

Il diritto all'oblio alla prova dell'intelligenza artificiale: dal diritto alla de-indicizzazione al diritto al de-addestramento?

Marco Orofino

Professore ordinario di Diritto costituzionale e pubblico, Università degli Studi di Milano

ORCID: <https://orcid.org/0000-0003-2777-3970>

DOI: 10.54103/milanoup.273.c589

ABSTRACT: Il contributo analizza l'evoluzione del diritto all'oblio alla luce delle sfide poste dall'intelligenza artificiale, con particolare riferimento all'interazione tra GDPR e AI Act. Il capitolo approfondisce i nodi giuridici relativi al rapporto tra le condizioni di liceità del trattamento e il diritto alla cancellazione dei dati, nonché alla portata temporale della cancellazione (*ex nunc* o *ex tunc*). Le questioni sono applicate alla cancellazione dei dati di addestramento e degli *output* generati dai modelli di IA. Vengono inoltre esaminate le misure tecniche e giuridiche volte a garantire l'effettività al diritto, tra cui il de-addestramento e i filtri di *output*, proposti come nuove forme di oblio volte a garantire la tutela della dignità e dell'identità personale nell'era digitale.

The chapter examines the evolution of the right to be forgotten in light of the challenges posed by artificial intelligence, with particular reference to the interaction between the GDPR and the AI Act. It explores the legal issues arising from the relationship between the conditions of lawfulness of processing and the right to erasure, as well as the temporal scope of erasure (ex nunc or ex tunc). These questions are applied to the deletion of training data and outputs generated by AI models. The analysis also considers technical and legal measures aimed at ensuring the effectiveness of this right, including machine unlearning and output filtering, proposed as new forms of oblivion designed to safeguard human dignity and personal identity in the digital age.

PAROLE CHIAVE: Intelligenza artificiale, GDPR, Diritto all'oblio, Diritto alla cancellazione dei dati personali, Diritto al de-addestramento.

KEYWORDS: *Artificial Intelligence, GDPR, Right to be forgotten, Right to erasure of personal data, Right to machine unlearning.*

SOMMARIO: 1. Introduzione. – 2. Il diritto all’oblio nel quadro della protezione dei dati personali. – 2.1. Origini giurisprudenziali: la sentenza *Google Spain / Costeja González*. – 2.2. Il diritto alla cancellazione (diritto all’oblio) nel GDPR: casi e limiti. – 3. Il legame tra esercizio del diritto alla cancellazione e condizioni di liceità del trattamento. – 4. Il diritto alla cancellazione dei dati tra GDPR e AI Act: verso una nuova declinazione? – 5. Il Parere EDPB n. 28/2024 e la qualificazione dei fornitori di modelli di IA. – 6. Effettività del diritto all’oblio nell’era dell’intelligenza artificiale. – 6.1. Le misure tecniche di mitigazione. – 6.2. Il “de-addestramento” come strumento per un’effettiva cancellazione *ex tunc* – 6.3. L’imposizione di filtri nei risultati di *output*. – 7. Osservazioni conclusive

1. Introduzione

Il diritto all’oblio costituisce una delle espressioni più emblematiche della tensione tra memoria e dimenticanza nella società digitale. Una formula più evocativa che descrittiva, il cui significato varia a seconda dei contesti in cui è usata e degli obiettivi che ne orientano l’invocazione¹. Proprio questa sua indeterminatezza ha portato alla definizione del diritto all’oblio come diritto proteiforme che oscilla tra diritto al rispetto della dignità della persona e della sua identità, diritto alla riservatezza, diritto alla protezione dei dati e limite alla libertà di manifestazione del proprio pensiero, di informazione e di stampa².

In senso letterale, il diritto all’oblio è il diritto alla dimenticanza prolungata, completa, alla perdita di ogni memoria, alla cancellazione del ricordo. Una pretesa soggettiva (una posizione giuridica di vantaggio *erga omnes*) a cui dovrebbe corrispondere un dovere di dimenticare (una corrispondente posizione giuridica di svantaggio). È del tutto evidente che, in termini formali, dimenticanza e ricordo non sono esigibili a terzi, per il semplice fatto che ciò che si dimentica (o si ricorda) non è il frutto di un atto di autonomia. L’oblio giuridico non coincide, dunque, con l’oblio psicologico o storico.

Questo spiega perché, più che un diritto all’oblio come fattispecie autonoma, l’ordinamento riconosca una “costellazione” di diritti serventi rispetto all’oblio: il diritto a non vedere divulgati determinati fatti e circostanze della propria vita privata, il diritto a non vedere riproposte continuamente notizie ed informazioni lesive della propria reputazione o identità, il diritto alla cancellazione dei dati personali, il diritto alla de-indicizzazione. Una serie di posizioni soggettive che soccorrono le persone nell’esigenza di tutela della propria dignità ed identità

1 Cfr. F. PIZZETTI, *Il prisma del diritto all’oblio* in F. PIZZETTI, *Il caso del diritto all’oblio*, Giappichelli, Torino, 2013, 22. Oblio e memoria hanno anche una dimensione collettiva che chiama direttamente in causa i pubblici poteri. V. in proposito A. MASTROMARINO, *Stato e memoria. Studio di diritto comparato*, Franco Angeli, Milano, 2018.

2 Così F. PIZZETTI, *Il prisma del diritto all’oblio*, cit., 30.

personale³. Un'esigenza che soprattutto nel contesto della società digitale, capace di alterare profondamente l'equilibrio tra memoria e dimenticanza⁴, emerge con forza.

La prima affermazione di una pretesa giuridica volta far valere il diritto all'oblio può essere collocata all'interno del complesso bilanciamento tra la libertà di cronaca e i diritti della personalità quali l'identità, la reputazione e l'onore⁵. In quel contesto il venir meno del requisito dell'attualità della notizia – anche a fronte di fatti veri, narrati in modo continente e originariamente di interesse pubblico – comporta la mancata operatività della causa di giustificazione penale del diritto di cronaca, aprendo così uno spazio per una specifica tutela del diritto alla dimenticanza (oblio)⁶.

3 Si osservi anche che l'alterazione prodotta dalla datizzazione è duplice: da un lato i dati tendono a permanere nella memoria della rete molto più a lungo ma, da un altro lato, essi sono anche volatili e possono improvvisamente sparire. Cfr. G. ZICCARDI, *L'avvocato hacker*, Giuffrè, Milano, 2012, 277. Sull'imprevedibilità della memoria di Internet v. anche M. BIANCA, *Memoria ed oblio: due reali antagonisti?*, in *Medialaws. Rivista di diritto dei media*, n. 3, 2019, 23 ss. Il timore di perdere la memoria della rete ha anche dato origine a progetti volti a conservare, fotografandoli, i contenuti di Internet. Tra di essi il più noto è il progetto *Internet Archive*. Sulle questioni giuridiche che tali progetti sollevano v. in questo volume il contributo di A. FOTI. *Il diritto all'oblio alla prova dell'archiviazione digitale: il caso di Internet Archive*.

4 V. in proposito l'analisi di S. MARTINELLI, *Diritto all'oblio e motore di ricerca*, Giuffrè, Milano, 2017, 5 ss.

5 Su questo complesso rapporto v. *ex multis* in dottrina, S. FOIS, *Principi costituzionali e libera manifestazione del pensiero*, Giuffrè, Milano, 1957; V. CRISAFULLI, *Problematica della libertà di informazione*, in *Il Politico*, 1964, 285 ss.; A. LOIODICE, *Informazione (diritto alla)*, in *Enciclopedia del diritto*, Milano XXI, 1971, 472 ss.; P. BARILE, *Libertà di manifestazione del pensiero*, in *Enciclopedia del diritto*, Milano, XXIV, 1974, 424 ss.; C. CHIOLA, *Manifestazione del pensiero (libertà di)*, in *Enciclopedia giuridica*, Roma, XIX, 1990; A. PACE, F. PETRANGELI, *Cronaca e critica (diritto di)*, in *Enciclopedia del diritto*, Milano, 1991, 306 ss.; P. PERLINGIERI, *Informazione, libertà di stampa e dignità della persona*, in *Rassegna di diritto civile*, 3, 1986, 624 ss.; A. PACE, M. MANETTI, *Art. 21: la libertà di manifestazione del proprio pensiero*, in G. BRANCA, A. PIZZORUSSO, *Commentario alla Costituzione*, Zanichelli- Soc. ed. del Foro italiano, Bologna-Roma, 2006. Sia consentito, per un'analisi delle nuove tensioni che la libertà di espressione incontra nella società digitale, rinviare a M. OROFINO, *La libertà di espressione tra Costituzione e Carte europee dei diritti. Il dinamismo dei diritti in una società in continua trasformazione*, Giappichelli, Torino, 2014. Cfr. anche recentemente la puntuale analisi di M.E. BUCALO, *I volti della libertà di manifestazione del pensiero nell'era digitale. Content moderation e regolazione di un diritto in evoluzione*, Giappichelli, Torino, 2023.

