back-artificial-intelligence-detection-claims>  
[https://www.ftc.gov/system/files/ftc\\_gov/pdf/decision\\_and\\_order.pages\\_from\\_232\\_3092\\_-\\_content\\_at\\_scale\\_ai\\_consent\\_package\\_without\\_signatures-3.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/decision_and_order.pages_from_232_3092_-_content_at_scale_ai_consent_package_without_signatures-3.pdf)

## 2025/2(11)RR

### **Il documento del 7.3.2025 sui metodi per individuare i contenuti sintetici generati da sistemi di IA, predisposto dalle autorità della Repubblica Popolare Cinese**

A partire dal 1° settembre 2025, la Cina introdurrà un nuovo quadro normativo che impone l'etichettatura obbligatoria per tutti i contenuti generati dall'Intelligenza Artificiale (IA). Questa misura, annunciata dalla *Cyberspace Administration of China* (CAC) in collaborazione con il Ministero dell'Industria e della Tecnologia dell'Informazione, il Ministero della Pubblica Sicurezza e l'Amministrazione Nazionale della Radio e della Televisione, mira a garantire maggiore trasparenza online e a combattere la disinformazione (v. in questa Rubrica la notizia n.23 nel [numero 1/2025](#) [2025/1(23) RRa]).

Attraverso la standardizzazione dei modelli di identificazione dei contenuti sintetici, invero, le autorità della Repubblica Popolare Cinese ritengono di poter promuovere uno sviluppo sano dell'Intelligenza Artificiale.

In questo contesto, in data 7 marzo 2025, è stato emanato un avviso dal titolo “*Metodi per l'identificazione di contenuti sintetici generati dall'intelligenza artificiale*”, volto a sollecitare i fornitori di servizi di informazione su Internet (di seguito denominati anche “fornitori di servizi”) che svolgono attività di identificazione di contenuti sintetici generati da IA in conformità con la “Gestione delle raccomandazioni degli algoritmi dei servizi di informazione su Internet”, le “Disposizioni per la gestione della sintesi profonda del servizio di informazione Internet” e le “Misure provvisorie per la gestione di sistemi di intelligenza artificiale generativa Servizi di intelligence”. Il documento è volto a meglio ribadire tutti quei meccanismi a cui tali soggetti possono (e in un certo senso devono) ricorrere allo scopo di identificare i loro diversi contenuti sintetici generati dall'Intelligenza Artificiale. A tal proposito, è doveroso evidenziare come, mediante l'espressione “contenuti sintetici”, si faccia riferimento, in particolare, a testi, immagini, audio, video, scene virtuali e altre informazioni generate e sintetizzate utilizzando, appunto, la tecnologia di intelligenza artificiale.

Passando ad analizzare nello specifico alcune delle indicazioni fornite dal documento, agli articoli 7 e 8 viene disposto l'obbligo per i fornitori di: i) dichiarare se offrono servizi di sintesi generati dall'intelligenza artificiale; ii) indicare chiaramente le modalità, gli stili e altre specifiche per la generazione di identificatori di contenuti sintetici. A tale scopo, si rinvengono diversi meccanismi di identificazione esplicita, tra i quali emergono l'inserimento di indicazioni vocali o segnali audio ritmici o altri segni all'inizio, alla fine o in posizione appropriata a metà dell'audio, come anche di segni di avviso prominenti nell'interfaccia della scena interattiva ovvero la predisposizione di cartelli di avvertimento ben visibili in posizioni appropriate sulle immagini o all'interno dei video. Ancora, sempre ai sensi dell'art. 4, è opportuno richiamare la previsione secondo la quale, in caso di presentazione di una scena virtuale, i fornitori del servizio dovrebbero inserire un logo di avviso prominente in una posizione appropriata sulla schermata iniziale.

Nonostante tutto quanto detto, si fa salva la possibilità per gli utenti di richiedere a un fornitore di servizi di fornire contenuti sintetici generati senza identificazione esplicita. Costui, a fronte della tale istanza, può, dopo aver chiarito gli obblighi di identificazione e le responsabilità d'uso dell'utente attraverso un accordo, fornire contenuti sintetici generati senza identificazione esplicita conservando i log pertinenti, come le informazioni sugli oggetti forniti, per almeno sei mesi.

Nella parte conclusiva dell'avviso, infine, è espressamente specificato che nessuna organizzazione o individuo può eliminare, manomettere, falsificare o nascondere in modo doloso gli identificatori di contenuti sintetici generati specificati in questi.

RACHELE RANIERI

[https://www.cac.gov.cn/2025-03/14/c\\_1743654684782215.htm](https://www.cac.gov.cn/2025-03/14/c_1743654684782215.htm)

### 2025/2(12)FR

**La Parte 3 “Generative AI Training” del Report “Copyright and Artificial Intelligence”, pubblicata sul sito dello U.S. Copyright Office nella versione “pre-publication” datata maggio 2025**

È arrivata a maggio 2025 anche la [terza parte](#) del report “*Copyright and Artificial Intelligence*” (di seguito anche solo “**Report**”) dello U.S. Copyright Office (USCO o l’**Ufficio**), dedicata all’addestramento delle AI generative (“*Generative AI Training*”) (per le prime due parti v., in questa Rubrica, la notizia n. 25 nel [numero 1/2025](#) [2025/1(25)FR])

Si tratta di una “pre-publication version”, rilasciata dall’Ufficio pochi giorni prima del licenziamento della Librarian of Congress Carla Hayden e della destituzione di Shira Perlmutter dal ruolo di Register of Copyrights e direttrice dell’USCO. Questi ultimi eventi, che hanno scosso un po’ le acque all’interno dell’Ufficio Copyright statunitense, hanno reso difficile formulare previsioni su quale sarà la linea che l’USCO adotterà in materia e persino

ipotizzare quando – e se – il Report sarà mai pubblicato nella sua versione finale.

La pubblicazione del Report che, con le sue 109 pagine, risulta ad oggi la parte più corposa dell'analisi dell'USCO, si inserisce nell'ambito della strategia dell'Ufficio in materia di AI, in virtù della quale, nell'agosto 2023, è stata pubblicata una Notice of Inquiry (**NOI**), da cui sono gemmate la Parte 1 (Digital Replicas) e la Parte 2 (Copyrightability) del Report (su cui v., in questa Rubrica, la notizia n. 25 nel [numero 1/2025](#) [2025/1(25)FR]) e a cui, nei prossimi mesi – fatte salve le incertezze di cui si è detto – dovrebbe seguire la pubblicazione di ulteriori riflessioni in tema di responsabilità civile e licenze.

Il Report è diviso in **cinque sezioni**. Dopo un'Introduzione in cui si richiamano a grandi linee le questioni giuridiche legate all'uso di opere protette da copyright nell'addestramento di sistemi di intelligenza artificiale, la Sezione II fornisce una panoramica dal punto di vista tecnologico sullo sviluppo e sull'impiego di tali sistemi; la Sezione III individua le fasi del training delle AI generative in cui gli atti potenzialmente lesivi del diritto d'autore possono essere posti in essere; la Sezione IV effettua una ricognizione degli aspetti principali della dottrina del fair use vigente negli Stati Uniti; infine, la Sezione V, illustra le opzioni di licenza potenzialmente impiegabili in tale contesto.

Nella **Introduzione**, si illustrano sinteticamente i profili dell'attività di training delle AI generative rilevanti per il diritto d'autore, richiamando a tal fine i termini in cui si è declinato di recente il dibattito sul punto e le numerose cause legali pendenti negli Stati Uniti.

Il Report dà atto del fatto che “la posta in gioco è alta, e le conseguenze” dell'attività di addestramento dei modelli di AI generativa “vengono spesso descritte in termini esistenziali”. Alcuni ritengono che obbligare le imprese AI ad ottenere licenze per tutte le opere coperte dal diritto d'autore usate ai fini del training dei loro modelli non sarebbe materialmente possibile, a causa della elevata quantità e varietà di contenuti necessari per alimentare i sistemi più avanzati, e ciò potrebbe rischiare di “soffocare” tale tecnologia trasformativa. Altri, al contrario, temono che l'addestramento non autorizzato possa impattare in modo eccessivo l'ecosistema creativo a causa della produzione massiva di contenuti in grado di competere con le opere intellettuali create da esseri umani senza l'ausilio dell'AI.

Il Report specifica che le principali questioni sorgono a causa delle quantità ingenti di dati usati per il training (“massive troves of data”). È interessante notare come, in nota 1, sia chiarito che i termini “dati” e “dataset” siano usati nel documento come “abbreviazione per tutti i tipi di contenuti utilizzati nell'addestramento dell'intelligenza artificiale generativa, incluse le opere intellettuali protette dal diritto d'autore”, nonostante tali opere non siano, in realtà, “dati” nel senso ordinario del termine, ma “espressioni creative”.

Infine, l'Ufficio chiarisce che la propria analisi riflette unicamente lo stato dell'arte attuale, ma che continuerà a osservarne e valutarne gli sviluppi, in considerazione della rapida evoluzione delle tecnologie e dei mercati coinvolti, nonché del fatto che tribunali e decisori politici si trovano ancora nelle fasi iniziali delle loro valutazioni. Tale analisi va intesa come parallela

agli sforzi di altre componenti dell'apparato governativo degli Stati Uniti, inclusi il Congresso e la Casa Bianca, che con il suo AI Action Plan sta cercando di promuovere la leadership americana nel campo dell'intelligenza artificiale.

La **Sezione II**, dedicata al technical background rilevante ai fini del diritto d'autore, offre una panoramica dal punto di vista tecnologico sullo sviluppo e sull'utilizzo corrente dei sistemi di IA generativa. Illustra, innanzitutto, come la tecnologia del machine learning (paragrafo A) venga usata, allo stato attuale, per creare modelli generativi, dei quali i generative language models costituiscono un esempio paradigmatico (paragrafo B). Inoltre, effettua un focus sui "training data", ovvero i dati necessari per addestrare i modelli generativi (paragrafo C) e descrive sinteticamente il processo di training, richiamandone le diverse fasi (paragrafo D). Infine, illustra come i modelli di AI generativa siano normalmente incorporati all'interno di più complessi sistemi di intelligenza artificiale. In effetti, "i modelli statistici che alimentano l'intelligenza artificiale generativa" vengono solitamente "integrati in sistemi di intelligenza artificiale più grandi, che elaborano e controllano le informazioni in ingresso e in uscita dai modelli, li collegano ad altri strumenti software e offrono un'interfaccia utente più comoda" ed è attraverso questi sistemi che gli utenti interagiscono con i modelli in questione (paragrafo E). Di tale Sezione, interessanti sono le definizioni di (i) machine learning, descritto come il "campo dell'intelligenza artificiale incentrato sulla progettazione di sistemi informatici in grado di apprendere e migliorare automaticamente il proprio funzionamento in base ai dati o all'esperienza, senza che siano necessarie a tal fine regole programmate esplicitamente" ("field of artificial intelligence focused on designing computer systems that can automatically learn and improve based on data or experience, without relying on explicitly programmed rules"); e di (ii) neural networks – quali tecnologie poste alla base delle Generative AI – intese come le "funzioni matematiche che trasformano dati di input in dati di output" ("mathematical functions that map, or transform, input data to output data").

