



LUIGI PIGNA\*

### IA GENERATIVA E TRATTAMENTO DEI DATI PERSONALI. LA TUTELA DEI DIRITTI FONDAMENTALI DELL'UTENTE ALLA LUCE DELLA RECENTE INIZIATIVA DI META PER L'ADDESTRAMENTO DELL'IA

SOMMARIO: 1. L'avvento dell'IA generativa. Cosa sono gli LLM e i connessi rischi per la privacy. Un'introduzione. – 2. I principi del RGPD come argine alle nuove tecnologie e il caso ChatGPT/GPDP. – 3. Meta alla ricerca del suo “posto al sole” nel settore dell'IA generativa. – 4. Segue. Il parere dell'EDPB nel segno della sentenza *Meta Platforms*. – 5. Riflessioni a margine dell'informativa di Meta – 6. Considerazioni conclusive

#### 1. L'avvento dell'IA generativa. Cosa sono gli LLM e i connessi rischi per la privacy. Un'introduzione

L'attenzione pubblica attuale sull'intelligenza artificiale riguarda l'IA generativa, o *GAI*, che è specializzata nella creazione di nuovi contenuti, siano essi testi, voci, immagini o video<sup>1</sup>. Un esempio di IA generativa è un *chatbot* basato su un modello linguistico di grandi dimensioni (*LLM*), come *ChatGPT*<sup>2</sup>. Gli utenti interagiscono con questi sistemi inserendo un *prompt*, ovvero una domanda o richiesta, a cui l'IA risponde generando contenuti nuovi e pertinenti<sup>3</sup>. Questi modelli sono progettati per produrre *output* originali basati sui dati utilizzati durante la fase di addestramento. Una delle qualità più significative è la loro capacità di adattarsi a molteplici utilizzi, anche diversi da quelli previsti nella fase iniziale di

---

\* Dottorando di ricerca in “Diritto pubblico, comparato e internazionale”, curriculum in “Ordine internazionale e diritti umani”, Università di Roma “La Sapienza”.

<sup>1</sup> Per un'analisi approfondita delle fasi in cui si articola la costruzione di un modello di intelligenza artificiale generativa si veda A. BANDI, P. ADAPA, Y. KUCHI, *The power of generative AI: A review of requirements, models, input-output formats, evaluation metrics, and challenges*, in *Future internet*, 2023.

<sup>2</sup> V. L. FLORIDI, *AI as agency without intelligence: On chatGPT, large language models, and other generative models*, in *Philosophy e technology*, 2023; AA.VV., *Generative AI and ChatGPT: Applications, challenges, and AI-human collaboration*, in *Journal of information technology case and application research*, 2023.

<sup>3</sup> Un *prompt* è un testo in linguaggio naturale che richiede all'IA generativa di eseguire una determinata attività. V. D. J. SOLOVE, *Artificial intelligence and privacy*, in *Florida Law Review*, 2025; C. GRIECO, *Il diritto d'autore nell'AI Act: Error 404 – page not found?*, in F. FERRI (a cura di), *L'Unione europea e la nuova disciplina sull'intelligenza artificiale: questioni e prospettive*, Rivista Quaderni AISDUE, Fascicolo speciale, 2/2024, Editoriale Scientifica, pp. 157-180.

addestramento e adattati a contesti specifici tramite tecniche di riaddestramento, integrazione o *fine-tuning*, basate su *set* di dati mirati e coerenti con le esigenze dell'utente o con uno specifico settore applicativo<sup>4</sup>. Tuttavia, sia nella fase di sviluppo sia nell'uso successivo, l'impiego dell'IA comporta il trattamento di dati personali, che nel tempo sono aumentati in quantità e varietà, con implicazioni rilevanti in termini di tutela della *privacy*.

Orbene, a partire dalla fine del 2022, con il successo di *ChatGPT* e di altri strumenti ad alte prestazioni, l'IA generativa ha conosciuto una crescita senza precedenti, affermandosi come protagonista non solo dell'innovazione tecnologica, ma anche del dibattito giuridico e regolatorio. Il termine “generativo” non è casuale, ma si riferisce ad un dominio dove le macchine diventano veri e propri creatori, dotati di un'abilità straordinaria, la capacità non solo di predire, ma di concepire e plasmare realtà del tutto nuove. Gli *LLM*, infatti, sono sistemi capaci di generare linguaggio naturale come *output*, a partire da un addestramento effettuato su enormi quantità di dati testuali<sup>5</sup>. Sebbene ogni modello di IA, in senso tecnico, possa essere considerato “generativo” in quanto produce risultati (come previsioni o regole), la nozione assume rilevanza specifica quando ci si riferisce a sistemi che generano informazioni nuove e non predefinite, intrinsecamente legate ai dati d'addestramento<sup>6</sup>. In questo contesto si inseriscono anche i modelli multimodali (*Large Multimodal Models, LMM*), come *GPT-4* o *LLaMA 4* di *Meta*, in grado di processare simultaneamente testo, immagini, suoni e video, ampliando in modo significativo le potenzialità applicative dell'IA<sup>7</sup>. Questi modelli si distinguono per la loro versatilità, configurandosi come strumenti di “utilizzo generale”, in grado di svolgere compiti eterogenei: dalla traduzione linguistica al riassunto testuale, dal supporto alla programmazione alla generazione creativa di contenuti, fino all'assistenza nella presa di decisioni complesse<sup>8</sup>.

La crescente autonomia e versatilità di tali modelli consente loro di cogliere strutture profonde nei dati e generare contenuti sempre più sofisticati, ma al contempo solleva interrogativi rilevanti sul piano della trasparenza, della responsabilità e, soprattutto, della tutela dei diritti fondamentali<sup>9</sup>. In effetti, gli *LLM* emergono come una risorsa preziosa, offrendo diversi vantaggi. È imperativo, tuttavia, riconoscere e comprenderne appieno le

<sup>4</sup> DPC, *AI, Large Language Models and Data Protection*, <https://www.dataprotection.ie/en/dpc-guidance/blogs/AI-LLMs-and-Data-Protection> (6 luglio 2025).

<sup>5</sup> Per un'analisi approfondita delle fasi in cui si articola la costruzione di un modello di intelligenza artificiale generativa si veda A. BANDI, P. ADAPA, Y. KUCHI, *The power of generative AI: A review of requirements, models, input-output formats, evaluation metrics, and challenges*, in *Future internet*, 2023, pp. 7-10.

<sup>6</sup> V. D. FOSTER, *Generative deep learning*, O'Reilly Media, California, 2023, p. 5.

<sup>7</sup> Per una disamina approfondita dei vari approcci definitivi si veda M. C. BUITEN, *Towards intelligent regulation of artificial intelligence*, in *European journal of risk regulation*, 2019, p. 41 ss.

<sup>8</sup> In ambito sanitario, per esempio, l'impiego degli *LLM* nei sistemi di supporto alle decisioni cliniche ha aperto nuovi scenari: questi strumenti offrono raccomandazioni terapeutiche basate su evidenze e mostrano un potenziale significativo nel migliorare l'efficienza e la qualità dell'assistenza medica. È recente la notizia dello sviluppo da parte di Microsoft di un'IA in grado di identificare correttamente la diagnosi in fino all'85% dei casi clinici pubblicati sul *New England Journal of Medicine (NEJM)*, con un tasso di successo oltre quattro volte superiore rispetto a un gruppo di medici esperti. MAI-DxO raggiunge inoltre la diagnosi corretta in modo più efficiente dal punto di vista dei costi rispetto ai medici. V. Microsoft AI, *The Path to Medical Superintelligence*, <https://microsoft.ai/new/the-path-to-medical-superintelligence/> (16 luglio 2025).

<sup>9</sup> V. M. L. MINSKY, *The emotion machine: Commonsense thinking, artificial intelligence, and the future of the human mind*, Simon e Schuster, New York, 2006, p. 95.

limitazioni. Sebbene possano costituire uno strumento efficace per la ricerca, le spiegazioni e l'ottimizzazione, esiste il rischio che le risposte siano fuorvianti o imprecise<sup>10</sup>.

È in questo contesto che l'Unione europea ha avviato una risposta normativa organica con il Regolamento sull'intelligenza artificiale (*Artificial Intelligence Act, AIA*), che si propone di disciplinare in modo trasversale l'intero ciclo di vita dei sistemi di IA, compresi quelli generativi<sup>11</sup>. Tuttavia, per comprendere appieno la portata della disciplina, è necessario considerare anche altri strumenti normativi già esistenti nell'ordinamento dell'Ue, primo fra tutti il Regolamento generale sulla protezione dei dati (RGPD), il cui intreccio con l'IA generativa si sta rivelando sempre più complesso e strategico<sup>12</sup>.

