Quaderni AISDUE - Rivista quadrimestrale
ISSN 2975-2698 - Fascicolo n. 1/2026

BlogDUE

# Il *Digital Omnibus* e le principali proposte di modifica al GDPR: semplificazione normativa o progressiva erosione del diritto alla protezione dei dati personali?

Lorenzo Di Anselmo (Borsista di ricerca *post-doc* in diritto dell'Unione europea, Università di Roma "La Sapienza") – 25 febbraio 2026



**1.** Il 19 novembre 2025, la Commissione europea ha presentato il *Digital Omnibus Package*, ossia un pacchetto di proposte legislative volto a semplificare il quadro normativo in ambito digitale. Tale pacchetto si articola in due proposte di regolamento: da un lato, il *Digital Omnibus* (COM (2025) 837final), che riunisce le modifiche al regolamento (UE) 2016/679 (GDPR), alla direttiva 2002/58/CE (direttiva *ePrivacy*), alla direttiva (UE) 2022/2555 (direttiva NIS 2) e al regolamento (UE) 2023/2854 (*Data Act*); dall'altro, il *Digital Omnibus* sull'intelligenza artificiale (COM (2025) 836final), che interviene su taluni aspetti specifici del regolamento (UE) 2024/1689 (*AI Act*). Secondo quanto affermato dalla Commissione, le iniziative si propongono, nel loro insieme, di razionalizzare il quadro normativo nel settore digitale, nella convinzione che la sua progressiva stratificazione abbia generato incertezza giuridica e aumentato gli oneri amministrativi a carico delle imprese, specialmente quelle di piccole dimensioni, ostacolando l'innovazione tecnologica. Dopo anni di intensa attività regolatoria, tale scenario inaugura, se non una rivoluzione, quantomeno un'inversione di tendenza degna di nota.

Da questo punto di vista, il pacchetto si inserisce nel contesto di una complessiva strategia di razionalizzazione normativa promossa dalla Commissione sulla scia della pubblicazione, a settembre 2024, del rapporto di Mario Draghi sul futuro della competitività europea, il quale individuava nell'eccessiva regolamentazione uno dei fattori suscettibili di frenare la

crescita economica dell'Unione europea (per una lettura critica del rapporto si rinvia a N. DIVISSENKO, *From Draghi Report to the European Commission's Regulatory Agenda: Regulatory Transformation or Deregulation?*, in *European Law Blog*, 26 March 2025). Per affrontare le criticità evidenziate in quella sede, la Commissione, nel contesto della c.d. "Bussola per la competitività" adottata a gennaio 2025, ha reso nota l'intenzione di snellire la burocrazia e gli obblighi di conformità imposti alle imprese in vari ambiti al fine di accelerare lo sviluppo industriale e il progresso tecnologico (per un commento della *Bussola*, cfr. M. MARESCA, *Il "Competitiveness Compass" della Commissione europea*, in questa *Rivista*, n. 1, 2025, p. 417 ss.).

Tale approccio, associando semplificazione normativa e promozione della competitività, rischia di dare il via a una stagione di deregolamentazione suscettibile di ridimensionare il livello di protezione dei diritti fondamentali garantito dal diritto dell'Unione. Sotto questo profilo, il pacchetto *Omnibus I* presentato a febbraio 2025, il quale si propone di restringere l'ambito di applicazione soggettivo della direttiva (UE) 2024/1760 sulla *due diligence* aziendale e della direttiva (UE) 2022/2464 sulla rendicontazione sostenibile, rinviandone al contempo i tempi di attuazione, costituisce un precedente tutt'altro che rassicurante (per un'analisi esaustiva delle modifiche proposte, cfr., *ex multis*, A. BONFANTI, *EU Corporate Sustainability at a Crossroads: the Omnibus Proposal to Amend the EU Directive on Corporate Sustainability Due Diligence and Its Ongoing Negotiation*, in *Diritti umani e diritto internazionale*, 2025, p. 532 ss.; E. CORCIONE, *Meno diritti umani, più competitività? Alcune considerazioni sul pacchetto Omnibus proposto dalla Commissione europea*, in *SIDIBlog*, 17 marzo 2025; M. FERRARI, *È tempo di competitività in UE: un nuovo sguardo alla direttiva due diligence*, in questa *Rivista*, n. 2, 2025, p. 97 ss.).

Lo slancio verso la competitività, anche a costo di snellire i vincoli normativi nei confronti dei soggetti privati operanti nel mercato, ha parimenti ispirato il *Digital Omnibus Package*. Mentre alcune modifiche proposte, configurando dei meri adeguamenti tecnici, ci sembrano condivisibili – ci si riferisce, ad esempio, al chiarimento circa la nozione di "ricerca scientifica" ai sensi del GDPR – altre, intervenendo su taluni aspetti sostanziali dell'*acquis* in materia digitale, sollevano maggiori criticità. È il caso di buona parte delle modifiche proposte in relazione al GDPR, su cui, pertanto, si intende porre l'attenzione in questa sede.