6 Come è noto, il diritto di cronaca trova riscontro nella giurisprudenza della Cassazione come causa di giustificazione dei reati contro l'onore e la reputazione. Cfr. Cass. pen., sez. V, 5 marzo 1960, n. 103, in *Giustizia Penale*, 1961, II, 103 ss. Successivamente la Corte ha elaborato i tre requisiti che consentono la prevalenza del diritto di cronaca. V. Cass. civ., sez. I, 18 ottobre 1984, n. 5259. Il criterio dell'attualità della notizia e dell'interesse pubblico si è aggiunto grazie ad una giurisprudenza più recente. Cass. civ., sez. I, 9 aprile 1998, n. 3679; Cass. pen., sez. un., 30 maggio 2001, n. 37140; Cass. pen., sez. V, 24 novembre 2009, n. 45051; e più recentemente Cass. civ., sez. I, 20 marzo 2018, n. 6919; Cass. civ., sez. un., 22 luglio 2019, n. 19681. Per una dettagliata analisi dell'evoluzione giurisprudenziale in punto di attualità v. F. PARUZZO, *Tra diritto all'oblio e libertà di informazione: la sussistenza dell'interesse pubblico alla diffusione di una notizia*, in *Medialaws. Rivista di diritto dei media*, n. 2, 2018, 368 ss.

Con la progressiva datizzazione che caratterizza l'affermazione della società digitale, il tradizionale bilanciamento si complica e nuove pretese emergono e finiscono con collocarsi prevalentemente nell'ambito della protezione dei dati personali⁷. In questo contesto, il punto di partenza è il diritto alla cancellazione dei dati personali, riconosciuto sin dalla direttiva 95/46/CE come diritto dell'interessato ossia della persona a cui i dati si riferiscono⁸.

Di qui prende avvio la parabola evolutiva del diritto alla cancellazione – come emerge dalla giurisprudenza della Corte di giustizia dell'Unione europea e dalla sua nuova formulazione nel Regolamento generale sulla protezione dei dati (cd. GDPR) – che ne confermano la natura dinamica e la strutturale apertura all'adattamento tecnologico.

Tale traiettoria è oggi chiamata a confrontarsi con le sfide dell'intelligenza artificiale.

2. Il diritto all'oblio nel quadro della protezione dei dati personali

2.1. Origini giurisprudenziali: la sentenza *Google Spain / Costeja González*

Il riconoscimento del diritto all'oblio in chiave di protezione dei dati personali si deve, com'è noto, alla celebre sentenza *Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, resa dalla Corte di giustizia dell'Unione europea il 13 maggio 2014⁹.

7 V. G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, in *Il diritto dell'informazione e dell'informatica*, 3, 2010, 391ss.

8 Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati, GU L 281 del 23.11.1995, p. 31–50.

9 Cfr. almeno F. PIZZETTI, *Le autorità garanti per la protezione dei dati personali e la sentenza della Corte di giustizia sul caso Google Spain: è tempo di far cadere il velo di Maya*, in *Dir. Inform.*, 2014, 801 ss.; ID., *Tutela della persona, diritto all'oblio, web reputation e identità digitale. Internet e la luce delle stelle*, in F. PIZZETTI (a cura di) *Internet e la tutela della persona. Il caso del motore di ricerca*, Passigli, Firenze, 2015, 7 ss.; T.E. FROSINI, *Diritto all'oblio e Internet*, in *Federalismi.it*, 1, 2014, 1ss.; ID., *Il diritto all'oblio e la libertà informatica*, in *Dir.inf.*, 2012, 911 ss. O. POLLICINO, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in *Dir. inform.*, 4-5/2014, 569-589; ID., *Diritto all'oblio e conservazione di dati. La Corte di giustizia a piedi uniti: verso un digital right to privacy (osservazione a Corte di giustizia dell'Unione europea - Grande Sezione - 13 maggio 2014 - n. C-131/12 e 8 aprile 2014 - n. C-293/12, C-594/12)*, in *Giur. cost.*, 3/2014, 2949-2958; M. BASSINI, *Google davanti alla Corte di giustizia: il diritto all'oblio*, in *Quad. cost.*, 3/2014, 730 ss.; S. MARTINELLI, *Diritto all'oblio e motori di ricerca*, cit., spec. 156 ss.; E. STRADELLA, *Cancellazione e oblio: come la rimozione del passato, in bilico tra tutela dell'identità personale e protezione dei dati, si impone anche nella Rete, quali anticorpi si possono sviluppare e, infine, chi predesti?*,

La pronuncia della Corte di giustizia, vale la pena ricordare, si fondava sulla Direttiva 95/46/CE ed interveniva su alcune delle nozioni e degli istituti cardine di quella prima stagione della protezione dei dati personali. Molte delle affermazioni contenute nella sentenza sarebbero poi confluite, con formulazione quasi letterale, nel testo del Regolamento (UE) 2016/679 (GDPR), allora ancora in fase di discussione presso le Istituzioni europee, contribuendo così a delineare il nuovo modello normativo.

Basti pensare alla questione dell'applicabilità delle norme europee alle imprese extra europee. Nella sentenza la Corte si pronunciava sulla nozione di stabilimento, chiarendo che la Direttiva 95/46/CE si applicava ai trattamenti di dati personali effettuati al di fuori dell'Unione europea, qualora l'impresa operasse nel territorio di uno Stato membro mediante una filiale o una controllata incaricata di promuovere o commercializzare, come era appunto il caso di *Google Spain*, servizi inscindibilmente connessi all'attività di trattamento dei dati¹⁰.

Questa prima estensione della sovranità giuridica europea nello spazio digitale ha aperto la strada all'affermazione – dapprima in casi specifici nel quadro del GDPR¹¹ e, successivamente, in via generalizzata negli atti normativi del cd. decennio digitale europeo – del principio secondo cui se i dati trattati riguardano persone che si trovano nel territorio dell'Unione oppure se i servizi digitali sono offerti sul mercato europeo a beneficio di persone che si trovano in Europa, allora si applicano le regole europee in materia di dati e di responsabilità dei fornitori di servizi di intermediazione o di sistemi di intelligenza artificiale¹².

Per quanto riguarda il “diritto all'oblio”, la Corte di giustizia nella citata sentenza affermava, in primo luogo, che il gestore di un motore di ricerca fosse da considerare un “titolare del trattamento” ai sensi della Direttiva 95/46/CE, in quanto la sua attività di indicizzazione e organizzazione dei risultati di ricerca

in *Rivista Aic*, 4, 2016; e più di recente M.R. ALLEGRI, *Dimenticare, rievocare, rappresentare: dove conduce la via dell'oblio*, in *Medialmas. Rivista di diritto dei media*, n. 2, 2022, 1 ss.

10 Per una ricostruzione dei pareri del *Working Group Art. 29* – il network delle autorità nazionali di protezione dei dati che, nella vigenza della Direttiva 95/46/CE, ha contribuito a formare l'*humus* interpretativo entro cui si colloca la decisione della Corte di giustizia – v. G. CAGGIANO, *L'interpretazione del criterio di collegamento del 'contesto delle attività di stabilimento' dei responsabili del trattamento dei dati personali*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Romatre-Press, Roma, 2015, 43 ss.

11 Cfr. art. 4, par. 1, lett. a), Dir. 95/46/CE; oggi, art. 3, par. 1–2, Reg. (UE) 2016/679 (GDPR).

12 Il tentativo di affermare la sovranità digitale dell'Unione europea passa innanzitutto dall'estensione dell'ambito di applicabilità delle norme europee verso imprese che non sono stabilite sul territorio dell'Unione, ma offrono i loro servizi o trattano i dati relativi a persone che si trovano nell'Unione. V. in proposito: Regolamento (UE) 2016/679 (GDPR), art. 3; Regolamento (UE) 2022/1925 (*Digital Markets Act* – DMA), art. 1, par. 2; Regolamento (UE) 2022/2065 (*Digital Services Act* – DSA), art. 2, par. 1; nonché Regolamento (UE) 2024/1689 (*Artificial Intelligence Act* – AIA), art. 2 par. 1. Cfr. su questa specifica tendenza evolutiva e sulle sue conseguenze, A. BRADFORD, *Digital Empires. The Global Battle to Regulate Technology*, Oxford University Press, New York, 2023, spec. 105 ss.

integra un trattamento di dati personali autonomo rispetto a quello del sito sorgente. Ne consegue che anche il motore di ricerca, in quanto titolare autonomo del trattamento, è tenuto a rispettare gli obblighi normativi e a garantire i diritti riconosciuti all'interessato, compreso il diritto alla cancellazione dei dati.

Proseguendo il ragionamento, la Corte, ex art. 12, lettera b) e 14, paragrafo 1, lettera a) della Direttiva 95/46/CE, riconosceva che l'interessato può chiedere al gestore del motore di ricerca – in quanto titolare del trattamento – la cancellazione o il blocco dei dati personali che lo riguardano, quando essi risultino inadeguati, non pertinenti o non più necessari rispetto alle finalità originarie della raccolta.

La Corte, tuttavia, precisava anche che il gestore del motore di ricerca, pur essendo tenuto a garantire i diritti dell'interessato, non “dispone” dei contenuti presenti in rete e, pertanto, non può eliminarli alla fonte.