Una delle questioni più controverse riguarda, infatti, il trattamento dei dati personali nei processi di addestramento e utilizzo dei modelli di intelligenza artificiale. Problemi quali la memorizzazione involontaria di dati sensibili, le tecniche di *model inversion* (che permettono la ricostruzione di dati individuali a partire dai parametri del modello)<sup>13</sup>, e la gestione dei dati inseriti nei *prompt* dagli utenti, pongono sfide significative rispetto ai principi fondamentali del RGPD: liceità del trattamento, trasparenza, limitazione della finalità, minimizzazione e tutela dei soggetti vulnerabili, come i minori.

In particolare, si discute della correttezza della base giuridica utilizzata per il trattamento dei dati a fini di addestramento. Emblematico, in tal senso, è il recente caso *Meta*, che ha annunciato l'intenzione di utilizzare, a partire da maggio 2025, i contenuti pubblici condivisi dagli utenti dell'Ue per addestrare i propri modelli di IA generativa, facendo leva sulla base giuridica del legittimo interesse (art. 6, par. 1, lett. f, RGPD). Tale iniziativa ha fatto seguito a un precedente stop dovuto alle obiezioni sollevate da autorità di regolazione e attivisti per la *privacy*<sup>14</sup>. In risposta, la *Data Protection Commission (DPC)* irlandese ha richiesto un parere formale al Comitato europeo per la protezione dei dati (*EDPB*) ai sensi dell'art. 64 del RGPD. Il parere, pubblicato nel dicembre 2024, ha indicato una serie di criteri che le autorità nazionali devono tenere in considerazione nella valutazione della legittimità di questi trattamenti<sup>15</sup>.

<sup>10</sup> D. GANGULI ET AL., *Predictability and surprise in large generative models*, in *ACM Conference on Fairness, Accountability, and Transparency*, 2022.

<sup>11</sup> Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), in GU L, 2024/1689, 12.7.2024.

<sup>12</sup> Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), in GU L 119, 4.5.2016, p. 1–88.

<sup>13</sup> Le tecniche di *model inversion* (letteralmente, inversione del modello) sono metodi attraverso i quali, analizzando i parametri interni di un modello di intelligenza artificiale già addestrato, è possibile ricostruire informazioni sensibili o personali presenti nei dati su cui è stato addestrato. Più semplicemente, se ChatGPT non memorizza direttamente tutti i dati con cui è stato addestrato, potrebbe comunque contenere nei suoi parametri delle tracce di quei dati. Le tecniche di *model inversion* cercano di estrarre o dedurre queste informazioni. Relativamente alle tecniche di *model inversion*, si veda AA.VV., *Deep Learning Model Inversion Attacks and Defenses: A Comprehensive Survey*, consultabile al sito <https://arxiv.org/pdf/2501.18934>.

<sup>14</sup> Uno su tutti, l'associazione noyb di Maximilian Schrems. V. *nobyb urges 11 DPAs to immediately stop Meta's abuse of personal data for AI*, consultabile al sito <https://nobyb.eu/en/nobyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai>.

<sup>15</sup> V. EDPB, Parere 28/2024 su taluni aspetti relativi alla protezione dei dati ai fini del trattamento dei dati personali nel contesto dei modelli di IA, adottato il 17 dicembre 2024.

Questo contributo si propone di analizzare il rapporto tra intelligenza artificiale generativa e protezione dei dati personali, con un focus specifico sulle implicazioni normative del reg. 2016/679 e sulle recenti evoluzioni interpretative fornite dall'EDPB. Particolare attenzione sarà dedicata alla valutazione della base giuridica del legittimo interesse, ai margini di applicazione del consenso, e alla necessità di una *governance* trasparente e bilanciata del ciclo di vita dei modelli generativi. Il tutto alla luce della coesistenza, e talvolta tensione, tra il regolamento sull'IA e il quadro giuridico sulla protezione dei dati.

## 2. I principi del RGPD come argine alle nuove tecnologie e il caso ChatGPT/GDPD.

La protezione dei dati personali rappresenta una delle sfide più rilevanti nello sviluppo e nell'impiego dell'intelligenza artificiale generativa. Il corretto funzionamento dei sistemi di intelligenza artificiale richiede la disponibilità di ingenti quantità di dati<sup>16</sup>. Un passaggio cruciale in questo senso è proprio quello della raccolta dei dati che derivano dall'impiego di dati personali nel *training*, dalla possibile memorizzazione involontaria delle informazioni, dall'inserimento di dati personali nei prompt da parte degli utenti e, infine, dai contenuti generati dagli stessi modelli. Al riguardo, il nuovo regolamento sull'intelligenza artificiale non si occupa della raccolta e del trattamento dei dati, i quali rimangono pertanto soggetti agli strumenti vigenti e, in particolare, al regolamento 2016/679, sulla protezione dei dati personali<sup>17</sup>.

È possibile dunque individuare diverse aree problematiche che vanno dalla definizione di una base giuridica appropriata per l'addestramento; al diritto alla cancellazione (*right to erasure*), dalla tutela dei minori alla più generale gestione dei dati sensibili, fino al principio di limitazione delle finalità e di minimizzazione dei dati<sup>18</sup>.

Tra i principi fondamentali previsti dal RGPD, particolare rilievo assumono quelli della minimizzazione<sup>19</sup> e del consenso dell'interessato<sup>20</sup>. Il principio di minimizzazione prevede la raccolta unicamente dei dati necessari al raggiungimento della finalità del trattamento. Esso si fonda sull'idea che trattare solo i dati strettamente necessari riduca il rischio di violazioni della *privacy* o fughe di informazioni<sup>21</sup>. Il requisito del consenso prevede invece che l'interessato debba manifestare espressamente la sua volontà che i dati vengano trattati per una o più specifiche finalità. Il consenso deve essere, oltre che inequivocabile, anche libero, specifico e informato<sup>22</sup>.

<sup>16</sup> European Parliament Research Service, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, 2020, consultabile online al sito [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS\\_STU\(2020\)641530\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf).

<sup>17</sup> V. G. CONTALDI, *Intelligenza artificiale e dati personali*, in *Ordine Internazionale e Diritti Umani*, 2021.

<sup>18</sup> V. C. NOVELLI, F. CASOLARI, P. HACKER, G. SPEDICATO, L. FLORIDI, *Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity*, in *Computer Law & Security Review*, 2024.

<sup>19</sup> Art. 5 reg. 2016/679.

<sup>20</sup> Art. 6, par. 1, lett. a) e art. 7 reg. 2016/679.

<sup>21</sup> V. AA.VV., *The Data Minimization Principle in Machine Learning*, in *FACt '25: Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*, 2025; H. VAN KOLFSCHOOTEN, *EU regulation of artificial intelligence: Challenges for patients' rights*, in *Common Market Law Review*, 2022, pp. 100 ss.

<sup>22</sup> Sull'argomento cfr. A. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale. Sfide tecnologiche e soluzioni giuridiche*, Napoli, 2019; C. KOOLEN, *Transparency and Consent in Data-Driven Smart Environment*, in *European Data Protection Law Review*, 2021; Y. POULLET, *Consentement et Rgpd: des zones d'ombre!*, in *Droit de la consommation*, 2019.

Entrambi questi principi appaiono, in verità, poco rispondenti al funzionamento concreto dei sistemi di intelligenza artificiale. Tali sistemi, infatti, utilizzano una vasta quantità di dati. Del resto, maggiore è la disponibilità e l'accuratezza delle informazioni utilizzate, più performanti risultano le previsioni indirizzate agli utenti<sup>23</sup>. Allo stesso tempo, i sistemi di IA generativa utilizzano dati collazionati con finalità diverse per elaborare i propri modelli predittivi. Una delle manifestazioni più rilevanti dei *LLM* consiste proprio nella loro versatilità come strumento di utilizzo generale per una vasta gamma di compiti, compresi quelli non specificamente contemplati durante l'addestramento<sup>24</sup>.

Parallelamente, per i sistemi di IA generativa, l'aggregazione automatica dei dati su larga scala può complicare il rispetto dei principi del consenso<sup>25</sup>. La base giuridica più rilevante nel RGPD è il consenso. Tuttavia, nel caso di *set* di dati di grandi dimensioni, che includono informazioni personali provenienti da un numero elevato di persone sconosciute agli sviluppatori, ottenere un consenso valido da ciascun individuo non è realisticamente possibile a causa degli elevati costi di transazione<sup>26</sup>. Inoltre, l'utilizzo di *LLM* basati su dati raccolti dal web e impiegati per scopi non sempre prevedibili è difficilmente compatibile con un consenso informato e specifico<sup>27</sup>. Inoltre, è sostanzialmente accertato che la maggior parte degli utenti tende a prestare poca attenzione nel momento in cui presta il proprio assenso. Nell'attuale ecosistema digitale, il consenso ha progressivamente perso efficacia. Di fronte al potere delle grandi piattaforme, risulta evidente come gli utenti difficilmente prestino un consenso davvero libero e informato<sup>28</sup>.