Sebbene siano state rimosse alcune delle modifiche più discutibili presenti in una prima bozza circolata sugli organi di stampa – come la previsione secondo cui la nozione di "dati particolari" di cui all'art. 9 del GDPR dovesse estendersi solo ai dati che rivelassero *direttamente* informazioni sensibili – la proposta presentata dalla Commissione appare comunque destinata ad incidere in modo significativo sulla portata degli obblighi di protezione dei dati stabiliti dal regolamento. A tal proposito, dopo aver ricostruito rapidamente il dibattito da cui prende le mosse la proposta di riforma del GDPR, ci si soffermerà su tre aspetti del *Digital Omnibus* ritenuti di particolare interesse: la nuova definizione di "dati personali" di cui all'art. 4,

par. 1; la disciplina relativa al trattamento dei dati nel contesto dello sviluppo e del funzionamento dei sistemi di intelligenza artificiale (IA); le limitazioni all'esercizio del diritto di accesso ai dati personali sancito dall'art. 15.

**2.** Il GDPR è notoriamente considerato un esempio virtuoso di regolamentazione del sistema di protezione dei dati personali. Chiaramente, il rapido avanzamento delle tecnologie digitali rende inevitabile un aggiornamento del tessuto normativo anche in questo settore. Tale esigenza riflette, del resto, la *ratio* del regolamento in parola, la quale si sostanzia nella necessità di assicurare un adeguato bilanciamento tra gli interessi dei titolari del trattamento e i diritti di protezione degli utenti coinvolti (sul punto, cfr. F. FERRI, *Il bilanciamento dei diritti fondamentali nel mercato unico digitale*, Torino, 2022, p. 269 ss.). Va da sé che siffatto equilibrio possa mutare in ragione delle sfide poste dall'innovazione tecnologica, purché tale evoluzione non si traduca in un indebolimento degli *standard* di protezione garantiti agli individui, in conformità all'art. 8 della Carta dei diritti fondamentali (A. FIORENTINI, *The Protection and Free Movement of Personal Data in the EU: An Evolving Legal Framework*, in C. SCHEPISI, V. CAPUANO, S. LATTANZI (eds.), *An Introduction to Digital Data Law in the EU Regulatory Framework and Future Perspectives*, Turin, 2025, p. 17). Ragion per cui qualsiasi modifica al GDPR dovrebbe essere attentamente ponderata, nonché orientata a risolvere le eventuali criticità individuate.

A tal proposito, viene da chiedersi in che misura le motivazioni alla base del *Digital Omnibus*, da un lato, siano supportate da evidenze concrete, dall'altro, trovino effettivo riscontro nelle modifiche proposte dalla Commissione. Sotto il primo profilo, né il già citato Rapporto Draghi, né la relazione della Commissione che accompagna la proposta di regolamento, spiegano in che modo il GDPR sarebbe di ostacolo all'innovazione e allo sviluppo economico. Il Rapporto si limita a segnalare soltanto un'eccessiva "frammentazione" nell'attuazione del regolamento tra i vari Paesi membri (p. 69), mentre la Commissione riconosce che gli *stakeholders* abbiano generalmente ritenuto il GDPR "equilibrato e solido e […] adatto allo scopo", sebbene le imprese e le associazioni di minore entità abbiano manifestato talune "preoccupazioni" in merito all'applicazione di alcuni degli obblighi previsti (COM (2025) 837final, cit., pp. 6-7). Da tale scenario deriva una richiesta di semplificazione normativa che, tuttavia, sembra aver indirizzato solo parzialmente l'iniziativa della Commissione.

Per semplificazione si intende, solitamente, il processo legislativo finalizzato a ridurre le incongruenze e le duplicazioni normative, senza alterare lo scopo essenziale e gli obiettivi di una norma (S. TODESCHINI, *The Great EU Reversal: Fast-Track Deregulation and the Erosion of Europe's Sustainability Ambition with the Omnibus I Regulation*, in *European Law Blog*, 27 October 2025). Ebbene, salvo alcune eccezioni – ci si riferisce, ad esempio, all'istituzione di un punto unico di accesso per la notifica dei *data breach* da parte delle entità che gestiscano dati personali, nonché alla centralizzazione, in capo al Comitato europeo per la protezione dei dati

(EDPB), del compito di redigere un elenco delle tipologie di trattamenti soggetti all'obbligo di una valutazione d'impatto sulla protezione dei dati *ex* art. 35 GDPR – il pacchetto non prevede modifiche puntuali volte a rispondere alle esigenze delle aziende di piccole dimensioni. Piuttosto, riguardando questioni strutturali relative alla *governance* dei dati, le modifiche proposte sembrano orientate a favorire una compressione generalizzata degli obblighi previsti: un'evoluzione di cui beneficerebbero soprattutto le aziende che trattano grosse quantità di dati (H. RUSCHEMEIER, *Reforming the GDPR Dilution or Progress?*, in *VBlog*, 10 July 2025).