Inoltre, rilevanti sono i richiami alle caratteristiche dei dati di training: finalità, quantità e qualità. A tal proposito, il Report chiarisce che la selezione dei dati avviene normalmente tenendo conto delle finalità per cui si intendono usare i relativi modelli – con la specificazione che "quando si addestrano foundation models (cioè modelli di grandi dimensioni pensati per un'ampia varietà di casi d'uso), vengono usati materiali di addestramento molto eterogenei" ed in elevate quantità. Ad ogni modo, con l'evoluzione della tecnologia, stanno emergendo sempre più studi su modelli competitivi che usano quantità minori di dati, ma di migliore qualità.

Interessante è infine la ricostruzione dell'attività di training non come evento isolato, ma come processo iterativo "che può essere interrotto in qualsiasi momento e continuato con dati diversi, un obiettivo diverso, o persino sotto la guida di un soggetto terzo". Nell'ambito di questo processo, è possibile individuare almeno due fasi, rispettivamente di "pre-training" e di "post-training" (o "fine-tuning"), così come identificate dalla rilevante letteratura sul tema.

Nella **Sezione III**, dedicata alle violazioni “prima facie” dei diritti esclusivi di cui alla normativa autoriale, il Report specifica che quando, per lo sviluppo di un sistema di AI, vengono utilizzati contenuti protetti dal diritto d’autore e non vi sia stata autorizzazione del titolare, è possibile che un simile uso leda le prerogative di tale titolare.

Perché sussistano simili violazioni “prima facie”, devono, dunque, essere presenti almeno i due elementi de: (i) la titolarità del diritto d'autore in capo a chi ritiene di essere stato leso; e (ii) la riproduzione di parti essenziali dell'opera che presentano carattere di originalità.

Gli atti di riproduzione (di parti) delle opere rilevanti a tal fine possono

- (i) sussistere nella fase di creazione e gestione – “curation” – dei dataset (Paragrafo A), nella fase di training vera e propria (Paragrafo B), o nella fase di c.d. “RAG” - “retrieval-augmented generation” (Paragrafo C), oppure
- (ii) manifestarsi nell’output stesso del processo creativo “algoritmico” (Paragrafo D), che talvolta può replicare o presentare una forte somiglianza con opere protette dal diritto d’autore.

La **Sezione IV** è dedicata al *fair use*.

Qualora vi sia stata una violazione *prima facie* del diritto d’autore, la prima difesa che può essere generalmente fatta valere è quella del *fair use*. È un istituto statunitense di origine giurisprudenziale, oggi codificato nella Sezione 107 del Copyright Act del 1976, attraverso il quale, di fronte all’emergere di nuove tecnologie, i giudici statunitensi hanno storicamente cercato di promuovere la “finalità fondamentale” del diritto d’autore: il progresso culturale.

Tale dottrina stabilisce che “l’uso corretto (fair use) di un’opera protetta da copyright [...] non costituisce violazione del diritto d’autore” purché venga effettuata una valutazione caso per caso dei seguenti quattro fattori (non esaustivi): (i) lo scopo e la natura dell’uso, ivi incluso se tale uso abbia finalità commerciali o sia destinato a scopi educativi senza fini di lucro; (ii) la natura dell’opera protetta da copyright, con relativa distinzione tra opere più “creative ed espressive” e opere più “fattuali e funzionali”; (iii) la quantità e la rilevanza della parte utilizzata rispetto all’opera nel suo complesso; (iv) l’effetto dell’uso sul mercato potenziale o sul valore dell’opera protetta.

Dopo aver illustrato il contenuto di tutti i fattori, il Report giunge alla conclusione che l’utilizzo di opere protette da copyright nell’addestramento dei sistemi di intelligenza artificiale è da considerarsi tendenzialmente trasformativo e, in quanto tale, astrattamente in grado di superare il primo fattore (“further purpose or different character”) – di gran lunga il più problematico, insieme al quarto. Il training implica, infatti, la trasformazione di “un’enorme raccolta di ‘esempi di training’ in un modello statistico capace di generare un’ampia gamma di output in una varietà di situazioni nuove e diverse”.

Tuttavia, il fatto che tale uso possa rientrare o meno nel fair use nel caso concreto dipende da ulteriori diverse valutazioni: quali opere sono state utilizzate, da quale fonte, per quale scopo, ecc..

In particolare, tra le considerazioni più problematiche in tal senso, vi è quella – pertinente alla valutazione del quarto fattore (“the effect of the use upon the potential market for or value of the copyrighted work”) – che l’attività di

training delle AI generative può comportare “un rischio significativo per il mercato o per il valore economico delle opere protette da copyright”. In particolare, “quando un modello è in grado di generare output sostanzialmente simili che si sostituiscono direttamente alle opere presenti nei training data, ciò può comportare una diminuzione delle vendite (lost sales)”. Inoltre, “anche quando gli output del modello non sono simili a una specifica opera protetta, essi possono comunque impattare negativamente sul mercato delle opere utilizzate nel training”.

Della Sezione IV val la pena, infine, richiamare la sottosezione G, dedicata agli “Approcci internazionali”, ove si fa espresso riferimento ad altri ordinamenti giuridici che si sono occupati in vario modo della questione del training delle AI generative. Tra questi, vi sono i riferimenti alla normativa UE, del Giappone, di Singapore, di Regno Unito, di Israele, della Corea del Sud, della Cina e del Brasile.

La **Sezione V** (“Licensing for AI Training”) esamina la praticabilità e l’opportunità delle diverse opzioni di licenza utilizzabili nel contesto dell’addestramento dell’intelligenza artificiale. Il Report analizza dapprima le questioni relative alle licenze volontarie e, successivamente, quelle legate ad un eventuale intervento legislativo – ad esempio avente ad oggetto la previsione di un “Compulsory Licensing regime”, “Extended Collective Licensing regime” o “opt-out mechanism”, sulla scorta di quello vigente nell’Unione europea.

Tra i profili critici delle licenze volontarie – che possono essere negoziate sia su base individuale che collettiva – il Report richiama le analisi sulla materiale capacità di ottenere con tali strumenti una quantità e varietà di opere sufficienti per addestrare modelli di alta qualità, nonché quelle sulla fattibilità, anche economica, di una simile soluzione e, infine, quelle sulla effettiva possibilità per i titolari dei diritti di beneficiare dei compensi ottenibili tramite le licenze.

Per quanto riguarda l’introduzione per via legislativa di un regime di licenza obbligatoria (compulsory licensing), il Report ritiene che esso comporterebbe notevoli svantaggi. Al contrario, per quei casi in cui le licenze volontarie si rivelassero impraticabili o inattuabili, la licenza collettiva estesa (extended collective licensing, ECL) rappresenterebbe un’opzione meno invasiva. Infine, in merito alla possibilità di prevedere per via legislativa un meccanismo di opt-out alla stregua di quello eurounitario, l’Ufficio ritiene che imporre ai titolari dei diritti d’autore l’onere di esercitare il diritto di escludere le proprie opere del training delle AI sia incompatibile con il principio secondo cui, per gli usi che rientrano nell’ambito dei diritti esclusivi previsti dalla legge, sia necessario il consenso del loro titolare. Ad ogni modo, poiché la questione del fair use non è ancora stata risolta in modo definitivo, l’Ufficio raccomanda, allo stato attuale, di lasciare che il mercato delle licenze continui a svilupparsi senza un intervento legislativo.

FRANCESCA ROTOLO

<https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-3-Generative-AI-Training-Report-Pre-Publication-Version.pdf>

<https://www.copyright.gov/ai/>

## 2025/2(13)EB

### Le azioni avviate l'11.6.2025 da Disney e Universal in California (USA) contro Midjourney per violazione del copyright sui loro personaggi.

| 643

L'11 giugno 2025 una serie di società facenti capo ai gruppi di due delle principali major dell'intrattenimento, Disney e Universal (precisamente: Disney Enterprises Inc, Marvel Characters Inc., MVL Film Finance LLC, Lucasfilm Ltd LLC, Twentieth Century Fox Film Corporation, collettivamente **Disney**; Universal City Studios Productions LLLP e Dreamworks Animation L.L.C., collettivamente **Universal**; e tutte, collettivamente, i **Ricorrenti**) hanno proposto in California (Stati Uniti d'America), davanti alla United States District Court, Central District of California (la **Corte**), un'azione nei confronti di Midjourney Inc. (**Midjourney**), società sviluppatrice dell'omonimo e noto sistema di generazione automatica di immagini. Tale azione solleva questioni cruciali riguardo alla sostenibilità giuridica ed economica dell'industria creativa nel contesto tecnologico attuale.

A differenza di altri giudizi che vertono sulle stesse questioni, i Ricorrenti non hanno chiesto in questo caso la rimozione dei materiali protetti dall'archivio di Midjourney, bensì solamente la cessazione del loro utilizzo come output.

Secondo quanto affermato dai Ricorrenti, Midjourney avrebbe violato in modo diretto e indiretto numerose disposizioni del Copyright Act statunitense (17 U.S.C. § 101 e ss.), agendo attraverso il proprio servizio di generazione di immagini, definito in sede giudiziaria come un vero e proprio "pozzo senza fondo di plagio" ("*a bottomless pit of plagiarism*"). In particolare, l'accusa si concentra sull'uso, da parte della società convenuta, di un'enorme quantità di materiale coperto da copyright per addestrare il proprio modello di intelligenza artificiale, senza ottenere alcuna forma di consenso dai titolari dei diritti. Lo stesso fondatore della società, David Holz, avrebbe ammesso pubblicamente a Forbes nel 2022 che Midjourney raccoglie tramite *webscraping* i dati di training e che "non esisterebbe un modo per ottenere cento milioni di immagini sapendo da dove provengono".

L'attività di addestramento del modello, secondo i Ricorrenti, comporterebbe la riproduzione e la fissazione di copie delle opere originali in un supporto tangibile, integrandole strutturalmente all'interno del funzionamento dell'intelligenza artificiale. Ma le condotte illecite contestate non si esaurirebbero nella fase di training: Midjourney permetterebbe agli utenti di generare, attraverso semplici comandi testuali, immagini che riproducono personaggi riconoscibili dei repertori Disney e Universal. Esemplicativamente, prompt come "Yoda con spada laser" oppure "personaggio dei cartoni animati 3D giallo con occhiali e salopette" genererebbero immagini direttamente riferibili a figure come Yoda o i Minions, anche in assenza di un'esplicita menzione ai marchi o ai titoli delle opere originali. Secondo i Ricorrenti, tali output costituirebbero a tutti gli

effetti copie o opere derivate, illecitamente distribuite agli utenti abbonati al servizio.