L'aspetto della base giuridica per le attività di trattamento dei dati resta tuttavia una questione fondamentale. Qualsiasi trattamento di dati personali, comprese operazioni come la raccolta, la memorizzazione o la diffusione, deve fondarsi su una base giuridica ai sensi dell'art. 6 del RGPD. I modelli generativi vengono addestrati su grandi moli di dati, spesso tratti da fonti online accessibili pubblicamente, che possono contenere informazioni personali. Senza un fondamento giuridico specifico, tale trattamento risulterebbe illecito. Seguendo l'approccio adottato dal legislatore nel regolamento generale sulla tutela dei dati personali, il consenso costituisce solo uno dei fondamenti giuridici del trattamento, assumendo così la stessa valenza delle altre condizioni possibili di liceità<sup>29</sup>. Tale flessibilità consente di prendere in considerazione i presupposti di legittimità più appropriati sia per il titolare che per l'interessato. Se però è vero che tutte queste condizioni presentano analoga valenza (eccetto, stando al considerando 46, la residualità del trattamento dei dati necessario a proteggere un interesse vitale dell'interessato o di terzi), va tenuto presente che il ventaglio dei diritti dell'interessato si diversifica rispetto ad esse. In questo modo, il diritto alla

<sup>23</sup> V. T.Z. ZARSKY, *Incompatible: The GDPR in the Age of Big Data*, in *Seton Hall Law Review*, 2017.

<sup>24</sup> Cfr. AA.VV., *Is chatGPT a general-purpose natural language processing task solver?*, in *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing*, 2023.

<sup>25</sup> V. EDPB, Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, adottate il 4 maggio 2020.

<sup>26</sup> M. MOURBY, K.O. CATHAOIR, C.B. COLLIN, *Transparency of machine-learning in healthcare: the GDPR & European health law*, in *Computer Law Security Review*, 2021.

<sup>27</sup> Al riguardo, vedi il parere della *Autoriteit Persoonsgegevens*, *scraping bijna altijd illegal*, 1 May 2024, consultabile al sito <https://www.autoriteitpersoonsgegevens.nl/actueel/ap-scraping-bijna-altijd-illegaal>.

<sup>28</sup> Sul consenso nel mercato digitale, v. F. BATTAGLIA, *Il consumatore digitale nel diritto dell'Unione europea*, Napoli, 2023. Si veda anche D.J. SOLOVE, *Murky consent: An approach to the fictions of consent in privacy law*, in *Boston university law review*, 2024.

<sup>29</sup> In particolare: art. 6, lett b) esecuzione di un contratto; c) adempimento di un obbligo legale; d) salvaguardia di un interesse vitale dell'interessato; e) tutela di un interesse pubblico; f) legittimo interesse del titolare o di terzi, del reg. 2016/679.



portabilità<sup>30</sup> opera solo quando il trattamento si basi sul consenso o sia necessario per l'esecuzione di un contratto, mentre il diritto di opposizione<sup>31</sup>, salvo il trattamento diretto alle finalità di *marketing*, riguarda solo il trattamento compiuto ai sensi dell'art. 6, par. 1, lett. e) o f)<sup>32</sup>.

Per ragioni sia giuridiche che economiche (ossia i costi legati alla raccolta del consenso), la formazione degli *LLM* può quindi basarsi solo sul cosiddetto *test* di bilanciamento previsto dall'art. 6, par. 1, lett. f) RGPD<sup>33</sup>. Secondo tale disposizione, è lecito trattare i dati personali se ciò è “necessario per il perseguimento del legittimo interesse del titolare del trattamento” (cioè l'ente che sviluppa il modello), purché tali interessi non prevalgano sui diritti e le libertà fondamentali degli interessati (ossia le persone i cui dati vengono utilizzati).

Tuttavia, l'ipotesi del legittimo interesse del titolare o di terzi merita particolare attenzione, in quanto rappresenta una delle condizioni di liceità più complesse da applicare<sup>34</sup>. Essa si basa, innanzitutto, su un concetto indeterminato (non è prevista una definizione all'interno del regolamento) e richiede un bilanciamento tra l'interesse del titolare del trattamento e i diritti e le libertà fondamentali dell'interessato, in particolare se si tratta di un minore. Sia il RGPD che la Corte di giustizia hanno riconosciuto espressamente che diversi interessi possono costituire un interesse legittimo ai fini del trattamento dei dati personali<sup>35</sup>. È il titolare a dover valutare autonomamente la prevalenza del proprio interesse, assumendosi la responsabilità di tale scelta, in linea con il principio di *accountability*<sup>36</sup>. Allo stesso tempo, questa base giuridica non può diventare né una scorciatoia per eludere la richiesta di consenso, né una clausola inapplicabile per eccesso di rigidità. Il RGPD, unitamente al ruolo del Comitato e del Garante europeo per la protezione dei dati, ha fornito criteri per guidare i titolari in questa valutazione, che deve essere concreta, documentata e rispettosa dei diritti degli interessati<sup>37</sup>.

Orbene, stabilire se il *test* di bilanciamento costituisca una base giuridica valida richiede una valutazione caso per caso<sup>38</sup>. In generale, quando l'intelligenza artificiale viene utilizzata per scopi socialmente utili o positivi<sup>39</sup>, la posizione del titolare del trattamento dei dati è vista in modo più favorevole sotto il profilo giuridico; inoltre, se l'interessato può ragionevolmente aspettarsi che i propri dati vengano utilizzati per l'addestramento di un'IA, questo rafforza la

<sup>30</sup> Art. 20 reg. 2016/679.

<sup>31</sup> Art. 21 reg. 2016/679.

<sup>32</sup> V. D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giurisprudenza italiana*, 2019.

<sup>33</sup> V. F. ZUIDERVEEN BORGESIU, S. KRUIKEMEIER, S. BOERMAN, N. HELBERGER, *Tracking walls, take-it-or-leave-it choices, the GDPR, and the ePrivacy regulation*, in *European Data Protection Law Review*, 2018, p. 353-368.

<sup>34</sup> V. C.A. TSCHIDER, *AI's Legitimate Interest: Towards a public benefit privacy model*, in *Houston journal of health law & policy*, 2021, p. 178 ss.

<sup>35</sup> V. EDPB, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*, adopted on 8 October 2024, *cit.*, p. 7.

<sup>36</sup> Art. 5, par. 2 reg. 2016/679: «2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di provarlo («responsabilizzazione»).

<sup>37</sup> Considerando 47, 48 e 49 reg. 2016/679; cfr. EDPB, *Guidelines 1/2024*.

<sup>38</sup> V. E. GIL GONZÁLEZ, P. DE HERT, *Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles*, in *ERA Forum* 19, 2019, pp. 597-621; M. DONNELLY, M. McDONAGH, *Health Research, Consent and the GDPR Exemption*, in *European Journal of Health Law*, 2019, pp. 97-119.

<sup>39</sup> Ad esempio, per migliorare l'assistenza sanitaria, ridurre le disuguaglianze, ottimizzare l'accesso ai servizi pubblici o promuovere la sostenibilità ambientale.

posizione del titolare<sup>40</sup>. Tuttavia, questa condizione è difficilmente soddisfatta nella pratica. Non a caso, l'adozione di strategie mirate a rafforzare la tutela della *privacy*, come la pseudonimizzazione, la trasparenza nei confronti degli interessati o l'utilizzo di tecniche di crittografia<sup>41</sup>, può contribuire in modo significativo a rendere legittimo l'addestramento dei modelli di intelligenza artificiale quando questo si fonda sulla base giuridica del legittimo interesse del titolare del trattamento. Allo stesso tempo, la legittimità del trattamento può essere esclusa qualora emergano fattori critici, come la natura e l'estensione del trattamento, la tipologia dei dati coinvolti, soprattutto se si tratta di dati sensibili, un insufficiente livello di trasparenza o un grado limitato di controllo esercitabile dalle persone interessate. In tali casi, il bilanciamento potrebbe dare esito negativo, impedendo al titolare di invocare il legittimo interesse come base giuridica per l'addestramento del modello.

Ulteriore questione, legata all'uso di ampi dataset per l'addestramento dei modelli di IA, riguarda il coinvolgimento di categorie particolari di dati personali, il cui trattamento è generalmente vietato ai sensi dell'art. 9 del RGPD. Tuttavia, alla luce di una recente sentenza della Corte di giustizia, tali informazioni non devono necessariamente riferirsi direttamente a categorie protette, come origine etnica o razziale, religione, età o salute, per rientrare nell'ambito dell'art. 9. È sufficiente che il trattamento dei dati consenta di rivelare informazioni rientranti in una di queste categorie<sup>42</sup>. Ciò che conta è la capacità del titolare del

<sup>40</sup> Così il considerando 47 del reg. 2016/679: «I legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. Ad esempio, potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento. In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali. Posto che spetta al legislatore prevedere per legge la base giuridica che autorizza le autorità pubbliche a trattare i dati personali, la base giuridica per un legittimo interesse del titolare del trattamento non dovrebbe valere per il trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti. Costituisce parimenti legittimo interesse del titolare del trattamento interessato trattare dati personali strettamente necessari a fini di prevenzione delle frodi. Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto».