Ad impossibilia nemo tenetur, sembra ricordare la Corte, “accontentandosi” di garantire quel tanto (o molto) di oblio che può discendere dalla cancellazione di quelle indicizzazioni di informazioni relative ad una persona, che il motore di ricerca fornisce a partire da richieste (*queries*) che riportano il nome e cognome dell'interessato¹³.

Di qui prende forma il concetto di diritto alla de-indicizzazione, inteso come modalità specifica e tecnica di attuazione del diritto alla cancellazione nel contesto digitale, e che costituirà il punto di partenza per la successiva codificazione del diritto all'oblio nell'articolo 17 del Regolamento (UE) 2016/679 (GDPR)¹⁴.

2.2. Il diritto alla cancellazione (diritto all'oblio) nel GDPR: casi e limiti

La pronuncia *Google Spain* e la successiva elaborazione dottrinale hanno inciso in modo significativo sull'inclusione del “diritto all'oblio”, ancorché tra parentesi, nella rubrica dell'art. 17 del Regolamento (UE) 2016/679 (GDPR), dedicato al diritto alla cancellazione¹⁵.

La norma in questione prosegue in realtà a disciplinare essenzialmente il diritto alla cancellazione dei dati personali, di cui il diritto alla de-indicizzazione appare evoluzione tecnicamente obbligata e possibile.

13 S. SICA, V. D'ANTONIO, *La procedura di de-indicizzazione* e C. COMELLA, *Indici, sommari, ricerche e aspetti tecnici della 'de-indicizzazione'* entrambi in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, cit., 147 ss. e 177 ss.

14 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), GU L 119 del 4.5.2016, p. 1–88.

15 Sul fatto che si tratti di un'espressione infelice perché capace di confondere i trattamenti di dati personali nell'ambito dell'attività di informazione e i trattamenti di dati personale per finalità commerciali o di profilazione v. F. PIZZETTI, *Il prisma del diritto all'oblio*, cit. 48. V. a commento di tale norma, G. FINOCCHIARO, *Diritto alla cancellazione (“diritto all'oblio”)* (comm. Art. 17 GDPR), in *Codice della privacy e data protection*, Giuffrè, Milano, 2021, 325 ss.

Il par. 1 dell'art. 17, individua in modo assai preciso i motivi che consentono all'interessato di far valere il proprio diritto ed obbligano il titolare alla cancellazione dei dati personali. E bene ricordare che il diritto alla cancellazione sorge solo in casi specifici, ossia quando:

- a. i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti;
- b. l'interessato revoca il consenso e non sussiste altra base giuridica per il trattamento;
- c. l'interessato si oppone al trattamento ai sensi dell'art. 21 e non prevalgono motivi legittimi per proseguirlo¹⁶;
- d. i dati sono stati trattati illecitamente¹⁷;
- e. i dati devono essere cancellati per adempiere un obbligo legale;
- f. i dati sono stati raccolti relativamente all'offerta di servizi della società dell'informazione destinati a minori.

Al ricorrere di una di queste condizioni, il titolare del trattamento è tenuto, sempre ai sensi del par. 1 dell'art. 17 GDPR, a cancellare i dati senza ingiustificato ritardo.

Come specificato nel Cons. 60 del GDPR «per rafforzare il “diritto all'oblio” nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare gli ulteriori titolari che si sono giovati della pubblicazione della richiesta di cancellazione». In modo tale che essi possano provvedere a cancellare a loro volta i dati personali così come qualsiasi *link* verso di essi o copia o riproduzione.

Questa previsione trova la sua trasposizione normativa nel par. 2 dell'art. 17 che si riferisce ai dati resi conoscibili a tutti, come avviene assai spesso in rete ed obbliga il titolare oltre che a cancellarli anche ad informare, attraverso misure ragionevoli, i titolari del trattamento che stanno trattando i medesimi dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. Quest'obbligo, volto a rafforzare nel contesto digitale il controllo degli interessati sui propri dati, è apparso sin da subito assai gravoso, ancorché esso sia in parte attenuabile dal riferimento normativo al criterio della ragionevolezza, della tecnologia disponibile e dei costi di attuazione¹⁸. Resta chiaro ed evidente che tale obbligo sia sottoposto ad una forte tensione di fronte all'emergere di fenomeni diffusi di *web-scraping* – ossia processi di raccolta

16 Se l'opposizione, ai sensi dell'art. 21, par. 2, riguarda il trattamento di dati personali per finalità di marketing diretto, il titolare del trattamento deve sempre interrompere il trattamento non potendo dimostrare l'esistenza di motivi legittimi al fine della continuazione del medesimo.

17 ... a meno che l'interessato chieda la limitazione del trattamento ex art. 20 GDPR opponendosi così alla cancellazione dei dati personali.

18 Questa è la parte più innovativa della formulazione normativa di cui all'art. 17. Così F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018, 28.

automatizzata di informazioni da siti web utilizzando *software* chiamati “bot” o appunto “scrapper” – oggi fondamentali per l’addestramento dei modelli di intelligenza artificiale.

A fronte delle condizioni che legittimano l’esercizio del diritto alla cancellazione, l’art. 17, par. 3, del GDPR esclude esplicitamente che il titolare debba dare corso alla richiesta nei casi in cui la prosecuzione del trattamento è necessaria:

- a. per l’esercizio della libertà di espressione e di informazione;
- b. per l’adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell’Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- c. per l’esecuzione di un compito svolto nel pubblico interesse oppure nell’esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- d. per motivi di interesse pubblico nel settore della sanità pubblica, per finalità di medicina preventiva o di medicina del lavoro, per la valutazione della capacità lavorativa del dipendente, per diagnosi, assistenza o terapia sanitaria o sociale ovvero per gestione dei sistemi e servizi sanitari o sociali o conformemente al contratto con un professionista della sanità, se trattati sotto la responsabilità di un professionista soggetto al segreto professionale.
- e. a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici nella misura in cui il diritto alla cancellazione rischi di rendere impossibile o gravemente pregiudicato il conseguimento degli obiettivi di tale trattamento¹⁹.
- f. per l’accertamento, l’esercizio o la difesa di un diritto in sede giudiziaria.

Il titolare del trattamento è, quindi, chiamato in prima battuta – in virtù del principio di *accountability* che ispira l’intero sistema normativo – a valutare ogni richiesta di cancellazione pervenuta alla luce tanto delle condizioni che la legittimano quanto delle limitazioni appena richiamate.

3. Il legame tra esercizio del diritto alla cancellazione e condizioni di liceità del trattamento

L’analisi dei presupposti che consentono all’interessato l’esercizio del diritto alla cancellazione, così come delle relative eccezioni, rivela la stretta connessione esistente tra tale diritto e le condizioni di liceità del trattamento, quelle “ordinarie” di cui all’art. 6 del GDPR e quelle deroganti al divieto di trattamento per le categorie particolari di dati di cui all’art. 9 GDPR²⁰.

19 Cfr. sulla portata dell’art. 89, GDPR, in un quadro più ampio, L. PASERI, *Scienza aperta. Politiche europee per un nuovo paradigma della ricerca*, Mimesis, Milano, 2024, spec. 162 ss. V. anche A. FOTI, *Il diritto all’oblio alla prova dell’archiviazione digitale: il caso di Internet Archive*, cit.

20 V. sul punto anche l’analisi casistica di A. MANTELETO, *Right to object and right to erasure*, 9 dicembre 2022: https://www.edpb.europa.eu/system/files/2023-02/one-stop-shop_case_digest_on_the_right_to_object_and_right_to_erasure_en.pdf.

Questa connessione emerge in modo evidente con riguardo all'esigibilità della richiesta di cancellazione: mentre, nel caso di trattamento fondato sul consenso, la richiesta deve essere accolta, negli altri casi l'obbligo di cancellazione è subordinato alla valutazione dei termini contrattuali, del contenuto dell'obbligo di legge, della natura del compito di interesse pubblico o della portata dell'interesse legittimo del titolare in esito al bilanciamento con i diritti e le libertà dell'interessato.

C'è però anche un'altra questione che dipende dalla base legale del trattamento e che diventa oggi, nel contesto dell'intelligenza artificiale, assai importante. Si tratta della "portata" della cancellazione: in altri termini, la questione è se la cancellazione operi solo ad escludere nuovi trattamenti successivi alla richiesta oppure se la richiesta possa avere degli effetti anche sui trattamenti già avvenuti ossia sui dati inferenziali eventualmente ricavati ed oggetto di successivi trattamenti. Si tratta dunque di chiarire se, e nel caso a quali condizioni, la richiesta di cancellazione produca effetti non solo *ex nunc* ma pure *ex tunc*.

Il testo dell'art. 17 e i considerando 65 e 66 del GDPR non precisano la portata temporale della cancellazione. Il riferimento al fatto che il titolare debba operare "senza ingiustificato ritardo" appare in linea con un'efficacia *ex nunc* della richiesta di cancellazione. D'altra parte il "legislatore" europeo aveva certamente in mente contesti in cui il trattamento costituisce una singola operazione unitaria, caratterizzata da una finalità determinata e univoca, destinata ad esaurirsi.