**3.** La proposta presentata dalla Commissione interviene, innanzitutto, sulla nozione di "dati personali" sancita all'art. 4, par. 1, GDPR. Allo stato attuale, tale disposizione qualifica come dato personale "qualsiasi informazione riguardante una persona fisica identificata o identificabile". Dal momento che nell'ecosistema digitale si moltiplicano le tracce lasciate da ciascun individuo, tale definizione, volutamente ampia, ha permesso alla Corte di includere nel concetto di "dati personali" un'ampia gamma di informazioni, come ad esempio gli indirizzi IP degli utenti di Internet (sentenza della Corte del 19 ottobre 2016, causa C-582/14, *Breyer*). In estrema sintesi, se è possibile collegare un'informazione a un soggetto, oppure risalire a quest'ultimo aggregando dati apparentemente non correlati, anche se *non* in possesso di una sola persona (sentenza *Breyer*, cit., punto 43), siffatte informazioni costituiscono dati personali ai sensi del GDPR (sulla definizione di "dato personale" nel quadro del GDPR, cfr., *ex multis*, L. A. BYGRAVE, L. TOSONI, *Article 4(1). Personal data*, in C. KUNER, L. A. BYGRAVE, C. DOCKSEY (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford, 2020, p. 103 ss.; M. COPPOLA, F. GUERRIERI, *Art. 4. Definizioni*, in G. M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, Milano, 2018, p. 30 ss.).

Ferma restando detta definizione generale, la proposta aggiunge una disposizione volta a precisare che le informazioni relative a una persona fisica non configurino dati personali per una determinata entità qualora quest'ultima non sia in grado "di identificare la persona fisica cui si riferiscono le informazioni, tenendo conto dei mezzi di cui tale entità si può ragionevolmente avvalere". Detto altrimenti, nel caso in cui non disponga di mezzi adeguati ad identificare una persona, il titolare del trattamento può trattare i dati di quest'ultima in quanto anonimi.

Se la riforma venisse approvata nei termini proposti dalla Commissione, la nozione di dati personali acquisirebbe una connotazione dinamica, giacché verrebbe associata a un parametro soggettivo basato sui mezzi a disposizione di un'entità per identificare un individuo in modo "ragionevolmente" prevedibile. In altre parole, la modifica suggerita dalla Commissione ridefinisce il concetto di "identificabilità" – criterio fondamentale ai fini della qualificazione di un'informazione come dato personale – intesa non più come un rischio ipotetico, bensì come un'eventualità correlata alle effettive capacità del titolare del trattamento. Di conseguenza, per valutare la natura dei dati, è

necessario verificare se l'entità che ne è in possesso disponga di mezzi idonei (intesi come l'insieme di risorse economiche, manodopera e tecnologie disponibili) a risalire all'identità del soggetto cui i dati si riferiscono. In quest'ottica, la qualificazione di un dato come "personale" non deriverebbe da una valutazione oggettiva correlata alla natura stessa dell'informazione in questione, bensì dipenderebbe dalle caratteristiche specifiche dell'entità che ne è in possesso. Siffatta impostazione, integrando la prospettiva del titolare nella definizione di "dato personale", allo stato attuale ispirata primariamente ad esigenze di protezione dell'individuo, appare suscettibile di restringere la portata applicativa dell'art. 4, par. 1, GDPR, sinora interpretata in modo piuttosto estensivo dal giudice dell'Unione (cfr. F. ROSSI DAL POZZO, L. ZOBOLI, *To protect or (not) to protect: definitional complexities concerning personal (and non-personal) data within the EU*, in rivista.eurojus.it, n. 1, 2021, p. 315 ss.).

A prima vista, la modifica proposta sembrerebbe, invero, in linea con la giurisprudenza della Corte. In *GEPD/SRB*, infatti, i giudici di Lussemburgo hanno elaborato un'interpretazione contestuale della nozione di dati personali, escludendo che i dati pseudonimizzati vadano considerati, "in ogni caso e per qualsiasi persona", dati personali ai sensi del GDPR (sentenza della Corte del 4 settembre 2025, causa C-413/23 P, punto 86). Siffatta affermazione si basava, tuttavia, sulle circostanze specifiche della vicenda all'origine della controversia. In quel caso, infatti, i dati erano stati modificati dal titolare in modo tale che non fosse effettivamente più possibile, per il destinatario, associarli ad alcuna persona fisica: in simili circostanze, tali dati non rientrano, con riferimento all'attività del destinatario, nell'ambito di applicazione del GDPR (per un commento, si rinvia a P. G. CHIARA, *The Court of Justice Upholds a Relative Approach to EU Data Protection Law*, in EDPL, 2025, p. 566 ss.; T. S. CABRAL, *Relative or Objective: The End of the Saga Concerning the Interpretation of The Concept of Personal Data: SRB v. EDPS (C-413/23)*, in eulawlive.com, 11 September 2025). Viceversa, la proposta della Commissione eleva il *test* elaborato in *GEPD/SRB* a criterio generale volto ad integrare la definizione stessa di dati personali, circoscrivendone *a priori* il perimetro applicativo. Senza considerare, peraltro, che la proposta intende autorizzare la Commissione a rivedere tale definizione attraverso l'adozione di atti di esecuzione, aggiungendo ulteriore incertezza giuridica (art. 41 *bis*). Dal momento che la distinzione tra dati personali e *non* costituisce l'asse portante dell'impianto regolatorio stabilito dal GDPR, modificare nei termini proposti detto regolamento rischia di ridurre la quantità di dati nei confronti dei quali si applichino gli obblighi di protezione in favore degli utenti (F. BEIKER, *Schroedinger's data: SRB and the Digital Omnibus*, in European Law Blog, 20 January 2026).

Letta isolatamente, la modifica proposta dalla Commissione appare condivisibile: se un'entità è priva dei mezzi che le consentano di identificare un soggetto, esonerarla dalle responsabilità gravanti sul titolare del trattamento risponde a un criterio di ragionevolezza. Da una prospettiva

sistemica, tuttavia, la revisione delineata dal *Digital Omnibus* suscita maggiori perplessità.

