Nexa Center for Internet & Society
Politecnico di Torino

Il Digital Omnibus tra competitività economica e arretramento delle garanzie fondamentali

Analisi critica delle modifiche al GDPR e al quadro ePrivacy nella Proposta della Commissione europea COM(2025)837 final

Autrice:

Dott.ssa Laura Fabiani

Supervisione scientifica:

Prof. Maurizio Borghi

Prof. Daniele Imbruglia

Giugno 2026

Via Pier Carlo Boggio 65/A, 10129 Torino, Italia

(http://nexa.polito.it/contacts-en)

+39 011 090 7217 (Telephone)

+39 011 090 7216 (Fax)

info@nexa.polito.it

Mailing address:

Nexa Center for Internet & Society

Politecnico di Torino - DAUIN

Corso Duca degli Abruzzi, 24

10129 TORINO

ITALY

The Nexa Center for Internet & Society is a research center affiliated to the Department of Control and Computer Engineering of Politecnico di Torino (http://dauin.polito.it).

© Nexa Center for Internet & Society 2026

Il Digital Omnibus tra competitività economica e arretramento delle garanzie fondamentali*

Sommario

Il contributo esamina criticamente la Proposta *Digital Omnibus* presentata dalla Commissione europea il 19 novembre 2025 (COM(2025) 837 final), al fine di scrutinare se la proposta di riforma in esso contenuta realizzi un effettivo consolidamento e una razionalizzazione dell'*acquis* digitale dell'Unione europea, ovvero se introduca, sotto la veste della semplificazione normativa, dinamiche di deregolamentazione idonee a incidere sull'equilibrio tra competitività economica e tutela dei diritti fondamentali.

L'analisi si concentra sulle principali modifiche proposte al Regolamento (UE) 2016/679 e al quadro ePrivacy, valutandone l'impatto sistemico sulla governance europea dei dati e dell'intelligenza artificiale.

Particolare attenzione è dedicata all'impiego della tecnica legislativa omnibus, esaminata sia in relazione ai precedenti applicativi nell'ordinamento dell'Unione sia alla luce dell'assenza di una valutazione d'impatto adeguata, quale requisito essenziale per la legittimità costituzionale dell'intervento normativo.

Il quesito è se il Digital Omnibus ecceda l'ambito di una revisione meramente tecnica o di coordinamento normativo, configurandosi piuttosto come una riconsiderazione estesa del *digital acquis* eurounitario. In tale prospettiva, l'ampliamento delle deroghe soggettive, l'introduzione di nuove basi giuridiche per il trattamento dei dati personali e la rimodulazione di obblighi centrali in materia di trasparenza, accountability ed enforcement appaiono suscettibili di determinare una riduzione del livello di tutela dei diritti fondamentali, senza che emergano in modo sufficientemente chiaro esigenze di interesse pubblico superiore idonee a giustificare tale compressione.

In conclusione, la promessa di semplificazione normativa rischia, in assenza di adeguati contrappesi, di tradursi in un arretramento delle garanzie che hanno tradizionalmente caratterizzato il modello europeo di regolamentazione digitale.

* Il presente documento ha beneficiato dei commenti e delle osservazioni critiche dei Fellow del Centro Nexa, che si ringraziano per il loro apporto alla stesura finale.

Abstract

This contribution critically examines the Digital Omnibus Proposal presented by the European Commission on 19 November 2025 (COM(2025) 837 final), with a view to assessing whether the reform proposal contained therein achieves an effective consolidation and rationalisation of the European Union's digital *acquis*, or whether, under the guise of regulatory simplification, it introduces deregulatory dynamics capable of affecting the balance between economic competitiveness and the protection of fundamental rights.

The analysis focuses on the main amendments proposed to Regulation (EU) 2016/679 and the ePrivacy framework, assessing their systemic impact on European data and artificial intelligence governance.

Particular attention is devoted to the use of the omnibus legislative technique, examined both in relation to previous applications within the Union legal order and in light of the absence of an adequate impact assessment, as an essential requirement for the constitutional legitimacy of the regulatory intervention.

The question is whether the Digital Omnibus exceeds the scope of a merely technical or coordinating revision, configuring itself rather as an extensive reconsideration of the European digital *acquis*. From this perspective, the expansion of subjective derogations, the introduction of new legal bases for the processing of personal data, and the reshaping of core obligations concerning transparency, accountability and enforcement appear likely to determine a reduction in the level of protection of fundamental rights, without sufficiently clear superior public interest requirements emerging to justify such compression.

In conclusion, the promise of regulatory simplification risks, in the absence of adequate counterbalances, translating into a rollback of the safeguards that have traditionally characterised the European model of digital regulation.

Indice

Sommario 3

Abstract 4

0. Background e perimetro dell'analisi 6

I. Modifiche al GDPR e al quadro ePrivacy 9

1. Osservazioni generali sulle modifiche al GDPR 9

2. La nuova definizione di dato personale 12

3. Ricerca Scientifica 16

4. Un nuovo "interesse legittimo" per lo sviluppo e il funzionamento dell'intelligenza artificiale. 18

5. Diritti di accesso e di informazione 24

6. Processo individuale automatizzato 31

7. Data breach, istituzione del single entry point e DPIA 33

8. Trasposizione delle norme ePrivacy nel GDPR 35

II. Osservazioni conclusive e prospettive 40

0. Background e perimetro dell'analisi

Nel quadro della strategia europea di semplificazione normativa volta a rafforzare la competitività dell'Unione, la Commissione europea ha avviato una pluralità di interventi legislativi raggruppati nel cosiddetto pacchetto Omnibus, inteso quale insieme coordinato di modifiche dirette a incidere sul *corpus* normativo in materia di sostenibilità aziendale, oneri amministrativi per le imprese, competitività e investimenti. Lo scopo dichiarato è indubbiamente ambizioso: una riduzione dei costi amministrativi in capo alle imprese di almeno il 25% e di almeno il 35% per le piccole e medie imprese entro il 2030[1].

La spinta verso una "*simpler and faster Europe*" è il risultato di dinamiche di diversa natura. In particolare, con la Dichiarazione di Budapest sul nuovo patto per la competitività europea del 2024, gli Stati membri hanno espresso l'esigenza di assicurare prosperità economica e di rafforzare la competitività europea, facendo dell'UE il primo continente al mondo a impatto climatico zero e garantendo la sovranità, la sicurezza, la resilienza e l'influenza globale[2].

L'espletarsi di tali esigenze non costituisce, peraltro, un elemento di novità nel dialogo europeo, ma si inserisce in un contesto caratterizzato da impulsi chiaramente individuabili, provenienti, in particolare, dal Rapporto Draghi sulla competitività europea e dal Rapporto Letta sullo stato e le prospettive del mercato unico[3].

---

[1] Consiglio dell'Unione europea (2026), *Semplificazione delle norme UE*, disponibile su: https://www.consilium.europa.eu/it/policies/simplification/.

[2] Consiglio dell'Unione europea (2024), Dichiarazione di Budapest sul nuovo patto per la competitività europea, disponibile su: https://www.consilium.europa.eu/it/press/press-releases/2024/11/08/the-budapest-declaration/.

[3] Il rapporto Letta sostiene che l'eccessiva regolamentazione e la frammentazione del mercato interno in settori strategici (energia, telecomunicazioni, servizi finanziari) incidono negativamente sulla competitività delle imprese europee, proponendo un rafforzamento della dimensione unionale e un maggiore collegamento con l'Unione dei mercati dei capitali per il finanziamento delle transizioni verde e digitale. Il rapporto Draghi, dal canto suo, individua nel rallentamento della produttività la principale causa della debole crescita europea, sottolineando il venir meno di alcuni fattori esterni che avevano sostenuto l'economia dell'Unione, tra cui la disponibilità di energia dalla Russia, e il permanere di un divario di innovazione rispetto a Stati Uniti e Cina, indicando la necessità di intervenire su innovazione, costi energetici e sicurezza economica. E. Letta, *Much more than a market. Speed, security, solidarity,* , 2024 disponibile su: https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf ; M. Draghi, The future of European competitiveness, 2024, disponibile su: https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd.

In questa prospettiva, il *Competitiveness Compass* del gennaio 2025 ha tradotto tali indicazioni in un quadro operativo, delineando una strategia di semplificazione normativa sistematica fondata sul ricorso alla legislazione omnibus[4].

Sebbene la riduzione degli oneri amministrativi rappresenti da tempo una priorità nell'azione della Commissione europea, l'attuale fase segna un cambiamento non marginale nelle modalità di intervento. In particolare, il ricorso alla tecnica legislativa omnibus quale principale strumento di semplificazione evidenzia uno slittamento rispetto alle sue tradizionali funzioni, storicamente deputate a interventi di natura formale, e non già a modifiche sostanziali dell'assetto regolatorio, con possibili implicazioni in termini di riequilibrio o indebolimento delle garanzie esistenti[5].

In altri termini, la Commissione europea qualifica le proposte omnibus come strumenti idonei a modificare *"multiple EU laws at the same time, usually across the same policy area"*, nella prospettiva di assicurare rapidità ed efficienza degli interventi regolatori a sostegno della competitività. Resta tuttavia da interrogarsi sul costo di tale operazione, poiché la concentrazione di modifiche simultanee, se da un lato accelera il processo decisionale, dall'altro riduce gli spazi di scrutinio, come dimostrato dall'assenza di valutazioni d'impatto in riferimento ad alcune delle proposte omnibus[6].

Con l'entrata in vigore della Direttiva (UE) 2026/470, pilastro normativo dell'Omnibus I, si è sedimentata la semplificazione del quadro europeo sulla sostenibilità, intervenendo su Direttive chiave come la *Corporate Sustainability Reporting Directive* (CSRD) e la *Corporate*

[4] Nel *Competitive Compass* si legge: "Over the last two decades, Europe's potential has remained strong, even as other major economies have grown at a faster pace. The EU has everything it takes to unlock its full potential and drive faster, more sustainable growth: we boast a talented and educated workforce, capital, savings, the single market, and a unique social model. To restore our competitiveness and unleash growth, we need to tackle the barriers and weaknesses that are holding us back. In January 2025, the Commission presented the competitiveness compass, a new roadmap to restore Europe's dynamism and boost our economic growth". European Commission, Communication on the Competitiveness Compass for the EU, COM(2025) 60 final, 29 January 2025, disponibile su https://commission.europa.eu/topics/competitiveness/competitiveness-compass_en.

[5] In tal senso, A. Alemanno, *The legality of Omnibus Legislation Under EU Law*, in SSRN, 2025, disponibile su: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5727822.

[6] Ad esempio, in riferimento all'Omnibus I, proposta volta a modificare in modo significativo il quadro europeo della sostenibilità, intervenendo su direttive chiave come la Corporate Sustainability Reporting Directive (CSRD) e la Corporate Sustainability Due Diligence Directive (CSDDD), l'assenza di una valutazione d'impatto si pone in contrasto con la giurisprudenza consolidata della Corte di giustizia dell'Unione Europea, secondo cui tale lacuna può essere giustificata esclusivamente da una "situazione particolare", da interpretare restrittivamente, in presenza di situazioni di emergenza. In tal senso V. C-482/17, C-343/09.

Sustainability Due Diligence Directive (CSDDD)[7]. Questo primo passo si colloca all'interno di un più ampio disegno di razionalizzazione normativa, destinato a proseguire con ulteriori pacchetti Omnibus, tra cui i pacchetti IV e V, attualmente in via di approvazione e relativi, rispettivamente, all'economia digitale e agli investimenti nella tecnologia militare[8].

Nel contesto di questa evoluzione, il presente contributo si concentra specificamente sull'Omnibus VII, comunemente conosciuto come Digital Omnibus, in ragione della sua particolare rilevanza per l'assetto della regolazione europea dei dati e dell'intelligenza artificiale. Infatti, il Digital Omnibus, componendosi di due Proposte, mira a "semplificare" da un lato, il *data acquis* nella sua interezza e, dall'altro, il recente Regolamento (UE) 2024/1689[9]. L'obiettivo dichiarato è quello di un'armonizzazione finalizzata ad eliminare duplicazioni normative e facilitare l'utilizzo di dati personali da parte delle aziende operanti nel settore digitale, anche in relazione all'addestramento di sistemi di intelligenza artificiale.

Il Digital Omnibus si inserisce in una più ampia strategia di semplificazione che comprende iniziative complementari quali il Digital Fitness Check[10]. Quest'ultimo, avviato contestualmente alla presentazione della Proposta Digital Omnibus e accompagnato da una consultazione pubblica estesa, è volto ad analizzare l'impatto cumulativo delle norme digitali

[7] Directive (EU) 2026/470 of the European Parliament and of the Council of 24 February 2026 amending Directives 2006/43/EC, 2013/34/EU, (EU) 2022/2464 and (EU) 2024/1760 as regards certain corporate sustainability reporting requirements and certain corporate sustainability due diligence requirements, disponibile su: https://eur-lex.europa.eu/eli/dir/2026/470/oj.

[8] Proposal for a regulation of the European Parliament and of the council, amending Regulations (EU) 2016/679, (EU) 2016/1036, (EU) 2016/1037, (EU) 2017/1129, (EU) 2023/1542 and (EU) 2024/573 as regards the extension of certain mitigating measures available for small and medium sized enterprises to small mid-cap enterprises and further simplification measures, COM(2025)501 final, disponibile su: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0501R(01); Proposal for a Directive of the European Parliament and the council amending Directives 2009/43/EC and 2009/81/EC, as regards the simplification of intra EU transfers of defence-related products and the simplification of security and defence procurement, COM(2025)823final , disponibile su: https://defence-industry-space.ec.europa.eu/document/download/cd1e5e0f-5c51-47f9-b147.