Questa prospettiva *ex nunc* è certamente coerente e compatibile con la cessazione della necessità del trattamento rispetto alla finalità, con la revoca del consenso, con una legittimazione contrattuale nonché con un sopravvenuto obbligo legale che imponga la cancellazione.

Tuttavia, secondo una logica di sistema, qualora il trattamento risulti *ab origine* privo di base giuridica, ad esempio perché illecito, o viziato da illegittimità originaria – vuoi per errata individuazione del legittimo interesse del titolare o mancato bilanciamento del legittimo interesse del titolare con i diritti e le libertà fondamentali dell'interessato, vuoi per l'assenza del requisito della necessità per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri – si apre la strada a casi in cui la cancellazione debba produrre effetti *ex tunc* e cioè anche sui trattamenti già effettuati e, quindi, sui dati prodotti da un trattamento originariamente viziato.

In tali ipotesi, oltre alla cancellazione dei dati trattati, si dovrebbe procedere alla rimozione dei dati inferenziali o derivati, ricavati da trattamenti realizzati in assenza di una valida condizione di liceità, almeno nella misura in cui tali dati siano stati generati grazie ai dati personali di cui si domanda la cancellazione.

È evidente come, in una tale prospettiva, la cancellazione dei dati non è configurabile come un mero esercizio di un diritto dell'interessato, quanto piuttosto deve essere inteso come atto di ripristino di una legalità violata.

Questa distinzione riveste particolare importanza nel contesto dell'intelligenza artificiale, in cui enormi quantità di dati, anche di natura personale, sono trattate per finalità di addestramento di modelli e sistemi di intelligenza artificiale, generando a loro volta *output* o inferenze potenzialmente riconducibili a persone fisiche.

La corretta individuazione della base giuridica del trattamento dei dati e delle categorie di dati utilizzati in fase di addestramento o di prova costituisce, pertanto, il presupposto imprescindibile non solo per determinare l'ampiezza, l'effettività e la declinazione del diritto alla cancellazione (oblio) ma, più in generale, per garantire la legittimità complessiva dello sviluppo e dell'utilizzo dei modelli e dei sistemi di intelligenza artificiale.

4. Il diritto alla cancellazione dei dati tra GDPR e AI Act: verso una nuova declinazione?

Come la dottrina ha messo in evidenza, l'adozione del Regolamento (UE) 2024/1689 cd. AI Act²¹ segna un passaggio cruciale nel tentativo dell'Unione di disciplinare un fenomeno tecnologico in dirompente divenire nonché per sua natura trasversale, cioè capace di intersecare diversi settori e ambiti normativi²².

Tra di essi certamente quello della protezione dei dati personali. Pertanto, per identificare la corretta portata del diritto alla cancellazione di cui al GDPR, nel contesto dell'IA, occorre partire dagli effetti di questa interazione.

In primo luogo, occorre considerare il dato testuale del considerando 10 dell'AI Act. Esso, infatti, afferma espressamente che la nuova normativa «non mira a pregiudicare l'applicazione del vigente diritto dell'Unione che disciplina il trattamento dei dati personali, inclusi i compiti e i poteri delle autorità di controllo indipendenti competenti a monitorare la conformità con tali strumenti.»

21 Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regolamento sull'intelligenza artificiale), GU L 202 del 12.7.2024, p. 1–222

22 Si rinvia in argomento ai saggi in F. PIZZETTI, S. CALZOLAIO, A. IANNUZZI, E. LONGO, M. OROFINO, *La regolazione europea dell'intelligenza artificiale nella società digitale*, Giappichelli, Torino, 2025. V. anche, *ex multis*, nella dottrina italiana A. MANTELEO, G. RESTA, G.M., RICCIO (a cura di), *Intelligenza artificiale. Commentario. Regolamento (UE) 2024/1689-AI ACT*, Wolters Kluwer, Milano, 2025; M. FASCIGLIONE, O. POLLICINO, F. PAOLUCCI, *AI e sostenibilità. Verso una compliance integrata*, Giappichelli, Torino, 2025; F. DONATI, G. FINOCCHIARO, O. POLLICINO, F. PAOLUCCI (a cura di), *La disciplina dell'Intelligenza artificiale*. Giuffrè, Milano, 2025; E. M. TRIPODI, G. CASSANO (a cura di), *Il regolamento europeo sull'intelligenza artificiale: commento al reg. UE n. 1689-2024*, Maggioli, Santarcangelo di Romagna, 2024; R. RAZZANTE, *Manuale Sull'Intelligenza Artificiale*, I ed., Giappichelli, Torino, 2024. G. FINOCCHIARO, *Intelligenza artificiale: quali regole?*, Il Mulino, Bologna, 2024.

Inoltre, l'AI Act, sempre secondo il citato considerando, «lascia impregiudicati gli obblighi dei fornitori e dei *deployers* dei sistemi di IA nel loro ruolo di titolari del trattamento o responsabili del trattamento (...) nella misura in cui la progettazione, lo sviluppo o l'uso di sistemi di IA comportino il trattamento di dati personali»²³.

Ne consegue che fornitori e *deployer*, se riconducibili al ruolo di titolari o di responsabili del trattamento dei dati personali, devono rispettare anche tutti gli obblighi che scaturiscono dal GDPR e, nello specifico, garantire (anche proattivamente) l'esercizio dei diritti dell'interessato e tra di essi ovviamente del diritto alla cancellazione (oblio) di cui all'art. 17.

Il primo nodo interpretativo è, dunque, verificare in quali circostanze tali soggetti possano essere considerati titolari o responsabili del trattamento dei dati personali²⁴.

A tal fine occorre compiere due valutazioni secondo i criteri elaborati dalla giurisprudenza della Corte di giustizia e dal Comitato europeo per la protezione dei dati (EDPB). La prima valutazione riguarda l'effettivo utilizzo di dati qualificabili come personali e non, dunque, di dati anonimi o anonimizzati; la seconda consiste nell'accertare se fornitori o *deployer* compiano attività che provano un loro effettivo controllo sulle finalità e sui mezzi del trattamento.

In secondo luogo, occorre verificare se l'AI Act sia configurabile – e nel caso in quali circostanze – come base legale del trattamento di dati personali. Questo perché ciò porterebbe – come si è visto – a restringere in modo assai significativo la portata del diritto dell'interessato a richiedere la cancellazione del dato potendosi, infatti, il titolare giovare della corrispondente causa di esclusione dell'obbligo legale.

In proposito, il Regolamento afferma, in via generale, di non introdurre alcuna base legale generale ed autonoma per il trattamento dei dati personali necessari al funzionamento (addestramento e prova) dei sistemi di intelligenza artificiale.

A fronte di questa previsione generale, l'AI Act enumera due casi specifici in cui invece ciò avviene. Il primo caso specifico è quello dei trattamenti connessi

23 La traduzione normativa di quanto espresso nel considerando 10 si ha innanzitutto nell'art. 2, par. 5, del Regolamento (UE) 2024/1689, che stabilisce espressamente che «il presente regolamento lascia impregiudicata l'applicazione del diritto dell'Unione in materia di protezione dei dati personali, in particolare del regolamento (UE) 2016/679», norma che recepisce in termini vincolanti quanto già affermato dal considerando 10. Ulteriori rinvii funzionali al GDPR sono presenti nel considerando 67 in materia di trasparenza nella *governance* dei dati, nel considerando 69 circa l'applicazione del principio di minimizzazione e di protezione dei dati *by default*, nel considerando 70 sui trattamenti di dati particolari al fine di correggere *bias* e discriminazioni e nel considerando 159 sui poteri delle autorità di controllo.

24 V. in proposito, B.A. JULIUSSEN, J.P. RUI, D. JOHANSEN, *Algorithms that forget: Machine unlearning and the right to erasure*, in *Computer Law & Security Review*, 51, 2023, 1 ss.

ad attività di sperimentazione e sviluppo dei sistemi di intelligenza artificiale (cd. *sandboxes*)²⁵. Questo avviene ai sensi degli artt. 59 e 60 dell'AI Act²⁶.

L'art. 59 prevede, infatti, che i dati personali legalmente raccolti per altre finalità possono essere trattati ancorché ai soli fini dello sviluppo, dell'addestramento e delle prove di determinati sistemi di IA nello spazio di sperimentazione. La previsione normativa, corredata da precise condizioni e limiti, è la base del nuovo trattamento non dovendosi ricercare altra condizione di legittimità²⁷.

L'articolo 60 regola, invece, le prove in condizioni reali dei sistemi di IA ad alto rischio, imponendo un quadro rigoroso di autorizzazioni, controlli e garanzie per i partecipanti. Elemento centrale è il consenso informato (art. 61): i soggetti coinvolti devono essere chiaramente informati e acconsentire volontariamente alla partecipazione alle prove. Tale consenso può essere revocato in qualsiasi momento, senza pregiudizio e senza necessità di motivazione, con la conseguenza che i dati personali devono essere cancellati immediatamente e in modo permanente. La norma prevede un'eccezione specifica per le attività di contrasto: in tali casi, se chiedere il consenso informato renderebbe impossibile condurre la prova del sistema di IA, essa può comunque essere effettuata, a condizione che i test non producano alcun effetto negativo sui soggetti coinvolti e che i loro dati personali siano cancellati una volta conclusa la sperimentazione²⁸.