In primo luogo, l'art. 11 del GDPR già differenzia le responsabilità del titolare nell'ipotesi in cui il trattamento non richieda l'identificazione, rendendo inapplicabili i diritti conferiti all'interessato ai sensi degli artt. 15-20 (sul punto, cfr. N. CHAUDHURI, *Must "personal data" always be "relative"?*, in *European Law Blog*, 13 May 2025): sotto questo profilo, la modifica rischia di complicare inutilmente il quadro normativo (in tal senso, cfr. S. STALLA-BOURDILLON, *Déjà vu in data protection law: the risks of rewriting what counts as personal data*, in *Privacy and Data Protection*, n. 2, 2025, p. 9 ss.).

In secondo luogo, occorre ricordare che la pseudonimizzazione rientra tra le tecniche cui può ricorrere il titolare per contrastare i rischi intrinseci connessi al trattamento dei dati, in conformità all'art. 24 del GDPR (cfr. F. BIEKER, *The Right to Data Protection. Individual and Structural Dimensions of Data Protection in EU Law*, The Hague, 2022, pp. 195-202). Lo ha ribadito la Corte nella già citata sentenza *GEPD/SRB*, evidenziando che la pseudonimizzazione non configura un "elemento della definizione dei dati personali", ma costituisce una pratica finalizzata a "ridurre il rischio di mettere in correlazione un insieme di dati con l'identità degli interessati" (sentenza *GEPD/SRB*, cit., punto 72). Detto altrimenti, sebbene possa influire sull'applicabilità del GDPR, la pseudonimizzazione non rappresenta un mezzo in grado di esonerare il titolare e il responsabile del trattamento dal rispettare i propri obblighi di protezione dei dati, bensì, al contrario, uno strumento volto ad agevolare l'adempimento degli obblighi ad essi incombenti (GDPR, considerando n. 28). Orbene, se l'art. 4, par. 1, GDPR, venisse modificato nei termini proposti dalla Commissione, le entità potrebbero sostenere di non avere sufficienti mezzi di reidentificazione, con la conseguenza di trattare dati pseudonimizzati al di fuori del GDPR, con effetti pregiudizievoli per i diritti degli interessati (cfr. H. RUSCHEMEIER, *The Omnibus Package of the EU Commission. Or How to Kill Data Protection Fast*, in *VBlog*, 17 November 2025).

Le implicazioni di un simile scenario sarebbero significative. Non costituendo dati personali per l'entità che le possiede, tali informazioni potrebbero essere condivise con entità terze potenzialmente capaci di risalire all'identità degli interessati: secondo quanto proposto dalla Commissione, tale operazione non avrebbe l'effetto di rimettere in discussione la natura dei dati in controllo della prima entità. Infatti, ai sensi dell'art. 4, par. 1, GDPR, come modificato dalla proposta di regolamento *Omnibus*, le informazioni non diventano personali per un'entità per il solo fatto che un destinatario successivo disponga di "mezzi di cui si può ragionevolmente avvalere per identificare la persona fisica cui le informazioni si riferiscono". Ebbene, tale disposizione contraddice la giurisprudenza della Corte secondo cui il carattere *impersonale* di taluni dati non esclude *in toto* che essi possano acquisire carattere "personale", qualora il titolare del trattamento li metta a disposizione di altre entità "ragionevolmente" in grado di identificare l'interessato

(sentenza della Corte del 9 novembre 2023, causa C-319/22, *Gesamtverband Autoteile-Handel*, punto 49): in questo contesto, i dati presentano un carattere personale "tanto per tali persone quanto, indirettamente, per il titolare del trattamento" (sentenza *GEPD/SRB*, cit., punto 84). Su tali aspetti, cfr. D. KORFF, *Digital Omnibus: Proposed Changes to the Definition of Personal Data in the EU GDPR Analysed in the Light of the SRB and Earlier CJEU Judgments*, in *SSRN*, 9 December 2025, pp. 6-7).

Per effetto del *Digital Omnibus*, le eventuali capacità identificative del destinatario successivo risulterebbero, invece, del tutto irrilevanti. Nell'epoca governata dalle reti virtuali, in cui enormi quantità di dati circolano globalmente con grande velocità, siffatto approccio sottovaluta i pericoli derivanti dai casi di identificabilità secondaria (cfr. H. RUSCHEMEIER, *The Omnibus Package of the EU Commission*, cit.). Dal momento che lo sfruttamento dei dati costituisce una delle maggiori fonti di profitto degli operatori economici attivi nel mercato digitale, *in primis* le piattaforme *online* (F. BATTAGLIA, *What "Data" Really are in the Digital Market. Some Reflections on their Relevance and Value under EU Law*, in *Ordine internazionale e diritti umani*, 2024, p. 218), la prospettiva delineata nel *Digital Omnibus* indebolirebbe ulteriormente la posizione degli utenti.