[9] Di seguito AI Act.

[10] Il Digital Fitness Check è un processo di consultazione e valutazione promosso dalla Commissione Europea. Il suo scopo è analizzare l'intero corpus delle leggi digitali dell'UE (il cosiddetto "*acquis* digitale") per individuare sovrapposizioni, lacune, burocrazia eccessiva o incoerenze e semplificare il quadro normativo a vantaggio di imprese e cittadini. Per un ulteriore approfondimento v. A. KÜSTER - P. ECKHARDT. – H. VÖPEL, "Un commento sul Digital fitness Check dell'UE", disponibile al link: https://www.cep.eu/it/aree-tematiche/details/eu-digital-fitness-check.html

sulla competitività dell'Unione, individuando sovrapposizioni, lacune e possibili ambiti di ulteriore allineamento[11].

La scelta qui operata di delimitare l'analisi al solo Digital Omnibus consente di indagare un ambito in cui le istanze di semplificazione normativa incidono direttamente su settori operanti nel campo dei diritti digitali, nei quali la semplificazione può tradursi in una narrazione rassicurante, dietro cui si manifesta una più profonda rimodulazione e, in taluni casi, un arretramento delle garanzie[12].

In tale contesto, la tutela dei dati personali, quale diritto fondamentale, viene a confrontarsi con esigenze di competitività che, pur centrali nell'azione dell'Unione, non ne condividono il medesimo statuto costituzionale.

I. Modifiche al GDPR e al quadro ePrivacy

1. Osservazioni generali sulle modifiche al GDPR

Gli emendamenti del Digital Omnibus al GDPR sembrano veicolare l'idea che i diritti digitali siano negoziabili in funzione dell'obiettivo di rafforzare la competitività delle imprese europee[13]. In questa prospettiva, si assiste a una compressione dei diritti della persona a fronte

[11] La Commissione ha inoltre delineato un calendario articolato di interventi, prevedendo, già nel breve periodo, la revisione del Digital Markets Act, l'adozione di un programma di politica per il decennio digitale, nonché interventi sul Chips Act, sulla Direttiva SMA. Il programma si presenta particolarmente ambizioso e si estende anche agli anni successivi. Per il 2027, figurano tra gli atti oggetto di valutazione, tra gli altri, il Cyber Solidarity Act, il regolamento sull'internet aperto, la direttiva NIS 2 e il Digital Services Act. Nel 2028 è prevista la valutazione dell'European Media Freedom Act. Act. V. Explanatory Memorandum, Proposal for a Regulation Proposal for a REGULATION 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).

[12] Invero, la Proposta Digital Omnibus sta suscitando il malumore di molti, soprattutto a livello nazionale. Ad esempio, In un rapporto informativo del 13 maggio 2026, la Commissione per gli affari europei del Senato francese ha espresso forti riserve nei confronti del Digital Omnibus, evidenziando il rischio che le misure di semplificazione proposte dalla Commissione europea determinino un indebolimento della tutela dei diritti digitali. In particolare, il rapporto si oppone alla modifica della nozione di dato personale nel GDPR, all'ampliamento delle possibilità di utilizzo di dati sensibili da parte dei sistemi di IA, al trasferimento della disciplina dei cookie dalla direttiva ePrivacy al GDPR e alla centralizzazione delle notifiche di incidenti di cybersicurezza presso ENISA, sottolineando la necessità di preservare l'elevato livello di protezione garantito dall'attuale *acquis* europeo in materia digitale. Il Report è disponibile al sito: https://www.senat.fr/rap/r25-626/r25-6260.html.

[13] Vanno segnalate analisi secondo cui la Commissione Europea avrebbe risentito della narrazione per cui la protezione dei dati costituirebbe un ostacolo alla crescita economica e all'innovazione. Tali istanze verrebbero promosse mediante risorse economiche riferibili alle grandi imprese tech, impegnate in una intensa attività di lobbying dai costi crescenti: la spesa annuale per tali attività sembra essere passata da 113 milioni di euro nel

di un ampliamento degli spazi di utilizzo dei dati personali da parte degli operatori economici, soprattutto nel campo dell'intelligenza artificiale[14].

Lo scopo perseguito dal legislatore è quello di rendere il continente europeo terreno fertile per lo sviluppo nel mercato digitale delle PMI e delle cosiddette Small Mid-Caps (SMCs)[15], anche mediante un ridimensionamento delle garanzie poste a tutela degli interessati.

In questa prospettiva è interessante accennare all'esperienza degli Stati Uniti, attore spesso richiamato come termine di confronto rispetto al presunto eccesso regolatorio europeo, dove, tuttavia, si registra una crescente attenzione critica, da parte dell'opinione pubblica, verso la scarsa regolamentazione del digitale, accompagnata da forze di regolamentazione endogena, sotto il profilo settoriale e statale, che si pongono in forte contrasto con la spinta del Governo federale alla deregolamentazione[16]. Si configura, dunque, un evidente scarto paradigmatico: mentre l'ordinamento europeo sembra muoversi in direzione di un'attenuazione dell'approccio garantista in funzione della competitività, l'esperienza statunitense evidenzia, sia pure in forma frammentata, una tendenza opposta, che rimette in discussione l'assunto secondo cui la deregolamentazione costituisca condizione necessaria per lo sviluppo tecnologico.

Il Digital Omnibus muove dalla constatazione, espressamente formulata dalla Commissione europea, secondo cui l'attuale *data acquis* risulterebbe frammentato e caratterizzato da regole poco coerenti in materia di governance dei dati. Secondo la Commissione, la

---

2023 a 151 milioni di euro, con un incremento del 33,6 per cento in due anni. V. l'analisi del *Corporate Europe Observatory*, Disponibile su: https://corporateeurope.org/en/2026/01/article-article-how-big-tech-shaped-eus-roll-back-digital-rights.

[14] In tal senso, v. M. Borghi, "Verso un'austerity dei diritti digitali (e non solo)", in Forum Disuguaglianze Diversità, disponibile su: https://www.forumdisuguaglianzediversita.org/verso-unausterity-dei-diritti-digitali-e-non-solo/.

[15] Le Small Medium Cap sono imprese a media capitalizzazione che, pur superando I parametri dimensionali delle PMI, non dispongono ancora delle risorse e dell'organizzazione propria delle grandi imprese. Nello specifico hanno un numero di dipendenti compreso tra 250 e 750 con un fatturato annuo non superiore a 150 milioni di euro, oppure un totale di bilancio inferiore a 129 milioni di euro.

[16] Un esempio di questa spinta endogena è l'approccio californiano. Recentemente, il Governatore di Sacramento Gavin Newsom, ha firmato un Executive order senza precedenti che impone alle imprese di intelligenza artificiale che stipulano contratti con lo Stato l'adozione di garanzie in materia di sicurezza e tutela della privacy, v. Executive Order N. 5-26. Ulteriori esempi di attivismo legislativo si segnalano in Connetticut e in Colorado, v. M. Martorana, "California vs Trump: gli Stati Uniti si spaccano sulla governance dell'AI" disponibile su: https://www.agendadigitale.eu/cultura-digitale/california-vs-trump-gli-stati-uniti-si-spaccano-sulla-governance-dellai/-. Lo scontento statunitense si registra anche nell'opinione pubblica, v. The Guardian, "US Student handcuffed after AI System apparently mistook bag of chips for gun", 24 ottobre 2025, disponibile su: https://www.theguardian.com/us-news/2025/oct/24/baltimore-student-ai-gun-detection-system-doritos.

coesistenza di diversi atti normativi, caratterizzati da definizioni sovrapposte, genererebbe incertezze e duplicazioni, la soluzione proposta dalla Commissione per portare *"immediate relief to businesses, public administrations, and citizens alike, to stimulate competitiveness"* è l'emendamento normativo prescelto, con lo scopo di "sbloccare" opportunità nell'uso dei dati, considerati risorsa fondamentale nell'economia europea[17].

Su tale presupposto, la Proposta mira a ricondurre l'intera disciplina dei dati sotto l'unica cornice regolatoria del Data Act, trasformandolo nel perno del mercato unico europeo dei dati. In questa direzione si inseriscono interventi di semplificazione e integrazione: da un lato, l'abrogazione del Regolamento 2018/1807 (*Free flow of non personal data Regulation*), di cui viene tuttavia mantenuto il principio della libera circolazione dei dati non personali integrandolo nel Data Act[18]; dall'altro, per quel che concerne il riutilizzo dei dati nel settore pubblico, l'integrazione degli elementi della Open Data Directive e del Data Governance Act in un nuovo capitolo del Data Act[19].

Quanto all'annoso problema della *consent fatigue*, con il fine di superare l'uso di *banner* di consenso ripetitivi e poco trasparenti, la Proposta consolida le condizioni di liceità per la memorizzazione o l'accesso ai dati personali sulle apparecchiature terminali in uso dalle

[17] È di tutta evidenza come l'impulso normativo dell'UE in materia digitale prenda atto del grande mutamento del mercato negli ultimi anni che ha visto il progressivo affermarsi della cosiddetta data economy. La stima operata dalla Commissione europea nel Digital Decade 2030 riporta come il valore dell'economia dei dati in Europa potrebbe superare i 1.000 miliardi di euro entro il 2030. V. https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade.

[18] La relazione di accompagnamento al Digital Omnibus specifica come questa misura manterrebbe la possibilità per le imprese di collocare i dati non personali nella posizione più efficiente all'interno dell'UE.

[19] Il Capo II del regolamento (UE) 2022/868 (*Data Governance Act*) integra la direttiva (UE) 2019/1024 (*Open Data Directive*) per il riutilizzo dei dati pubblici soggetti a restrizioni, mentre lo stesso regolamento disciplina anche intermediazione dei dati, data altruism e accessi da parte di paesi terzi. Parallelamente, il regolamento (UE) 2023/2854 (*Data Act*) introduce obblighi di condivisione dei dati e regole sui contratti.

Il *Digital Omnibus* interviene su questo quadro proponendo, da un lato, l'abrogazione del regolamento (UE) 2018/1807 sulla libera circolazione dei dati non personali, mantenendone il divieto di localizzazione, e, dall'altro, una riorganizzazione del Data Governance Act. Le norme sul riutilizzo dei dati pubblici vengono accorpate con quelle della Open Data Directive all'interno del Data Act, configurando un unico regime.

La proposta prevede inoltre la possibilità di introdurre condizioni differenziate per il riutilizzo da parte di grandi imprese e *gatekeeper,* con l'obiettivo di incidere sugli effetti della loro posizione di mercato.

Nel complesso, l'intervento mira a concentrare discipline eterogenee nel Data Act, attraverso abrogazioni e riallineamenti normativi, nel tentativo di ridurre la frammentazione del quadro giuridico europeo dei dati.

persone fisiche tramite la trasposizione del *corpus* della Direttiva ePrivacy in un nuovo art. 88-bis del GDPR[20].

Tuttavia, le modifiche più rilevanti e controverse nel dibattito attuale, riguardano il *General Data Protection Regulation* (GDPR). Il Digital Omnibus toccherà diverse definizioni del GDPR, incidendo sulla loro portata e interpretazione. Da tali modifiche emergono potenziali contrasti con la Carta dei diritti fondamentali dell'UE, incoerenze sistematiche, rischi di compressione dei diritti degli interessati e un potenziale scostamento dalla logica attuale del GDPR e dalla giurisprudenza della Corte di giustizia dell'Unione europea. Si può dubitare che l'obiettivo dichiarato di una maggiore chiarezza del diritto risulti, in definitiva, disatteso: anziché ridurre l'incertezza interpretativa, la Proposta introduce definizioni opache e concettualmente indeterminate, che ampliano i margini di discrezionalità applicativa e compromettono la prevedibilità della disciplina.

2. La nuova definizione di dato personale

Una prima rilevante modifica riguarda la definizione di dato personale. Nell'ordinamento vigente, tale nozione è formulata in termini ampi e comprende «qualsiasi informazione riguardante una persona fisica identificata o identificabile»; si considera identificabile la persona fisica che può essere individuata, direttamente o indirettamente, con particolare riferimento a un identificativo, quale il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online, oppure a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale[21]. Si tratta di una nozione centrale che delimita l'ambito di applicazione dell'intero sistema di protezione dei dati personali e si inserisce nel quadro delineato dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea e dall'art. 16 TFUE.

[20] In riferimento al nuovo art. 88c, lo European data protection board (EDPB) e il Garante europeo per la protezione dei dati (GEPD) si sono espressi favorevolmente affermando: "L'EDPB e il GEPD sostengono fermamente l'obiettivo di fornire una soluzione normativa per affrontare l'affaticamento del consenso e la proliferazione dei banner sui cookie. Ciò riguarda, ad esempio, i requisiti proposti sull'uso di indicazioni automatizzate e leggibili meccanicamente delle scelte delle persone in merito al trattamento dei loro dati. L'uso di mezzi tecnici può semplificare la conformità da parte dei titolari del trattamento e aiutare le persone a rendere efficaci le loro scelte online". V. https://www.edpb.europa.eu/news/news/2026/digital-omnibus-edpb-and-edps-support-simplification-and-competitiveness-while_it.

[21] Art. 4, Regolamento (UE) 2016/679.