<sup>41</sup> Cfr. art. 25 reg. 2016/679: «1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati».

<sup>42</sup> V. la sentenza della Corte del 4 luglio 2023, causa C-252/21, *Meta Platforms Inc. e a. c. Bundeskartellamt* (Condizioni generali di utilizzo di un social network) ECLI:EU:C:2023:537, punto 73: «Alla luce di quanto precede, occorre rispondere alla seconda questione, lettera a), dichiarando che l'articolo 9, paragrafo 1, del RGPD deve essere interpretato nel senso che, nel caso in cui un utente di un social network online consulti siti Internet oppure applicazioni correlati a una o più delle categorie menzionate da tale disposizione e, se del caso, inserisca in essi dati, iscrivendosi oppure effettuando ordini online, il trattamento di dati personali da parte dell'operatore di tale social network online – consistente nel raccogliere, tramite interfacce integrate, cookie o simili tecnologie di registrazione, dati risultanti dalla consultazione di tali siti e di tali applicazioni nonché i dati inseriti dall'utente, nel mettere in relazione l'insieme di tali dati con l'account del social network di quest'ultimo e nell'utilizzare detti dati – deve essere considerato un «trattamento di categorie particolari di dati personali» ai

trattamento di dedurre tratti sensibili dai dati disponibili, indipendentemente dall'intento dell'operatore.

Pertanto, gli sviluppatori di modelli di IA, dinanzi alla possibilità di dedurre dati sensibili in fase di addestramento o deployment, e rientrare con il trattamento, nell'ambito dell'art. 9, dovranno ricorrere a una delle deroghe previste al par. 2 della medesima disposizione. Tuttavia, al di fuori del consenso esplicito, tali eccezioni sono raramente disponibili<sup>43</sup>.

Sul diritto all'oblio, previsto dall'art. 17 del RGPD, i modelli linguistici di grandi dimensioni possono memorizzare dati specifici del *set* di addestramento, migliorando le prestazioni su distribuzioni sbilanciate, ma esponendo gravi rischi per la *privacy*. Attacchi come il *membership inference* e il *training data extraction* dimostrano che è possibile risalire a informazioni sensibili, anche solo interrogando il modello<sup>44</sup>. Inoltre, anche se i produttori di

---

sensi di detta disposizione, il quale è in linea di principio vietato, fatte salve le deroghe previste da detto articolo 9, paragrafo 2, qualora tale trattamento di dati sia tale da rivelare informazioni rientranti in una di dette categorie, a prescindere dal fatto che tali informazioni riguardino un utente di tale social network o qualsiasi altra persona fisica».

<sup>43</sup> Art. 9, par. 2 reg. 2016/679: «Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegue finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitano le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».

<sup>44</sup> Ritornando all'esempio dell'ambito medico, gli *LLM* raccolgono una vasta quantità di dati, come possono essere quelli relativi ad una determinata malattia. Se in un dataset ci sono pochi dati riguardanti questa specifica malattia, il modello di IA risponderebbe ugualmente ai prompt/domande inseriti dagli utenti (quale ad esempio i sintomi legati alla stessa), ma questo non attraverso una generalizzazione, ma perché ricorda direttamente il contenuto originale di quei pochi dati a disposizione sempre relativi a quella malattia. Al riguardo v. F.



LLM, come OpenAI, dichiarano di rispettare il diritto alla cancellazione, non è chiaro come ciò sia possibile, poiché le informazioni personali possono essere contenute in più forme all'interno di un LLM, rendendo molto complesso identificare ed eliminare punti specifici, soprattutto quando i dati non sono strutturati, come possono essere i numeri di telefono. Inoltre, le richieste di rimozione avviate da un singolo interessato possono risultare insufficienti, in particolare nei casi in cui informazioni identiche siano state diffuse da più utenti durante l'interazione con il modello<sup>45</sup>. Detto in altri termini, il diritto alla cancellazione applicato ai modelli di GAI non pare rappresentare una garanzia adeguata a tutela della *privacy*, avendo gli stessi la capacità di inferire ugualmente dettagli di informazioni dai dati originali anche una volta eliminati<sup>46</sup>.

I modelli di *Generative AI* hanno sollevato preoccupazioni anche riguardo al consenso dei minori riguardo ai contenuti adatti all'età, vista la possibilità di generare output non adatti ai minori<sup>47</sup>.

Emblematico è stato il caso del Garante per la protezione dei dati personali italiano, che nel 2023 ha disposto un blocco temporaneo di ChatGPT<sup>48</sup>. Le principali criticità individuate riguardavano l'assenza di una base giuridica valida per la raccolta dei dati personali, una scarsa trasparenza nel trattamento dei dati utilizzati per l'addestramento del modello e la mancanza di sistemi efficaci per impedire l'accesso ai minori, con il rischio che questi fossero esposti a contenuti non adeguati alla loro età e maturità<sup>49</sup>.

In risposta, OpenAI ha sospeso temporaneamente l'accesso al servizio in Italia, introducendo misure correttive tra cui un sistema per consentire agli utenti di richiedere la cancellazione dei propri dati personali ai sensi del RGPD e un modulo per la verifica dell'età durante la registrazione. Dopo l'adozione di queste modifiche e l'adeguamento delle *policy*, il GPDP ha revocato il blocco ad aprile 2023<sup>50</sup>.

Nel frattempo, l'EDPB, il Comitato europeo per la protezione dei dati, ha avviato una *task force* per monitorare a livello europeo la conformità dei modelli generativi come ChatGPT al quadro normativo. Tra i nodi più delicati, vi è la legittimità del trattamento dei dati personali, che deve sempre basarsi su una delle condizioni previste dall'art. 6 RGPD e, in caso di dati sensibili, anche su una delle eccezioni indicate all'art. 9.

Una delle principali aree critiche ha riguardato la raccolta dei dati tramite *web scraping*, ovvero l'estrazione automatizzata di informazioni da fonti pubblicamente accessibili online. Questi dati possono includere anche elementi sensibili, per cui l'adozione di misure di salvaguardia risulta essenziale. OpenAI ha invocato come base giuridica il legittimo interesse, ma ciò, come visto, richiede un attento bilanciamento tra gli interessi dell'azienda e i diritti e le libertà

---

DERNONCOURT, J. Y. LEE, O. UZUNER, P. SZOLOVITS, *De-identification of patient notes with recurrent neural networks*, in *Journal of the American Medical Informatics Association*, 2017, pp. 596–606.

<sup>45</sup> Al riguardo, v. AA.VV., *What Does it Mean for a Language Model to Preserve Privacy?*, in *FACCT '22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, 2022, pp. 2282 ss.

<sup>46</sup> E. DE CRISTOFARO, *An overview of privacy in machine learning*, 2020, consultabile al sito <https://arxiv.org/pdf/2005.08679v1>.

<sup>47</sup> Ai sensi dell'art. 8, par. 2 del reg. 2016/679, il titolare del trattamento deve adottare «sforzi ragionevoli per verificare [...] che il consenso dei minori sia prestato o autorizzato da chi esercita la responsabilità genitoriale, tenendo conto della tecnologia disponibile».

<sup>48</sup> Su tutte le questioni relative all'utilizzo di ChatGPT, si veda K. NAGHIYEV, *ChatGPT From a Data Protection Perspective*, in *Baku State University Law Review*, 2024.

<sup>49</sup> V. F. GUALDI, A. CORDELLA, *Theorizing the regulation of generative AI: lessons learned from Italy's ban on ChatGPT*, in *Proceedings of the 57th Hawaii International Conference on System Sciences*, 2024.

<sup>50</sup> Si rimanda a Garante per la protezione dei dati personali, *ChatGPT: OpenAI riapre la piattaforma in Italia garantendo più trasparenza e più diritti a utenti e non utenti europei*, consultabile al sito <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9881490>.

degli interessati. È stato inoltre chiarito che il semplice fatto che un'informazione sia pubblicamente accessibile non equivale a un consenso esplicito dell'interessato alla diffusione dei suoi dati sensibili, come richiesto dall'art. 9, par. 2, lett. e) RGPD.

Per mitigare i rischi, sono state suggerite misure tecniche e organizzative come l'anonimizzazione preventiva dei dati, l'esclusione di alcune fonti (ad esempio i profili *social* pubblici), e l'impiego di filtri per evitare la raccolta di dati appartenenti a categorie particolarmente protette. Anche i contenuti generati dagli utenti, come i *prompt* inseriti e gli *output* del sistema, sono oggetto di trattamento da parte di OpenAI, che ha dichiarato di utilizzarli per migliorare le proprie tecnologie. Anche in questo caso è stato invocato il legittimo interesse, ma resta fondamentale che gli utenti siano pienamente informati di tale utilizzo e messi nella condizione di esercitare un'opposizione effettiva<sup>51</sup>.