La questione si aggrava, si sostiene, con la funzione “Explore” presente sul sito web della società convenuta, tramite la quale sono visibili migliaia di immagini generate che riproducono opere protette, accompagnate da descrizioni che incentivano l’uso dei medesimi prompt da parte di altri utenti. L’esposizione e promozione pubblica di questi contenuti, oltre a facilitare ulteriori infrazioni, rafforzerebbe l’impressione di legittimità del servizio, alimentando così una diffusa confusione tra gli utenti in merito all’origine e all’autorizzazione delle immagini.

Sul piano della responsabilità indiretta, da un lato, si sostiene che Midjourney abbia la capacità di controllare le attività degli utenti, filtrando contenuti potenzialmente illeciti (come già avviene per contenuti violenti o sessualmente espliciti), e che quindi tragga un vantaggio economico diretto non bloccando i contenuti protetti, in virtù dei piani di abbonamento a pagamento. Dall’altro, si afferma che Midjourney fosse consapevole, o “deliberatamente cieca”, rispetto alle violazioni commesse dai propri utenti e che, attraverso la struttura e le scelte progettuali del proprio servizio, abbia concretamente contribuito e incentivato tali condotte.

Secondo quanto rappresentato nell’atto introduttivo del giudizio, la condotta della società convenuta non rappresenterebbe un fenomeno isolato, ma una minaccia sistemica che rischia di minare i principi stessi su cui si fonda la disciplina del diritto d’autore. Midjourney, a detta dei Ricorrenti, si approprierebbe indebitamente dei benefici economici dell’attività creativa altrui senza sostenerne i costi, realizzando una forma di concorrenza sleale rispetto a coloro che rispettano gli obblighi di licenza e le limitazioni contrattuali. Tale dinamica comporterebbe un’erosione progressiva dei diritti esclusivi spettanti agli autori, riducendo drasticamente la possibilità di controllare la riproduzione, distribuzione ed elaborazione delle opere originarie.

A ciò si aggiungerebbe un danno irreparabile per i titolari dei diritti, non solo in termini economici, ma anche in relazione alla percezione pubblica dell’autenticità delle opere. La diffusione massiva e incontrollata di immagini “simil-originali” contribuirebbe a generare confusione nei consumatori e a svilire il valore stesso della produzione creativa. In ultima analisi, l’intero modello di business di Midjourney viene descritto dai ricorrenti come un vero e proprio “*contrabbando digitale*”, idoneo a minacciare la sostenibilità dell’intera industria cinematografica statunitense, che rappresenta un settore strategico tanto per l’economia nazionale quanto per la cultura globale.

Le richieste rivolte alla Corte sono molteplici e comprendono il risarcimento dei danni subiti, la restituzione dei profitti illeciti ottenuti dalla società convenuta, l’adozione di un’ingiunzione preliminare e permanente per impedire ulteriori violazioni, nonché il rimborso delle spese legali. I Ricorrenti invocano inoltre l’applicazione del massimo dei danni statuari previsti dalla legge, pari a 150.000 dollari per ogni opera violata, in ragione del carattere volontario e sistematico delle infrazioni. È infine stata richiesta l’instaurazione di un giudizio con giuria.

In conclusione, la vertenza tra Disney, Universal e Midjourney si configura come un banco di prova per la tenuta del diritto d'autore nell'era dell'intelligenza artificiale. Essa evidenzia la necessità urgente di aggiornare il quadro normativo esistente, al fine di bilanciare il progresso tecnologico con la tutela effettiva dei diritti dei creatori e la salvaguardia di un'economia culturale equa e sostenibile.

EMANUELA BURGIO

<https://news.justia.com/wp-content/uploads/2025/06/Disney-Universal-v.-Midjourney-Complaint.pdf>

### 2025/2(14)MM

#### **L'ordine di conservazione dei log di output impartito a Open AI il 13.5.2025 dalla corte distrettuale di New York nella causa intentata dal New York Times per violazione di copyright**

Con ordine del 13 maggio 2025 nella causa OpenAI, Inc., Copyright Infringement Litigation (n. 1:23-cv-11195), la corte distrettuale di New York (la **Corte**) ha ordinato ad OpenAI, Inc. (**OpenAI**) di conservare e separare fino a nuova disposizione tutti i log di output degli utenti del noto servizio ChatGPT che altrimenti verrebbero eliminati, inclusi i dati la cui cancellazione è espressamente richiesta dagli utenti o comunque imposta da leggi e regolamenti in materia di privacy.

La questione relativa all'eliminazione dei log di output da parte di OpenAI era già stata sollevata nel gennaio 2025 dalle società attrici (New York Times Company, Center for Investigative Reporting, Daily News, LP, et al.; di seguito, le **Attrici**), le quali ritengono che tali dati siano fondamentali per dimostrare le proprie allegazioni di violazione di copyright in quanto essi potrebbero contenere riproduzioni identiche o sostanzialmente identiche di ampie porzioni delle proprie opere dell'ingegno. Nel corso dell'udienza del 22 gennaio 2025, la Corte, pur respingendo la richiesta delle Attrici di una "conservazione integrale dei log di output", aveva chiesto a OpenAI se fosse tecnicamente possibile separare da tutti i dati conservati quelli degli utenti che avevano espressamente richiesto la cancellazione dei propri log, oppure di anonimizzarli in modo da bilanciare le esigenze istruttorie con le "preoccupazioni" espresse da OpenAI in materia di privacy. OpenAI, infatti, si era opposta alla "richiesta generale e indiscriminata di conservazione totale dei dati" avanzata dalle Attrici, richiamando non solo i propri obblighi contrattuali nel rispettare le preferenze e le richieste degli utenti alla cancellazione dei dati, ma anche la necessità di osservare le numerose leggi e regolamenti in tema di privacy che prevedono il diritto degli utenti alla cancellazione dei propri dati personali.

Ciò premesso, gli sviluppi più recenti hanno spinto le Attrici, con istanza del 12 maggio 2025, a richiedere alla Corte di anticipare l'udienza istruttoria per discutere della cancellazione, da parte di OpenAI, di alcuni log di output. In particolare, il 31 marzo 2025 OpenAI aveva dichiarato – in risposta a un

ordine di informazioni della Corte – che il volume delle “conversazioni degli utenti” eliminate a partire dal 27 dicembre 2023 (data del deposito del ricorso da parte del New York Times Company) era “sostanziale”. Successivamente, l’11 aprile 2025 OpenAI aveva fornito alle Attrici oltre tre terabyte di metadati che documentavano il volume delle conversazioni utente detenute, alla data di inoltro, per i servizi ChatGPT Free, Pro e Plus.

Sulla base di detti elementi, le Attrici hanno sostenuto che: (i) nei mesi immediatamente successivi al deposito del ricorso introduttivo OpenAI aveva cancellato una quota significativa delle conversazioni utente inerenti ai servizi ChatGPT Free, Plus e Pro; e (ii) anche dopo il gennaio 2025, nonostante il tentativo delle Attrici di ottenere un ordine di conservazione delle conversazioni utenti rilevanti, OpenAI aveva continuato a eliminarle.

Considerati gli elementi rappresentati dalle Attrici e preso atto che OpenAI non ha indicato se abbia adottato o intenda adottare misure per conservare e separare i log di output destinati ad essere eliminati, la Corte ha ordinato ad OpenAI di conservare e separare tutti i log di output che altrimenti verrebbero eliminati, a partire dal 13 maggio 2025 fino a nuova disposizione. Tale obbligo, per espressa indicazione della Corte, si applica indipendentemente dal fatto che i dati in questione dovrebbero essere cancellati per espressa richiesta dell’utente oppure in applicazione di leggi e regolamenti in materia di privacy.

MATTEO MANSI

<https://storage.courtlistener.com/recap/gov.uscourts.nysd.640396/gov.uscourts.nysd.640396.551.0.pdf>

### 2025/2(15)FG

**Le delibere AGCOM n. 142/25/CONS del 13.6.2025 e n. 172/25/CONS del 3.7.2025 relative alla valutazione della rappresentatività degli organismi di gestione collettiva (OGC) e delle entità di gestione indipendenti (EGI) per il 2024**

Il 13 giugno 2025 è stata pubblicata sul sito istituzionale dell’Autorità per le Garanzie nelle Comunicazioni (**AGCOM** o **Autorità**) la **delibera n. 142/25/CONS**, avente ad oggetto la valutazione della rappresentatività degli organismi di gestione collettiva (**OGC**) e delle entità di gestione indipendenti (**EGI**) per l’anno 2024, ai sensi dell’art. 8 del Regolamento sull’equo compenso di autori, artisti, interpreti ed esecutori e sulla gestione dei diritti connessi da parte degli OGC e delle EGI, adottato dall’Autorità in attuazione dell’articolo 180-ter della legge 22 aprile 1941, n. 633 sul diritto d’autore (**LDA**) nonché dell’art. 180(2)(1) LDA, come modificato dalla legge 30 dicembre 2023, n. 214, contenuto nell’Allegato A alla delibera n. 95/24/CONS (il **Regolamento**) (su cui v. in questa Rubrica la notizia n. 27 nel [numero 2/2024](#) [2024/2(27)FG]).

Il Regolamento si colloca all’interno di un percorso normativo di riforma della gestione collettiva dei diritti d’autore e dei diritti connessi, volto a

garantire maggiore trasparenza, certezza giuridica e parità di trattamento fra i diversi soggetti operanti nel settore, anche in considerazione dell'apertura del mercato a nuove entità di gestione indipendenti, a seguito della sentenza LEA c. JAMENDO SA (causa C10/22 sentenza della Corte di giustizia del 21 marzo 2024, su cui v. in questa Rubrica la notizia n. 5 nel [numero 1/2024 \[2024/1\(5\)FG\]](#)).

Il provvedimento emanato con la delibera n. 142/25/CONS costituisce la prima applicazione concreta del Regolamento.

La determinazione dei livelli di rappresentatività è funzionale, in particolare, all'individuazione degli organismi legittimati a stipulare licenze collettive estese, che producono effetti anche nei confronti dei soggetti non associati ad alcun organismo di gestione, i cosiddetti "apolidi". Come ricordato dall'Autorità nella parte motivazionale del provvedimento, il d.lgs.177/2021, trasponendo l'articolo 12 della direttiva (UE) 2019/790 (direttiva copyright nel mercato unico digitale), ha introdotto per la prima volta nel nostro ordinamento una disciplina organica delle licenze collettive estese, attribuendo rilevanza alla rappresentatività degli organismi collettivi in relazione alla stipulazione di contratti aventi effetti anche nei confronti dei soggetti non aderenti a nessuna collecting. La norma, nello specifico, prevede che, per i diritti cosiddetti "a compenso" (quali quelli disciplinati dagli articoli 18-bis, 46-bis, 73, 73-bis, 80 e 84 LDA), gli accordi di licenza sottoscritti dai tre organismi maggiormente rappresentativi producano effetti erga omnes, salvo l'esercizio del diritto di opt-out da parte dei titolari dei diritti.