Il Digital Omnibus interviene sul punto in modo tutt'altro che neutro. L'art. 3 stabilisce infatti che un'informazione non sia qualificabile come dato personale con riferimento a una determinata entità qualora questa non disponga dei mezzi "ragionevolmente utilizzabili" per identificare l'interessato.[22] Si assiste così a un'inversione dell'approccio precauzionale che ha caratterizzato fino ad ora l'art. 4 del GDPR[23]: la qualificazione di dato personale non dipende più dalla sua identificabilità in termini oggettivi e potenziali, ma da valutazioni legate alla capacità tecnica e alle scelte del titolare del trattamento o del terzo destinatario dei dati[24]. La disposizione si presenta come il risultato del processo di codificazione di alcuni sviluppi giurisprudenziali in materia di pseudonimizzazione. In particolare, si richiama l'orientamento secondo cui un dato pseudonimizzato non è, di per sé, anonimo, ma può non essere qualificato come dato personale per il destinatario che non disponga delle informazioni aggiuntive necessarie alla reidentificazione[25].

Tuttavia, il riferimento a tale giurisprudenza appare parziale. Nella pronuncia richiamata, infatti, la Corte si limita a escludere la qualificazione di dato personale in capo a un soggetto privo di mezzi effettivi di identificazione, senza mettere in discussione il carattere oggettivo della nozione né il suo fondamento unitario. La Proposta normativa, al contrario, assume questo elemento come criterio generale, trasformando un'eccezione legata a circostanze specifiche in regola, senza considerare peraltro che l'arbitrarietà nella perimetrazione della

[22] Art. 3, COM(2025)837final. L'articolo recita: «le informazioni relative a una persona fisica non sono necessariamente dati personali per qualsiasi altra persona o entità per il solo fatto che un'altra entità può identificare tale persona fisica. Le informazioni non sono personali per una determinata entità se quest'ultima non è in grado di identificare la persona fisica cui si riferiscono le informazioni, tenendo conto dei mezzi di cui tale entità si può ragionevolmente avvalere. Tali informazioni non diventano personali per tale entità per il solo fatto che un potenziale destinatario successivo dispone di mezzi di cui si può ragionevolmente avvalere per identificare la persona fisica cui le informazioni si riferiscono».

[23] L'ampiezza della attuale definizione è motivata dal fatto che gli odierni strumenti di analisi dei dati, sempre più sofisticati, rendono possibile risalire all'identità di un individuo anche a parte da informazioni che appaiono, di primo acchitto, anonime o distanti dalla sua sfera personale.

[24] D'altro canto, c'è chi accoglie favorevolmente la razionalizzazione della definizione di dato personale, ritenendo che questa possa favorire l'innovazione, in particolare nei processi di addestramento dei sistemi di IA. La modifica è inoltre considerata funzionale a un'ampia adozione delle c.d. Privacy Enhancing technologies (PETs) quali la pseudonimizzazione, in quanto strumenti idonei a sostenere la privacy by design e a promuovere la fiducia nella condivisione delle informazioni. V. FEDMA, Position paper-Digital & AI Omnibus proposal. Per un maggior approfondimento sulla nozione di PETs v. «Cosa sono le PETs (Privacy Technologies) per la privacy?», 2023, disponibile al sito: https://focus.namirial.com/it/privacy/

[25] C-413/23, Sentenza Deloitte. La Corte di giustizia ha rilevato che il dato pseudonomizzato è per definizione non anonimo ma non può essere considerato un dato personale nell'eventualità in cui il terzo destinatario delle informazioni non sia in possesso degli ulteriori mezzi o strumenti per poter individuare la persona fisica.

nozione di dato personale sarà acuita dalla possibilità riconosciuta alla Commissione europea di rivedere tale definizione attraverso l'adozione di atti di esecuzione[26].

Il risultato che ne deriva è una codificazione selettiva e decontestualizzata che non tiene conto della traiettoria complessiva delle pronunce degli ultimi anni, espressive di un orientamento interpretativo unitario, che ha visto la Corte di giustizia valorizzare una nozione ampia e funzionale di dato personale nella prospettiva di una tutela profonda e capillare[27].

Quanto alla capacità dell'operatore di identificare l'interessato mediante "mezzi ragionevolmente utilizzabili", il problema si sposta sul parametro minimo di identificabilità. Il Considerando 26 del GDPR, infatti, nel ricomprendere anche i dati pseudonimizzati e nel valorizzare il fenomeno del *singling out*, assume come rilevante non già l'identificazione in senso nominale, ma anche la mera possibilità di isolare dati relativi all'individuo all'interno di un insieme di dati, vale a dire, distinguerlo come unità unica rispetto agli altri, anche in assenza di elementi identificativi diretti[28]. È su questo piano che la nuova formulazione dell'art. 4 mostra le sue ambiguità: non è chiaro se i "mezzi ragionevolmente utilizzabili" includano anche quelli che consentano tale isolamento.

Ancora, le controversie sulla qualificazione dei ruoli di titolare, contitolare o responsabile costituiscono già una fonte ricorrente di conflitti nei rapporti B2B. La modifica proposta è destinata ad accentuare tali criticità, poiché ciascuna parte sarebbe chiamata a valutare in via autonoma e soggettiva l'applicabilità del GDPR al proprio trattamento. Ne possono derivare

[26] Art. 41bis COM(2025)837final.

[27] C-582/14 (Breyer), secondo cui gli indirizzi IP dinamici possono costituire dati personali qualora esista un mezzo legale per ottenere informazioni aggiuntive; è irrilevante che tale mezzo sia effettivamente utilizzando, essendo sufficiente la mera possibilità; C-434/16 (Nowak), che afferma che un dato è personale anche in assenza di nome o identificativo per il soggetto che lo esamina, qualora il trattamento produca comunque effetti su una persona; C-21/23 (Lindenapotheke) dove la CGUE ha sostenuto che esiste un nesso tra il prodotto medicinale, le sue indicazioni terapeutiche o i suoi usi, e una persona identificata o identificabile attraverso i dati forniti. C-683/21 (Nacionalinis visuomenės svikatos centras) dove viene affermato che informazioni attribuibili a una persona fisica mediante l'uso di dati devono essere considerate riferite a una persona identificabile, senza che rilevino l'intenzione soggettiva o la probabilità di utilizzo di tali mezzi; C-579/21 (Pankki), chiarisce come l'espressione "qualsiasi informazione" nella definizione di dato personale debba essere interpretata in senso ampio, riflettendo la volontà del legislatore di attribuire a tale nozione una portata estesa. In sostanza, la giurisprudenza della Corte di giustizia si orienta in senso opposto rispetto alle modifiche prospettate dalla Commissione.

[28] In riferimento alla nozione di *singling out*, il Working Group Article 29, Opinion *on the concept of Personal data*, sviluppa il significato di "identificabile, direttamente o indirettamente". Una persona è identificata "all'interno di un gruppo di persone quando essa è distinta da tutti gli altri membri del gruppo". Un modo per distinguere una persona da un gruppo è quello di specificare "criteri che permettono di riconoscerla restringendo il gruppo cui appartiene". Se il gruppo viene ristretto a un individuo, quell'individuo è stato oggetto di *singling out*.

situazioni in cui operatori coinvolti nel medesimo flusso di dati giungano a conclusioni opposte.

Questa impostazione determina una dispersione delle responsabilità. Soggetti privi di capacità tecniche di reidentificazione potrebbero sostenere che i dati pseudonimizzati esulino dall'ambito di applicazione del GDPR, oppure organizzare i trattamenti in modo da sottrarsi ai relativi obblighi.

Ne deriva un indebolimento dei diritti degli interessati: se il GDPR non si applica, non trovano applicazione né i diritti riconosciuti dal regolamento, né il principio di limitazione delle finalità[29].

Da ultimo, il considerando 41 della Proposta sembra estendere, in via implicita, le modifiche apportate al GDPR anche alla *Law Enforcement Directive* (LED). Ne deriverebbe l'applicazione della nozione ristretta di dato personale anche alle attività delle autorità di polizia e, più in generale, agli organismi del sistema di giustizia, con possibili ulteriori ricadute sul piano delle garanzie[30].

In conclusione, è opportuno interrogarsi sulla reale necessità di una modifica del GDPR che definisca il dato personale in negativo, indicando ciò che dato non è, anziché ciò che lo è. Le esigenze interpretative e di chiarimento avrebbero potuto essere affrontate con strumenti diversi, senza incidere su un elemento così centrale dell'impianto normativo a tutela dei dati personali[31]

---

[29] Un esempio eclatante riguarda l'applicazione dell'art. 15 GDPR in tema di accesso. In questo caso si assiste ad un cortocircuito logico: qualsiasi controversia circa la qualificazione di un'informazione come "dato personale" finirebbe per escludere l'esercizio del diritto di accesso, determinando un evidente cortocircuito applicativo: senza accesso non è possibile contestare la qualificazione del dato, ma proprio tale qualificazione impedisce l'accesso.

[30] In tal senso, EDRI in *Why the Digital Omnibus puts GDPR and ePrivacy at Risk,* afferma: "La portata della modifica appare ancora più significativa alla luce del contesto attuale, caratterizzato da un progressivo ampliamento dei poteri delle autorità di contrasto e da un uso crescente di strumenti tecnologici avanzati, inclusi sistemi basati su dati biometrici e tecniche di analisi automatizzata. In tale scenario, l'estensione delle modifiche introdotte dall'Omnibus finisce per incidere su ambiti in cui le conseguenze del trattamento dei dati personali sono più rilevanti, determinando un ridimensionamento delle garanzie in settori particolarmente sensibili".

[31] A tal riguardo, EDPB-EPBS, *joint opinion On the Proposal for a Regulation as regards the simplification on the legislative framework,* 2026. Il contributo recita: "l'EDPB e l'EDPS ricordano che l'EDPB sta predisponendo orientamenti aggiornati sulla pseudonimizzazione a seguito di una consultazione pubblica e sta elaborando nuove linee guida sull'anonimizzazione, che terranno conto, tra l'altro, della sentenza EDPS c. SRB. Tale consultazione ha evidenziato che questa nuova pronuncia solleva numerose questioni pratiche e giuridiche, anche alla luce dell'intero corpus giurisprudenziale della CGUE. L'EDPB e l'EDPS ritengono che tali questioni siano più opportunamente affrontate mediante ulteriori orientamenti dell'EDPB, che supportino le organizzazioni

3. Ricerca Scientifica

Il GDPR è cosparso di riferimenti alla "ricerca scientifica"[32]. Nel testo vigente, tuttavia, tale nozione non è definita a livello normativo, ma è richiamata nel considerando 159, che ne offre una definizione di natura non vincolante, secondo cui le finalità di ricerca scientifica devono essere interpretate in senso ampio, includendo, ad esempio, *"technological development and demonstration, fundamental research, applied research and privately funded research"*[33].

La Commissione propone di introdurre nel GDPR una nuova definizione, estremamente opaca, destinata a incidere su tutte le disposizioni che richiamano la ricerca scientifica, le quali, nella maggior parte dei casi, comportano deroghe o attenuazioni rispetto ai diritti e agli obblighi previsti dal Regolamento. L'art. 3 della Proposta positivizza la nozione di ricerca scientifica in un nuovo punto 38 all'art. 4 definendola come: «qualsiasi tipo di ricerca che possa anche favorire l'innovazione, come lo sviluppo tecnologico e la dimostrazione. Le azioni condotte nel quadro di tale ricerca contribuiscono al miglioramento delle conoscenze scientifiche esistenti o applicano tali conoscenze in modi nuovi, hanno l'obiettivo di contribuire ad accrescere le conoscenze e il benessere generali della società e rispettano le norme etiche nel settore di ricerca pertinente. Ciò non esclude che la ricerca possa anche mirare a promuovere un interesse commerciale».

---

nella prassi applicativa e tengano conto dell'intera giurisprudenza, piuttosto che attraverso una modifica della definizione stessa. Le linee guida dell'EDPB offriranno inoltre chiarimenti sulle implicazioni della sentenza EDPS c. SRB per altre disposizioni del GDPR, inclusi gli articoli 26 e 28 e il capo V. (Digital Omnibus)

[32] Artt. 5, par. 1, lett. b) ed e), 9, par. 2, lett. j), 14, par. 5, lett. b), 17, par. 3, lett. d), 21, par. 6 e 89.

[33] Considerando 159, Regolamento (UE) 2016/679. «Qualora i dati personali siano trattati per finalità di ricerca scientifica, il presente regolamento dovrebbe applicarsi anche a tale trattamento.

Nell'ambito del presente regolamento, il trattamento di dati personali per finalità di ricerca scientifica dovrebbe essere interpretato in senso lato e includere ad esempio sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati, oltre a tenere conto dell'obiettivo dell'Unione di istituire uno spazio europeo della ricerca ai sensi dell'articolo 179, paragrafo 1, TFUE.

Le finalità di ricerca scientifica dovrebbero altresì includere gli studi svolti nell'interesse pubblico nel settore della sanità pubblica.

Per rispondere alle specificità del trattamento dei dati personali per finalità di ricerca scientifica dovrebbero applicarsi condizioni specifiche, in particolare per quanto riguarda la pubblicazione o la diffusione in altra forma di dati personali nel contesto delle finalità di ricerca scientifica.

Se il risultato della ricerca scientifica, in particolare nel contesto sanitario, costituisse motivo per ulteriori misure nell'interesse dell'interessato, le norme generali del presente regolamento dovrebbero applicarsi in vista di tali misure».

Il riferimento a "qualsiasi ricerca" che "possa anche" favorire l'innovazione amplia sensibilmente l'ambito applicativo, includendo anche attività che solo in via potenziale o indiretta possono avere ricadute innovative[34].