Nel gennaio 2024, il GPDP ha notificato un nuovo provvedimento correttivo e sanzionatorio nei confronti di OpenAI, concludendo l'istruttoria avviata l'anno precedente<sup>52</sup>. Secondo l'Autorità, l'azienda ha trattato i dati personali degli utenti senza aver stabilito una base giuridica adeguata, ha violato i principi di trasparenza previsti dal RGPD e non ha segnalato una violazione dei dati avvenuta nel marzo 2023. Inoltre, ha omesso di adottare misure per la verifica dell'età, esponendo potenzialmente i minori a contenuti inadatti.

Per rimediare, e utilizzando per la prima volta i nuovi poteri previsti dall'articolo 166 del Codice *Privacy*<sup>53</sup>, il Garante ha ordinato a OpenAI di realizzare una campagna di comunicazione istituzionale della durata di sei mesi su media tradizionali e digitali. Lo scopo è quello di informare il pubblico sul funzionamento di *ChatGPT*, sul trattamento dei dati, anche dei non utenti, e sui diritti esercitabili, come opposizione, rettifica e cancellazione.

Come ulteriore conseguenza, il Garante ha imposto a *OpenAI* una sanzione amministrativa di 15 milioni di euro, valutata anche alla luce della collaborazione dimostrata dalla società durante il procedimento<sup>54</sup>. Infine, poiché OpenAI ha stabilito la propria sede europea in Irlanda, il GPDP ha trasmesso il fascicolo all'autorità irlandese, che diventa ora l'autorità capofila competente per le eventuali violazioni ancora in corso, in base al meccanismo dello sportello unico previsto dal RGPD<sup>55</sup>. Tale vicenda diventa rilevante alla luce delle implicazioni che può avere sul caso oggetto della presente trattazione.

### 3. Meta alla ricerca del suo "posto al sole" nel settore dell'IA generativa.

Passando alla recente iniziativa di Meta, l'obiettivo dichiarato è quello di potenziare le capacità di Meta *AI*, l'assistente basato su intelligenza artificiale integrato nei servizi di

<sup>51</sup> EDPB, *Report of the work undertaken by the ChatGPT Taskforce*, 23 May 2024, consultabile al sito [https://www.edpb.europa.eu/system/files/2024-05/edpb\\_20240523\\_report\\_chatgpt\\_taskforce\\_en.pdf](https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf)

<sup>52</sup> Anche in seguito al parere dell'EDPB del 18 dicembre 2024 richiesto dalla DPC irlandese sul caso Meta e che sarà oggetto di esame nei capitoli a seguire.

<sup>53</sup> L'articolo 166 del Codice della Privacy (Decreto Legislativo n. 196/2003), come modificato dal D.Lgs. 101/2018, disciplina i criteri per l'applicazione delle sanzioni amministrative pecuniarie e il procedimento per l'adozione dei provvedimenti correttivi e sanzionatori, raccordandosi con le disposizioni del reg. 2016/679, in particolare l'art. 83.

<sup>54</sup> Si rimanda al GPDP, *Comunicato stampa - ChatGPT, il Garante privacy chiude l'istruttoria. OpenAI dovrà realizzare una campagna informativa di sei mesi e pagare una sanzione di 15 milioni di euro*, consultabile al sito <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10085432>.

<sup>55</sup> Considerando 127 reg. 2016/679.

Facebook, Instagram e WhatsApp. A tal fine, la società prevede di utilizzare contenuti pubblici condivisi da utenti adulti su Facebook e Instagram, come *post*, didascalie, commenti e *reel*. Con oltre 500 milioni di utenti mensili nell'Unione europea, Meta dispone di un patrimonio informativo vasto e variegato sia dal punto di vista linguistico che demografico, che intende valorizzare per rafforzare la propria posizione in un settore sempre più competitivo<sup>56</sup>. Meta potrà inoltre raccogliere dati da fonti pubblicamente accessibili *online*, anche attraverso tecniche di *web scraping*, o ottenere informazioni fornite da soggetti terzi. Restano esclusi da tale attività i messaggi privati (protetti da crittografia end-to-end e soggetti a misure di trattamento riservato)<sup>57</sup>, così come i contenuti pubblici provenienti da *account* appartenenti a utenti di età inferiore ai 18 anni.

Su quest'ultimo punto, l'informativa sulla *privacy* di Meta chiarisce che, nel caso in cui un utente pubblichi foto, *tag* o informazioni riguardanti un minore (ad esempio, un genitore che condivide immagini del proprio figlio) tramite un *account* pubblico, tali dati potrebbero essere utilizzati da Meta per addestrare i suoi sistemi di intelligenza artificiale<sup>58</sup>. In tal caso, il minore, non essendo titolare di un *account* né avendo accettato alcuna informativa, non ha alcun controllo né possibilità di opporsi al trattamento. Lo stesso vale per gli adulti che non dispongono di un *account* o non utilizzano i servizi di Meta: anche loro possono essere coinvolti inconsapevolmente, qualora vengano menzionati o ritratti in contenuti pubblici pubblicati da altri utenti.

Ai sensi dell'art. 6 del RGPD, ogni trattamento di dati personali deve basarsi su una valida base giuridica. Meta fa riferimento all'interesse legittimo come fondamento per l'uso dei dati personali degli utenti, sostenendo che lo sviluppo e il miglioramento dell'intelligenza artificiale siano utili sia per sé stessa, sia per gli utenti, per soggetti terzi e per il pubblico in generale. L'obiettivo è fornire strumenti efficaci, sicuri e affidabili, favorendo l'accesso all'informazione, l'innovazione e la condivisione, anche attraverso la collaborazione con sviluppatori e ricercatori<sup>59</sup>.

Considerando tale fondamento, gli utenti hanno il diritto di opporsi a questo tipo di trattamento ai sensi dell'art. 21 del RGPD. Per questo Meta ha previsto un meccanismo di *opt-out* per chi non vuole che i propri dati siano utilizzati in questo modo; tale diritto si estende anche ai non utenti, i cui dati personali pubblici o forniti da terzi potrebbero essere inclusi nel *dataset* per l'addestramento dell'IA<sup>60</sup>.

Orbene, questa *policy*, come già accennato, è stata oggetto di accertamenti da parte della *Data Protection Commission* irlandese e ha incontrato opposizioni in Germania, dove la *Verbraucherzentrale NRW* (organizzazione tedesca per i diritti dei consumatori) ha richiesto un blocco urgente del trattamento. Tuttavia, il Tribunale Superiore Regionale di Colonia ha

<sup>56</sup> European Commission, *Supervision of the designated very large online platforms and search engines under DSA*, consultabile al sito <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses#ecl-inpage-metaplatforms>.

<sup>57</sup> Meta, *About Private Processing*, consultabile al sito [https://faq.whatsapp.com/2089630958184255?fbclid=IwY2xjawLQ1I5leHRuA2FlbQlXMAbicmlkETfVeGtwQ0Z5bjFyQXFzb3hFAR7uabUsXBkKrwYNrtaagv2tHFqovmV9PwH1tEXWbF8Zh-SYdHr23wT4V8GiBQ\\_aem\\_t4Bd-9D05f0PXe\\_1pOP0Mg](https://faq.whatsapp.com/2089630958184255?fbclid=IwY2xjawLQ1I5leHRuA2FlbQlXMAbicmlkETfVeGtwQ0Z5bjFyQXFzb3hFAR7uabUsXBkKrwYNrtaagv2tHFqovmV9PwH1tEXWbF8Zh-SYdHr23wT4V8GiBQ_aem_t4Bd-9D05f0PXe_1pOP0Mg).

<sup>58</sup> Meta, Centro sulla privacy, *In che modo Meta utilizza le informazioni per i modelli e le funzioni dell'IA generativa*, consultabile al sito <https://www.facebook.com/privacy/genai>.

<sup>59</sup> Meta, Centro sulla privacy, *Normativa sulla privacy, Che cos'è l'Informativa sulla privacy e cosa contempla?*, consultabile al sito <https://www.facebook.com/privacy/policy>.

<sup>60</sup> Facebook, Centro Assistenza, *Opponiti all'uso delle tue informazioni per l'IA in Meta*, consultabile al sito [https://www.facebook.com/help/contact/6359191084165019?entrypoint=privacy\\_center](https://www.facebook.com/help/contact/6359191084165019?entrypoint=privacy_center).

respinto tale richiesta, riconoscendo preliminarmente la legittimità del trattamento basato sull'interesse legittimo di Meta, ai sensi dell'art. 6, par. 1, lett. f) del RGPD, ritenendo che gli obiettivi perseguiti non possano essere raggiunti con misure meno invasive. Inoltre, le autorità di controllo, tra cui il Garante di Amburgo, hanno confermato che il trattamento di dati pubblicamente accessibili, anche tramite motori di ricerca, è conforme alla normativa, anche quando si tratta di dati sensibili o riferiti a terzi, inclusi i minori, grazie alle garanzie rafforzate adottate da Meta, come le tecniche di de-identificazione, il filtraggio dei dati e i sistemi di controllo sui risultati prodotti<sup>61</sup>. Il trattamento rimarrà comunque sotto stretta supervisione della DPC, che ha richiesto a Meta un report sull'efficacia delle misure implementate, previsto per ottobre 2025<sup>62</sup>.