Si tratta, a tutta evidenza, di un meccanismo peculiare: il consenso menzionato non è un consenso al trattamento dei dati personali in senso stretto, bensì un consenso alla partecipazione alla prova sperimentale. Da ciò deriva un diritto alla cancellazione *sui generis*, introdotto dall'AI Act per bilanciare l'interesse pubblico alla sperimentazione con la tutela delle persone coinvolte.

Il secondo caso specifico in cui l'AI Act si configura come base legale è quello del trattamento di categorie particolari di dati personali in via eccezionale e nella misura strettamente necessaria al fine di garantire il rilevamento e la correzione delle distorsioni (*bias*) in relazione ai sistemi di IA qualificati come ad alto rischio. Ad esempio, nel caso di un sistema di IA ad alto rischio impiegato per la selezione del personale, laddove il fornitore o il *deployer* riscontrino che l'algoritmo produce esiti sistematicamente sfavorevoli nei confronti di determinati gruppi di candidati, può rendersi necessario trattare, in via eccezionale e nei limiti della stretta necessità, categorie particolari di dati personali – ad esempio dati relativi all'origine etnica o al genere – al solo fine di verificare se il sistema discrimini indirettamente gli specifici gruppi testati²⁹.

25 Cfr. E. LONGO, *Gli spazi di sperimentazione normativa o anche regulatory sandboxes nell'AI Act*, in F. PIZZETTI, S. CALZOLAIO, A. IANNUZZI, E. LONGO, M. OROFINO, *La regolazione europea dell'intelligenza artificiale nella società digitale*,

26 V. anche cons 140 e 141, AIA.

27 L'art. 59 AIA definisce con estrema precisione una serie di condizioni che debbono essere soddisfatte.

28 Art. 60, par. 4, lett. i), AIA.

29 Il cons. 70 prevede che tale trattamento debba avvenire predisponendo le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche e previa attuazione di tutte le condizioni

In entrambi i casi qui analizzati, l'esercizio del diritto alla cancellazione ex art. 17 del GDPR è limitato all'ipotesi in cui i dati non siano più necessari rispetto alle finalità per le quali sono stati successivamente trattati e, in ogni caso, qualora accolto ha una portata solo *ex nunc*.

Il tema dell'introduzione di specifiche previsioni di legge che legittimano il trattamento di dati personali per finalità diverse rispetto a quella originarie – in particolare per l'addestramento e la prova di modelli di IA – riveste oggi un rilievo crescente.

Tali norme abilitanti non si limitano infatti a introdurre eccezioni puntuali al principio generale di finalità, ma delineano piuttosto un nuovo assetto della circolazione dei dati, fondato su presupposti funzionali all'interesse pubblico, all'innovazione tecnologica e allo sviluppo di sistemi di intelligenza artificiale. Questa tendenza appare sempre meno come una deroga eccezionale e sempre più come uno strumento strutturale di *governance* dei dati nell'ecosistema digitale contemporaneo³⁰. Tali previsioni sono di norma accompagnate da specifiche garanzie procedurali, organizzative e tecniche, che mirano a contenere i rischi per i diritti e le libertà degli interessati senza però arrestare i processi di sperimentazione e apprendimento automatico.

Il caso più eclatante, ma non l'unico³¹, che dimostra questa linea di tendenza è quello del Regolamento UE 2025/327 *sullo spazio europeo dei dati sanitari* (cd. EHDS) che autorizza il trattamento di dati sanitari elettronici raccolti per le finalità primarie di prevenzione, diagnosi e cura nonché per molteplici altre finalità definite come secondarie. Ai sensi del Regolamento, per uso secondario si intende il riutilizzo dei dati sanitari a fini di sanità pubblica, attività d'istruzione o d'insegnamento, statistica, definizione delle politiche e medicina personalizzata ed attività di ricerca³². Nella finalità di ricerca è specificamente menzionata «l'attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, dispositivi medico-diagnostici in vitro, sistemi di IA e

applicabili previste dal presente regolamento unitamente alle condizioni previste dai regolamenti (UE) 2016/679 e (UE) 2018/1725 e dalla direttiva (UE) 2016/680.

30 Sia consentito rinviare per una più approfondita riflessione sulla trasformazione in corso a M. OROFINO, *The New Balance Between Data Circulation and Data Protection in the Digital Single Market*, in F. DAL POZZO, I. ANRÒ, (a cura di), *Il mercato unico digitale tra antichi problemi e nuove sfide*. Fascicolo speciale, *Eurofus*, 2025, 45 ss.

31 Incidono in materia di protezione dei dati personali, sia i Regolamenti del cd. *Digital Package* (il *Digital Services Act* e il *Digital Markets Act*), sia il *Data Governance Act* ed il *Data Act*. V. per un esame del loro impatto i saggi di A. IANNUZZI, *I regolamenti intersettoriali per l'istituzione dei data spaces: Data Governance Act e Data Act*, M. OROFINO, *Il Digital Service Act tra continuità (solo apparente) ed innovazione* e ID, *Il Digital Market Act: una regolazione asimmetrica a cavallo tra diritto della protezione dei dati e diritto antitrust*, in F. PIZZETTI, S. CALZOLAIO, A. IANNUZZI, E. LONGO, M. OROFINO, *La regolazione europea della società digitale*, cit., rispettivamente 107 ss., 134 ss. e 175 ss.

32 V. Art. 53, Regolamento EHDS. Sulla regolazione dei neurodati (e sulla loro qualificazione come dati personali particolari v. F.G. PIZZETTI, *Dispositivi medici, neurodati e diritti fondamentali: verso una nuova regolazione europea per le neurotecnologie?*, in G. DE MINICO, M. OROFINO (a cura di), *Regole telecomunicazioni dati nell'Europa digitale*, Jovene, Napoli, 2025, 69 ss.

applicazioni di sanità digitale»³³. A fronte di questa apertura verso il riuso di dati sanitari elettronici, il Regolamento EHDS prevede una serie di garanzie e anche un peculiare meccanismo di *opting out* per l'interessato³⁴.

Per l'oggetto dell'indagine occorre dire che la proliferazione di norme abilitanti il riuso ha un innegabile impatto sulla portata dei diritti dell'interessato e, in particolare, sul diritto alla cancellazione dei dati che lo riguardano. Questo perché è sempre più la legge a definire le condizioni, le finalità ed i tempi del trattamento restringendo di conseguenza l'autonomia individuale.

Infine, de iure condendo, occorre anche menzionare la proposta di Regolamento presentata dalla Commissione europea il 15 novembre 2025, cd. *Digital Omnibus*³⁵, perché essa, tra gli altri interventi, mira a modificare la definizione di dato personale, specificando come l'identificabilità della persona a cui il dato si riferisce deve essere valutata nel contesto reale e non solo potenzialmente. Pur essendo prematuro fare ipotesi sull'impatto di tale innovazione, essa potrebbe potenzialmente incidere sui dati di addestramento andando a ridurre la quota di dati che sono considerati come personali ed il cui trattamento è, quindi, soggetto alle regole del GDPR.

5. Il Parere EDPB n. 28/2024 e la qualificazione dei fornitori di modelli di IA

Particolare rilievo assume, nel contesto di interazione tra intelligenza artificiale e protezione dei dati personali, il Parere n. 28/2024 del Comitato europeo per la protezione dei dati (EDPB), adottato il 17 dicembre 2024 e dedicato ai modelli di intelligenza artificiale³⁶.

Pur non affrontando, nel suo complesso, il tema della qualificazione dei fornitori di sistemi di IA, il documento fornisce importanti chiarimenti in ordine all'applicabilità del GDPR ai modelli di intelligenza artificiale.

Il Parere individua, anzitutto, il criterio distintivo per stabilire se il fornitore di un modello di IA debba essere considerato titolare del trattamento. Secondo

33 Art. 53, par. 1, lett. E), pt. ii. Regolamento EHDS.

34 Sia consentito il rinvio a M. OROFINO, *Digital Health e diritto alla salute: l'impatto del Regolamento EHDS sui sistemi sanitari nazionali*, in *Italian Papers on Federalism*, n. 1, 2025, 174 ss.

35 V. *Proposal of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)*, 19 Novembre 2025 {SWD(2025) 836 final}.

36 Comitato europeo per la protezione dei dati (EDPB), Parere n. 28/2024 sui modelli di intelligenza artificiale, 17 dicembre 2024. V. in dottrina S. STALLA-BOURDILLON, A. ROSSI, *A critical assessment of EDPB Opinion 28/2024: Towards a principle-based approach to innovation?*, in *Privacy and Data Protection*, 6, 2025, 12 ss Il Parere EDPB n. 28/2024 è stato seguito dalle Linee guida EDPB n. 01/2025 sulla pseudonimizzazione.

PEDPB ciò dipende dal grado di anonimizzazione del modello e dalla possibilità di re-identificare, anche indirettamente, i dati personali utilizzati nella fase di addestramento. Pertanto, il modello può essere considerato “anonimo” solo se non consente, neppure in via probabilistica, la ricostruzione dei dati individuali originari o la produzione di *output* riferibili a persone identificate o identificabili³⁷.