Alcuni ritengono che l'introduzione di una definizione espressa e operativa consenta di attribuire rilievo normativo a quanto già affermato dal Considerando 159, in particolare nella parte in cui ricomprende la ricerca scientifica tanto nelle attività svolte nel settore pubblico quanto in quelle condotte in contesti privati. La positivizzazione della nozione contribuirebbe a rafforzare la certezza giuridica, soprattutto nei settori della ricerca sanitaria e industriale, nei quali non sono mancate interpretazioni restrittive circa la possibilità di utilizzare i dati personali al di fuori di contesti strettamente pubblici e accademici.[35] Altri ritengono, viceversa, che la nuova definizione, riferendosi allo sviluppo tecnologico, presenti uno sbilanciamento verso ambiti tecnico-industriali, subordinando funzionalmente la ricerca scientifica all'innovazione, a detrimento di altri settori quali le scienze umane o naturali, con il rischio di escludere attività accademiche con finalità diverse[36].

D'altro canto, molte delle deroghe previste dalla Proposta per la ricerca scientifica incidono direttamente su diritti garantiti dalla Carta di Nizza e, in quanto tali, dovrebbero essere sottoposte al vaglio di necessità e proporzionalità di cui all'art. 52, par.1. Infatti, se è pacifico che la ricerca scientifica, quale espressione della libertà garantita dall'art. 13 della Carta, possa costituire un interesse pubblico idoneo a giustificare la limitazione di altri diritti fondamentali, è altrettanto pacifico che un'autorizzazione generalizzata al trattamento

[34] Se è pacifico che la ricerca scientifica, quale espressione della libertà garantita dall'art. 13 della Carta, possa costituire un interesse pubblico idoneo a giustificare limitazioni di altri diritti fondamentali, una autorizzazione generalizzata al trattamento ulteriore fondata su una nozione ampia e indeterminata di "ricerca" rischia di porsi in contrasto con la Carta, tanto più in assenza di una adeguata valutazione d'impatto da parte della Commissione. Giova ricordare che l'EDPS definisce la ricerca scientifica come: *'scientific method' of observing phenomena, formulating and testing a hypothesis for those phenomena, and concluding as to the validity of the hypothesis*", v. EDPS, A Preliminary Opinion on data protection and scientific research, 2020. Parimenti restrittiva la definizione fornita dall'EDPB nel 2020: "*the notion may not be stretched beyond its common meaning and understands that 'scientific research' in this context means a research project set up in accordance with relevant sector-related methodological and ethical standards, in conformity with good practice*", v. EDPB, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, 2020.

[35] V. Digital Europe, *Digital ombinibus: a first step and what must come next,* 2026.

[36] In tal senso, v. NOYB, Digital Omnibus: Analysis of Selected GDPR and ePrivacy Propoals by the European Commission.

ulteriore, fondata su una nozione ampia e indeterminata di ricerca, rischia di porsi in contrasto con principi espressi dall'art. 5 GDPR (limitazione delle finalità e minimizzazione dei dati).

Successivamente alla presentazione della Proposta, l'EDPB ha adottato le *Guidelines 1/2026 on processing of personal data for scientific research purposes* (15 aprile 2026)[37], con l'obiettivo di fornire maggiore certezza interpretativa sul trattamento dei dati personali a fini di ricerca scientifica, garantendo al contempo il rispetto dei diritti fondamentali degli interessati. In luogo di una definizione normativa generale della nozione di "ricerca scientifica", il Comitato individua sei criteri sostanziali, tra cui il carattere metodico e sistematico dell'attività, il rispetto degli standard etici, la verificabilità dei risultati e la finalità di accrescimento della conoscenza, utili a qualificare, caso per caso, un'attività come ricerca scientifica ai sensi del GDPR. Le Linee guida chiariscono, inoltre, che la presunzione di compatibilità del trattamento ulteriore per finalità di ricerca ex art. 5, par. 1, lett. b), GDPR non esonera dall'individuazione di un'autonoma base giuridica e riconoscono l'ammissibilità del *broad consent* e del *dynamic consent*, purché accompagnati da adeguate garanzie di trasparenza, governance e tutela degli interessati. L'impostazione adottata dall'EDPB si distingue da quella perseguita nella proposta originaria di modifica del GDPR contenuta nel Digital Omnibus: mentre quest'ultima mirava a positivizzare una nozione ampia di ricerca scientifica, idonea ad estendere il regime derogatorio previsto dal Regolamento anche ad attività orientate all'innovazione tecnologica e agli interessi commerciali, le Guidelines privilegiano un approccio funzionale e sostanziale, volto a circoscrivere l'applicazione delle deroghe attraverso criteri qualitativi e garanzie procedurali piuttosto che mediante una definizione legislativa di carattere generale.

4. Un nuovo "interesse legittimo" per lo sviluppo e il funzionamento dell'intelligenza artificiale.

Il Digital Omnibus introduce alcune modifiche finalizzate ad agevolare il trattamento dei dati personali nel contesto del ciclo di vita dei sistemi di intelligenza artificiale.

Come noto, lo sviluppo dell'IA ha da sempre sollevato rilevanti criticità in termini di compatibilità con il quadro normativo europeo in materia di protezione dei dati personali.

[37] Disponibili al sito: https://www.edpb.europa.eu/public-consultations/guidelines-12026-on-processing-of-personal-data-for-scientific-research_en

Difatti, l'impostazione "*human-centric*", alla base del GDPR, mal si concilia con quella "business-centric" e con la logica del trattamento massivo di dati personali[38].

Tale tensione emerge in maniera particolarmente evidente con riferimento all'individuazione, nell'art. 6, par. 1, GDPR, della base giuridica idonea a legittimare il trattamento dei dati personali[39]. Gran parte dei sistemi di IA, specie quelli generativi, si alimenta mediante l'elaborazione di ingenti quantità di dati reperiti online, circostanza che rende necessario individuare la base giuridica maggiormente idonea rispetto alle concrete modalità di trattamento. Nella prassi, gli operatori tendono frequentemente a fare affidamento sul legittimo interesse del titolare ai sensi dell'art. 6, par.1, lett. f), GDPR, ritenendolo la base giuridica più coerente con le caratteristiche proprie delle attività di sviluppo e addestramento dei modelli di IA.

Come noto, tale disposizione richiede il soddisfacimento di tre condizioni cumulative: anzitutto, il perseguimento di un *interesse legittimo* del titolare del trattamento o del terzo cui i dati sono comunicati; in secondo luogo, la *necessità* del trattamento rispetto al perseguimento di tale interesse, nel senso che il medesimo risultato non potrebbe essere conseguito mediante strumenti meno invasivi per i diritti degli interessati; infine, ai fini del ricorso alla norma, i diritti e libertà degli interessati devono resistere al *balancing test* con l'interesse legittimo perseguito dal titolare o da terzi[40]. Tuttavia, proprio l'operazione di

[38] Sul punto, T. Z. ZARSKY*, Incompatible: The GDPR in The Age of Big Data,* in Seton Hall Law Review, 2017, p. 995 ss., il quale evidenzia come i principi cardine del GDPR, in particolare quelli di minimizzazione, limitazione delle finalità e consenso informato, risultino strutturalmente difficili da conciliare con il funzionamento dei sistemi di IA, fondati sull'elaborazione massiva di dati e sul riutilizzo degli stessi per finalità ulteriori rispetto a quelle originariamente dichiarate. In senso analogo, G. MOBILIO, *L'intelligenza artificiale e le regole giuridiche alla prova: il caso paradigmatico del GDPR*, in federalismi.it, n. 16/2020, p. 266 ss., spec. p. 282, sottolinea come il modello "human-centric" del GDPR si confronti con logiche economiche e tecnologiche tipicamente "data-driven" e orientate allo sfruttamento intensivo delle informazioni personali.

[39] Sul progressivo ridimensionamento del consenso quale presidio sostanziale di controllo sui dati personali nell'ecosistema digitale e sulla possibile valorizzazione del legittimo interesse quale base giuridica per l'addestramento dei sistemi di IA generativa, v. O. POLLICINO, Generative AI and the rediscovery of the legitimate interest clause, in IEP@BU, 24 gennaio 2024. Il contributo, richiama, in particolare, la vicenda ChatGPT/OpenAI in Italia del 2023, osservando come il Garante Privacy abbia contestato l'assenza di un'idonea base giuridica per il trattamento dei dati utilizzati nell'addestramento del modello, prospettando il ricorso al legittimo interesse ex art. 6, par. 1, lett. f), GDPR quale possibile soluzione compatibile con il principio di accountability.

[40] In tal senso, CGUE C-597/1, la Corte afferma al punto 106: "Pertanto, la suddetta disposizione prevede tre condizioni cumulative affinché un trattamento di dati personali sia lecito, vale a dire, in primo luogo, il perseguimento del legittimo interesse del titolare del trattamento o di terzi, in secondo luogo, la necessità del trattamento dei dati personali per il perseguimento del legittimo interesse e, in terzo luogo, la condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato dalla tutela dei dati (v., in tal senso, per

bilanciamento, implicando una valutazione necessariamente ancorata alle circostanze concrete del caso, risulta difficilmente replicabile nel contesto dei sistemi di IA generativa e, più in generale, delle tecnologie ad alta intensità di dati, caratterizzate da trattamenti massivi, continui e spesso non pienamente prevedibili *ex ante*[41].

Per arginare l'ostacolo, il Digital Omnibus introduce il nuovo art. 88-quater, prevedendo che, ove necessario per lo sviluppo e il funzionamento dei sistemi di IA, il trattamento dei dati personali possa fondarsi sul legittimo interesse del titolare, a condizione che siano rispettati il principio di minimizzazione dei dati e il diritto di opposizione riconosciuto dall'art. 21 GDPR. Questa disposizione rappresenta uno dei profili più controversi dell'intera iniziativa Digital Omnibus, nella misura in cui sembra sottendere una riconfigurazione del paradigma europeo di protezione dei dati personali, progressivamente orientato a contemperare e, per taluni aspetti, subordinare, le garanzie individuali alle esigenze di sviluppo dell'ecosistema europeo dell'intelligenza artificiale.

La proposta si colloca nel solco dell'elaborazione interpretativa sviluppata dall'EDPB nel Parere 28/2024, nel quale il Comitato ha affrontato il tema del trattamento dei dati personali nell'ambito dello sviluppo e dell'addestramento dei modelli di IA[42]. In tale sede, l'EDPB ha ritenuto che il legittimo interesse possa costituire una base giuridica idonea ai sensi dell'art. 6, par.1, lett. f), GDPR, purché il trattamento sia accompagnato da un'adeguata valutazione degli interessi convolti, tenga conto delle ragionevoli aspettative degli interessati e sia assistito da appropriate garanzie tecniche e organizzative [43]. Il Digital Omnibus recepisce e positivizza tale impostazione, trasformando criteri sino ad oggi elaborati nell'ambito della soft law in una disciplina espressamente prevista dal GDPR.

---

quanto riguarda l'articolo 7, lettera f), della direttiva 95/46, sentenza del 4 maggio 2017, Rīgas satiksme, C-13/16, EU:C:2017:336, punto 28)".

[41] Per un approfondimento sulle tre fasi della valutazione dell'interesse legittimo nel contesto dello sviluppo e della diffusione dei modelli di IA v. EDPB Opinion (article 64), p. 22, disponibile su: https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202428_ai-models_it_0.pdf.

[42] Ivi, p. 20

[43] Ivi, Il parere fa riferimento all'adozione di "misure di attenuazione" per limitare l'impatto del trattamento sull'interessato. L'elenco delle misure non è esaustivo né prescrittivo ma ricomprende: Le misure tecniche, (quelle di cui alla sezione 3.2.2.), le misure di pseudonimizzazione, le misure per mascherare i dati personali o sostituirli; le misure che facilitano l'esercizio dei diritti individuali; misure di trasparenza, misure di attenuazione nel contesto del web scraping. V. p. 30 e ss.

Nel settore dell'intelligenza artificiale la Commissione compie, tuttavia, un ulteriore passaggio. Se il Parere 28/2024 si limitava infatti a delineare i presupposti interpretativi entro i quali il legittimo interesse poteva essere invocato quale base giuridica del trattamento, il Digital Omnibus ne recepisce l'impostazione, attribuendole valore normativo mediante l'introduzione di una specifica previsione legislativa riferita allo sviluppo e al funzionamento dei sistemi di IA. La differenza non riguarda, pertanto, il contenuto sostanziale della soluzione prospettata, quanto il passaggio da un criterio interpretativo di soft law a una regola di diritto positivo destinata a incidere direttamente sulla strategia di compliance degli operatori.

Il nuovo art 88-quater deve essere esaminato congiuntamente alla proposta di modifica dell'art. 9 GDPR, concernente il trattamento di categorie particolari di dati personali. Nella sua formulazione vigente, l'articolo stabilisce un divieto generale di trattamento, la cui portata applicativa si estende anche alle informazioni idonee a rivelare, anche indirettamente, dati sensibili dell'interessato, salvo le deroghe tassativamente previste al par. 2[44]. Il Digital Omnibus interviene proprio sul piano delle deroghe, attraverso l'introduzione di due nuove eccezioni al divieto generale di trattamento delle categorie particolari di dati personali, mediante l'introduzione delle lettere k) e l) al paragrafo 2. Nello specifico, la lettera k) consentirebbe, in via eccezionale, il trattamento di dati sensibili nel contesto dello sviluppo e del funzionamento di sistemi di intelligenza artificiale, mentre la lettera l) introdurrebbe una specifica esenzione per il trattamento di dati biometrici, purché la verifica avvenga sotto il controllo esclusivo dell'interessato.