#### 4. *Segue. Il parere dell'EDPB nel segno della sentenza Meta Platforms*

In questo contesto si inserisce il parere dell'EDPB, richiesto dall'autorità irlandese per la protezione dei dati nel caso Meta, che ha offerto chiarimenti interpretativi sul trattamento dei dati personali ai fini dell'addestramento dei modelli di intelligenza artificiale. Il Comitato si è pronunciato su temi centrali come l'anonimizzazione, l'interesse legittimo e i confini del trattamento lecito, facendo riferimento a un consolidato orientamento giurisprudenziale della Corte di giustizia. Con specifico riguardo all'interesse legittimo, che rappresenta la base giuridica invocata da Meta, il titolare è tenuto a effettuare una valutazione articolata in tre fasi per determinare la liceità del trattamento dei dati personali. L'EDPB cita, in particolare, la decisione della Corte nella causa *Meta Platforms*. In quella pronuncia, la Corte aveva chiarito quanto già ribadito in una precedente sentenza, per cui il ricorso alla base giuridica del legittimo interesse, prevista dall'art. 6, par. 1, lett. f) del RGPD, richiede la presenza congiunta di tre condizioni: innanzitutto, deve esistere un interesse legittimo effettivamente perseguito dal titolare o da un terzo; in secondo luogo, il trattamento deve essere strettamente necessario al raggiungimento di tale finalità; infine, è necessario che gli interessi, i diritti o le libertà fondamentali della persona interessata non prevalgano su quelli del titolare<sup>63</sup>.

Con riferimento al *test* di necessità, finalizzato a indagare se il trattamento sia effettivamente e realmente necessario per il perseguimento dell'interesse del titolare del trattamento, sempre la Corte, nel già citato caso *Meta Platforms*, ha stabilito che «spetta al giudice del rinvio verificare che il legittimo interesse al trattamento dei dati perseguito non possa ragionevolmente essere raggiunto in modo altrettanto efficace mediante altri mezzi meno pregiudizievoli per i diritti fondamentali degli interessati»<sup>64</sup>. Condizione di necessità che andrebbe esaminata unitamente al principio della minimizzazione dei dati<sup>65</sup>. Inoltre, tra le considerazioni necessarie da tener conto in sede di *test* di necessità, vi sono la possibilità di informare previamente gli utenti e chiedere a questi ultimi se desiderano che i loro dati siano

<sup>61</sup> Oberlandesgericht Köln, *Meta darf Daten aus öffentlich gestellten Nutzerprofilen für KI-Training verwenden*, [https://www.olg-koeln.nrw.de/beh\\_toppmeldungen\\_archiv/Default-Toppmeldung-2/index.php](https://www.olg-koeln.nrw.de/beh_toppmeldungen_archiv/Default-Toppmeldung-2/index.php) (13 luglio 2025).

<sup>62</sup> DPC, *DPC statement on Meta AI*, 21st May 2025, consultabile al sito <https://www.dataprotection.ie/en/news-media/latest-news/dpc-statement-meta-ai>.

<sup>63</sup> V. sentenza della Corte (Seconda Sezione) del 4 maggio 2017, causa C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde c. Rīgas pašvaldības SLA "Rīgas satiksme"*, ECLI:EU:C:2017:336, punto 28.

<sup>64</sup> *Meta Platforms*, punto 108.

<sup>65</sup> *Ibidem*, punto 109.

trattati per determinate finalità, il che consente loro di «conservare il controllo sulla divulgazione dei loro dati personali e di limitare così la divulgazione di tali dati a quanto è effettivamente necessario e pertinente rispetto alle finalità per le quali detti dati sono trasmessi e trattati»<sup>66</sup> e l'attuazione di garanzie tecniche, come l'anonimizzazione, che limitano comunque la facilità con cui gli interessati possono essere identificati<sup>67</sup>.

Relativamente all'esercizio del bilanciamento, che consiste «nell'identificare e descrivere i diversi diritti e interessi contrapposti in gioco, vale a dire da un lato gli interessi, i diritti fondamentali e le libertà degli interessati, e dall'altro gli interessi del titolare del trattamento o di terzi»<sup>68</sup>, la valutazione deve tenere in considerazione le circostanze specifiche del singolo caso<sup>69</sup>. È infatti fondamentale valutare ogni volta quali siano le legittime aspettative della persona interessata, così come l'entità e le modalità del trattamento dei dati in questione. In particolare, la Corte, nel caso *Meta Platforms*, ha rilevato che, sebbene il «miglioramento del prodotto» non possa essere escluso, in linea di principio, come legittimo interesse, ha altresì osservato che «appare dubbio che [...] l'obiettivo diretto al miglioramento del prodotto possa – tenuto conto della portata di tale trattamento e del suo notevole impatto sull'utente, nonché della circostanza che quest'ultimo non possa ragionevolmente attendersi che tali dati siano trattati [...] – prevalere sui diritti fondamentali e sugli interessi di detto utente, tanto più nel caso in cui quest'ultimo sia minorenne»<sup>70</sup>. È inoltre necessario considerare la gravità dei rischi potenziali per gli interessati. A tal fine, possono essere valutati diversi aspetti, come le modalità del trattamento (ad esempio, se i dati personali vengono incrociati con altri *set* di dati), l'estensione e la quantità del trattamento (ossia il volume totale dei dati, la quantità di dati per ciascun individuo, il numero complessivo degli interessati), la condizione dell'interessato (ad esempio, se si tratta di minori o soggetti vulnerabili), nonché la natura del rapporto tra l'interessato e il titolare del trattamento (ad esempio, se si tratta di un cliente). Un caso esemplificativo è rappresentato dall'uso del *web scraping* durante le fasi di sviluppo: se mancano adeguate garanzie, questa pratica può comportare effetti rilevanti sulle persone, a causa dell'elevata quantità di dati raccolti, del grande numero di soggetti coinvolti e della raccolta indiscriminata di informazioni personali<sup>71</sup>.

L'EDPB rileva che alcune questioni rilevanti in materia di protezione dei dati e intelligenza artificiale non sono state approfondite nel Parere, poiché escluse dall'ambito della richiesta formulata dall'Autorità irlandese. Tra queste rientra il trattamento dei dati particolari ai sensi dell'art. 9 RGPD, per il quale si dispone il divieto generale, salvo che i dati siano stati resi pubblici dall'interessato in modo esplicito e inequivocabile, attraverso un atto che manifesti in modo chiaro e volontario la volontà dell'interessato stesso<sup>72</sup>. Sempre l'EDPB ricorda il disposto di cui alla sentenza della Corte di giustizia nel caso *Meta Platforms*, secondo la quale, qualora un *dataset* contenga dati particolari non suscettibili di separazione da altre categorie di dati, il relativo trattamento deve essere qualificato come trattamento di dati particolari<sup>73</sup>.

<sup>66</sup> V. sentenza della Corte del 4 ottobre 2024, causa C-621/22, *Koninklijke Nederlandse Lawn Tennisbond*, ECLI:EU:C:2024:857, punti 51-53.

<sup>67</sup> EDPB, Parere 28/2024, punto 75.

<sup>68</sup> EDPB, Parere 28/2024, punto 76.

<sup>69</sup> G. PROIETTI, *Algoritmi e interesse del titolare del trattamento nella circolazione dei dati*, in *Contratto e impresa*, 2022, p. 891.

<sup>70</sup> *Meta Platforms*, (punto 123).

<sup>71</sup> V. EDPB, Parere 28/2024, punto 86.

<sup>72</sup> Art. 9, par. 2 re. 2016/679.

<sup>73</sup> *Meta Platforms*, punto 73.



In conclusione, anche se l'esistenza di tali vantaggi può portare un'autorità di controllo, come la Commissione irlandese, a concludere che sugli interessi del titolare del trattamento o di un terzo non prevalgono gli interessi, i diritti e le libertà fondamentali degli interessati, tale conclusione può essere tratta solo a seguito di un'analisi effettuata caso per caso che tenga conto di tutti questi fattori.

##### 5. *Riflessioni a margine dell'informativa di Meta*

Il quadro giuridico dell'Unione europea in materia di addestramento dell'intelligenza artificiale, in particolare dei modelli linguistici di grandi dimensioni (*LLM*), a partire da dati personali, si è delineato attraverso pareri delle autorità garanti e pronunce della Corte di giustizia. Tuttavia, casi recenti come quello di Meta, evidenziano come persistano significative incertezze sulla legittimità di tali pratiche. Si ritiene dunque necessaria una disamina specifica dell'informativa privacy di Meta, anche alla luce delle considerazioni fatte sul caso *ChatGPT*.