D'altro lato, l'art. 180(2)(1) LDA, stabilendo che le licenze siano concesse a condizioni economiche ragionevoli e proporzionate non solo al valore economico dell'utilizzo, ma anche alla rappresentatività di ciascun organismo di gestione, ha ulteriormente rafforzato la funzione del calcolo della rappresentatività come strumento di trasparenza e di riequilibrio nelle dinamiche negoziali.

In sede di prima applicazione, come previsto dall'art. 8(7) del Regolamento, l'Autorità ha stabilito di utilizzare un criterio basato sulla media annua dei compensi incassati dagli organismi di gestione collettiva per ciascuna tipologia di diritto, rilevata sugli ultimi tre esercizi, sulla base dei bilanci certificati. La ratio di tale scelta metodologica risiede nella volontà di individuare un parametro oggettivo e di facile riscontro, idoneo a restituire una fotografia il più possibile neutrale della capacità economica di ciascun soggetto, pur nella consapevolezza che si tratta di una soluzione transitoria e non definitiva.

Nel dettaglio, la delibera n. 142/25/CONS evidenzia che il criterio del fatturato incassato è stato preferito, nella fase di prima applicazione, alla luce delle esigenze di celerità poste dal legislatore. L'Autorità ha tuttavia sottolineato che questo metodo, pur rappresentando un passaggio necessario, è destinato a essere superato dal criterio dell'effettivo utilizzo dei repertori, che diverrà operativo a partire dall'esercizio successivo (2025), secondo le modalità dettagliate nell'Allegato B alla delibera n. 95/24/CONS.

In sintesi, la delibera n. 142/25/CONS fa emergere una dominanza nettissima della SIAE sia nel segmento degli autori musicali che in quello degli autori cinematografici. Per gli artisti interpreti e i produttori fonografici, la



rappresentatività è più frammentata, con Nuovo Imaie e SCF a dominare rispettivamente nei settori musicali e fonografici, mentre altri soggetti gestiscono quote più contenute.

A tal riguardo, la delibera n. 142/25/CONS chiarisce che i dati di rappresentatività approvati devono intendersi come indicatori di carattere generale, volti a fornire un orientamento per le negoziazioni, ma non vincolanti laddove l'utilizzatore e l'organismo siano in grado di documentare, con dati analitici, un diverso grado di effettivo sfruttamento del repertorio. La tabella allegata al provvedimento riporta le percentuali di rappresentatività per ciascuna categoria di titolari di diritti (autori di opere musicali, autori di opere cinematografiche e assimilate, artisti interpreti o esecutori, produttori fonografici).

L'Autorità ha inoltre richiamato l'importanza di vigilare affinché tali dati non siano utilizzati in modo strumentale o distorsivo, ad esempio per escludere soggetti di minori dimensioni o di più recente costituzione, che potrebbero non disporre di storicità sufficiente nei dati di fatturato incassato. In questa prospettiva, la Delibera sottolinea che l'Autorità si riserva di esercitare i poteri di controllo previsti dall'art. 40 del d.lgs. 35/2017 e di adottare ogni opportuno provvedimento per scongiurare condotte anticoncorrenziali.

Di rilievo, in un'ottica di progressivo consolidamento del nuovo regime, è anche la **successiva delibera n. 172/25/CONS**, pubblicata il 3 luglio 2025, con la quale l'Autorità ha disposto l'estensione dei termini per il deposito dei dati necessari ai fini della determinazione della rappresentatività per l'esercizio 2025. La proroga si è resa opportuna al fine di consentire agli organismi di gestione collettiva e alle entità di gestione indipendenti di adeguare le proprie procedure interne e predisporre la documentazione richiesta in maniera completa e conforme agli standard definiti dall'Autorità. Il differimento dei termini ha altresì lo scopo di ridurre al minimo eventuali disallineamenti interpretativi, garantendo uniformità e qualità dei dati che diverranno la base del prossimo aggiornamento degli elenchi.

La delibera n. 172/25/CONS evidenzia la volontà di AGCOM di accompagnare l'attuazione del nuovo quadro regolatorio con un approccio pragmatico e collaborativo, che tenga conto delle difficoltà operative connesse alla fase di avvio e della necessità di evitare effetti penalizzanti per gli operatori di più recente costituzione o di dimensioni contenute. Tale impostazione appare coerente con i principi di proporzionalità e di non discriminazione sanciti dalla normativa europea e con la finalità di favorire un mercato contendibile e aperto alla concorrenza.

In prospettiva, l'assetto delineato dalla delibera n. 142/25/CONS e integrato dalla successiva proroga introdotta con la delibera n. 172/25/CONS rappresenta un passaggio fondamentale verso un modello di gestione collettiva e indipendente dei diritti improntato a criteri di maggiore trasparenza, equità e accountability. La sfida per i prossimi esercizi sarà quella di consolidare un sistema di raccolta e verifica dei dati idoneo a rappresentare in modo attendibile l'effettiva capacità degli organismi di generare valore economico per i titolari dei diritti, tenendo conto dell'evoluzione del mercato digitale e della crescente pluralità degli operatori.

La corretta implementazione di tale disciplina, unita alla capacità dell’Autorità di monitorarne gli effetti e di intervenire in caso di criticità, rappresenterà un fattore decisivo per assicurare un equilibrio tra la tutela dei diritti degli autori e degli artisti interpreti o esecutori e la promozione di un ambiente competitivo e innovativo.

FRANCESCO GROSSI

[https://www.agcom.it/sites/default/files/provvedimenti/delibera/2025/Delibera%20142\\_25\\_CONS\\_Calcolo%20rappresentativit%C3%A0%20%2B%20ALLEGATO%20A.pdf](https://www.agcom.it/sites/default/files/provvedimenti/delibera/2025/Delibera%20142_25_CONS_Calcolo%20rappresentativit%C3%A0%20%2B%20ALLEGATO%20A.pdf)

[https://www.agcom.it/sites/default/files/provvedimenti/delibera/2025/Delibera%20172\\_25\\_CONS%20.pdf](https://www.agcom.it/sites/default/files/provvedimenti/delibera/2025/Delibera%20172_25_CONS%20.pdf)

## 2025/2(16)RA

### I provvedimenti dell’AGCM del 11.6.2025 in materia di pratiche commerciali scorrette relativi a pratiche di “influencer marketing” realizzate da sei influencer

L’11 giugno 2025, l’Autorità Garante della Concorrenza e del Mercato (AGCM o **Autorità**) ha comunicato di avere adottato dei provvedimenti nei confronti di alcuni *influencer*, i quali, in modo simile tra loro, secondo le verifiche e le valutazioni svolte dall’Autorità:

- hanno pubblicato sistematicamente, su *social network* e siti internet, foto e video in cui offrivano consigli a pagamento per ottenere guadagni ‘facili e sicuri’, sulla falsariga del modello vincente da loro incarnato, senza tuttavia utilizzare alcuna dicitura di *advertisement* per informare i consumatori della natura pubblicitaria dei contenuti diffusi;
- non hanno adeguatamente evidenziato gli elementi rilevanti per le decisioni di consumo dei loro *followers* (come il costo dei beni e dei servizi offerti, l’identificazione e/o il recapito del professionista);
- hanno vantato una popolarità sulle piattaforme *social* falsata dalla presenza di *followers* non autentici, oltretutto utilizzando testimonianze e recensioni esclusivamente positive e la cui autenticità non è risultata verificabile;
- hanno fatto ricorso a presunti *endorsement* da parte di *brand*, società giornalistiche e programmi televisivi non riscontrabili;
- hanno vantato risultati professionali e personali eccezionali non verificabili.

Alla luce di tali condotte, l’AGCM ha ipotizzato la possibile realizzazione di pratiche commerciali scorrette da parte di tali *influencer*, in violazione degli artt. 20 e seguenti del D.lgs. 206/2005 (**Codice del consumo**).

A fronte di tale prospettiva, alcuni professionisti – in particolare, Luca Marani, Alessandro Berton, Hamza Mourai e Davide Caiazzo – hanno proposto degli impegni volti a rimuovere i profili di contestata scorrettezza della loro condotta. L’Autorità, reputandoli idonei, ha chiuso i relativi

procedimenti senza accertare le infrazioni e rendendo vincolanti gli impegni proposti dagli *influencer*. Tra questi impegni rilevano, in particolare, quelli volti a: rimuovere le espressioni che enfatizzano guadagni facili o privi di rischi da tutti i canali *social* e siti internet utilizzati; inserire *disclaimer* pubblicitari; rimuovere dai propri profili *social follower* non autentici e a monitorarli con strumenti idonei; integrare le comunicazioni concernenti il costo dei beni e dei servizi offerti e i recapiti del professionista; rendere verificabili le affermazioni relative al proprio prestigio sui *post* e sui siti internet.

Due *influencer*, che nel corso del procedimento dinnanzi all’Autorità hanno insistito strenuamente nel difendere la liceità della loro condotta, sono stati invece sanzionati. Si tratta di Luca De Stefani (alias Big Luca) e di Michele Leka, nei confronti dei quali è stata irrogata una sanzione, rispettivamente, di 60.000 euro e di 5.000 euro.

Nei provvedimenti emessi verso tali soggetti, in particolare, l’AGCM ha avuto modo di precisare: da un lato, che l’*influencer* riveste la qualifica di professionista ai sensi dell’art. 18 del Codice del consumo, svolgendo frequentemente attività promozionali rivolte ai consumatori e alle microimprese; dall’altro, che la pervasività del mezzo utilizzato da tali soggetti – vale a dire, i *social* e più in generale i siti internet – incide (in aumento) sulla quantificazione della sanzione da irrogare nei loro confronti.

RICCARDO ALFONSI

<https://www.agcm.it/media/comunicati-stampa/2025/6/PS12814-PS12815-PS12816-PS12817-PS12818-PS12826>

### 2025/2(17)FGu

#### Il provvedimento dell’AGCM del 20.5.2025 contro Poste italiane per pratica scorretta sulle app Banco Posta e Postepay

Il 20 maggio 2025, l’Autorità garante della concorrenza e del mercato (AGCM o Autorità) ha irrogato una sanzione amministrativa pecuniaria di 4 milioni di euro nei confronti di Poste Italiane (anche **Professionista** o **Società**), a seguito dell’accertamento di una pratica commerciale scorretta posta in essere dal Professionista nell’erogazione del servizio sulle app Banco Posta e Postepay a partire dall’aprile 2024.

Tale pratica, ritenuta contraria alla diligenza professionale e caratterizzata da profili di aggressività, in violazione degli articoli 20, 24 e 25 del d.lgs. 206/2005 (**Codice del consumo**), consisteva nel blocco delle suddette applicazioni installate negli smartphone con sistema operativo Android, in caso di mancato rilascio da parte degli utenti dell’autorizzazione ad accedere ai dati del proprio smartphone.