Ulteriore elemento di rilievo è rappresentato dall'introduzione del par. 5. La disposizione delinea una forma di "tutela" articolata su tre livelli prevedendo che il titolare del trattamento sia tenuto a svolgere azioni gradate volte a prevenire l'ulteriore trattamento di categorie

[44] Sul punto, la Sentenza CGUE, C-252/21 afferma: « 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 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».

particolari di dati personali. In primo luogo, il titolare sarebbe tenuto ad adottare misure tecniche e organizzative al fine di evitare la raccolta e il trattamento di categorie particolari di dati; in secondo luogo, qualora il titolare "identifichi" dati personali sensibili nei dataset utilizzati per l'addestramento, la verifica e la validazione dei sistemi di IA, sarà tenuto alla loro rimozione; infine, laddove tale rimozione richieda uno sforzo sproporzionato, il titolare del trattamento dovrebbe, in ogni caso, proteggere efficacemente tali dati senza indebito ritardo affinché non siano utilizzati per produrre output, né divulgati o altrimenti messi a disposizione di terzi.

Sussistono anche in questo caso rilevanti interrogativi circa la compatibilità della Proposta con l'impianto garantistico del GDPR. In primo luogo, si introduce un regime eccezionale che consente il trattamento di dati protetti proprio in un ambito, quello dell'intelligenza artificiale, tradizionalmente caratterizzato da rischi elevati, senza che sia fornita un'adeguata valutazione di proporzionalità ai sensi dell'art. 52, par. 1, della Carta[45]. La giustificazione offerta si limita a richiamare, in modo generico, l'esigenza di non ostacolare lo sviluppo e il funzionamento dei sistemi di IA, adottando una prospettiva centrata sull'operatore economico piuttosto che sulla tutela dell'interessato[46].

In secondo luogo, le condizioni poste dal nuovo paragrafo 5 risultano caratterizzate da un elevato grado di indeterminatezza: espressioni quali "misure adeguate", "evitare", "sforzo sproporzionato" o "protezione efficace" non sono definite e rischiano di ampliare in modo significativo il margine di discrezionalità dei titolari del trattamento, compromettendo la certezza del diritto.

A ciò si aggiungono criticità di ordine tecnico, legate al funzionamento stesso dei sistemi di IA. In particolare, nonostante l'adozione delle misure che il titolare è obbligato a adottare ai sensi della norma, non è sempre possibile prevenire il fenomeno della cosiddetta *data regurgitation*, ossia la riproduzione nei risultati di dati utilizzati in fase di addestramento, con il conseguente rischio che informazioni sensibili riemergano negli output di sistema. Ne deriva che l'effettiva attuazione delle garanzie previste appare difficilmente realizzabile nella pratica. Peraltro,

[45] Qualsiasi limitazione dei diritti di cui all'art. 8 della Carta di Nizza deve essere "proporzionato" ai sensi dell'art. 52. Questa nuova base giuridica costituisce una limitazione della protezione dei dati personali e, pertanto, dovrebbe essere accompagnata da una valutazione di proporzionalità che, tuttavia, non è stata effettuata.

[46] V. considerando 33, COM(2025) 837final.

l'introduzione della clausola dello "sforzo sproporzionato" rischia di svuotare di contenuto l'obbligo di rimozione dei dati, come già avvenuto in altre disposizioni del GDPR, nelle quali tale formula è stata frequentemente invocata dai titolari per sottrarsi agli obblighi di trattamento.

Sotto un diverso profilo, le modifiche al GDPR in materia di interesse legittimo devono essere coordinate con le modifiche apportate dal Digital Omnibus on AI all'art. 10, par. 5 dell' IA Act[47], disposizione che, nella formulazione vigente, consente ai fornitori e ai deployers di sistemi di IA ad alto rischio di trattare categorie particolari di dati esclusivamente nella misura strettamente necessaria alla rilevazione e correzione dei *bias,* subordinando tale possibilità al rispetto di determinate garanzie. La nuova formulazione, collocata nel proposto art. 4bis, sembrerebbe perseguire l'obiettivo di superare le ambiguità interpretative che avevano caratterizzato l'attuale testo, ampliandone tuttavia significativamente l'ambito applicativo: la disposizione non sarebbe circoscritta ai soli sistemi ad alto rischio, ma verrebbe estesa, sia dal punto di vista materiale che personale, a tutti i sistemi e modelli di IA.

Indubbia la pericolosità di *bias* nell'ambito del funzionamento dei sistemi di IA per i diritti e le libertà fondamentali dei soggetti coinvolti. Indubbio, altresì, che il trattamento di categorie di dati personali è, in linea di principio, vietato dall'Unione europea salvo eccezioni, che dovrebbero essere definite in maniera restrittiva. In questo senso, risultano significative le scelte lessicali adottate dalla Commissione: il testo attuale dell'art. 10, par. 5, fa riferimento soltanto a quanto "necessario" (art. 4-bis, par.1) o "necessario e proporzionato" (art. 4bis, par.2)[48] . Tale slittamento terminologico non appare privo di conseguenze sul piano delle garanzie previste a livello europeo. Non sorprende, pertanto, che l'EDPB-EDPS abbiano raccomandato il ripristino del criterio della "stretta necessità", evidenziando il rischio che una

[47] Art. 4bis, COM(2025) 836final.

[48] Art. 4bis, COM(2025) 836 final. Il par. 2 fa riferimento a quanto "necessario e proporzionato".

formulazione eccessivamente ampia della deroga possa tradursi in un'estensione difficilmente delimitabile delle ipotesi di trattamento lecito di dati particolari[49][50].

Inoltre, la disposizione non contiene alcuna definizione giuridicamente circoscritta della nozione di *bias,* tradotta nel testo italiano come "distorsione", né chiarisce i parametri sulla base dei quali tale fenomeno dovrebbe essere individuato. In assenza di criteri normativi sufficientemente determinati, il rischio è quello di attribuire agli operatori un margine di discrezionalità particolarmente ampio nell'individuazione delle situazioni che giustificano il trattamento di categorie particolari di dati personali, con possibili tensioni rispetto ai principi di proporzionalità, minimizzazione e limitazione delle finalità. Il rischio a cui si assiste è che una deroga concepita come eccezione possa progressivamente trasformarsi in un canale ordinario di accesso a dati sensibili per l'addestramento dell'IA. Tale rischio risulta ulteriormente amplificato dall'assenza di un chiaro coordinamento tra la nuova disposizione e i principi generali del GDPR, con la conseguente possibilità che gli operatori si orientino verso l'opzione normativa maggiormente favorevole.

L'ampliamento in esame pone, infine, un rilevante problema di ordine costituzionale. L'AI Act trova il proprio fondamento giuridico nell'art. 114 TFUE, relativo all'armonizzazione del mercato interno. L'attuale art. 10, par. 5, rappresentava una delle rare disposizioni dell'AI Act direttamente riconducibili all'art. 16 TFUE, ossia alla specifica competenza dell'UE in materia di protezione dei dati personali. La proposta di sostituzione della norma mediante un nuovo art. 4bis solleva dunque l'interrogativo circa la possibilità, per il legislatore europeo, di incidere indirettamente sul regime di trattamento dei dati personali, in particolare delle categorie particolari di dati senza ricorrere alla base giuridica specifica di cui all'art. 16 TFUE.

5. Diritti di accesso e di informazione

Il Digital Omnibus, ispirandosi a una proposta del Governo tedesco relativa all'uso dell'art. 15 GDPR nell'ambito della raccolta prove nei procedimenti civili, introduce alcune restrizioni

[49] Il Parlamento europeo, con l'approvazione della sua posizione lo scorso 26 marzo 2026 ha introdotto alcune cautele sul punto affermando: il trattamento è necessario per garantire il rilevamento e la correzione di possibili distorsioni suscettibili di incidere sulla salute e sulla sicurezza delle persone, di avere un impatto negativo sui diritti fondamentali o di comportare discriminazioni vietate dal diritto dell'Unione, specie laddove gli output di dati influenzano gli input per operazioni future". V. Considerando 6, Disponibile al link: https://www.europarl.europa.eu/doceo/document/TA-10-2026-0098_IT.html.

[50] EDPB-EDPS, Joint opinion 1/2026 "On the Proposal for a Regulation as regards the simplification of the implementation of harmonized rules on Artificial intelligence, p. 6, 2026.

all'esercizio del diritto di accesso ai dati personali[51]. La Proposta della Commissione sembra, infatti, orientata ad ampliare le ipotesi nelle quali il titolare del trattamento può legittimamente negare l'accesso richiesto dall'interessato[52]. Si tratta di un intervento di particolare rilievo, atteso che il diritto di accesso rappresenta uno degli strumenti centrali della normativa dell'Unione in materia di dati personali, in quanto presupposto indispensabile per l'effettivo esercizio di ulteriori prerogative riconosciute all'interessato, tra cui il diritto di rettifica, cancellazione e limitazione del trattamento[53].

Allo stato attuale, le richieste di accesso possono essere rigettate esclusivamente quando risultino "manifestamente infondate o eccessive", in particolare per il loro carattere ripetitivo (art. 12, par. 5, GDPR). La Corte di giustizia ha chiarito che tale disposizione costituisce espressione di un principio generale del diritto dell'Unione finalizzato ad arginare fenomeni di esercizio abusivo dei diritti conferiti ai singoli dall'ordinamento sovranazionale[54]. Al di fuori di tali ipotesi, il diritto di accesso non sembra soggetto a limitazioni di alcuna natura, neppure quando il soddisfacimento della richiesta comporti oneri particolarmente gravosi per il titolare, avuto riguardo alle risorse tecniche e organizzative di cui questi concretamente dispone[55].

La modifica contenuta nella Proposta di Regolamento Omnibus prevede che il rifiuto possa riguardare anche i casi in cui l'interessato eserciti i propri diritti previsti dal GDPR "per finalità diverse dalla protezione dei suoi dati personali"[56]. Tale restrizione è accompagnata da una

[51] German Proposal for simplification of the GDPR, 2025, consultabile al link: 11/German%20Proposal%20for%20simplification%20of%20the%20GDPR.pdf.

[52] Come precisato dalla Corte di giustizia europea nella Sentenza C-434/16, Nowak, punto 56. "il diritto di accesso intende garantire la tutela del diritto degli interessati alla vita privata e alla protezione dei dati rispetto al trattamento dei dati che li riguardano, e può agevolare l'esercizio dei diritti che derivano, ad esempio, dagli artt. 16 e 19, da 21 a 22 e 82 GDPR".

[53] Artt. 16, 17, 18, Regolamento (UE) 679/2016.

[54] V. CGUE, C-416/23, Österreichische Datenschitzbehörde, punto 49. La Sentenza fa riferimento all'art. 57, par. 4 del GDPR, il quale riflette un principio costante nel diritto dell'UE, fatto proprio dalla giurisprudenza della Corte, secondo cui i soggetti dell'ordinamento non possono avvalersi fraudolentemente o abusivamente delle norme di diritto europeo.

[55] V. EDPB, Linee guida 1/2022 sui diritti degli interessati – diritto di accesso, 2023. Consultabile al link: https://www.edpb.europa.eu/system/files/202404/edpb_guidelines_202201_data_subject_rights_access_v2_it.pdf

[56] L'articolo 3, par. 4, COM (2025)836final modifica l'art. 12 prevedendo che nel caso di richieste manifestatamente infondata o eccessive, il titolare può alternativamente: a) addebitare un contributo spese

riduzione dell'onere di prova gravante sui titolari del trattamento: questi ultimi potrebbero rifiutare di dare seguito all'esercizio dei diritti dell'interessato qualora sussistano "motivi ragionevoli" per ritenere che la richiesta sia eccessiva.

A un primo esame, la nuova formulazione potrebbe apparire come una corretta trasposizione normativa dell'orientamento giurisprudenziale sopra richiamato. Un'analisi più approfondita induce, tuttavia, a una maggiore prudenza interpretativa. La disposizione, infatti, rischia di essere letta in termini ampi, permettendo di qualificare come manifestatamente infondate o eccessive non soltanto richieste effettivamente abusive o ripetitive, ma anche quelle perseguite per finalità ulteriori rispetto alla tutela dei dati personali intesa in senso stretto. Una simile ricostruzione richiede, tuttavia, un approccio prudente. Se infatti la Corte di giustizia aveva progressivamente riconosciuto al diritto di accesso una portata tendenzialmente autonoma (motive-blind), escludendo che il suo esercizio potesse essere subordinato alle ragioni concrete che inducono l'interessato ad avvalersene[57][58], la successiva sentenza *Brillen Rottler GmbH & Co. KG(C-526/24),* ha tuttavia precisato che anche una prima richiesta di accesso può essere qualificata come eccessiva quando il titolare dimostri che essa è stata presentata non per consentire all'interessato di prendere conoscenza del trattamento e di verificarne la liceità, bensì con l'esclusivo intento di creare artificiosamente i presupposti per l'esercizio di pretese risarcitorie. La pronuncia sembra parzialmente confermare l'esigenza di contrastare gli utilizzi abusivi del diritto di accesso, collocandosi, almeno in parte, in linea con la ratio della Proposta. Essa, tuttavia, mantiene tale possibilità entro limiti rigorosi, subordinando il rigetto della richiesta alla dimostrazione di un intento abusivo da accertarsi caso per caso. Sotto questo profilo, la formulazione del Digital Omnibus appare potenzialmente più ampia, nella misura in cui consente di attribuire rilievo alle finalità perseguite dall'interessato e alla mera sussistenza di "motivi ragionevoli" per ritenere la

ragionevole, tenendo conto dei costi amministrativi sostenuto per fornire le informazioni o la comunicazione; oppure b) rifiutare di dare seguito alla richiesta.

[57] V. CGUE, C- 307/22. La Sentenza recita al punto 28: "Si deve necessariamente constatare che né la formulazione dell'articolo 12, paragrafo 5, del RGPD né quella dell'articolo 15, paragrafi 1 e 3, di tale regolamento subordinano la fornitura, a titolo gratuito, di una prima copia dei dati personali al fatto che i suddetti interessati invocano un motivo diretto a giustificare le loro richieste. Tali disposizioni non offrono pertanto al titolare del trattamento la possibilità di chiedere i motivi della richiesta di accesso presentata dall'interessato".