Qualora, invece, il modello mantenga tracce riconducibili ai dati personali utilizzati in addestramento o produca *output* riferibili, il fornitore deve essere considerato titolare del trattamento e, come tale, soggetto a tutti gli obblighi previsti dal GDPR, compreso quello di garantire l'esercizio dei diritti degli interessati, fra i quali il diritto alla cancellazione ai sensi dell'art. 17 GDPR. La portata della richiesta di cancellazione (*ex nunc* o *ex tunc*) dipenderà dalla base legale che il titolare ha utilizzato per l'addestramento.

Proprio con riferimento a questo aspetto, il Parere si sofferma sulla possibilità di fondare il trattamento dei dati d'addestramento sull'interesse legittimo del titolare (art. 6, par. 1, lett. f, GDPR). Una condizione di legittimità che, se da un lato, è particolarmente diffusa per l'addestramento dei modelli di intelligenza artificiale (in particolare per i *Large Language Models*) perché i fornitori del modello spesso fanno uso di dati anche personali diffusi *online* per addestrare sistemi di apprendimento automatico attraverso il cd. *web scraping*; da un altro lato non può essere usata per legittimare il trattamento di dati personali particolari ai sensi dell'art. 9 GDPR.

Inoltre, tale condizione di liceità è, come noto, al tempo stesso molto importante per favorire il riuso e la circolazione dei dati e fonte di incertezza, richiedendo sempre al titolare del trattamento un complesso bilanciamento – da effettuarsi prima dell'inizio dei trattamenti – tra il proprio interesse legittimo e i diritti e le libertà degli interessati. Un bilanciamento che, se non svolto correttamente dal titolare, può comportare un'illegittimità originaria del trattamento, la quale, come si è osservato, si riflette in punto di cancellazione determinando l'applicazione di una cancellazione *ex tunc* volta a rimuovere gli effetti di un trattamento sin dall'origine privo di base giuridica

L'EDPB riconosce la possibilità, in astratto, ma non di *default*³⁸, di fondare i trattamenti a fini di addestramento sul legittimo interesse (naturalmente non per i dati particolari o ex sensibili), ma precisa che ciò richiede un test rigoroso.

37 V. in proposito, anche per una ricostruzione dettagliata della giurisprudenza della Corte di giustizia, S. STALLA-BOURDILLON, *Identifiability, as a Data Risk: Is a Uniform Approach to Anonymisation About to Emerge in the EU?* in *European Journal of Risk Regulation*. 2025, doi:10.1017/err.2025.16.

38 L'EDPB richiama la responsabilità proattiva del titolare (accountability), sottolineando che il legittimo interesse non può essere utilizzato come base “di default” per l'addestramento dei modelli di IA.

Questa necessità era peraltro già sottolineata nelle Linee guida 1/2024 dell'EDPB ed ora è qui ribadita adattando il test al contesto dell'IA³⁹.

Il test descritto si articola in tre fasi.

La prima fase concerne la verifica della legittimità e della concretezza dell'interesse perseguito. Essa richiede l'identificazione di un interesse legittimo concreto e determinato, che sia effettivo, lecito e attuale, non meramente ipotetico o speculativo⁴⁰. Nel caso dei modelli di IA, l'interesse legittimo può consistere nello sviluppo, miglioramento o manutenzione del modello, purché tali finalità siano chiaramente documentate e non perseguite in modo eccessivo o sproporzionato.

La seconda fase consiste nell'analisi della necessità del trattamento rispetto a tale interesse. Tale condizione deve essere esaminata alla luce dei diritti e delle libertà fondamentali degli interessati e in relazione al principio di minimizzazione dei dati. Il che significa che il titolare deve valutare, nel contesto del trattamento, se le stesse finalità possano essere raggiunte con mezzi meno invasivi⁴¹. Nel contesto dell'addestramento di modelli di intelligenza artificiale, ciò implica un esame delle alternative tecniche (ad esempio, l'uso di dati sintetici, anonimizzati o pseudonimizzati) così come di misure di attenuazione.

La terza ed ultima fase attiene al bilanciamento vero e proprio tra il proprio interesse e i diritti e le libertà dell'interessato. Esso deve, innanzitutto, essere un bilanciamento concreto tra lo specifico interesse legittimo del titolare ed i diritti e le libertà fondamentali degli interessati che concretamente vengono in rilievo. In secondo luogo, deve tener conto della natura dei dati, del contesto, delle aspettative ragionevoli delle persone e dell'impatto potenziale sugli individui. Molto interessante è che con specifico riferimento ai modelli di IA, l'EDPB, da un lato, prevede che debbano essere considerati alcuni rischi concreti per gli interessi e per le libertà delle persone che possono derivare dall'addestramento e dalla diffusione del modello, quali ad esempio il rischio reputazionale, di sorveglianza di massa, di furto d'identità, il *chilling effect*, il reimpiego non autorizzato dei dati, la profilazione indebita o la possibilità di "rigurgito" di dati personali negli *output* generati dai sistemi di IA; da un altro lato, richiede di considerare anche gli impatti positivi che il modello può apportare per gli interessi e le libertà degli individui nonché per la società nel suo complesso. Ciò è evidentemente la spia di quanto sia cambiata, soprattutto grazie all'IA, la percezione della circolazione dei dati, da mero rischio per la protezione dei dati personali

39 Comitato europeo per la protezione dei dati (EDPB), *Linee guida 1/2024 sul trattamento dei dati personali in base all'articolo 6, paragrafo 1, lettera f), del RGPD, versione 1.0*, punto 17.

40 Parere n. 28/2024, cit. ptt. 68 e 69.

41 La questione del contesto del trattamento è assai importante, come la Corte di giustizia ha più volte richiamato, al fine di verificare che l'interesse sia effettivamente legittimo. CGUE, sentenza del 27 settembre 2017, causa C-73/16, *Peter Puškár* (ECLI:EU:C:2017:725), punto 113 nonché CGUE, sentenza del 4 ottobre 2024, causa C-621/22, *Koninklijke Nederlandse Lawn Tennisbond* (ECLI:EU:C:2024:857), punti 51-53.

e, di conseguenza, per le libertà individuali, a presupposto per garantire il raggiungimento di interessi di rango costituzionale e innalzare il grado di tutela dei diritti fondamentali⁴².

6. Effettività del diritto all'oblio nell'era dell'intelligenza artificiale

Sulla base delle osservazioni formulate e degli orientamenti espressi dall'EDPB, pare potersi affermare che l'effettività del "diritto all'oblio" nell'era dell'intelligenza artificiale richiede – come peraltro avvenuto per il diritto alla de-indicizzazione con riferimento ai motori di ricerca – di confrontarsi con i limiti e le possibilità offerte dallo stato dell'arte tecnologico⁴³.

In altri termini, la concreta attuazione del diritto alla cancellazione dei dati personali non può prescindere da una valutazione realistica di ciò che è tecnicamente possibile realizzare nei sistemi di IA, in particolare con riguardo ai modelli già addestrati e alla persistenza delle informazioni nei loro parametri⁴⁴.

Inoltre, come avverte l'EDPB, occorre tenere adeguatamente conto anche dell'impatto positivo che i sistemi di intelligenza artificiale hanno e avranno in futuro, al fine di ponderare gli interessi delle persone in materia di protezione dei dati personali e della vita privata con gli interessi individuali e generali sottesi allo sviluppo e all'impiego di tali tecnologie. Il che implica che, laddove l'unica soluzione prospettata fosse quella di non procedere affatto, occorra adottare particolare cautela, evitando esiti regolatori che, nel tentativo di tutelare in modo assoluto la sfera privata, finiscano per precludere in radice sviluppi tecnologici suscettibili di produrre benefici rilevanti sia per gli individui che per la collettività⁴⁵.

42 La questione della circolazione dei dati (anche personali) per garantire il soddisfacimento dei diritti fondamentali appare nella società digitale, e in particolar modo con riferimento agli strumenti di intelligenza artificiale, di particolare rilevanza. Per un approfondimento del tema sia consentito rinviare a M. OROFINO, *The New Balance Between Data Circulation and Data Protection in the Digital Single Market* cit. e con specifico riferimento al diritto alla salute a ID, *One Digital Health e circolazione dei dati: tra mercato unico e diritti costituzionali*, in *Corti supreme e salute*, 1, 2025, 257 ss.

43 Ciò, naturalmente, non implica che la politica abdichi alla tecnica, come efficacemente sottolineato da G. DE MINICO (ID, *Regole o libertà per le telecomunicazioni del futuro?* in G. DE MINICO, M. OROFINO, (a cura di), *Regole telecomunicazioni dati nell'Europa digitale*, cit., 1 ss.) al contrario, richiede che il legislatore e le autorità di regolazione esercitino un ruolo attivo di indirizzo e governo dell'innovazione tecnologica, orientando le soluzioni tecniche verso il rispetto dei diritti fondamentali e dei valori costituzionali, piuttosto che limitarsi a recepirne passivamente i vincoli.