**4.** Il *Digital Omnibus* introduce talune disposizioni volte a facilitare il trattamento dei dati personali nel contesto del ciclo di vita dei sistemi di IA. Come noto, lo sviluppo dell'IA ha sempre sollevato perplessità in termini di conformità al quadro normativo in materia di protezione dei dati, giacché la prospettiva incentrata sull'individuo alla base del GDPR mal si concilia con il massiccio impiego di dati che caratterizza l'addestramento e il funzionamento dei sistemi di IA (al riguardo, cfr, *ex multis*, C. GRIECO, *Intelligenza Artificiale e tutela degli utenti nel diritto dell'Unione europea*, Napoli, 2023, p. 103 ss.; G. CONTALDI, *Intelligenza artificiale e dati personali*, in *Ordine internazionale e diritti umani*, 2021, p. 1193 ss.; T. Z. ZARSKY, *Incompatible: the GDPR in the Age of Big Data*, in *Seton Hall Law Review*, 2017, p. 995 ss.). Tale tensione è particolarmente evidente allorché si tratti di individuare, in conformità all'art. 6, par. 1, GDPR, la base giuridica in grado di legittimare il trattamento dei dati ai fini dello sviluppo dell'IA. Ne è una riprova la vicenda che ha coinvolto ChatGPT in Italia nel 2023: come si ricorderà, il Garante per la protezione dei dati personali ordinò ad OpenAI di limitare temporaneamente il trattamento dei dati personali degli utenti italiani, sul presupposto che la raccolta dei dati ai fini dell'addestramento del modello avvenisse in assenza di un'adeguata base giuridica (per un commento, cfr. O. POLLICINO, *Generative AI and the rediscovery of the legitimate interest clause*, in *IEP@BU*, 25 January 2024).

Gran parte dei sistemi di IA, in particolar modo i c.d. modelli generativi, utilizzano un'ampia quantità di dati estrapolati direttamente dalla rete, rendendo difficilmente applicabile, in tale contesto, il requisito del consenso di cui all'art. 6, par. 1, lett. *a*), GDPR. Ne consegue che, in simili circostanze, il trattamento debba fondarsi necessariamente sul legittimo interesse del

titolare, in conformità all'art. 6, par. 1, lett. *f*). Detta disposizione presuppone, come noto, il rispetto di tre condizioni cumulative: in primo luogo, deve sussistere il perseguimento di un legittimo interesse da parte del titolare o del terzo a cui i dati vengono comunicati; in secondo luogo, il trattamento deve essere necessario al perseguimento del legittimo interesse, nel senso che quest'ultimo non potrebbe essere raggiunto attraverso altri mezzi meno pregiudizievoli per i diritti degli interessati; infine, i diritti dell'interessato non debbono prevalere sul legittimo interesse del responsabile del trattamento o di terzi (cfr., *ex multis*, sentenza della Corte del 17 giugno 2021, causa C-597/19, *M.I.C.M.*, punto 106). Siffatto *test*, implicando un bilanciamento tra interessi contrapposti, presuppone una valutazione ancorata alle circostanze specifiche del caso, in quanto tale difficilmente replicabile nel contesto delle tecnologie ad alta intensità di dati (H. RUSCHEMEIER, *Generative AI and Data Protection*, in *Cambridge Forum on AI: Law and Governance*, 2025, p. 1 ss.).

Per ovviare a tali criticità, il *Digital Omnibus* introduce *ex novo* l'art. 88 *quater*, il quale stabilisce che, qualora risulti necessario ai fini dello sviluppo e del funzionamento dei sistemi di IA, il trattamento dei dati personali possa fondarsi sul legittimo interesse del titolare ai sensi dell'art. 6, par. 1, lett. *f*), GDPR, purché sia rispettato il principio della minimizzazione dei dati e sia assicurato il diritto di opposizione *ex* art. 21 in capo ai soggetti interessati. Non vi sono dubbi che la nozione di legittimo interesse possa ricomprendere le finalità commerciali riconducibili all'esercizio della libertà di impresa di cui all'art. 16 della Carta (sul punto, cfr. EDPB, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR*, adopted on 8 October 2024, p. 7). Ciò non toglie, tuttavia, che sia compito del titolare, sotto la propria responsabilità, verificare di volta in volta l'invocabilità del legittimo interesse quale base giuridica per l'utilizzo dei dati, sulla base di un'attenta ponderazione degli interessi in gioco (al riguardo, cfr. EDPB, *parere 28/2024 su taluni aspetti relativi alla protezione dei dati ai fini del trattamento dei dati personali nel contesto dei modelli di IA*, adottato il 17 dicembre 2024, p. 25 ss.). Come evidenziato dalla Corte in *Meta Platforms*, tale valutazione acquisisce assoluta rigidità nell'ecosistema digitale, giacché gli operatori attivi nel mercato digitale, in particolar modo le piattaforme, potrebbero avere accesso a "dati potenzialmente illimitati", amplificando l'impatto delle attività di trattamento sui diritti degli utenti (sentenza della Corte del 4 luglio 2023, causa C-252/21, *Meta Platforms*, punto 118. Per un commento della sentenza, cfr. P. J. VAN DE WAERDT, *Meta v Bundeskartellamt: Something Old, Something New*, in *europeanpapers.eu*, 2024, p. 1077 ss.; F. BATTAGLIA, *La sentenza Meta Platforms: riflessioni in materia di valore dei dati e libera espressione del consenso*, in *Ordine internazionale e diritti umani*, 2023, p. 723 ss.). La modifica prevista dall'*Omnibus* rischia, viceversa, di trasformare il legittimo interesse in una scorciatoia volta ad agevolare il trattamento indifferenziato di dati di massa.