[58] V. Uber BV/ Uber drivers, Cantonal Court Amsterdam. La vicenda ha riguardato autisti Uber, i quali hanno utilizzato il proprio diritto di accesso per dimostrare e contestare pratiche lavorative illecite poste in essere dalla società.

richiesta eccessiva, con il rischio di estendere le ipotesi di rigetto oltre quelle delineate dalla Corte[59].

Dunque, così come formulata, la disposizione del Digital Omnibus in esame e la sua applicazione concreta risultano contornate da profili di ambiguità. Essa potrebbe significare semplicemente che le richieste abusive non sono consentite, oppure che qualsiasi utilizzo per finalità diverse dalla protezione dei dati debba essere considerato abusivo e, pertanto, respinto dal titolare del trattamento.

Nel considerando proposto a corredo della disposizione[60], la Commissione contribuisce ad accrescere, piuttosto che a chiarire, le incertezze interpretative. Da un lato, ribadisce che devono considerarsi abusive proprio quelle situazioni già qualificate come tali dalle linee guida EDPB, precisazione che appare sostanzialmente ridondante, oltre che inidonea a chiarire l'effettiva portata della disposizione principale. Dall'altro lato, il considerando afferma che i titolari del trattamento possono rigettare richieste "eccessivamente ampie o generiche"[61]. Una

[59] C-256/24, Brillen Rottler. Nella causa C-526/24, *Brillen Rottler GmbH & Co. KG*, la Corte di giustizia è stata chiamata a pronunciarsi su una controversia insorta tra un'impresa tedesca operante nel settore dell'ottica e un interessato che, dopo essersi iscritto alla newsletter dell'azienda, aveva esercitato il diritto di accesso ai sensi dell'art. 15 GDPR. Il titolare del trattamento aveva respinto la richiesta, ritenendola abusiva, in quanto l'interessato risultava presentare sistematicamente analoghe richieste nei confronti di diversi titolari, cui facevano seguito domande di risarcimento per presunte violazioni del GDPR. Il giudice del rinvio ha quindi chiesto alla Corte se anche una prima richiesta di accesso potesse essere qualificata come «manifestamente infondata o eccessiva» ai sensi dell'art. 12, par. 5, GDPR. Con sentenza del 19 marzo 2026, la Corte ha affermato che una prima richiesta può essere considerata abusiva qualora il titolare dimostri che essa, pur rispettando formalmente i requisiti previsti dal Regolamento, sia stata presentata non per consentire all'interessato di conoscere il trattamento dei propri dati personali e verificarne la liceità, bensì con l'esclusivo intento di creare artificiosamente i presupposti per ottenere un risarcimento ai sensi dell'art. 82 GDPR. La Corte ha altresì precisato che la sistematica presentazione di richieste di accesso, seguite da azioni risarcitorie nei confronti di diversi titolari, può costituire un elemento indiziario dell'intento abusivo, fermo restando che spetta al titolare del trattamento fornire la relativa prova e al giudice nazionale verificarne la sussistenza caso per caso. Quanto al diritto al risarcimento, la Corte ha ribadito che esso presuppone la dimostrazione di un danno effettivamente subito e non può essere riconosciuto quando il pregiudizio lamentato sia riconducibile al comportamento dello stesso interessato.

[60] Considerando 35, COM(2025) 837final.

[61] Vero è che il GDPR consente al titolare di chiedere al titolare precisazioni circa "l'informazione o le attività di trattamento cui la richiesta si riferisce" (considerando 63). Come specificato dalle linee guida dell'EDPB, si tratta di una misura a tutela dell'interessato, finalizzata a facilitare il ricevimento delle informazioni desiderate. La proposta della Commissione appare invece prevalentemente orientata alla riduzione degli oneri gravanti sul titolare del trattamento. Il Considerando 35 prevede che l'interessato, nell'esercizio del diritto di accesso ai sensi dell'art. 15 GDPR, dovrebbe formulare richieste "quanto più specifiche"; mentre le domande eccessivamente "ampie e generiche" potrebbero essere considerata manifestatamente eccessive e, pertanto, respinte. Tale impostazione trascura la possibilità che l'interessato non sia concretamente in grado di circoscrivere con precisione l'oggetto della richiesta proprio perché ignora quali dati siano effettivamente detenuti dal titolare. La facoltà riconosciuta al titolare di interloquire preventivamente con l'interessato, anziché costituire uno strumento volto ad agevolare l'adempimento dell'obbligo di facilitare l'esercizio dei diritti dell'interessato ex. art.

simile indicazione, tuttavia, solleva ulteriori dubbi e criticità: i considerando, infatti, non possono introdurre autonome limitazioni ai diritti riconosciuti dal GDPR. Ne consegue che il richiamo a tali richieste, in assenza di un'esplicita previsione nel testo normativo, rischia di amplificare ulteriormente l'incertezza applicativa della disciplina[62].

Contrariamente a quanto sostenuto dalla Commissione, secondo cui tali modifiche sembrerebbero meramente tecniche e idonee a preservare lo standard europeo di tutela dei diritti fondamentali, esse sembrano rappresentare un arretramento nella protezione dei diritti degli interessati. Gli elementi disponibili suggeriscono che i benefici sociali derivanti dal diritto di accesso superino di gran lunga i costi gravanti sui titolari del trattamento. Non mancano esempi di richieste di accesso apparentemente eccessive e/o non strettamente connesse alla produzione dei dati personali che hanno svolto un ruolo essenziale nella tutela del diritto alla vita privata e alla protezione dei dati personali, ma anche di altri diritti fondamentali[63].

Invero, se è condivisibile l'esigenza di valutare criticamente gli oneri regolatori gravanti sui titolari del trattamento alla luce delle sfide che interessano la competitività europea, meno evidente appare il nesso tra la riduzione di tali oneri, la contestuale limitazione del diritto di accesso e il perseguimento di obiettivi di innovazione. Tale conclusione sembra ancor più fondata se si considera che anche gli operatori economici extraeuropei che offrono beni o servizi a interessati situati nell'Unione continueranno, in ogni caso, a essere assoggettati al GDPR, a prescindere dalle modifiche introdotte dal Digital Omnibus.

La Proposta interviene altresì sugli obblighi informativi previsti dall'art. 13 GDPR, introducendo un'ulteriore attenuazione degli oneri gravanti sul titolare del trattamento. Nella formulazione vigente, il Regolamento impone al titolare di fornire all'interessato una serie di informazioni determinate; ai sensi del par. 4, tale obbligo non trova applicazione qualora l'interessato disponga già delle informazioni in questione.

12, par. 2 GDPR, rischia di trasformarsi in un meccanismo funzionale a limitare o respingere l'istanza di accesso ritenute insufficientemente circostanziate.

[62] Considerando 35, COM(2025)837final.

[63] In tal senso v. R. MAHIEU – J. AUSLOOS, "recognizing and Enabling the Collective Dimension of the GDPR and the Right of Access", 2020.

La Proposta Omnibus sostituirebbe il par. 4 dell'art. 13 estendendo tale deroga alle ipotesi in cui "*il trattamento riguardi dati personali raccolti nel contesto di una relazione chiara e circoscritta tra gli interessati e un titolare del trattamento che esercita un'attività che non è ad alta intensità di dati e vi sono ragionevoli motivi per presumere che l'interessato disponga già delle informazioni di cui al par. 1, lett. a) e c) a meno che il titolare del*

trattamento non trasmetta i dati ad altri destinatari o categorie di destinatari, trasferisca i dati a un paese terzo, effettui un processo decisionale automatizzato, compresa la profilazione, di cui all'articolo 22, paragrafo 1, o il trattamento possa presentare un rischio elevato per i diritti e le libertà degli interessati ai sensi dell'articolo 35"[64].

Dunque, secondo la Commissione, le circostanze sufficienti all'applicazione della nuova esimente, si verificherebbero, in particolare, nei rapporti caratterizzati da un'interazione chiara e circoscritta tra titolare e interessato, nonché in contesti in cui il trattamento non sia particolarmente intenso sotto il profilo dei dati trattati. Vengono richiamati, a titolo esemplificativo, i rapporti tra artigiani e clienti, oppure i trattamenti effettuati da associazioni e club sportivi ai fini della gestione delle adesioni, delle comunicazioni con i membri o dell'organizzazione delle attività associative[65].

Al tempo stesso, sono previste quattro contro-eccezioni, secondo le quali l'esenzione non può essere invocata dal titolare del trattamento nel caso in cui: il titolare trasmetta i dati ad altri destinatari o categorie di destinatari; il titolare trasferisca i dati verso un paese terzo; il titolare effettui processi decisionali automatizzati, compresa la profilazione, di cui all'art. 22, par. 1 GDPR; il trattamento sia suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati ai sensi dell'art. 35 GDPR.

Nell'ottica della Commissione, la modifica sarebbe volta a evitare adempimenti informativi ritenuti privi di un effettivo valore aggiunto per gli interessati, alleggerendo così gli oneri amministrativi, soprattutto per piccoli operatori economici.

La Proposta sembra tuttavia determinare un'ulteriore compressione delle prerogative di trasparenza che caratterizzano il sistema europeo di protezione dei dati personali. L'obbligo informativo previsto dall'art. 13 GDPR costituisce, infatti, uno degli strumenti essenziali

[64] Art. 3, par. 5, COM(2025)837final.

[65] Considerando 37, COM(2025)837final.

attraverso cui l'interessato acquisisce consapevolezza dell'esistenza del trattamento, delle sue finalità e delle modalità con cui esso viene effettuato. L'estensione della deroga rischia, pertanto, di ampliare significativamente i casi in cui il titolare può omettere tali informazioni sulla base di valutazioni ampiamente discrezionali circa la presumibile conoscenza dell'interessato. La criticità appare particolarmente evidente ove si consideri che alcune delle informazioni contemplate dall'art. 13 GDPR non risultano integralmente ricomprese nell'ambito del diritto di accesso disciplinato dall'art. 15 GDPR. Ciò in quanto il legislatore europeo ha costruito il sistema assumendo che tali informazioni siano previamente comunicate all'interessato attraverso gli obblighi informativi gravanti sul titolare del trattamento. L'ampliamento delle deroghe all'obbligo di informazione rischia, pertanto, di creare un significativo vuoto di tutela. Qualora l'interessato non riceva informazioni essenziali, potrebbe trovarsi nell'impossibilità di esercitare consapevolmente i diritti riconosciuti dal Regolamento, quali la revoca del consenso o il diritto di opposizione di cui all'art. 21 GDPR[66].

La Proposta modifica ulteriormente l'art. 13 GDPR, introducendo un nuovo paragrafo 5[67] riguardante i trattamenti effettuati per finalità di ricerca scientifica. In tali ipotesi, le informazioni di cui all'art. 13 possono non essere fornite qualora la comunicazione all'interessato risulti "impossibile" o implichi uno "sforzo sproporzionato. Il titolare del trattamento sarebbe comunque tenuto a compiere sforzi ragionevoli per acquisire i dati di contatto degli interessati, ove questi siano prontamente disponibili e la loro acquisizione non richieda uno sforzo sproporzionato.

Secondo la Commissione, uno sforzo sproporzionato ricorrerebbe, in particolare, nei casi in cui, al momento della raccolta dei dati personali, il titolare non sapesse né potesse ragionevolmente prevedere che tali dati sarebbero stati successivamente trattati per finalità di ricerca scientifica[68]. In tali casi, il titolare potrebbe non disporre dei recapiti degli interessati e

[66] Le criticità emergono con particolare evidenza nei casi in cui il trattamento si fondi sul consenso dell'interessato, infatti, non appare chiaro come questo possa considerarsi "informato"; come richiesto dagli artt. 4, punto 11; 6, par. 1, lett a) e 7 GDPR, laddove le informazioni previste dall'art. 13 non vengano integralmente fornite.

[67] Art. 3, par. 5 COM(2025) 837final.

[68] In questo caso, il testo vigente dell'art. 13 del GDPR prevede, al par. 3 che: "Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diverse finalità e ogni

dovrebbe pertanto adempiere agli obblighi informativi in via indiretta, ad esempio mediante la pubblicazione delle informazioni. La comunicazione dovrebbe comunque essere effettuata, in ogni caso, attraverso modalità idonee a raggiungere il maggior numero possibile di interessati, tenendo conto del contesto del progetto di ricerca e degli interessi coinvolti.

Dal punto di vista dell'interessato, l'assenza di qualsiasi informazione circa il mutamento delle finalità del trattamento rappresenta un rilevante problema sotto il profilo della certezza del diritto. Essa incide sul principio della "limitazione delle finalità", uno dei pilastri del GDPR, secondo cui gli interessati forniscono dati per una finalità specifica e possono generalmente confidare nel fatto che essi non vengano successivamente utilizzati per finalità ulteriori e non previste.

La nuova previsione si pone, dunque, in tensione con diverse disposizioni del GDPR. In particolare, essa appare difficilmente conciliabile con l'art. 13, par. 3, che impone di informare l'interessato nel caso di ulteriore trattamento per finalità diverse da quelle che hanno giustificato la raccolta dei suoi dati personali. Analoghe perplessità emergono con riferimento all'art. 21, par. 6, GDPR, che riconosce all'interessato il diritto di opporsi a un ulteriore trattamento per finalità di ricerca scientifica.

6. Processo individuale automatizzato

Le novità apportate al capo III, relativo ai diritti dell'interessato, si estendono all'art. 22 GDPR, oggetto di una riscrittura che incide profondamente sulla struttura e sulla ratio della disposizione.