44 In proposito, in questo volume, il saggio di S. NICOLAZZO, A. SAPIENZA, S. VILELLA, G. RUFFO (*De-)indicizzazione e diritto all'oblio al tempo dei Large Language Model*.

45 Lo sviluppo della società digitale caratterizzata da una strutturazione dei rapporti sociali prevalentemente su base individuale e mediata da sistemi tecnologici automatizzati, come

Sulla base di questa premessa possono essere individuate due direttrici complementari.

La prima direttrice è quella della prevenzione. Essa richiede delle misure tecniche ed organizzative idonee a minimizzare i rischi (previa la loro corretta identificazione) per gli interessati. La seconda direttrice è quella della cancellazione effettiva *ex post*, quando l'interessato esercita il proprio diritto ad ottenere la rimozione dei dati personali trattati. Questa seconda via, che opera a valle, può concretizzarsi attraverso due strumenti principali: il de-addestramento del modello e/o l'imposizione di filtri sugli *output*.

6.1. Le misure tecniche di mitigazione

La prima direttrice per garantire il diritto all'oblio nel contesto dell'intelligenza artificiale è, quindi, quella della prevenzione.

Le misure di mitigazione previste nel Parere EDPB n. 28/2024 sono da questo punto di vista gli strumenti più adeguati. Esse consistono sia in misure tecniche che in misure organizzative.

Tra le misure tecniche rientrano, in primo luogo, le tecniche di pseudonimizzazione e di mascheramento dei dati personali, volte a ridurre il rischio di re-identificazione e a limitare la disponibilità delle informazioni. A titolo esemplificativo, tali tecniche possono consistere nella rimozione o sostituzione degli identificativi diretti (come nomi, indirizzi o numeri identificativi), nell'aggregazione dei dati o nell'adozione di meccanismi che impediscano al modello di memorizzare informazioni personali specifiche. Esse operano sia sui *dataset* utilizzati per l'addestramento sia, indirettamente, sugli *output* del modello, ad esempio riducendo la probabilità che il sistema rigeneri dati personali presenti nei dati di *training*.

Le misure organizzative riguardano principalmente i meccanismi di *opt-out* preventivo.

In concreto, ciò può tradursi, da un lato, nella predisposizione di informative e strumenti accessibili agli interessati per opporsi all'utilizzo dei propri dati personali ai fini dell'addestramento dei modelli di IA⁴⁶, dall'altro lato, nella

magistralmente illustrato da F. BALAGUER CALLEJON, *La Costituzione dell'algoritmo*, Mondadori, Milano 2023 (2021) deve fare i conti, nell'era dell'intelligenza artificiale, con l'emersione sempre più marcata di interessi collettivi, che si affiancano e talora si pongono in tensione con la tradizionale centralità dell'individuo. Il tema che si profila all'orizzonte è sempre quello dell'equilibrio tra individuo e comunità. V. con particolare riferimento all'impatto che le due prospettive, quella individualista e quella comunitaria, possono avere sull'interpretazione costituzionale e sul bilanciamento tra diritti fondamentali ed interessi di rango costituzionale, F. PALLANTE, *Per scelta o per destino? La Costituzione tra individuo e comunità*, Giappichelli, Torino, 2018.

46 Si veda, in particolare, il caso Meta, che nel giugno 2024 ha comunicato agli utenti europei l'intenzione di utilizzare i loro dati personali per l'addestramento dei propri modelli di intelligenza artificiale, basandosi sull'interesse legittimo quale base giuridica ai sensi dell'art. 6, par.

possibilità per i titolari che hanno reso pubblici dati personali – ad esempio mediante la pubblicazione *online* di contenuti – di segnalare la propria opposizione al loro riutilizzo, sia in generale sia con riferimento a specifiche finalità, come l'addestramento dei modelli generativi⁴⁷.

6.2. Il “de-addestramento” come strumento per un’effettiva cancellazione *ex tunc*

La seconda direttrice per garantire il diritto all'oblio richiede di rendere effettivo il diritto alla cancellazione nel contesto dell'intelligenza artificiale, con specifico riguardo ai dati personali utilizzati per l'addestramento dei modelli.

Si distinguono due approcci principali.

Il primo approccio è il de-addestramento e il ri-addestramento del modello. Esso presuppone una cancellazione esatta. Le tecniche di cancellazione esatta si concentrano sul caso più complesso, in cui i dati personali sono incorporati (*embedded*) all'interno del modello di apprendimento automatico (*machine learning*) stesso. L'obiettivo è ottenere lo stesso modello distribuito (*deployed model*) che si sarebbe ottenuto se i dati dell'interessato, di cui è necessaria la cancellazione, non fossero mai stati inclusi nel *dataset* di addestramento.

Nel caso della cancellazione esatta, si presume che la semplice eliminazione dei dati personali dal *dataset* di addestramento (indipendentemente dal modello già addestrato) non sia sufficiente. Si tratta del requisito più rigoroso in materia di rimozione dei dati poiché richiede l'eliminazione dei dati oggetto della richiesta sia dai *dataset* di addestramento sia dal modello già addestrato e, se del caso, già distribuito. In molti casi, tuttavia, tale operazione può incidere in modo significativo sull'architettura e sulle prestazioni del sistema, fino a determinarne una sua inutilizzabilità di fatto, in ragione dei costi tecnici, dei tempi di re-ingegnerizzazione e del rischio di compromettere la funzionalità complessiva del modello⁴⁸.

Il secondo approccio è quello del de-addestramento parziale. Esso si fonda su una cancellazione approssimata che mira a rimuovere i dati personali dal

1, lett. f), GDPR. A seguito delle osservazioni formulate dalle autorità di protezione dei dati, in particolare dalla *Data Protection Commission* irlandese, nonché nel quadro degli orientamenti espressi dall'EDPB in materia di interesse legittimo e misure di mitigazione, Meta ha sospeso l'avvio del trattamento e introdotto un modulo online per l'esercizio del diritto di opposizione ai sensi dell'art. 21 GDPR. Cfr. EDPB, *Urgent Binding Decision 01/2023 requested by the Norwegian SA for the ordering of final measures regarding Meta Platforms Ireland Ltd (Art. 66(2) GDPR)*.

47 La misura in questione è di particolare utilità anche al fine di proteggere il *copyright* delle opere e dei contenuti diffusi, e qualora fossero rilasciati in *open access*, da usi non conformi alla licenza.

48 Cfr. K. HAWKINS, N. ALHUWAISH, S. BELGUTH, A. VRANAKI, A. CHARLESWORTH, *A Decision-Making Process to Implement the 'Right to Be Forgotten' in Machine Learning*, in K. RANNENBERG, P. DROGKARIS, C. LAURADOUX, (eds) *Privacy Technologies and Policy. APF 2023. Lecture Notes in Computer Science*, Springer, Cham, 2024, 20 ss., spec. 30.

modello già distribuito (cd. *deployed model*). La differenza principale rispetto alla cancellazione esatta consiste nel fatto che essa attenua i requisiti di rigore imposti da quest'ultima, al fine di rendere il problema gestibile dal punto di vista computazionale. Le tecniche di *un-learning* non garantiscono la completa eliminazione dei dati personali dell'interessato dal modello, ma abbassano in modo assai significativo la possibilità che i dati personali da cancellare riemergano. L'obiettivo della cancellazione approssimata è dunque quello di avvicinarsi ai parametri del modello che si otterrebbero mediante una cancellazione esatta. La cancellazione approssimata può risultare preferibile nei casi in cui il titolare del trattamento non sia in grado di riaddestrare il modello da zero, o quando le tecniche di cancellazione esatta risultino inapplicabili o eccessivamente onerose sotto il profilo computazionale⁴⁹.

Se il primo approccio rappresenta, in linea di principio, la soluzione maggiormente auspicata dagli interessati e quella che assicura il più elevato grado di effettività del diritto all'oblio nell'era dell'intelligenza artificiale, esso non può essere considerato automaticamente esigibile in ogni circostanza. L'impatto che il riaddestramento completo può avere sulla funzionalità, sulla sostenibilità tecnica ed economica e, in ultima analisi, sulla stessa utilizzabilità del modello impone di valutarne l'applicazione alla luce del principio di proporzionalità e del criterio di ciò che è tecnicamente possibile⁵⁰.

In tale prospettiva, il de-addestramento parziale, pur non garantendo una cancellazione assoluta dei dati personali, si configura come una soluzione pragmaticamente praticabile in molti contesti applicativi, idonea a realizzare un equilibrio ragionevole tra l'esigenza di tutela dei diritti degli interessati e l'interesse allo sviluppo e all'impiego di modelli di intelligenza artificiale funzionali e affidabili⁵¹. Una soluzione certamente di compromesso come peraltro lo è quella che garantisce il diritto alla de-indicizzazione rispetto ai motori di ricerca.

6.3 L'imposizione di filtri nei risultati di *output*

Nei casi in cui le misure di mitigazione non siano sufficienti e non sia praticabile, anche per ragioni economiche o tecniche, la via della cancellazione esatta, oppure qualora persista un rischio elevato di rigurgito di dati personali a seguito di de-addestramento parziale, occorre considerare anche l'opportunità di applicare filtri in fase di *output*.