Il procedimento è stato avviato a seguito delle numerose segnalazioni pervenute da parte di alcuni utenti titolari di rapporti Banco Posta e Postepay, i quali, all’apertura dell’app, si sono imbattuti in una notifica titolata

“Proteggi il tuo dispositivo”, seguita da un breve messaggio che informava in merito all’adozione da parte del Professionista di un nuovo presidio antifrode. Più nel dettaglio, per quanto concerne il carattere aggressivo della condotta, l’utente poteva rifiutare di fornire l’autorizzazione di accesso ai propri dati per un massimo di tre volte (successivamente divenute cinque), esaurite le quali veniva inibito l’utilizzo dei servizi in app, con la sola possibilità di modificare le impostazioni del proprio cellulare fornendo l’autorizzazione all’accesso dei dati.

Invero, l’alterazione del comportamento economico dei consumatori, dovuto all’obbligatorietà del consenso, emerge anche dal raffronto tra il primo periodo di adozione della misura da parte della Società e il periodo successivo al 4 luglio 2024 – con l’aumento degli accessi consentiti al servizio da tre a cinque – in cui le risultanze istruttorie evidenziano che una grande fetta di utenti che non aveva inizialmente fornito l’autorizzazione (pari a circa 1.500.000 – 2.500.000) ha reiterato la scelta di non prestare il consenso al trattamento dei dati.

Ulteriori contestazioni hanno riguardato la genericità dei dati per i quali il Professionista richiedeva l’accesso che, oltre a rendere indeterminate le finalità sottese al trattamento, consentiva il monitoraggio e l’analisi di altre app di operatori concorrenti in background durante l’utilizzo delle applicazioni di Poste Italiane (cd. running).

A seguito delle numerose audizioni e richieste di informazioni da parte dell’Autorità, il Professionista ha comunicato di aver rimosso il blocco delle app Banco Posta e Postepay, a far data dal 18 febbraio 2025, permettendo così agli utenti di confermare o revocare l’autorizzazione, prevedendo altresì la possibilità di continuare a utilizzare i servizi senza prestare necessariamente il consenso.

Nonostante l’adozione di tali misure correttive e ripristinatorie, nelle argomentazioni difensive Poste Italiane ha sostenuto che l’implementazione della piattaforma antifrode in esame fosse necessaria al rispetto delle prescrizioni contenute nella direttiva (UE) 2015/2366 (**PSD2** o **direttiva sui servizi di pagamento 2**) e degli Standard Tecnici di Regolamentazione (**RTS**) adottati con il regolamento (UE) 2018/839.

Inoltre, tanto nelle già citate argomentazioni difensive, quanto nelle controdeduzioni successive alla contestazione degli addebiti, il Professionista ha confutato la presunta natura economico/commerciale della pratica oggetto del provvedimento, specificando che i dati acquisiti avevano l’esclusiva finalità di contrasto alle frodi informatiche e che il processo di anonimizzazione e segregazione degli stessi su una piattaforma distinta portasse ad escludere la configurazione di una “pratica commerciale tanto più come scorretta e aggressiva”.

Come corollario di questa argomentazione, la Società ha eccepito l’inapplicabilità al caso di specie del Codice del consumo, stante l’asserita assenza di un utilizzo commerciale dei dati che non avrebbe consentito di qualificare il trattamento come controprestazione per un servizio.

Nella memoria difensiva depositata il 10 marzo 2025 il Professionista ha altresì dichiarato che l’adozione della misura antifrode, applicata esclusivamente ai dispositivi Android per via della loro natura aperta (cd.



Open source), non presenterebbe alcun profilo di costrizione o imposizione poiché i disagi riscontrati dall’Autorità e ascrivibili al blocco delle app erano comunque superabili dall’utente effettuando le operazioni tramite browser e/o Ufficio postale.

Infine, Poste Italiane ha reputato rilevante sottolineare – in ossequio al principio di leale collaborazione e buona fede – l’adozione spontanea delle misure ripristinatorie e migliorative che hanno consentito a tutti gli utenti, indipendentemente dalle scelte effettuate in precedenza, di revocare, modificare o confermare la prestazione del consenso, garantendo comunque un efficace sistema di protezione dalle frodi informatiche.

Tuttavia, dette osservazioni non hanno trovato un riscontro positivo nelle valutazioni conclusive effettuate dall’AGCM, la quale, acquisiti i pareri dell’Autorità garante per la concorrenza ed il mercato (**AGCOM**), della Banca d’Italia e dell’Autorità garante per la protezione dei dati personali, ha riscontrato la presenza di una pratica commerciale scorretta idonea a compromettere l’autodeterminazione degli utenti.

La violazione degli artt. 24 e 25 del Codice del consumo, infatti, si evince chiaramente dalla circostanza che la pratica in esame imponeva il rilascio del consenso quale condizione necessaria per accedere a funzionalità di un servizio oggetto di un rapporto contrattuale del quale i consumatori erano già titolari.

Pertanto, non rilevarebbe neanche l’argomentazione difensiva offerta dal Professionista in merito alla possibilità di usufruire parimenti dei servizi mediante i canali alternativi (browser e/o Ufficio postale), poiché tale tesi omette di considerare i vantaggi delle app sia da un punto di vista logistico rispetto all’Ufficio postale, per via del netto risparmio di tempo e della maggiore accessibilità soprattutto per coloro che hanno un impedimento fisico, sia in termini di immediatezza operativa rispetto al browser, per via delle interfacce più intuitive che contribuiscono a migliorare l’esperienza del consumatore.

L’ulteriore accertamento in merito alla violazione dell’art. 20 del Codice del consumo è agevolmente riscontrabile nel settore dei servizi finanziari e di pagamento che ha interessato la pratica oggetto del provvedimento, ove le eccessive differenze di dimensioni e conoscenze tra il Professionista e la clientela, hanno determinato un elevato grado di asimmetrie informative e un indebito condizionamento che avrebbe richiesto un livello di diligenza professionale particolarmente rigoroso.

L’autorità procedente ha altresì respinto la controdeduzione prodotta da Poste Italiane circa la necessità della condotta ai fini del rispetto delle prescrizioni contenute nella PSD2 e nei relativi standard tecnici RTS poiché, come riconosciuto anche dal Professionista successivamente alla contestazione degli addebiti, l’art. 2 del Regolamento (UE) 2018/389 dispone tra gli obblighi generali di autenticazione che i meccanismi di monitoraggio tengano conto, come minimo, dei segnali di presenza di eventuali malware, ma non prospetta in maniera specifica le modalità tecniche di funzionamento che il sistema anti-malware deve presentare per ottemperare a tale obbligo.

Peraltro, la solerzia dimostrata dal Professionista attraverso la rimozione del blocco delle app in seguito ai moniti ricevuti nelle varie audizioni, rivela

implicitamente la praticabilità di una soluzione alternativa e meno gravosa per l'utente che avrebbe consentito la piena fruizione dei servizi assicurando al contempo la tutela dalle frodi informatiche, in ossequio al principio di proporzionalità.

Oltretutto, ai fini della qualificazione della pratica come “scorretta”, non è in discussione il dato che emerge dal parere della Banca d'Italia, acquisito ai sensi dell'art. 27(1-*bis*) del Codice del consumo, in ordine alla circostanza che la condotta in esame abbia comunque garantito la continuità nei servizi di pagamento grazie alla sussistenza di canali alternativi.

Ciò che assume rilievo prioritario in relazione all'applicabilità della disciplina consumeristica, invece, è che siffatta pratica abbia limitato gli utenti nell'usufruire di tutte le prerogative loro spettanti sulla base del rapporto contrattuale, compresi dunque i servizi Banco Posta e Postepay tramite app.

Benché le argomentazioni difensive del Professionista depongano nel senso di escludere una finalità propriamente commerciale del trattamento, l'attività istruttoria svolta dall'AGCM dischiude un'intrinseca incompatibilità della libera manifestazione del consenso con la rinnovata veste patrimoniale che esso assume per l'erogazione dei servizi finanziari, specie nel caso in cui la scelta dell'utente non sia stata assunta in maniera libera e consapevole, bensì indebitamente condizionata dalla volontà di mantenere una prerogativa di cui è titolare in virtù di un rapporto di consumo con la Società.

Pertanto, in conformità ai criteri dettati dall'art.11 l. 689/1981, che per la determinazione della sanzione amministrativa pecuniaria prevedono che si tenga conto della gravità della violazione, dell'opera svolta dall'agente per eliminare o attenuare l'infrazione, della personalità dell'agente e delle sue condizioni economiche, l'Autorità ha fissato l'importo della sanzione amministrativa nella misura di 6 milioni di euro, ridotti a 4 milioni di euro in considerazione della circostanza attenuante del ravvedimento operoso.

Avverso tale provvedimento Poste Italiane potrà presentare ricorso al TAR del Lazio entro sessanta giorni dalla notificazione dello stesso, ai sensi dell'art. 135(1)(b) d.lgs. 104/2010 (Codice del processo amministrativo), ovvero ricorso straordinario al Presidente della Repubblica, ai sensi dell'art. 8 DPR 1199/1971, nel termine di centoventi giorni dalla data di notificazione del provvedimento.

FRANCESCO GUECI

<https://www.agcm.it/dotcmsdoc/bollettini/2025/22-25.pdf>

## 2025/2(18)IG

### Il provvedimento del Garante privacy italiano n. 232 del 10.4.2025 adottato nei confronti della società che gestisce il chatbot 'Replika'

L'Autorità garante per la protezione dei dati personali (**Autorità** o **Garante** o **GPDP**), con provvedimento n. 232 del 10.4.2025 (doc. web [10130115](#)) (il **Provvedimento** o la **Decisione**), ha irrogato alla società Luka Inc. (la **Società**) una sanzione amministrativa pari a 5 milioni di euro, a seguito dell'accertamento di plurime violazioni della normativa in materia di

protezione dei dati personali - in particolare degli articoli 5(1)(a) e (c), 6, 12, 13, 24 e 25(1) del regolamento (UE) 2016/679 (GDPR) - connesse all'erogazione del servizio Replika – un chatbot dotato di interfaccia scritta e vocale, sviluppato e gestito dalla stessa Società, basato su un sistema di intelligenza artificiale generativa (**Replika** o **chatbot**).

La Decisione è stata adottata all'esito di un'articolata e approfondita istruttoria, avviata a seguito del provvedimento d'urgenza del 2 febbraio 2023, con cui l'Autorità aveva disposto la limitazione provvisoria del trattamento dei dati personali relativi agli interessati stabiliti nel territorio italiano (su cui v. in questa Rubrica la notizia n. 12 nel [numero 1/2023 \[2023/1\(12\)IG\]](#), e in *Atlante*, p. 319), a cui è seguita la sospensione di tale misura, con provvedimento del 22 giugno 2023, condizionata all'adozione di interventi correttivi volti ad assicurare la conformità del trattamento alla normativa vigente.