Tale scenario normativo deve essere letto in parallelo alla proposta di revisione dell'art. 9 del GDPR, il quale disciplina il trattamento di categorie particolari di dati personali. Allo stato attuale, detta disposizione stabilisce un

divieto generale di trattamento – la cui portata applicativa si estende, peraltro, a tutte le informazioni suscettibili di rivelare anche *indirettamente* i dati sensibili dell'interessato (sentenza *Meta Platforms*, cit., punto 73) – fatta eccezione per le ipotesi previste dal par. 2. Al riguardo, il *Digital Omnibus* introduce un'ulteriore eccezione (lett. *k*), autorizzando il trattamento di tali dati nel contesto dello sviluppo e del funzionamento dei sistemi di IA.

Vero è che, ai sensi dell'art. 9, par. 5, GDPR, come modificato dalla proposta di regolamento *Omnibus*, il titolare sia tenuto ad adottare le "misure organizzative e tecniche adeguate" ad evitare il trattamento dei dati in questione, cosicché il loro utilizzo possa ritenersi lecito solo qualora la relativa rimozione richiederebbe uno "sforzo sproporzionato" da parte del titolare. Siffatta impostazione non offre, tuttavia, adeguate garanzie sotto il profilo della protezione dei dati: le entità, infatti, potranno giustificare l'impiego di dati sensibili per finalità di addestramento e convalida dei sistemi di IA semplicemente adducendo motivazioni di carattere tecnico o finanziario. Concepito in questi termini, il *test* delineato dalla disposizione *de qua* tiene conto soltanto delle esigenze operative dello sviluppatore o utilizzatore del modello di IA, senza alcuna considerazione dei diritti delle persone cui le informazioni sensibili si riferiscono.

**5.** Il *Digital Omnibus* introduce, infine, talune limitazioni all'esercizio del diritto di accesso ai dati personali di cui all'art. 15 del GDPR. Al riguardo, la modifica proposta dalla Commissione appare destinata ad ampliare il novero dei casi in cui l'accesso ai dati possa essere legittimamente respinto dal titolare. La questione è tutt'altro che marginale, posto che il diritto di accesso costituisca, come noto, un pilastro della normativa dell'Unione in materia di protezione dei dati, essendo funzionale all'esercizio di altri diritti da parte dell'interessato, come quello di rettifica, cancellazione e limitazione del trattamento (cfr., *ex multis*, sentenza della Corte del 27 febbraio 2025, causa C-203/22, *Dun & Bradstreet Austria*, punto 54).

Allo stato attuale, le richieste possono essere respinte solo allorché risultino "manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo" (art. 12, par. 5, GDPR). Come chiarito dai giudici di Lussemburgo, detta disposizione riflette un principio generale del diritto dell'Unione, volto ad evitare l'esercizio abusivo dei diritti conferiti a singoli dall'ordinamento sovranazionale (sentenza della Corte del 9 gennaio 2025, causa C-416/23, *Österreichische Datenschutzbehörde*, punto 49. Sulla rilevanza di tale principio nell'ordinamento dell'Unione, cfr. L. PANTALEO, *Abuse of Law in the European Union. The Rise of a Special General Principle*, The Hague, 2025). Ne consegue che vadano ritenute inammissibili le richieste finalizzate ad arrecare intenzionalmente un pregiudizio al titolare del trattamento: al di fuori di queste ipotesi, il diritto di accesso non incontra limiti sostanziali, neanche qualora le richieste dell'interessato risultino particolarmente gravose per il titolare, alla luce dei mezzi a sua disposizione (al riguardo, cfr. EDPB, *Guidelines 01/2022 on data subject rights - Right of access*, adopted on 28 March 2023, p. 51 ss.).

In base alla modifica contenuta nella proposta di regolamento *Omnibus*, il rifiuto dovrebbe estendersi ai casi in cui l'interessato eserciti i propri diritti ai sensi del GDPR "per finalità diverse dalla protezione dei suoi dati". A prima vista, tale precisazione sembrerebbe codificare la giurisprudenza poc'anzi richiamata. Una lettura più attenta suggerisce, tuttavia, maggiore cautela. In effetti, detta disposizione potrebbe essere interpretata nel senso di ritenere manifestamente infondate o eccessive non solo le richieste propriamente abusive, ma anche quelle che presentino finalità diverse dalla protezione dei dati in senso stretto. Una simile impostazione si discosterebbe dalla giurisprudenza della Corte, la quale ha privilegiato un'interpretazione autonoma del diritto di accesso, svincolandone l'esercizio dalle ragioni che ne costituiscano il presupposto.

Al riguardo, infatti, i giudici dell'Unione hanno stabilito che la possibilità di avere accesso ai propri dati prescinda dalle motivazioni che hanno indotto l'interessato a presentare la richiesta (sentenza della Corte del 26 ottobre 2023, causa C-307/22, *FT*, punto 38. Per un commento, cfr. G. DI FEDERICO, *From Dusk Till Dawn. The Case of* F.T. v D.W. *and the Right to Access Electronic Medical Records in Light of the Future European Health Data Space Regulation*, in *europeanpapers.eu*, 2024, p. 463 ss.). Ciò, del resto, è coerente con l'art. 8, par. 2, della Carta, il quale qualifica il diritto di accesso come un diritto autonomo, il cui esercizio è volto a permettere all'interessato di "effettuare le necessarie verifiche" circa la liceità del trattamento (sentenza della Corte del 17 luglio 2014, cause riunite C-141/12 e C-372/12, *YS e a.*, punto 44). Ritenere fondate solo le richieste di accesso finalizzate alla protezione dei dati significa, di fatto, autorizzare i titolari a richiedere all'interessato di motivare la propria istanza: uno scenario incompatibile con l'essenza del diritto fondamentale alla protezione dei dati (in tal senso, cfr. R. MAHIEU, *The Ominous Omnibus. Dismantling the Right of Access to Personal Data*, in *VBlog*, 3 December 2025).