Questa soluzione, che può richiamare le tecniche di de-indicizzazione con riferimento ai motori di ricerca, opera però su un piano differente: mentre la

49 *Ibidem*, 31.

50 Cfr. T.S. CABRAL, *Forgetful AI: AI and the Right to Erasure under the GDPR*, in *European Data Protection Law Review* (EDPL) n. 3, 2020, 378 ss., il quale mette in luce anche gli effetti negativi (in termini di chilling effect) che richieste di cancellazione possono comportare.

51 Cfr. S. NICOLAZZO, A. SAPIENZA, S. VILELLA, G. RUFFO, *(De-)indicizzazione e diritto all'oblio al tempo dei Large Language Model*, cit.

de-indicizzazione rimuove l'associazione tra un nome e un contenuto nel motore di ricerca, i filtri di *output* sono volti a disinnescare automaticamente le associazioni probabilistiche che porterebbero il modello a rigenerare dati personali di cui si è chiesta la cancellazione. Tali filtri possono avere natura e capacità diversa di garantire l'oblio. Tra di essi si possono richiamare: a) meccanismi di blocco semantico, che individuano e sopprimono dati sensibili o riferimenti personali nelle risposte del modello; b) strumenti di *post-processing* automatizzato, in grado di oscurare o riscrivere *output* problematici; c) sistemi di *watermarking* o etichettatura che segnalano contenuti potenzialmente lesivi e riferibili a persone fisiche.

Pur non incidendo né sui *dataset* di addestramento né sul modello, i filtri possono contribuire a garantire una protezione effettiva e immediata rispetto alla produzione di *output* lesivi del diritto alla cancellazione (oblio).

Non si può negare però che essi presentano alcune complicazioni sia di natura tecnica sia di natura sistemica legate cioè proprio al funzionamento delle associazioni algoritmiche⁵². I filtri, infatti, intervengono sempre a modificare artificialmente l'*output* che sarebbe prodotto sulla base del calcolo probabilistico. In questo modo essi alterano e diminuiscono l'accuratezza del modello⁵³.

Posto che spetterà ai tecnologi e agli informatici compiere un'analisi sulla praticabilità di tali direttrici nonché un'analisi costi/benefici circa l'adozione di tali strumenti, pare di potersi affermare che l'effettività del diritto alla cancellazione dei dati (oblio) nell'era dell'intelligenza artificiale dipenderà, in ultima analisi, dalla combinazione dinamica di soluzioni *ex ante* quali le misure di mitigazione e di soluzioni *ex post* quali il de-addestramento parziale (più che quello totale) e l'inserimento di filtri in *output*.

7. Osservazioni conclusive

L'indagine muoveva da due ipotesi di ricerca: verificare, da un lato, la configurabilità del diritto all'oblio nel contesto dell'intelligenza artificiale e, dall'altro, accertare se l'interazione tra GDPR e IA stia determinando l'emersione di una nuova declinazione del diritto alla cancellazione, analoga – per funzione sistemica – a quella che, sulla scia della sentenza *Google Spain*, ha condotto dalla cancellazione alla de-indicizzazione.

Quanto alla prima ipotesi, l'analisi conferma che il “diritto all'oblio” nel contesto dell'intelligenza artificiale continua a trovare il proprio baricentro normativo nel diritto alla cancellazione ex art. 17 GDPR, ma la sua effettività

52 *Ibidem*.

53 Y. YANG, X. HAN, Y. CHAI, R. EBRAHIMI, R. BEHNIA, B. PADMANABHAN, *From Machine Learning to Machine Unlearning: Complying with GDPR's Right to be Forgotten while Maintaining Business Value of Predictive Models*, 2024, 10.48550/arXiv.2411.17126.

nell'ecosistema dell'IA dipende in misura decisiva dalle condizioni di liceità del trattamento e, dunque, dalla base giuridica concretamente invocata dal titolare. È qui che il diritto alla cancellazione rivela la propria natura “relazionale”: esso non opera come pretesa assoluta, ma come rimedio la cui esigibilità varia in funzione della ragione giuridica che legittima il trattamento e delle eccezioni previste dal par. 3 dell'art. 17. Ne discende che, nel contesto dell'IA, la verifica della base giuridica non è soltanto un passaggio preliminare di *compliance*, bensì il presupposto che determina ampiezza, intensità e persino temporalità della cancellazione.

Proprio sul piano temporale emerge un primo elemento di discontinuità. L'architettura dell'art. 17 e dei considerando 65 e 66 del GDPR appare costruita avendo in mente trattamenti “unitari” e finalità relativamente stabili, risultando perciò tendenzialmente coerente con un'efficacia *ex nunc*. Tuttavia, nei casi in cui il trattamento risulti *ab origine* privo di base giuridica (o viziato da illegittimità originaria, ad esempio per un test di legittimo interesse ineseguito o incongruo), la cancellazione assume una diversa fisionomia: non più soltanto esercizio di un diritto, ma ripristino di una legalità violata, con potenziale proiezione *ex tunc* anche rispetto a dati derivati o inferenziali generati dal trattamento originariamente illecito.

La seconda ipotesi di ricerca – l'emersione di una nuova forma di oblio – trova riscontro nella dinamica che si determina quando la cancellazione incontra i limiti strutturali dei modelli già addestrati. Come la de-indicizzazione ha rappresentato una modalità tecnicamente specifica di attuazione del diritto alla cancellazione (oblio) rispetto ai motori di ricerca, così nel contesto dell'IA si affacciano strumenti funzionalmente analoghi, che non coincidono con la mera rimozione del dato “alla fonte”, ma mirano a neutralizzarne l'effetto nel sistema: de-addestramento e filtri sugli output.

In questo senso, l'oblio nell'IA tende a trasformarsi da cancellazione “documentale” a cancellazione “modellistica”: non riguarda soltanto *dataset* e archivi, ma la permanenza dell'informazione nei parametri e nelle capacità generative del modello. Ne deriva una nozione di cancellazione inevitabilmente graduata. Il de-addestramento “esatto” esprime il massimo grado di effettività, ma pone problemi di esigibilità per costi, impatti sulle prestazioni e sostenibilità anche ambientale⁵⁴; il de-addestramento “approssimato” e i filtri di *output* configurano

54 Il tema della sostenibilità ambientale è centrale nella società digitale che è per sua natura energivora. Questo impone non solo di sviluppare le energie rinnovabili e ricercare nuove fonti di energia, ma pure di considerare l'impronta ambientale delle nuove tecnologie. Su questi argomenti si v. i risultati della Ricerca Astrid coordinata da C. PINELLI su *Le nuove sfide del diritto dell'ambiente dopo la riforma degli artt. 9 e 41 Cost. - I doveri e le responsabilità delle imprese nella doppia transizione*, pubblicati in *Astrid Rassegna*, n. 4, 2024. In particolare si v. i contributi di M. OROFINO, *La tutela dell'ambiente nella costruzione della società digitale europea*; L. DEL CORONA, *Le norme tecniche per l'abbinamento delle due transizioni, digitale e verde*; M. CERIONI, *Norme dell'Unione europea e doppia transizione alla luce della riforma costituzionale n. 1 del 2022 tra compatibilità, difformità*

soluzioni più realistiche, orientate alla proporzionalità e allo “stato dell'arte”, pur introducendo margini di residualità e, nel caso dei filtri, creando il rischio di incidere sull'accuratezza e sulla neutralità degli *output*.

La prospettiva che emerge è quindi quella di un oblio come combinazione dinamica di strumenti: mitigazione *ex ante* (minimizzazione, pseudonimizzazione, *opt-out*) e rimedi *ex post* (de-addestramento/filtri), in un equilibrio che richiama, sul piano funzionale, il compromesso proprio della de-indicizzazione.

In conclusione, la ricerca consente di affermare che il diritto all'oblio non viene meno nell'era dell'intelligenza artificiale, ma muta la propria modalità di attuazione: la cancellazione, per restare effettiva, tende a tradursi in rimedi tecnici che agiscono non solo sui dati, ma sugli effetti del dato nel modello. Si profila così una nuova declinazione del diritto alla cancellazione che, sulla scia della de-indicizzazione, prende ora la forma del de-addestramento e/o dei filtri di *output*, entro i limiti della stretta necessità, della proporzionalità e di ciò che è tecnicamente realizzabile.

Una volta riconosciuta una nuova declinazione del diritto all'oblio nell'era dell'intelligenza artificiale, capace di contribuire alla riaffermazione della centralità della dignità della persona umana anche di fronte alla potenza espansiva della memoria digitale⁵⁵, la sfida futura è quella di definire – anche sul piano regolatorio e tecnico – standard verificabili di effettività, capaci di rendere controllabile il grado di rimozione e di riduzione del rischio residuo, senza precludere in radice gli impieghi dell'IA che producono utilità sociale.

ed intrecci verso nuovi bilanciamenti; G. CAVAGGION, *La sinergia tra transizione ecologica e transizione digitale nel PNRR* e F. PARUZZO, *Il ruolo dell'Agenzia europea per l'ambiente e nei processi decisionali in materia ambientale*.

55 V. per tutti F. BALAGUER CALLEJÓN, *La Costituzione dell'algoritmo*, cit., *passim*.