Nella formulazione vigente, l'art. 22 riconosce all'interessato il diritto di non essere sottoposto a una decisione basata unicamente su un trattamento automatizzato, inclusa la profilazione, che produca effetti giuridici o incida in modo analogo sulla sua persona[69]. Secondo l'interpretazione fornita dal Gruppo di lavoro Art. 29 nelle Guidelines WP251, successivamente recepite dall'EDPB, la disposizione è costruita attorno a un divieto generale, temperato dalla

ulteriore informazione pertinente i cui al paragrafo 2". Questa previsione permetterebbe agli interessati di contesta l'ulteriore utilizzo dei propri dati o di esercitare il diritto di opposizione di cui all'art. 21, par. 6 GDPR.

[69]Sebbene il dato testuale si riferisca espressamente a un "diritto" dell'interessato, il Gruppo di lavoro Art. 29, nelle Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251), successivamente fatte proprie dall'EDPB, ha interpretato la disposizione nel senso che essa introduce un divieto generale di decisioni esclusivamente automatizzate, applicabile indipendentemente dall'attivazione dell'interessato e derogabile soltanto nelle ipotesi previste dal paragrafo 2.

previsione di alcune eccezioni[70]. Si tratta di una disposizione caratterizzata da un elevato grado di elasticità applicativa, tanto da essere frequentemente aggirata nella prassi mediante l'inserimento, all'interno del processo decisionale, di forme di intervento umano meramente formali o prive di reale incidenza sostanziale. La disposizione è stata oggetto di un'interpretazione della Corte di giustizia volta a preservarne l'effettività, evitando che il divieto possa essere eluso mediante forme di intervento umano meramente apparenti[71].

L'Omnibus, in apparente contrasto con il recente orientamento, spezza il nesso tra automazione e necessità e consente ai titolari di ricorrere al processo decisionale automatizzato come scelta operativa, anziché come misura indispensabile. La proposta prevede infatti che "una decisione che produca effetti giuridici che riguardano un interessato o che incida in modo analogo su una persona *può essere basata* unicamente su un trattamento automatizzato, inclusa la profilazione". La modifica sembra segnare un vero e proprio ribaltamento di paradigma: da un sistema costruito attorno a un *divieto generale*, derogabile soltanto in presenza di specifiche eccezioni, si passerebbe a un modello di *autorizzazione condizionata*[72]. Con riferimento ai casi in cui è consentito sottoporre una persona a una decisione interamente automatizzata, vi è poiil compimento di un ulteriore passo, nella misura in cui si prevede che tale decisione possa essere adottata qualora sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento, anche quando il medesimo risultato potrebbe essere raggiunto mediante modalità diverse dalla sola automazione (art. 22, par.1, lett a)).

In altri termini, la nuova formulazione consentirebbe il ricorso a decisioni interamente automatizzate al ricorrere dei presupposti che l'attuale art. 22 GDPR configura invece come eccezioni al divieto di *automated decision-making*, vale a dire: a) sia necessaria per la

[70] Art. 22, Regolamento (UE) 679/2016. Il par. 2 prevede le seguenti eccezioni: "la decisione automatizzata a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato".

[71] CGUE, C-634/21 (SCHUFA). Con questa sentenza la CGUE ha stabilito che il *credit scoring* elaborato da una società che fornisce informazioni commerciali costituisce un processo decisionale automatizzato relativo alle persone fisiche ai sensi dell'art. 22 del GDPR, quando l'utilizzo dello stesso da parte di una società terza determini in modo decisivo la stipula, l'esecuzione o la cessazione di un rapporto contrattuale.

[72] V. M. Borghi, "verso un'austerity dei diritti digitali (e non solo)", in Forum Disuguaglianze Diversità, disponibile su: https://www.forumdisuguaglianzediversita.org/verso-unausterity-dei-diritti-digitali-e-non-solo/.

conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, (indipendentemente dalla possibilità che la decisione possa essere adottata in modo diverso rispetto al mezzo esclusivamente automatizzato)[73]; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato.

La scelta di abbandonare la formulazione precedente, espressamente costruita come diritto dell'interessato, pur mantenendo la disposizione nel Capo III del GDPR, dedicato ai "diritti dell'interessato", contribuisce ad alimentare dubbi circa la natura giuridica dell'art. 22. Nonostante la modifica prevista alla lett. a), tanto nella formulazione vigente quanto in quella proposta, l'art. 22 GDPR continua a fondarsi su uno schema di limitata possibilità di procedere a decisioni automatizzate. Sotto tale profilo, la nuova formulazione, costruita nei termini di una facoltà, appare tecnicamente meno chiara e comprensibile rispetto a una struttura normativa fondata, anzitutto, sull'affermazione del divieto e, successivamente, sull'individuazione delle deroghe a tale divieto.

7. Data breach, istituzione del single entry point e DPIA

Al fine di alleggerire gli obblighi gravanti sui titolari del trattamento, pur garantendo alle autorità di controllo l'accesso alle informazioni necessarie per l'esercizio delle proprie funzioni di vigilanza, la Proposta interviene sul regime di notificazione delle violazioni dei dati personali. In particolare, essa prevede di uniformare la soglia prevista dall'art. 33 GDPR per la notifica del *data breach* a quella stabilita dall'art. 34 per la comunicazione della violazione agli interessati nei casi in cui sussista un "rischio elevato" per i diritti e le libertà delle persone fisiche"[74]. Dunque, nel caso di violazione che non sia suscettibile di comportare un rischio elevato per i

[73] Nel mercato digitale molti servizi sono contrattualizzati in modo standardizzato; affermare che l'automazione è necessaria per concludere o eseguire il contratto, senza chiedersi se esistano alternative meno invasive, rischia di normalizzare decisioni automatizzate in settori ad alto impatto: credito, assicurazioni, lavoro, istruzione, accesso a servizi essenziali.

[74] Art. 33, par. 1, Regolamento (UE) 679/2016. La disposizione recita: "In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo". L'art. 34, par. 1, Regolamento (UE) 679/2016 recita: "1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo".

diritti e le libertà delle persone fisiche, il titolare non sarà tenuto all'obbligo di notificazione all'autorità competente.

In aggiunta, la Commissione propone di attribuire a ENISA il compito di istituire un *single entry point*, destinato a consentire ai soggetti obbligati di adempiere, attraverso un unico canale, agli obblighi di segnalazione degli incidenti previsti da una pluralità di normative settoriali[75]. La proposta si ispira al principio del *report once, share many times*, volto a ridurre gli oneri amministrativi.

Sebbene l'elevato numero di notifiche di *data breach*, spesso relative a incidenti di modesta entità, abbia indotto le autorità di controllo a non attribuire particolare rilievo a molte di esse, la modifica prospettata sembra suscettibile di incidere significativamente sull'equilibrio complessivo del sistema. La soglia del "rischio elevato" ricorre, infatti, ricorre soltanto in casi limitati e il suo accertamento rischia di essere rimesso a valutazioni ampiamente discrezionali del titolare del trattamento.

Al fine di mitigare tale criticità, il Digital Omnibus prevede l'introduzione di un par. 6 all'art. 33, imponendo all'EDPB l'obbligo di predisporre un modello comune per la notifica della violazione dei dati personali, nonché un elenco delle circostanze nelle quali si presume che una violazione presenti un rischio elevato per i diritti e le libertà della persona fisica. Con riferimento a tali strumenti, la Proposta attribuisce inoltre alla Commissione il potere di adottare atti di esecuzione finalizzati al loro eventuale riesame[76].

[75] l'utilizzo del punto di accesso unico è finalizzato a soddisfare una serie di obblighi di segnalazione degli incidenti previsti dalla Direttiva (UE) 2022/2555 (direttiva NIS 2), dal regolamento (UE) 2016/679 (GDPR), dal regolamento (UE) 2022/2554 (DORA), dal regolamento (UE) n. 910/2014 (regolamento eIDAS) e dalla direttiva (UE) 2022/2557 (direttiva CER). Anche altri obblighi di segnalazione settoriali, come quelli stabiliti nel quadro del codice di rete per gli aspetti di cybersicurezza dei flussi transfrontalieri di energia elettrica e dei pertinenti strumenti per il settore dell'aviazione, saranno riuniti sotto un punto di accesso unico mediante la modifica degli atti delegati e di esecuzione che stabiliscono gli obblighi di segnalazione nell'ambito di tali quadri normativi.

[76] Per mitigare il problema, la proposta prevede l'introduzione di un par. 6 all'art. 33: "Il comitato redige e trasmette alla Commissione una proposta di modello comune per la notifica di una violazione dei dati personali all'autorità di controllo competente di cui al paragrafo 1, nonché di un elenco delle circostanze in cui tale violazione può presentare un rischio elevato per i diritti e le libertà di una persona fisica. Le proposte sono presentate alla Commissione entro il [OP, inserire la data = nove mesi dopo l'entrata in applicazione del presente regolamento]. La Commissione, previa debita valutazione, le riesamina, se necessario, e ha il potere di adottarle mediante un atto di esecuzione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2".

Risponde alla medesima ratio legis, orientata a una maggiore standardizzazione a livello europeo delle procedure di compliance e della documentazione in materia di protezione dei dati personali, anche la modifica dell'art. 35 del GDPR in materia di Data Protection Impact Assessment (DPIA)[77]. La proposta prevede infatti la sostituzione degli attuali elenchi nazionali delle operazioni di trattamento soggette all'obbligo di DPIA con un elenco unico adottato a livello europeo, predisposto dall'EDPB e successivamente approvato dalla Commissione mediante atto di esecuzione. Parallelamente, diverrebbe obbligatoria la pubblicazione di un elenco delle tipologie di trattamento per le quali non è richiesta una valutazione d'impatto.

Nella medesima prospettiva di armonizzazione, all'EDPB verrebbe attribuito il compito di elaborare un modello comune e una metodologia uniforme per lo svolgimento della DPIA, da sottoporre a revisione periodica, almeno ogni tre anni, al fine di tenere conto dell'evoluzione tecnologica.

L'introduzione di elenchi comuni, modelli standardizzati e metodologie uniformi può certamente contribuire a rafforzare la certezza del diritto e a promuovere una maggiore armonizzazione applicativa. Tuttavia, Tuttavia, la centralizzazione della definizione del rischio elevato e dei relativi strumenti operativi, soprattutto ove demandata ad atti di esecuzione della Commissione, rischia di comprimere il ruolo delle autorità di controllo indipendenti e di ridurre la capacità di adattare tali valutazioni alle peculiarità dei diversi contesti nazionali e settoriali.

8. Trasposizione delle norme ePrivacy nel GDPR

La Direttiva ePrivacy (Direttiva 2002/58/CE) costituisce il principale strumento normativo dell'Unione europea volto a garantire la riservatezza delle comunicazioni elettroniche e la tutela della sfera privata degli utenti nell'ambiente digitale. In particolare, l'art. 5, par. 3[78],

[77] Art. 3, par. 9. L'articolo 35 è così modificato: "i paragrafi 4, 5 e 6 sono sostituiti dai seguenti: "4. Il comitato redige e trasmette alla Commissione una proposta di elenco delle tipologie di trattamenti soggetti all'obbligo di una valutazione d'impatto sulla protezione dei dati a norma del paragrafo 1. 5. Il comitato redige e trasmette alla Commissione una proposta di elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. 6. Il comitato redige e trasmette alla Commissione una proposta relativa a un modello comune e a una metodologia comune per lo svolgimento delle valutazioni d'impatto sulla protezione dei dati."

[78] Art. 5, par. 3, Direttiva 2002/58/CE. L'articolo recita: "Gli Stati membri assicurano che l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente interessato sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento in conformità della direttiva 95/46/CE e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento. Ciò non impedisce l'eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella

disciplina la memorizzazione di informazioni e l'accesso alle informazioni già archiviate nelle apparecchiature terminali degli utenti, ivi comprese le operazioni effettuate mediante cookie e tecnologie analoghe.

La disposizione mira a proteggere non soltanto i dispositivi utilizzati dagli utenti per accedere ai servizi di comunicazione elettronica, ma anche qualsiasi informazione in essi contenuta, indipendentemente dalla sua qualificazione come dato personale o non personale. A tal fine, essa stabilisce, quale regola generale, che la memorizzazione di informazioni sul terminale dell'utente o l'accesso a informazioni già ivi conservate siano subordinati alla preventiva fornitura di informazioni chiare e complete, nonché all'acquisizione del consenso dell'interessato.

Sebbene il legislatore europeo abbia previsto alcune deroghe a tale requisito, in particolare per i cookie strettamente necessari all'erogazione del servizio richiesto dall'utente o indispensabili al funzionamento dello stesso, il consenso continua a costituire il presupposto di liceità nella maggior parte delle operazioni di accesso e memorizzazione.

Per quel che concerne il rapporto tra la Direttiva ePrivacy e il GDPR, la prima opera come *lex specialis* rispetto al secondo nei casi in cui l'accesso alle informazioni contenute nel terminale dell'utente comporti altresì il trattamento di dati personali. In questa prospettiva, l'art. 5, par. 3, disciplina esclusivamente la fase di accesso alle informazioni presenti sul dispositivo dell'utente, mentre l'ulteriore trattamento dei dati personali eventualmente acquisiti resta assoggettato alle condizioni di liceità previste dal GDPR all'art. 6.

L'analisi delle modifiche prospettate in relazione al quadro ePrivacy non può prescindere da una preliminare ricostruzione delle criticità che la Commissione individua a supporto dell'iniziativa riformatrice.