Tra le varie violazioni accertate dal Garante, particolare rilievo assume la mancata adozione da parte della società Luka Inc. di misure tecniche e organizzative idonee a verificare l'età degli utenti del servizio Replika. Sebbene il servizio fosse formalmente destinato esclusivamente a soggetti maggiorenni, alla data del 2 febbraio 2023 non era stato implementato alcun meccanismo efficace per impedire l'accesso ai minori, né in fase di registrazione, né nel corso dell'utilizzo. L'accesso al servizio, infatti, richiedeva unicamente l'inserimento di dati anagrafici basilari (nome, email e genere), senza alcun sistema di verifica dell'età e senza blocchi automatici anche laddove l'utente avesse dichiarato la propria minore età. Ciò ha comportato il concreto rischio che anche soggetti al di sotto dei 13 anni potessero accedere liberamente al servizio del chatbot, entrando in contatto con contenuti potenzialmente inappropriati rispetto al loro sviluppo psicofisico, inclusi messaggi a sfondo sessuale.

Tale omissione ha messo in luce una inadeguata valutazione preventiva dei rischi derivanti dal trattamento dei dati personali di soggetti vulnerabili, in violazione sia del principio di minimizzazione (art. 5(1)(c) GDPR), sia degli obblighi in materia di protezione dei dati fin dalla fase di progettazione (artt. 24 e 25(1) GDPR). In sostanza, Luka Inc. ha effettuato trattamenti di dati personali non strettamente necessari rispetto alla finalità dichiarata – ossia l'erogazione del servizio esclusivamente a soggetti maggiorenni – coinvolgendo anche utenti per i quali non avrebbe dovuto essere prevista alcuna raccolta di dati.

Solo a seguito del provvedimento d'urgenza del Garante del 2 febbraio 2023 (su cui v. in questa Rubrica la notizia n. 12 nel [numero 1/2023 \[2023/1\(12\)IG\]](#), e in *Atlante*, p. 319), la Società ha introdotto un *age gate* nelle pagine di registrazione e un sistema di blocco temporaneo (*cooling off period*), volto a limitare il re-inserimento immediato di dati anagrafici falsi. Tuttavia, il sistema di verifica dell'età implementato da Luka Inc. è risultato, alla data del Provvedimento, ancora carente sotto diversi profili. È infatti emerso che: 1) l'utente, una volta creato il profilo, può modificare la data di nascita senza alcuna verifica da parte del titolare; 2) il meccanismo di blocco temporaneo (*cooling off*) può essere aggirato facilmente tramite la modalità di navigazione in incognito; 3) non sono attivi sistemi di analisi linguistica in

grado di rilevare automaticamente se un utente si identifica come minorenne, salvo i rari casi in cui l'utente si dichiara in modo inequivocabile sotto i 18 anni. In tali situazioni, l'applicazione si limita a chiedere una conferma generica della maggiore età; 4) pur essendo presente la funzione per segnalare contenuti inappropriati, non è chiaro se e quali conseguenze derivino da tali segnalazioni.

Nel Provvedimento è inoltre chiaramente indicato che le violazioni riscontrate sono da ritenersi di natura colposa, in linea con i principi affermati dal Gruppo Articolo 29 nelle linee Guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del GDPR - recepite dal Comitato europeo per la protezione dei dati (**EDPB**) il 25 maggio 2018 - e con la più recente giurisprudenza della Corte di giustizia dell'Unione europea (**CGUE**). In particolare, l'Autorità ha evidenziato che la Società non poteva ignorare l'illiceità delle proprie condotte, né sottrarsi al dovere di conoscere e applicare la normativa euro-unitaria, trattandosi di un servizio reso disponibile nel territorio dell'Unione europea e caratterizzato da un rilevante impatto sui diritti fondamentali degli interessati. La mancata adozione di misure tecniche e organizzative adeguate, è stata dunque considerata espressione di una colpa grave, “proprio per l'ampiezza e la natura innovativa del servizio offerto, che comporta un trattamento su larga scala di dati personali a livello mondiale”.

ILARIA GARACI

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10130115>

## 2025/2(19)EG

### Il provvedimento del Garante privacy italiano n. 243 del 29.4.2025 nei confronti della Regione Lombardia in relazione ai metadati di posta elettronica e ai log di navigazione internet dei suoi dipendenti

Il Garante per la protezione dei dati personali (**Autorità** o **Garante** o **GPDP**) con il provvedimento n. 243 del 29 aprile 2025 (doc. web [10134221](#)) (il **Provvedimento** o la **Decisione**) ha emesso la prima sanzione relativa all'illegittima conservazione dei metadati delle e-mail dei dipendenti e dei log di navigazione web. Il caso coinvolge la Regione Lombardia (**Regione** o **Ente**), destinataria di una sanzione pari a 50mila euro originata da numerose violazioni riscontrate dall'Autorità a seguito di un ciclo ispettivo volto a verificare l'osservanza da parte dell'Ente della normativa privacy nell'ambito dei trattamenti dei dati dei dipendenti, anche nel caso dello svolgimento del lavoro agile.

Il Provvedimento si contraddistingue per la sua portata innovativa, poiché rappresenta la prima concreta applicazione delle linee guida racchiuse nel discusso “Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati”, adottato, a seguito di consultazione pubblica, con Provvedimento

n. 364 del 6 giugno 2024 (il **Documento di indirizzo**) (su cui v. in questa Rubrica, la notizia n. 30 nel [numero 2/2024](#) [2024/2(30)EG]). Come ormai noto, nel Documento di indirizzo, il Garante ha chiarito che i metadati contenuti nelle e-mail dei dipendenti – comprendenti informazioni come mittente, destinatario, orari di invio, dimensioni e indirizzi IP – rappresentano dati personali, la cui conservazione deve essere limitata a 21 giorni. Tale periodo può essere prorogato solo in caso di documentate esigenze tecniche e organizzative che giustifichino un periodo più esteso di conservazione e solo previa stipula di un accordo sindacale o previo ottenimento di autorizzazione dell'Ispettorato Nazionale del Lavoro (INL). Detto in altre parole, il trattamento dei metadati oltre a dover rispettare il regolamento (UE) 2016/679 (**GDPR**) deve avvenire in coerenza con l'art. 4(1) della l. 300/1970 (**Statuto dei lavoratori**), in quanto può tradursi in un illegittimo strumento di controllo a distanza dei lavoratori. Secondo le indicazioni del Garante, dunque, il datore di lavoro che intende prorogare il termine di 21 giorni deve:

- fornire adeguata documentazione circa le ragioni tecniche e organizzative che giustificano la conservazione dei dati oltre il termine previsto;
- formalizzare un accordo con le rappresentanze sindacali o altrimenti ottenere l'autorizzazione dall'Ispettorato Territoriale del Lavoro.

Tanto ricordato, e tornando al Provvedimento, va detto che esso origina da una intensa attività ispettiva condotta dal Garante nei confronti della Regione, all'esito della quale sono state accertate diverse criticità.

**In primo luogo**, dall'esame degli elementi acquisiti nel corso dell'istruttoria, il Garante ha accertato che la Regione Lombardia conservava i **metadati** di posta elettronica dei propri dipendenti per “un ampio periodo temporale” complessivamente pari a 90 giorni per finalità di sicurezza informativa e assistenza tecnica, senza aver previamente stipulato un accordo sindacale.

Al riguardo, nel Provvedimento l'Autorità ricorda di aver affrontato il delicato tema della conservazione dei metadati di posta elettronica nel Documento di indirizzo che contiene indicazioni e chiarimenti volti proprio ad orientare le scelte organizzative e tecniche dei datori di lavoro. Ebbene, nel valutare la condotta posta in essere dall'Ente, il Garante richiama le linee guida contenute nel Documento di indirizzo rammentando che “I metadati di posta elettronica risultano assistiti da garanzie di segretezza, tutelate anche costituzionalmente (artt. 2 e 15 Cost.), intese ad assicurare protezione al nucleo essenziale della dignità della persona e al pieno sviluppo della sua personalità nelle formazioni sociali” e che nel contesto lavorativo permane una “legittima aspettativa di riservatezza in relazione alla corrispondenza e, analogamente, agli elementi ricavabili dai dati esteriori della stessa, che ne definiscono i profili temporali (come la data e l'ora di invio/ricezione) nonché gli aspetti quali-quantitativi anche in ordine ai destinatari e alla frequenza di contatto”.

Ciò premesso, l'Autorità precisa che la conservazione dei metadati per “tale ampio intervallo temporale” (90 giorni) non può essere ricondotta soltanto all'ambito del mero funzionamento delle infrastrutture del sistema della posta elettronica e del suo regolare utilizzo (comma 2 dell'art. 4 dello Statuto dei lavoratori) configurandosi, piuttosto, come “un'attività funzionale alla tutela

dell'integrità del patrimonio informativo e della sicurezza informatica, finalità riconducibile al comma 1 dell'art. 4" dello Statuto dei lavoratori. Il Garante sottolinea inoltre che non può essere invocato, ai fini della liceità del complessivo trattamento, che l'individuazione, da parte della Regione, del termine di 90 giorni per la conservazione dei metadati di posta elettronica sia avvenuta prima della pubblicazione del Documento di indirizzo sui metadati sopra citato. Ciò in quanto i chiarimenti forniti per il tramite di predetto Documento "si pongono in linea con la precedente interpretazione sostenuta dall'Autorità nel solco di un consolidato orientamento, sin dal 2016". Alla luce di tali rilievi, il Garante dichiara illecito il trattamento in quanto effettuato in assenza delle garanzie procedurali previste dall'art. 4(1) Statuto dei lavoratori, integrando altresì una violazione degli artt. 5(1)(a), 6 e 88(1) GDPR, nonché dell'art. 114 del d.lgs. 196/2003 (**Codice privacy**).

**La seconda violazione** riscontrata – di portata ancor più significativa – riguarda la gestione inadeguata dei **log di navigazione in Internet**. Dall'istruttoria il Garante ha appreso che l'Ente conservava per un periodo di 365 giorni informazioni inerenti ai siti web visitati dai dipendenti, inclusi quelli relativi ai tentativi falliti di accesso ai siti già censiti all'interno di una apposita black list, cui era comunque inibito l'accesso dal sistema, in assenza della previa stipulazione di un accordo collettivo con le rappresentanze sindacali.

Sul punto, l'Autorità ricorda che in forza della normativa in materia di controllo a distanza dell'attività dei lavoratori, tanto la raccolta quanto la successiva conservazione dei log di navigazione in Internet richiede il rispetto dell'art.4(1) Statuto dei lavoratori posto che "i sistemi che consentono la tracciatura degli accessi ad Internet non possono essere, in generale, ricompresi nell'ambito di applicabilità dell'art. 4, comma 2 [dello Statuto dei lavoratori], diversamente dai sistemi di inibizione automatica di consultazione in rete (senza conservazione dei tentativi di accesso), da parte dei dipendenti, di specifici contenuti vietati dall'organizzazione di appartenenza". **La Regione doveva, dunque, attenersi alle garanzie procedurali previste dall'art. 4(1) dello Statuto dei lavoratori, ritenute condizione di liceità del trattamento dei dati in questione.**

Peraltro, nel caso di specie, il sistema adottato per finalità di sicurezza della rete consentiva operazioni di tracciatura delle connessioni e dei collegamenti ai siti Internet visitati dai dipendenti che comportava il trattamento di informazioni anche estranee all'attività professionale. A tal proposito, l'Autorità specifica che la legittima esigenza del datore di lavoro di mitigare il rischio di utilizzi impropri della navigazione da parte dei dipendenti "non può giustificare ogni forma di interferenza nella vita privata", occorrendo, invece, privilegiare "la predisposizione di misure tecniche e organizzative idonee a prevenire in radice che le eventuali informazioni relative alla sfera extralavorativa vengano raccolte dando luogo a trattamenti di informazioni personali "non pertinenti" che ricadono nell'ambito di applicazione dell'art. 113 del Codice privacy".