Vero è che il GDPR già consenta al titolare di rivolgersi all'interessato affinché precisi "l'informazione o le attività di trattamento cui la richiesta si riferisce" (considerando n. 63). Tale circostanza rileva, tuttavia, allorché il titolare tratti una notevole quantità di dati dell'interessato, cosicché non sia agevole desumere se la richiesta di accesso abbia ad oggetto *tutti* i dati trattati o *tutti* i settori di attività del titolare. Come chiariscono le linee guida dell'EDPB, si tratta, in sostanza, di una misura a tutela dell'interessato, affinché quest'ultimo riceva effettivamente le informazioni desiderate, senza trovarsi costretto a gestire un'eccedenza di informazioni, rispetto alle quali potrebbe non avere familiarità (EDPB, *Guidelines 01/2022 on data subject rights*, cit., p. 16). Ne è una riprova il fatto che l'interessato possa, in ogni caso, rifiutarsi di dar seguito alla richiesta indirizzatagli dal titolare (*ivi*, p. 17).

La modifica proposta dalla Commissione sembra, viceversa, maggiormente orientata a snellire gli oneri gravanti sul titolare. Non a caso, nel preambolo che accompagna la proposta di regolamento *Omnibus*, si precisa che, nell'agire ai sensi dell'art. 15 del GDPR, l'interessato dovrebbe essere "quanto più specifico possibile", mentre le richieste di accesso "troppo

ampie e generiche" dovrebbero essere respinte in quanto eccessive (COM (2025) 837 final, cit., par. 35). Eppure, non possono escludersi situazioni in cui l'interessato, non avendo contezza dei dati effettivamente detenuti dal titolare, sia incapace di specificare la sua richiesta (R. MAHIEU, *op. cit.*). In questo modo, da strumento teso a facilitare l'adempimento, da parte del titolare, dell'obbligo ad esso incombente di agevolare l'esercizio del diritto di accesso (art. 12, par. 2, GDPR), la circostanza per cui il titolare possa rivolgersi all'interessato prima di fornirgli le informazioni richieste rischia di trasformarsi in un mezzo a sua disposizione per respingere le richieste di accesso non sufficientemente motivate. Da questo punto di vista, lungi dal semplificare il dettato normativo, la modifica proposta dalla Commissione renderebbe ancora più controversa l'applicazione di una disposizione – l'art. 12, par. 5, GDPR – già di per sé piuttosto nebulosa (cfr. L. DRECHSLER, *No Justification Needed: Court of Justice Confirms Broad Application of the Right of Access under the General Data Protection Regulation (Case C-307/22, FT v DW)*, in eulawlive.com, 24 November 2023).

**6.** La negoziazione del *Digital Package Omnibus* si annuncia come uno degli appuntamenti più rilevanti dell'agenda politica dell'Unione europea del prossimo futuro. Sulla scia del Rapporto Draghi, l'Unione ha eletto la competitività a parametro guida della propria strategia politica. La via scelta, quella della semplificazione normativa, appare però problematica, sia sotto il profilo della tecnica legislativa, giacché il ricorso allo strumento del pacchetto legislativo per interventi normativi di così ampia portata solleva perplessità in termini di trasparenza e garanzie procedurali (sulla prassi dei pacchetti legislativi, cfr. P. DE PASQUALE, *Dalla flessibilità delle basi giuridiche alla normazione integrata: tecniche legislative funzionali alla rigidità del riparto di competenze nell'UE*, in *Il diritto dell'Unione europea*, 2025, p. 43 ss., spec. p. 57 ss.), sia a livello sostanziale, poiché l'impianto regolatorio delineato privilegia l'efficienza amministrativa senza prevedere sufficienti tutele sul piano dei diritti fondamentali. In un settore già caratterizzato da significative asimmetrie di potere tra utenti e operatori economici, un simile approccio indebolisce ulteriormente la posizione degli individui, rivelando una traiettoria costituzionale tutt'altro che promettente (K. FAISAL, *The Digital Omnibus and the Future of EU Digital Governance: Simplification or Strategic Dilution?*, in eulawlive.com, 16 January 2026).

La proiezione economica costituisce da sempre la principale forza propulsiva del processo d'integrazione europea. Da questo punto di vista, la riforma dell'*acquis* digitale nell'ottica di snellire gli obblighi di conformità e gli oneri amministrativi gravanti sulle imprese intercetta un'ambizione legittima dell'Unione: promuovere l'efficienza tecnica e l'innovazione tecnologica, pur senza rinunciare alla difesa del patrimonio valoriale alla base della costruzione europea, di cui anche la transizione digitale dovrebbe essere espressione (al riguardo, cfr., *ex multis*, F. FERRI, *Transizione digitale e valori fondanti dell'Unione: riflessioni sulla costituzionalizzazione dello spazio digitale europeo*, in *Il diritto dell'Unione europea*, 2022, p. 277 ss.).