Anzitutto, nella Relazione di accompagnamento al Digital Omnibus, particolare attenzione è riservata al meccanismo del consenso previsto dall'art. 5, par. 3 della Direttiva ePrivacy. Secondo la Commissione, la necessità di acquisire il consenso per la generalità delle operazioni di accesso o memorizzazione di informazioni nelle apparecchiature terminali degli utenti avrebbe favorito la diffusione dei c.d. *cookie banner*, il cui utilizzo massivo ha generato,

misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente".

come noto, il fastidioso fenomeno della *consent fatigue*, inducendo frequentemente gli utenti ad accettare o rifiutare le richieste in modo automatico e non pienamente consapevole[7980].

La Commissione evidenzia inoltre come, nel corso di un apposito *reality check*, condotto con gli stakeholder, numerosi partecipanti abbiano ritenuto l'attuale disciplina eccessivamente rigida e non più adeguata all'evoluzione tecnologica. In particolare, è stato osservato come il requisito del consenso continui ad applicarsi anche ad attività considerate poco invasive, quali la misurazione dell'audience e la raccolta di statistiche sull'utilizzo di siti web[81].

Altro elemento di criticità, riportato nella Relazione di accompagnamento, riguarda la frammentazione dell'enforcement tra gli Stati membri. La natura di direttiva dello strumento normativo ha infatti determinato differenze sia nell'individuazione delle autorità competenti sia nelle modalità di applicazione della disciplina, con conseguenti incertezze interpretative e difficoltà nel garantire un livello uniforme di tutela all'interno dell'Unione.

Dal punto di vista economico, la Commissione rileva inoltre come gli oneri di conformità associati all'attuale disciplina siano significativi. Le stime richiamate nel documento di accompagnamento indicano un costo medio annuo di circa 400 euro per sito web, con un impatto complessivo stimato di circa 1,64 miliardi di euro l'anno[82].

Per le motivazioni appena esposte, la Commissione propone di semplificare il rapporto tra GDPR e disciplina ePrivacy, riconducendo il trattamento dei dati personali conservati nelle apparecchiature terminali o da queste raccolti nell'alveo di un unico quadro normativo.

---

[79] Meno del 43% degli utenti ritiene di avere pieno controllo sulle proprie attività online. In tal senso, v. BEUC (2023) *Connected, but unfairly treated: consumer survey results on the fairness of the online environment*. Disponibile su: BEUC-X-2023-113_Fairness_of_the_digital_environment_survey_results.

[80] IAB Europe (2025) *Optimisation over reform: understanding EU consumers' perception and knowledge of the ad-funded internet and related privacy rights issues*. Disponibile su: IAB-Europe-Ad-Funding-Online-Services-Report-2025-FINAL.pdf. Lo studio evidenzia come il senso di sopraffazione induca gli utenti ad accettare (statisticamente il 54 % degli utenti) o rifiutare (26%) tutti i cookie in modo sostanzialmente casuale, al solo scopo di accedere ai contenuti desiderati, senza compiere una scelta realmente informata.

[81] Consultabile nell'Allegato I al Digital Omnibus.

[82] Per un'analisi puntuale di tali statistiche v. Deloitte, *Evaluation and Review of Directive 2002/58 on Privacy and the Electronic Communication Sector*, richiamato dalla Commissione europea nel *Commission Staff Working Document – Impact Assessment* che accompagna la proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla protezione dei dati personali nelle comunicazioni elettroniche e che abroga la Direttiva 2002/58/CE (*Regulation on Privacy and Electronic Communications*), COM(2017) 10 final, parte 1/3, p. 37.

In particolare, la proposta introduce un nuovo art. 88-bis nel GDPR[83], destinato a trasporre nel Regolamento il nucleo essenziale dell'attuale disciplina contenuta nell'art. 5, par. 3 della Direttiva ePrivacy.

La nuova disposizione conserva il consenso quale regola generale per l'accesso e la memorizzazione di dati personali nei dispositivi terminali[84], ma introduce una serie di ipotesi tassative nelle quali tali operazioni possono avvenire in assenza del consenso dell'interessato. In particolare, il successivo trattamento dei dati è considerato lecito qualora risulti necessario per le specifiche finalità individuate dal legislatore, mentre per le ulteriori attività di trattamento continuano ad applicarsi le basi giuridiche previste dagli artt. 6 e, ove pertinente, 9 GDPR.

Al fine di rafforzare il controllo degli utenti sui propri dati e sui dispositivi utilizzati, nonché di contrastare il ricorso ai c.d. dark patterns, vale a dire interfacce progettate in modo manipolativo o fuorviante per incrementare artificialmente il tasso di consenso, la proposta introduce l'obbligo di consentire all'utente di prestare o negare il consenso mediante un pulsante attivabile con un solo clic (*single-click button*) ogniqualvolta il consenso costituisca la base giuridica del trattamento [85]. Inoltre, il titolare del trattamento sarebbe tenuto a rispettare la scelta intrapresa dall'utente. In particolare, qualora l'interessato abbia negato il consenso, la proposta vieta al titolare di richiederlo nuovamente per un periodo di sei mesi[86].

[83] Art. 3, par. 15, COM(2025)837final.

[84] Il par. 1 del proposto art. 88bis recita: "La conservazione di dati personali nell'apparecchiatura terminale di una persona fisica o l'accesso a dati personali già conservati in tale apparecchiatura sono consentiti solo se tale persona ha espresso il proprio consenso, conformemente al presente regolamento".

[85] Ivi, art. 88bis, par. 4: "Qualora la conservazione di dati personali nell'apparecchiatura terminale di una persona fisica o l'accesso a dati personali già conservati in tale apparecchiatura siano basati sul consenso, si applicano le seguenti disposizioni: a) l'interessato può respingere le richieste di consenso in modo semplice e comprensibile con un solo click o modalità equivalenti; b) se l'interessato dà il proprio consenso, il titolare del trattamento non presenta una nuova richiesta di consenso per la stessa finalità per il periodo durante il quale può legittimamente avvalersi del consenso dell'interessato; c) se l'interessato rifiuta una richiesta di consenso, il titolare del trattamento non presenta una nuova richiesta di consenso per la stessa finalità per un periodo di almeno sei mesi".

[86] Il requisito del *one-click button* sembra collocarsi a un livello di tutela inferiore rispetto a quanto previsto dalle linee guida adottate dalle autorità di protezione dei dati personali singoli stati membri. Vedi a titolo esemplificativo:https://uoou.gov.cz/verejnost/qa-otazky-a-odpovedi/cookies, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677876, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9677876

Il nuovo art. 88-bis solleva alcune criticità. Anzitutto, rispetto all'attuale art. 5, par. 3 della Direttiva ePrivacy, l'articolo proposto presenta tre elementi di novità. In primo luogo, esso circoscrive il proprio ambito applicativo ai soli dati personali, superando l'approccio dell'art. 5, par. 3, che tutela indistintamente qualsiasi informazione presente sull'apparecchiatura terminale. In secondo luogo, amplia le ipotesi nelle quali l'accesso ai dati e la memorizzazione possono avvenire senza consenso, includendo finalità statistiche e di sicurezza del servizio. Rispetto a quest'ultimo punto, le basi giuridiche previste al par. 3, lett. a) e b) possono essere interpretate come forme di consenso implicito, analogamente a quanto avviene nell'ambito dell'art. 6, par. 1, lett b), GDPR[87]. Problematiche appaiono, invece, le deroghe di cui al par. 3, lett. c) e d). Tali disposizioni configurano vere e proprie autorizzazioni generali, nell'ambito delle quali, il bilanciamento necessario richiesto dall'art. 52, par.1, della Carta di Nizza viene effettuato direttamente dal legislatore, anziché essere svolto in concreto al momento dell'applicazione della norma, come invece richiesto nell'ambito del legittimo interesse di cui all'art. 6, par. 1, lett f) GDPR[88].

L'art. 88-bis deve essere letto anche alla luce del successivo 88ter, concernente le *"Indicazioni automatizzate e leggibili da dispositivo automatico delle scelte dell'interessato in relazione al trattamento dei dati personali nelle apparecchiature terminali delle persone fisiche"*. I titolari del trattamento sarebbero tenuti a rispettare le preferenze degli interessati, espresse in modo automatizzato e *machine-readable* e comunicate attraverso le loro interfacce online, quali browser web o applicazioni mobili. Tale obbligo giuridico dovrebbe essere accompagnato dallo sviluppo di standard tecnici comuni, al fine di garantire che esso possa essere agevolmente rispettato e che i requisiti rigorosi previsti dal GDPR siano incorporati sin dalla progettazione (by design) nelle soluzioni tecnologiche in esame. Secondo la Commissione, ciò è necessario affinché sia i fornitori di siti web e applicazioni, sia i fornitori di servizi utilizzati per impostare i segnali di preferenza possano fare affidamento su un vocabolario comune delle finalità di trattamento e utilizzare le medesime specifiche tecniche.

La proposta si inserisce nel solco di numerosi tentativi, avviati ormai da oltre vent'anni, di sostituire i tradizionali cookie banner con strumenti tecnici in grado di comunicare

[87] Il legislatore può ragionevolmente presumere che l'interessato desideri il trattamento.

[88] In particolare, in riferimento alla lett. d), che consente il trattamento per finalità di mantenimento o ripristino della sicurezza dei servizi del titolare, non è affatto evidente che tale interesse, in una prospettiva di bilanciamento, possa prevalere in ogni circostanza sui diritti garantiti dall'art. 7 e 8 della Carta di Nizza.

automaticamente le preferenze privacy agli utenti. A differenza delle esperienze pregresse, come quella riguardante il sistema Do Not Track[89], la Commissione intende consentire la trasmissione automatizzata delle preferenze privacy ai titolari del trattamento, analogamente a quanto già avviene per altre informazioni tecniche comunicate dai browser, quali la lingua o la risoluzione dello schermo.

Va da sé che un sistema europeo siffatto dovrebbe essere in grado di trasmettere informazioni sufficientemente articolate, tali da consentire il rispetto dei requisiti di specificità del consenso previsti dall'art. 6, par. 1, lett. a) GDPR e dall'art. 8, par. 2 della Carta di Nizza.

La Proposta in esame sta suscitando un vivace dibattito. Se, da un lato, l'obiettivo dichiarato dalla Commissione è quello di semplificare l'esperienza di navigazione degli utenti e ridurre gli effetti della c.d. *consent fatigue* derivanti dalla proliferazione dei cookie banner, dall'altro lato non mancano perplessità circa il rischio di una vera e propria delegittimazione di tali strumenti. Sebbene spesso percepiti come invasivi o ridondanti, i cookie banner continuano a rappresentare lo strumento tramite il quale l'interessato è posto nelle condizioni di conoscere e valutare le conseguenze del trattamento.

II. Osservazioni conclusive e prospettive

L'analisi svolta consente di formulare alcune considerazioni di carattere generale che trascendono le singole modifiche introdotte dal Digital Omnibus e investono, più in profondità, la traiettoria attuale della regolazione europea del digitale.

La questione centrale non riguarda, infatti, la legittimità dell'obiettivo di semplificazione in sé considerato. In un ecosistema normativo caratterizzato dalla stratificazione di fonti, dalla sovrapposizione di obblighi e dalla crescente complessità degli adempimenti, l'esigenza di rendere il quadro regolatorio più chiaro, coerente e accessibile appare non solo condivisibile, ma in molti casi necessaria. Un diritto eccessivamente complesso rischia di diventare privo di effetti tanto per i destinatari delle norme quanto per le autorità chiamate ad applicarle.

[89] Do Not Track (DNT) è una tecnologia web che permette agli utenti di decidere autonomamente se vogliono che le loro visite sui siti web siano registrate da software di tracciamento. V. https://www.digitale.co/sicurezza-it/do-not-track.

Ciò che emerge dal Digital Omnibus è, tuttavia, qualcosa di diverso dalla mera semplificazione. La Proposta sembra inserirsi in una più ampia trasformazione del linguaggio e delle priorità dell'azione normativa europea, nella quale la semplificazione assume progressivamente i tratti di una categoria retorica capace di ricomprendere interventi eterogenei, accomunati non tanto dalla riduzione della complessità normativa quanto dalla ridefinizione del punto di equilibrio tra competitività economica e tutela dei diritti fondamentali.

Sotto questa prospettiva, la semplificazione cessa di essere una tecnica legislativa e diviene una narrazione. Una narrazione che presenta come meri interventi di razionalizzazione modifiche destinate, in realtà, a incidere sull'ambito applicativo delle garanzie esistenti, ad ampliare gli spazi di utilizzazione dei dati personali e ad attenuare alcuni meccanismi di accountability che hanno caratterizzato il modello europeo di regolazione digitale sin dalla sua origine.

Il Digital Omnibus costituisce, in tal senso, un osservatorio privilegiato. Molte delle modifiche esaminate non si limitano a chiarire norme incerte o a coordinare discipline sovrapposte, ma intervengono su concetti strutturali del sistema, dalla nozione di dato personale alle basi giuridiche del trattamento, dai diritti degli interessati agli obblighi di trasparenza, producendo effetti che travalicano la dimensione della semplificazione amministrativa. Il rischio è che, sotto l'etichetta della riduzione degli oneri, si realizzi una progressiva normalizzazione dell'idea secondo cui le garanzie possano essere ridimensionate ogniqualvolta vengano percepite come ostacolo alla competitività.

In definitiva, il Digital Omnibus solleva un interrogativo che va oltre il settore della protezione dei dati personali e dell'intelligenza artificiale: se la semplificazione debba essere intesa come strumento per rendere più efficace la tutela dei diritti oppure come veicolo attraverso cui ridimensionarne la portata. È proprio su questo terreno che si misurerà il futuro della regolazione digitale europea. Se la competitività diviene il parametro esclusivo dell'azione normativa, il rischio è che l'Unione rinunci progressivamente a quel modello di costituzionalismo digitale che, negli ultimi anni, ne ha rappresentato uno dei principali elementi distintivi nel panorama globale.