Quanto, invece, alla profondità temporale della conservazione dei dati, il Garante conclude che alla luce di una valutazione globale delle caratteristiche del sistema doveva ritenersi che, pur in presenza di alcune misure sul piano

tecnico ed organizzativo, il trattamento in esame non poteva ritenersi “complessivamente proporzionato rispetto alla finalità perseguita”. Il principio di “limitazione della conservazione” impone, infatti, che i dati personali siano conservati in una forma che consenta l’identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. In quest’ottica, il titolare del trattamento deve altresì adottare – “fin dalla progettazione” e “per impostazione predefinita” (art. 25 GDPR) - misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati, integrando nel trattamento le necessarie garanzie per soddisfare i requisiti del GDPR e tutelare i diritti e le libertà degli interessati. Alla luce degli elementi emersi, il Garante ha ritenuto che il sistema impiegato dalla Regione, fondato sulla registrazione analitica dei siti consultati dal personale dipendente e sulla loro prolungata conservazione, integrava una violazione degli articoli 5(1)(a), (c) ed (e), e 25 GDPR (principi di liceità, minimizzazione, limitazione della conservazione e privacy by design) e dell’art. 113 del Codice Privacy, in relazione all’art. 8 dello Statuto dei lavoratori (divieto di indagine sulle opinioni) e all’art. 10 d.lgs. 276/2003 (divieto di indagini sulle opinioni e trattamenti discriminatori).

**In terzo luogo**, con riferimento ai trattamenti sopra menzionati, il Garante individua un’ulteriore violazione consistente nel mancato svolgimento di una **valutazione d’impatto sulla protezione dei dati ai sensi dell’art. 35 GDPR**.

Il Garante rileva, infatti, che sia il trattamento dei metadati relativi all’utilizzo del servizio di posta elettronica - consistente nella sistematica raccolta dei dati esteriori afferenti alla corrispondenza e-mail (incluse le informazioni relative al mittente/destinatario e all’oggetto di ciascuna e-mail) e nella relativa memorizzazione per 90 giorni – sia il trattamento dei log relativi alla navigazione in Internet - consistente nella raccolta preventiva e generalizzata dei dati concernenti le connessioni ai siti web dei singoli dipendenti e nella relativa memorizzazione per 365 giorni – comportavano rischi specifici per i diritti e le libertà degli interessati nel contesto lavorativo (art. 35 GDPR). La conservazione così prolungata dei metadati e dei dati relativi alle connessioni ai siti web consentiva – ad avviso del Garante - una minuziosa ricostruzione delle abitudini di navigazione e delle relazioni professionali, incidendo così, secondo la valutazione dell’Autorità, in modo significativo sulla sfera privata dei lavoratori, considerati dal legislatore europeo “interessati vulnerabili”.

Proprio questa vulnerabilità, unita alla natura sistematica del monitoraggio, rendeva ineludibile – secondo il Garante - una valutazione d’impatto sulla protezione dei dati da condurre prima dell’avvio dei trattamenti, in conformità alle Linee guida WP29 248 del 4 aprile 2017 e all’art. 88 GDPR, che impone garanzie rafforzate nei contesti occupazionali.

Per tali ragioni, pur prendendo atto del deposito nel corso dell’istruttoria della valutazione di impatto, l’Autorità ha sancito la violazione dell’art. 35 GDPR in quanto anteriormente a tale adempimento, i trattamenti sono stati effettuati in assenza di valutazione di impatto.

**Infine**, nell’ambito del sistema di assistenza tecnica (c.d. “ticketing”), il Garante ha riscontrato che le cronologie dei ticket venivano conservate per oltre sei anni in assenza di accordi formalizzati ex art. 28 GDPR con i fornitori

esterni. Secondo il Garante, ciò ha determinato una duplice violazione: da una parte, il superamento evidente dei limiti massimi di conservazione in assenza di comprovate idonee ragioni “che potessero giustificare una conservazione tanto prolungata dei dati in questione” in contrasto con i principi di limitazione della conservazione e di protezione dei dati personali fin dalla progettazione e per impostazione predefinita, in violazione degli artt. 5(1)(e), e 25 GDPR; dall'altra, la mancanza di garanzie contrattuali che assicurassero ai responsabili del trattamento istruzioni documentate e conformi alla normativa privacy, in violazione dell'art. 28 GDPR.

In conclusione, a fronte delle violazioni riscontrate, il Garante ha irrogato alla Regione Lombardia una sanzione complessiva di 50mila euro, articolata in tre voci distinte che riflettono la diversa gravità e autonomia delle condotte contestate: 20mila euro per l'illiceità del trattamento dei metadati di posta elettronica, 25mila euro per il trattamento dei log di navigazione in Internet e 5mila euro per le anomalie riscontrate nella gestione dei dati relativi alle richieste tecnica del personale dipendente.

La decisione non si esaurisce, tuttavia, nella dimensione afflittiva. Il Garante ha accompagnato la sanzione con un pacchetto di misure correttive di immediata applicazione, imponendo alla Regione:

- l'anonimizzazione dei log relativi ai tentativi di accesso falliti ai siti web presenti nella black list, inclusi quelli già nei sistemi;
- la conservazione dei log di navigazione internet limitata a 90 giorni, con possibilità di estensione previa anonimizzazione per evitare l'identificabilità del dipendente, e cancellazione dei dati oltre tale termine;
- la cifratura dei nomi dei dipendenti assegnatari delle macchine, con specifiche istruzioni al fornitore responsabile del trattamento e limitazione del numero di persone autorizzate al trattamento a soggetti espressamente designati e formati sui rischi connessi;
- l'aggiornamento degli accordi sindacali ai sensi dell'art. 4 dello Statuto dei lavoratori.

ELISA GROSSI

<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10134221>

## 2025/2(20)FN

**La sentenza del TAR Lazio Sez. Prima n. 7625/2025 del 17.4.2025 di interpretazione dell'art. 52(7) Codice privacy sulla diffusione anche integrale del contenuto delle sentenze e degli altri provvedimenti giurisdizionali**

Il TAR Lazio, Sezione Prima, con la sentenza n. 7625/2025, pubblicata il 17 aprile 2025 (la **Sentenza**), si è pronunciato in materia di diffusione del contenuto delle sentenze e degli altri provvedimenti giurisdizionali, offrendo un'interpretazione rilevante dell'art. 52(7) del d.lgs. 196/2003 (**Codice privacy**).

La questione trae origine dalla scelta del Ministero della Giustizia di pubblicare, nella nuova banca dati pubblica delle decisioni di merito, versioni integrali delle sentenze con oscuramento sistematico dei dati personali delle parti, anche in assenza di specifiche richieste di anonimizzazione o provvedimenti del giudice in tal senso. Tale scelta era motivata dall'esigenza di bilanciare il diritto di cronaca e la trasparenza con la protezione dei dati personali, alla luce del GDPR e delle disposizioni interne.

Con la Sentenza il giudice amministrativo ha annullato il provvedimento con cui il Ministero della Giustizia, il 1° dicembre 2023, aveva disposto la dismissione dei web services dell'archivio giurisprudenziale nazionale e l'avvio della nuova banca dati pubblica di merito (**b.d.p.**), nella quale i provvedimenti giurisdizionali sarebbero stati pubblicati in forma integralmente anonima, indipendentemente da specifiche previsioni di legge o decisioni giudiziarie.

Il ricorso era stato proposto da operatori del settore editoriale, dal Consiglio dell'Ordine degli Avvocati di Milano, che avevano evidenziato come l'anonimizzazione massiva dei dati identificativi compromettesse la funzione conoscitiva e culturale della banca dati, rendendo di fatto impossibile lo studio e la comprensione delle pronunce.

Il TAR ha affermato che la normativa vigente – in particolare gli artt. 51 e 52 del Codice Privacy – prevede come regola generale la pubblicazione integrale dei provvedimenti giurisdizionali, ammettendo l'oscuramento solo in casi specifici e su decisione del giudice. Il bilanciamento tra il principio di pubblicità della giurisdizione e la tutela dei dati personali deve avvenire caso per caso e compete esclusivamente all'autorità giudiziaria, non all'amministrazione incaricata della gestione della banca dati.

Il Tribunale ha inoltre rilevato che l'oscuramento indiscriminato non è ragionevole né proporzionato: la comprensione di una pronuncia giurisdizionale richiede infatti la conoscenza dei dati fattuali in essa contenuti, che consentono di coglierne l'esatta portata e i principi applicati. È stato anche sottolineato come un dato personale possa essere inserito in qualsiasi parte del testo, persino nel principio di diritto, rendendo impossibile definire a priori i contenuti oscurabili.

La sentenza ha messo in luce la contraddittorietà dell'assetto introdotto dal Ministero, per cui, mentre la banca dati pubblica conteneva decisioni anonimizzate, un ristretto gruppo di editori privati autorizzati poteva accedere e ripubblicare integralmente le stesse sentenze grazie ad accordi conclusi con il Ministero stesso.

Con l'annullamento del provvedimento impugnato, il TAR ha riaffermato che la pubblicazione integrale dei provvedimenti rappresenta la regola e che eventuali esigenze di tutela della riservatezza, che sono straordinarie, devono essere valutate e disposte caso per caso dal giudice procedente.

In conclusione, la Sentenza riafferma la centralità del principio di pubblicità della giurisdizione – sancito dagli artt. 6 CEDU, 111 Cost. e 47 della Carta di Nizza – che, quindi, non si esaurisce nella celebrazione pubblica dell'udienza, ma si estende anche all'accesso del pubblico al contenuto integrale della sentenza, salvo eccezioni espressamente previste dalla legge o dall'autorità giudiziaria.

FEDERICO NESPEGA

[https://mdp.giustizia-amministrativa.it/visualizza/?nodeRef=frJTQpYBEWCyJRSbLEbl&schema=tar\\_rm&nrg=202401496&nomeFile=202507625\\_01.xml&subDir=Provvedimenti](https://mdp.giustizia-amministrativa.it/visualizza/?nodeRef=frJTQpYBEWCyJRSbLEbl&schema=tar_rm&nrg=202401496&nomeFile=202507625_01.xml&subDir=Provvedimenti)

| 661

## 2025/2(21)SR

### **L’Ordinanza n. 1832/2025 della Corte di Cassazione: tutela del minore tra conflitto genitoriale e dipendenza tecnologica**

L’Ordinanza n. 1832/2025, depositata il 25 gennaio 2025 dalla Prima Sezione Civile della Corte di Cassazione, affronta un tema di crescente rilievo nella giurisprudenza minorile: la tutela del minore in presenza di gravi disfunzionalità familiari e comportamenti autodistruttivi connessi all’uso eccessivo di dispositivi elettronici. Il caso trae origine da un procedimento avviato dal Tribunale per i minorenni di Salerno, successivamente confermato in sede di gravame, culminato con la decisione di collocare un minore tredicenne in una casa-famiglia, sospendendo contestualmente la responsabilità genitoriale di entrambi i genitori.