È proprio il ricorso all'interesse legittimo, su cui si basa l'informativa di Meta, a sollevare le maggiori criticità. La questione, tuttavia, si presenta particolarmente complessa. Si consideri che se nella sentenza *Meta Platforms*, più volte citata, la Corte di giustizia ha stabilito che Meta non può fare affidamento sull'art. 6, par. 1, lett. f) del RGPD per la pubblicità personalizzata all'interno di una piattaforma, anche perché gli interessati non si aspetterebbero ragionevolmente che i loro dati vengano usati a tali fini. Eppure, essendo le piattaforme Meta finanziate prevalentemente tramite pubblicità, tale trattamento risulterebbe sicuramente più prevedibile rispetto all'addestramento dell'IA, una tecnologia del tutto nuova e sconosciuta per gli utenti iscritti.

Si può senz'altro discutere come l'addestramento dell'intelligenza artificiale possa rispettare il principio di limitazione della finalità o di minimizzazione dei dati. Questi principi, sanciti rispettivamente dall'art. 5, par. 1, lett. b) e c) del RGPD, trovano un'esplicita conferma anche nell'*AI Act*, in particolare nei considerando 69 e 71, che delineano un approccio *human-centric* al trattamento dei dati. In particolare, il considerando 69 ribadisce la necessità di garantire la protezione dei dati lungo l'intero ciclo di vita dei sistemi di intelligenza artificiale, attraverso l'applicazione sistematica dei principi di minimizzazione e della protezione dei dati fin dalla progettazione e per impostazione predefinita<sup>74</sup>. A sua volta, il considerando 71 sottolinea il ruolo essenziale della documentazione tecnica come strumento di trasparenza, volto a rendere verificabili le scelte progettuali e a tutelare i diritti fondamentali degli interessati. In tale contesto normativo, la conformità dell'addestramento degli algoritmi a questi principi non può essere presunta, ma richiede un'attenta valutazione *ex ante* delle finalità perseguite e della proporzionalità dei dati utilizzati<sup>75</sup>.

Relativamente alla distinzione tra categorie di dati, l'informativa di Meta ammette che i contenuti utilizzati per l'addestramento dell'IA possono riguardare anche informazioni sensibili, come contatti personali o opinioni su temi delicati. Questo solleverebbe rilevanti questioni giuridiche, in particolare rispetto alle categorie particolari di dati personali<sup>76</sup>, tra cui

---

<sup>74</sup> Art. 25 reg. 2016/679.

<sup>75</sup> V. B. O. OZPARLAK, E. METIN, *Designing Trust and Privacy: The Role of Legal Design in Ensuring Compliance with the EU AI Act*, in A. MOALLEM (eds), *HCI for Cybersecurity, Privacy and Trust*, 2025, p. 116 ss.

<sup>76</sup> Art. 9 reg. 2016/679.

orientamento sessuale, convinzioni religiose o politiche, frequentemente condivise su piattaforme come Facebook e Instagram. Il trattamento di tali dati è in linea di principio vietato, salvo specifiche eccezioni, tra cui quella prevista dall'art. 9, par. 2, lett. e), quando è l'interessato stesso a renderli manifestamente pubblici. Tuttavia, in assenza di impostazioni consapevoli o di un'adeguata informazione, non si può presumere che questi dati siano liberamente riutilizzabili, se non previo consenso esplicito. Sul punto, la Corte di giustizia si è espressa in modo chiaro nella sentenza *Schrems c. Meta Platforms Ireland Ltd*<sup>77</sup>, chiarendo che un contenuto può essere considerato “manifestamente pubblico” solo se l'utente ha consapevolmente configurato i parametri di visibilità affinché sia accessibile a un numero illimitato di persone. In altre parole, è necessario che vi sia stato un consenso esplicito alla pubblicazione in senso ampio<sup>78</sup>.

L'informativa solleva inoltre dubbi sul rispetto del principio di trasparenza e correttezza, soprattutto quando nei contenuti trattati compaiono soggetti terzi o minori, che non sono stati informati e non hanno strumenti per opporsi. L'RGPD richiede infatti una tutela rafforzata per i dati dei minori nel contesto digitale<sup>79</sup>, e il semplice carattere pubblico di un contenuto non basta a legittimarne l'uso: occorre sempre una base giuridica adeguata. In questo contesto, il ricorso all'interesse legittimo da parte di Meta appare particolarmente controverso, soprattutto quando coinvolge soggetti vulnerabili<sup>80</sup>.

In merito al sistema di *opt-out*, ossia al diritto di opporsi al trattamento, sussistono diverse criticità. Molti utenti, infatti, potrebbero non comprendere pienamente cosa implichi la qualificazione dei propri contenuti come “pubblici” nell'ambito dell'addestramento algoritmico, oppure potrebbero non accorgersi delle notifiche che li informano in merito. Inoltre, una volta che i dati sono stati acquisiti nei sistemi di addestramento, non sembra esistere una reale possibilità di rimuoverli. A ciò si aggiunge il fatto che, in alcuni casi, le informazioni personali potrebbero comunque essere trattate nonostante l'opposizione espressa, come ad esempio quando l'utente compare in un'immagine condivisa pubblicamente da altri, o viene menzionato in un *post* o in una didascalia pubblicata da terzi (oltre al dettaglio, non così irrilevante, degli effetti non retroattivi del diritto di opposizione)<sup>81</sup>. Si tratta di situazioni che toccano direttamente la tematica del diritto all'oblio, come delineato nella nota sentenza *Google Spain*<sup>82</sup>.

Oltre a queste considerazioni legate al RGPD, è necessario il riferimento all'art. 5, par. 1, lett. b) e c) del *Digital Markets Act* (DMA), per cui il legislatore dell'Unione stabilisce limiti molto precisi all'uso dei dati personali da parte dei *gatekeeper*<sup>83</sup>. In particolare, Meta non

<sup>77</sup> V. sentenza della Corte del 4 ottobre 2024, causa C-446/21, *Maximilian Schrems c. Meta Platforms Ireland Limited*, ECLI:EU:C:2024:834, punto 83.

<sup>78</sup> Si veda anche L. PIGNA, *Schrems c. Meta. La Corte di giustizia si pronuncia sui limiti al trattamento dei dati personali per fini di pubblicità mirata*, in *Ordine Internazionale e Diritti Umani*, 2024.

<sup>79</sup> Considerando 38 e art. 8 reg. 2016/679.

<sup>80</sup> Sul trattamento di categorie particolari di dati, v. A. BUSACCA, *Le “categorie particolari di dati” ex art. 9 GDPR. Divieti, eccezioni e limiti alle attività di trattamento*, in *Ordine Internazionale e Diritti Umani*, 2018.

<sup>81</sup> Facebook, Centro assistenza, *Opponiti all'uso delle tue informazioni per l'IA in Meta*, consultabile al sito [https://www.facebook.com/help/contact/6359191084165019?entrypoint=privacy\\_center](https://www.facebook.com/help/contact/6359191084165019?entrypoint=privacy_center).

<sup>82</sup> V. sentenza della Corte del 13 maggio 2014, causa C-131/12, *Google Spain*, ECLI:EU:C:2014:317. In tema di diritto all'oblio, cfr. S. MARTINELLI, *Diritto all'oblio e motori di ricerca: il bilanciamento tra memoria e oblio in internet e le problematiche poste dalla de-indicizzazione*, in *Il diritto dell'informazione e dell'informatica*, 2017; M. TAMPIERI, *Il diritto all'oblio e la tutela dei dati personali*, in *Responsabilità civile e previdenza*, 2017.

<sup>83</sup> Regolamento (Ue) 2022/1925 del parlamento europeo e del consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali), in GU L 265, 12.10.2022, pagg. 1–66.

potrebbe combinare dati da servizi diversi, come dati presi da Facebook con quelli raccolti da Instagram, WhatsApp, o da servizi esterni (es. un sito che usa il *login* di Facebook), a meno che non abbia il consenso esplicito dell'utente, così come non potrebbe trasferire e usare in modo incrociato dati personali da un servizio all'altro del medesimo *gatekeeper*<sup>84</sup>.

## 6. Considerazioni conclusive

Lo sviluppo e l'addestramento di sistemi di intelligenza artificiale comportano necessariamente il trattamento di grandi quantità di dati (anche personali). Il paradosso è che la progettazione, la sperimentazione e la validazione di sistemi di IA affidabili e rispettosi dei diritti fondamentali richiedono l'accesso a dati personali rappresentativi e attendibili, sia sotto il profilo quantitativo che qualitativo. Ne consegue una tensione tra le esigenze tecniche dello sviluppo dell'IA e la normativa sulla protezione dei dati personali, specialmente per quanto riguarda la liceità della raccolta e del trattamento dei dati destinati alla costruzione dei *dataset* per l'addestramento di modelli di IA e di apprendimento automatico<sup>85</sup>.