Alla luce di ciò, viene da chiedersi se l'obiettivo della semplificazione possa giustificare una revisione del GDPR nel senso prospettato dal *Digital Omnibus*. Se esaminate singolarmente, le modifiche proposte dalla Commissione sembrano ragionevoli, nonché coerenti con le acquisizioni giurisprudenziali. Da una prospettiva sistemica, tuttavia, gli sviluppi normativi all'orizzonte evidenziano il rischio di un arretramento degli *standard* in materia di protezione dei dati garantiti dall'ordinamento dell'Unione. Tanto il chiarimento circa l'invocabilità del legittimo interesse quale base giuridica idonea a consentire il trattamento dei dati ai fini dello sviluppo dei sistemi di IA, quanto l'inasprimento delle ipotesi di inammissibilità delle richieste di accesso ai dati, rispondono alla medesima finalità: ricalibrare il bilanciamento degli interessi in gioco in modo più favorevole alla posizione dei titolari, penalizzando i diritti di protezione degli utenti.

Sotto questo profilo, più che risolvere le criticità affrontate dalle piccole imprese, il *Digital Omnibus* sembra allineare il GDPR alle esigenze delle aziende che già trattano massicce quantità di dati: se le modifiche proposte verranno mantenute durante l'*iter* legislativo, gli attori commerciali potranno beneficiare di un apprezzabile margine di discrezionalità per trattare i dati ai fini dello sviluppo dell'IA, nonché per respingere le richieste di accesso non sufficientemente motivate, spesso utilizzate dagli utenti quale veicolo per denunciare pratiche illecite diffuse (R. MAHIEU, *op. cit.*). Senza considerare, peraltro, che le soluzioni avanzate non convincono del tutto neanche sul piano della chiarezza normativa. La riformulazione della nozione di "dati personali", nonché l'ampliamento delle limitazioni all'esercizio del diritto di accesso, aggiungono incertezza giuridica, preparando il terreno a frequenti contenziosi tra gli utenti e le entità che ne trattano i dati (H. C. H. HOFMANN, *This Is Not Simplification. How to Simplify the Digital Acquis Without Undermining Rights*, in *VBlog*, 3 January 2026).

La semplificazione dovrebbe tendere a rafforzare la coerenza del quadro normativo, eliminando le duplicazioni e promuovendo, in definitiva, un'applicazione più uniforme e prevedibile delle regole esistenti, senza ridurne la portata applicativa (cfr. S. TODESCHINI, *op. cit.*). Al contrario – perlomeno in relazione ai profili esaminati in questa sede – il *Digital Omnibus* fa leva sulle esigenze di razionalizzazione normativa per comprimere gli obblighi di protezione stabiliti dal GDPR, senza apportare un effettivo valore aggiunto in termini di coerenza sistemica. Sul tavolo, com'è evidente, non c'è soltanto la capacità dell'Unione di tenere il passo delle economie più forti, bensì la solidità del suo sistema valoriale. Se aspira a preservare la propria *competitività* a livello globale, l'Unione non può permettersi di isolare le traiettorie dello sviluppo economico dalle garanzie costituzionali e dalla responsabilità democratica. Spetterà al legislatore il compito di fare in modo che la spinta verso l'innovazione non si traduca in un compromesso al ribasso suscettibile di erodere i valori fondamentali dell'Unione.

**ABSTRACT (ITA)**

Il contributo si propone di approfondire le principali modifiche al GDPR previste nell'ambito del *Digital Omnibus*, il pacchetto di proposte legislative presentato dalla Commissione il 19 novembre 2025. Tale pacchetto mira a semplificare il quadro normativo in ambito digitale allo scopo di promuovere la competitività e l'innovazione tecnologica a livello dell'Unione europea. Nonostante tali premesse, la proposta interviene su taluni aspetti sostanziali dell'*acquis* in materia digitale, incidendo in modo significativo sulla portata degli obblighi di protezione dei dati stabiliti dal GDPR. A tal proposito, l'analisi si concentra su tre aspetti del *Digital Omnibus* ritenuti di particolare interesse: la nuova definizione di "dati personali" di cui all'art. 4, par. 1; la disciplina relativa al trattamento dei dati nel contesto dello sviluppo e del funzionamento dei sistemi di intelligenza artificiale; le limitazioni all'esercizio del diritto di accesso ai dati personali sancito dall'art. 15.

**ABSTRACT (ENG)**

The paper aims to examine the main changes to the GDPR envisaged in the *Digital Omnibus*, the package of legislative proposals presented by the Commission on 19 November 2025. This package aims to simplify the legal framework governing the digital sector in order to promote competitiveness and technological innovation at the European Union level. Despite these premises, the proposal addresses some fundamental aspects of the digital *acquis*, affecting the scope of the data protection obligations established by the GDPR. In this regard, the analysis focuses on three aspects of the *Digital Omnibus* that are considered to be of particular interest: the new definition of "personal data" in Article 4(1); the rules on data processing in the context of the development and operation of artificial intelligence systems; and the limitations on the exercise of the right of access to personal data enshrined in Article 15.