Il nucleo familiare interessato risultava segnato da elevata conflittualità, episodi di violenza domestica, e dalla manifesta incapacità di gestione educativa del minore, il quale presentava una forte dipendenza dallo smartphone, atteggiamenti aggressivi, disinteresse per la scuola e totale mancanza di regole. Di fronte a tale situazione, l’intervento giudiziario ha previsto, oltre al collocamento etero-familiare, il divieto assoluto per il minore di utilizzare dispositivi elettronici.

I genitori hanno proposto ricorso in Cassazione, lamentando – tra gli altri motivi – la mancata nomina di un curatore speciale in primo grado, in violazione dell’art. 473-*bis*.8 c.p.c., norma che impone la designazione di tale figura quando vi sia conflitto d’interessi tra genitori e figli, o quando i primi risultino temporaneamente inidonei a rappresentarli.

La Corte ha tuttavia rigettato il ricorso, affermando che eventuali vizi procedurali non avevano prodotto alcun concreto pregiudizio nei confronti del minore. In particolare, è stato rilevato che la nomina del curatore speciale, sebbene rilevante, non costituisce elemento tale da determinare l’annullabilità automatica del provvedimento in assenza di prova di lesione effettiva del diritto di difesa del minore. Il giudizio della Suprema Corte si fonda su una valutazione sostanzialistica dell’interesse superiore del minore (*best interest of the child*), principio cardine del diritto minorile sia nazionale che internazionale.

L’ordinanza rappresenta un punto di snodo importante nel diritto di famiglia e nel diritto minorile. Essa conferma l’orientamento giurisprudenziale volto a privilegiare l’interesse concreto del minore rispetto a mere formalità processuali, ma al contempo evidenzia la crescente necessità di considerare la dipendenza tecnologica come un fattore rilevante nel giudizio sull’idoneità

genitoriale e sul benessere psico-sociale del minore. La decisione si inserisce in una tendenza più ampia del diritto minorile contemporaneo, orientata a tutelare il minore da contesti familiari disfunzionali anche attraverso misure drastiche, quali il collocamento extrafamiliare.

Sul punto, infatti, si legge « il Tribunale minorile [...] ha disposto l'affidamento [...] al servizio sociale, il collocamento in casa famiglia con assoluto divieto di dispositivi elettronici e contatti con i genitori da modulare in seguito [...]»

In conclusione, l'Ordinanza n. 1832/2025 segnala l'urgenza di un ripensamento del ruolo genitoriale e delle responsabilità educative nell'era digitale, riaffermando il principio secondo cui la protezione del minore deve prevalere su ogni altro interesse, compreso quello – pur legittimo – alla continuità dell'esercizio della responsabilità genitoriale.

SAMUELE FRANCESCO ROSA

<https://shorturl.at/ZrHgO>

### 2025/2(22)BG

#### **I primi provvedimenti sull'uso improprio di ChatGPT nella redazione delle difese giudiziali (Trib. Firenze sez. imprese ordinanze del 14.3.2025 e del 2.5.2025)**

Due recenti ordinanze della sezione specializzata imprese del Tribunale di Firenze (di seguito anche solo il **Tribunale**) offrono l'opportunità di riflettere sulle implicazioni e le criticità legate all'impiego di sistemi di AI generativa nella pratica giuridica ed in particolare nell'attività forense. Si tratta di: *(i)* un'ordinanza collegiale emessa il 14 marzo 2025, in un procedimento per reclamo, la prima a nostra conoscenza, emessa in materia di responsabilità aggravata ex art. 96 c.p.c. (**Trib. Firenze 14.3.2025** o la **prima ordinanza**); *(ii)* di una successiva ordinanza sempre della sezione specializzata imprese del Tribunale di Firenze, del 2 maggio 2025 (**Trib. Firenze 2.5.2025** o la **seconda ordinanza**).

La prima ordinanza ha riguardato l'episodio dell'inserimento nel corpo di una difesa di precedenti giurisprudenziali inesistenti, ovvero di sentenze il cui contenuto reale non corrispondeva a quello riportato, generate da ChatGPT, e la successiva valutazione di tale condotta alla luce dell'articolo 96 del codice di procedura civile (c.p.c.), concernente la responsabilità aggravata per lite temeraria.

L'attore, alla luce dell'inconferenza dei precedenti citati dal convenuto, rilevava l'omessa verifica circa la veridicità delle ricerche effettuate attraverso lo strumento di IA e, sottolineando l'abusivo utilizzo dello strumento processuale, ha chiesto la condanna di controparte ex art. 96 c.p.c. L'attore argomentava che l'importanza del falso precedente risiede nella sua idoneità a orientare in modo improprio l'attività ermeneutica del giudice, incidendo potenzialmente sull'esito del giudizio, aggiungendo che l'introduzione di un precedente artefatto è suscettibile di compromettere

l'affidabilità del procedimento decisionale e, conseguentemente, di pregiudicare il corretto esercizio della funzione giurisdizionale, posto che il precedente giurisprudenziale rappresenta senz'altro un elemento di rilievo nell'interpretazione e nell'applicazione delle norme.

Invocava quindi l'applicazione dell'articolo 96, commi 1 e 2, c.p.c., recante la disciplina della responsabilità aggravata della parte che abbia agito o resistito in giudizio con mala fede o colpa grave (comma 1) e che abbia agito senza la normale prudenza nel richiedere ed eseguire provvedimenti basati su un diritto inesistente (comma 2).

A seguito della contestazione sul suo operato, il difensore riconosceva l'omesso controllo sui dati ottenuti dal sistema di IA, ma si limitava a richiedere che tali riferimenti fossero espunti, dichiarando di ritenere già sufficientemente fondata la propria linea difensiva.

Il dichiarante affermava specificamente che i riferimenti giurisprudenziali menzionati nell'atto erano il risultato della ricerca condotta da una collaboratrice di studio utilizzando il servizio ChatGPT, senza che il patrocinatore in mandato ne fosse a conoscenza.

Il Tribunale ha escluso l'applicazione dell'articolo 96 c.p.c., ritenendo che, nonostante l'omessa verifica dell'esistenza delle sentenze, la condotta non fosse sorretta da mala fede o colpa grave. Il Collegio ha motivato la decisione considerando che l'indicazione dei falsi precedenti mirava a rafforzare una tesi difensiva già sostenuta, basata sull'assenza di malafede degli assistiti, e non a fuorviare intenzionalmente il giudicante. Il Tribunale si è limitato a censurare il "*disvalore relativo all'omessa verifica dell'effettiva esistenza delle sentenze risultanti dall'interrogazione dell'IA*".

Le conseguenze nel caso concreto sono state dunque limitate a un rilievo deontologico implicito, senza sanzioni pecuniarie a carico del difensore o della parte.

Diverso è il contesto nell'ambito del quale è stata emessa la seconda ordinanza.

In questo caso, il Tribunale ha rilevato che l'apparato argomentativo dispiegato nell'atto introduttivo di parte attrice, dopo una sommaria delineazione delle condotte contestate alla controparte, si esauriva in allegazioni generiche, senza ulteriori specificazioni assertive o indicazioni di mezzi di prova. In particolare, il Tribunale osservava che la produzione dell'attore si caratterizzava per la mera citazione di orientamenti dottrinali in assenza di richiami completi e per la proposizione asettica e reiterata di orientamenti giurisprudenziali che, oltre a risultare perlopiù generici e non conferenti al caso di specie, si rivelavano di contenuto non rispondente a quello delle pronunce effettivamente rinvenute agli estremi indicati. Le sentenze citate, infatti, risultavano attinenti a materie difformi e non pertinenti rispetto al tema di decisione. Infine, nel corpo dell'atto introduttivo esaminato, veniva significativamente notato il seguente inciso: "*Se ha bisogno di un'integrazione più dettagliata o adattata a un caso specifico, posso riformularlo in base alle esigenze*".

Nella seconda ordinanza, il Tribunale ha richiamato il precedente deciso con la prima ordinanza, osservando che in tale sede la condotta non era stata sanzionata ai sensi dell'art. 96 c.p.c. solo perché la citazione di precedenti

errati era avvenuta per la prima volta in sede di reclamo e a supporto di un argomento difensivo già sostenuto con precedenti pertinenti, rendendo le citazioni erranee un'attività *ad colorandum*. Nel fare questo richiamo, nella seconda ordinanza il Tribunale sottolineava la differenza con la condotta del difensore sottoposta al suo esame, dove le citazioni errate costituivano parte integrante dell'iniziale impianto argomentativo, portando a considerare le argomentazioni spiegate dal difensore della parte attrice nel merito “di esigua consistenza”.

Tali notazioni, hanno verosimilmente assunto rilievo nella proposta conciliativa formulata dal Tribunale nella seconda ordinanza, che prevedeva l'abbandono della causa a spese compensate. Deve sottolinearsi la specificazione contenuta nella seconda ordinanza a tenore della quale, nel caso di mancata accettazione della proposta conciliativa ivi formulata, e, comunque, in caso di mancata conciliazione anche a diverse condizioni, “sarà altresì valutata l'eventuale applicazione dell'art. 96 c.p.c., ove il rifiuto [della proposta di conciliazione] appaia privo di giustificazione (Tribunale di Genova, Sez. Imprese, Sent. n. 139/18 del 16/01/18)”.

I due casi, emessi a distanza di pochi mesi l'uno dall'altro dal medesimo Tribunale, offrono un chiaro esempio di come la questione in esame sia destinata a futuri sviluppi.

La prima ordinanza del Tribunale, sebbene connotata da un approccio indulgente rispetto al caso concreto, non può indurre a sottovalutare il potenziale pregiudizio derivante dalla diffusione nelle difese delle parti in giudizio di citazioni di precedenti giurisprudenziali fittizi, né la conseguente necessità che i professionisti del diritto adottino modalità operative improntate alla consapevolezza e alla responsabilità nell'impiego delle tecnologie basate sull'intelligenza artificiale. La tolleranza manifestata dal Tribunale nella prima ordinanza può essere interpretata alla luce della novità del fenomeno, soprattutto in Italia, e della potenziale mancanza di consapevolezza diffusa sui limiti e i rischi specifici delle AI generative in ambito giuridico.

È verosimile ritenere che, in considerazione della progressiva integrazione dell'intelligenza artificiale nell'attività forense, le autorità giudiziarie italiane tenderanno in futuro ad adottare criteri più severi nella valutazione di condotte professionali connotate da negligenza nella validazione delle informazioni ottenute tramite tali strumenti.

BEATRICE GALLUCCI

<https://shorturl.at/HaQZk>