Il trattamento di qualsiasi informazione relativa a una persona fisica identificata o identificabile è soggetto al rispetto delle norme in materia di protezione dei dati. Pertanto, al momento della raccolta e dell'utilizzo di dati personali, il titolare del trattamento deve individuare una valida base giuridica, che può consistere nel consenso dell'interessato oppure in un'altra delle condizioni previste dal RGPD.

Considerate le difficoltà pratiche legate all'ottenimento di un consenso realmente informato e significativo nel contesto dello sviluppo dell'IA, e alla sua idoneità come base giuridica, l'interesse legittimo perseguito dal titolare o da un terzo emerge come una possibile alternativa. Molti titolari del trattamento, come le piattaforme digitali, tendono a fondare il trattamento dei dati personali sull'interesse legittimo. Tale interesse viene spesso formulato in termini di sviluppo tecnologico e innovazione, con riferimento alla creazione, fornitura e miglioramento di tecnologie basate sull'IA. Si richiama anche un presunto interesse di terzi, come sviluppatori o partner commerciali, e, più in generale, dell'interesse del pubblico nel beneficiare di tali tecnologie. A ciò si aggiunge un ulteriore livello giustificativo, legato alla sicurezza e all'affidabilità dei sistemi, nel tentativo di dimostrare che il trattamento è volto anche a tutelare gli stessi utenti o l'ecosistema digitale<sup>86</sup>.

Tuttavia, il recente parere 28/2024 del Comitato Europeo per la Protezione dei Dati, che, come visto, ha ripreso una consolidata giurisprudenza della Corte in materia e i risultati della *task-force* per *ChatGPT*, ha chiarito ancora una volta alcuni punti fondamentali che mettono in discussione la piena sostenibilità di queste formulazioni. Il ricorso all'interesse legittimo come base giuridica per l'addestramento dei modelli di IA non può essere invocato in modo generico o strumentale. Esso deve fondarsi su un interesse concreto e specifico del titolare, e che deve essere effettivamente bilanciato con i diritti e le libertà fondamentali degli interessati. Non sono sufficienti, a tal fine, motivazioni di ordine economico o tecnologico, né l'invocazione di interessi pubblici generici. L'uso di tale base giuridica comporta un onere

<sup>84</sup> Cfr. R. PODSZUN, *Should Gatekeepers Be Allowed to Combine Data? Ideas for Art. 5(a) of the Draft Digital Markets Act*, in *GRUR International*, 2022.

<sup>85</sup> V. P. T. KRAMCSÁK, *Can legitimate interest be an appropriate lawful basis for processing Artificial Intelligence training datasets?*, in *Computer Law and Security Review*, 2023, *cit.*

<sup>86</sup> Meta, *Che cos'è l'Informativa sulla privacy e cosa contempla?*.

significativo per il titolare, che deve dimostrare la necessità del trattamento, adottare misure tecniche e organizzative adeguate, come la minimizzazione dei dati e la trasparenza, e garantire un livello di tutela coerente con le aspettative legittime degli interessati. Lo stesso regolamento sull'IA, richiamando esplicitamente il principio della *data protection by design* e *by default*<sup>87</sup>, nonché l'obbligo di documentazione tecnica trasparente per i sistemi ad alto rischio, conferma che la protezione dei dati personali deve essere garantita lungo l'intero ciclo di vita dei sistemi di IA<sup>88</sup>. Inoltre, come previsto dal considerando 67 del nuovo testo legislativo, il principio di trasparenza gioca anch'esso un ruolo chiave, che deve essere garantito con riguardo alla finalità originaria della raccolta dei dati utilizzati per l'addestramento. Tale protezione implica, tra l'altro, la minimizzazione dei dati trattati, in linea con quanto previsto dall'art. 5, par. 1, lett. c) e dall'art. 25 RGPD. Proprio questo principio di "progettazione preventiva" esclude approcci meramente reattivi o *ex post*, come tentativi di mitigare i rischi attraverso il filtraggio degli *output* o la limitazione delle risposte del sistema.

L'invocazione dell'interesse legittimo come base giuridica per il trattamento dei dati personali nel contesto dell'intelligenza artificiale non può dunque essere interpretata come un espediente per semplificare gli obblighi del titolare: al contrario, essa comporta un rafforzamento delle sue responsabilità. E l'interpretazione data dall'EDPB ha escluso, in definitiva, ogni approccio formalistico, ribadendo come la protezione dei dati personali non può essere subordinata agli obiettivi commerciali o di innovazione tecnologica.

Proprio perché caratterizzato da una certa elasticità applicativa, il ricorso a tale fondamento richiede un'analisi rigorosa e caso-specifica delle finalità perseguite, della proporzionalità del trattamento e dell'effettiva necessità dei dati trattati rispetto allo scopo dichiarato. Anche se, come visto nel caso dell'iniziativa di Meta, i dubbi vanno oltre la scelta della base giuridica del trattamento. A sollevare preoccupazione è soprattutto l'impatto dell'addestramento sui dati cosiddetti "particolari", specie quelli riguardanti minori. Su questo punto, l'*AI Act* dispone una tutela rafforzata di tali categorie di informazioni personali, prevista dall'art. 10, par. 5, che oltre ad essere soggette a limitazioni tecniche, nonché a misure più avanzate di sicurezza, le stesse non possono essere trasmesse, trasferite o consultate da terzi. I titolari del trattamento devono inoltre raccogliere solo i dati personali necessari e pertinenti a una finalità specifica<sup>89</sup>. Anche l'*AI Act* riflette questo principio, richiedendo una valutazione della quantità e adeguatezza dei dati<sup>90</sup>.

Inoltre, con l'aumento della dimensione e complessità dei *dataset* utilizzati dai fornitori di *LLM*, diventa sempre più importante potenziare le misure per la protezione dei dati personali contro possibili violazioni<sup>91</sup>. I metodi tradizionali, come la pseudonimizzazione e la cifratura, restano validi, ma possono non essere sufficienti da soli. Una nuova frontiera è

<sup>87</sup> Considerando 69 reg. 2024/1689.

<sup>88</sup> Considerando 71 reg. 2024/1689.

<sup>89</sup> Rispettivamente, art. 5, lett. b) e c) del reg. 2016/679: «I dati personali sono: b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»).

<sup>90</sup> Art. 10, par. 2, lett. e) del reg. 2024/1689: «I set di dati di addestramento, convalida e prova sono soggetti a pratiche di governance e gestione dei dati adeguate alla finalità prevista del sistema di IA ad alto rischio. Tali pratiche riguardano in particolare: e) una valutazione della disponibilità, della quantità e dell'adeguatezza dei set di dati necessari».

<sup>91</sup> Il riferimento dell'*AI Act* a questi metodi (articolo 10(5)(b)) ne sottolinea l'importanza,

quella del *machine unlearning*, una tecnica che consente di eliminare ogni traccia dell'informazione indesiderata all'interno del modello stesso<sup>92</sup>. Anche l'addestramento su banche dati più ridotte potrebbe ridurre eventuali rischi per la privacy degli utenti. Tuttavia, tali limitazioni avrebbero come effetto collaterale quello di ridurre la flessibilità e il potenziale innovativo dei modelli. In alternativa, può essere più efficace rafforzare le misure di protezione della *privacy* proporzionalmente alla grandezza del *dataset*<sup>93</sup>.

In conclusione, gli strumenti per uno sviluppo delle nuove tecnologie, come la *GAI*, orientato al rispetto dei diritti fondamentali, sono già disponibili. Il quadro normativo delineato dal binomio RGPD–*AI Act* conferma la possibilità di un approccio integrato, capace di tutelare le libertà individuali e, al contempo, promuovere un'innovazione responsabile. Molto dipenderà dalle modalità concrete di utilizzo, che rifletteranno anche il grado di consapevolezza, da parte delle cosiddette “fabbriche dell'IA”<sup>94</sup>, del necessario passaggio, evidenziato anche dall'*EDPB*, da un'impostazione massimalista in materia di protezione dei dati a un più maturo e realistico bilanciamento tra interessi collettivi e diritti individuali.

---

<sup>92</sup> V. AA.VV., *A Survey of Machine Unlearning*, consultabile al sito <https://arxiv.org/abs/2209.02299>.

<sup>93</sup> Per un maggiore approfondimento delle tecniche per la tutela della privacy nell'addestramento e diffusione degli LLM si veda AA.VV., *What Does it Mean for a Language Model to Preserve Privacy?*, in *FAccT '22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, 2022.

<sup>94</sup> Commissione europea, *Fabbriche di IA*, consultabile al sito <https://digital-strategy.ec.europa.eu/it/policies/ai-factories>.