ARRIVA IL "DIGITAL OMNIBUS": L'IMPATTO SUL GDPR DELLA PROPOSTA DI REGOLAMENTO DELLA COMMISSIONE EUROPEA PER LA SEMPLIFICAZIONE DEL QUADRO NORMATIVO UE IN AMBITO DIGITALE

1. Il contesto, gli obiettivi e ambiti di intervento della proposta di regolamento "Digital Omnibus"

Il 19 novembre 2025, la Commissione europea ha pubblicato la proposta di regolamento comunemente nota come "Digital Omnibus" (di seguito, il "**Regolamento Digital Omnibus**[1]"), finalizzata a razionalizzare e semplificare il complesso quadro normativo dell'Unione europea (di seguito, "**UE**") in materia di regolamentazione **digitale**, ridurre gli **oneri burocratici** per le imprese e pubbliche amministrazioni dell'UE, nonché facilitare l'accesso da parte di quest'ultime a **dati di alta qualità** per l'**intelligenza artificiale**.

Gli obiettivi primari che la Commissione europea si pone con il Regolamento Digital Omnibus[2] - nel solco delle indicazioni contenute nella relazione sulla competitività UE dell'ex

[1] Proposta di regolamento omnibus digitale | Plasmare il futuro digitale dell'Europa.

[2] Il Regolamento Digital Omnibus è costituito da un "pacchetto" di tre diverse iniziative, ovvero il COM (2025) 835, 836 e 837; per motivi di sintesi e semplicità verranno considerati nel presente documento come un documento unitario, salvo ove diversamente specificato.

Presidente della Banca centrale europea[3], Mario Draghi - sono, pertanto, quelli di favorire l'**innovazione** e la **competitività**, senza sacrificare gli elevati *standard* di protezione dei **diritti fondamentali**, specialmente in ambito di protezione dei **dati personali**.

L'intervento normativo si caratterizza per un approccio organico, che mira a consolidare e coordinare diverse discipline dell'*acquis* digitale dell'UE, eliminando le sovrapposizioni di norme e modificandone alcune, in particolare:

- la Direttiva 2002/58/CE e sue successive modifiche (di seguito, la "**Direttiva ePrivacy**");
- il Regolamento (UE) 910/2014 (il c.d. "EUDIW");
- il Regolamento (UE) 2016/679 (Regolamento Generale sulla Protezione dei Dati – di seguito, il "**GDPR**");
- il Regolamento (UE) 2018/1724 (il c.d. "SDG");
- il Regolamento (UE) 2018/1725 (il c.d. "EUDPR");
- la Direttiva (UE) 2022/2555 (di seguito, la "**Direttiva Nis2**");
- la Direttiva (UE) 2022/2557 (la c.d. "Direttiva Dora");
- il Regolamento (UE) 2023/2854 (di seguito, il "**Data Act**");
- il Regolamento (UE) 2024/1689 sull'intelligenza artificiale (di seguito, l' "**Ai Act**").

In aggiunta alla proposta di modifica delle normative sopracitate, il provvedimento in esame si prefigge di procedere a un accorpamento e riordino del quadro normativo dell'UE in materia di economia dei dati.

Nello specifico, il Regolamento (UE) 2022/868 (il c.d. "Data Governance Act"), la Direttiva (UE) 2019/1024 (la c.d. "Direttiva Open Data") e il Regolamento (UE) 2018/1807 Free Flow of Non-Personal Data sul libero flusso dei dati non personali (il c.d. "Free Flow of Non-Personal Data") dovrebbero sostanzialmente essere assorbiti nel Data Act.

Nel presente documento esamineremo le principali novità del Regolamento Digital Omnibus, soffermandoci sulle proposte di modifica al GDPR e alla Direttiva ePrivacy.

2. Le principali modifiche al GDPR e alla Direttiva ePrivacy

Uno degli aspetti più rilevanti del Regolamento Digital Omnibus riguarda le revisioni che esso si propone di apportare

[3] https://commission.europa.eu/topics/competitiveness/draghi-report_en.

al GDPR e, per riflesso, alla Direttiva ePrivacy, alcune delle quali destinate a incidere sull'operatività di imprese, pubbliche amministrazioni, professionisti e cittadini dell'UE, soprattutto in relazione a trattamenti non ad alto rischio.

2.1. La ridefinizione di dato personale: la proposta di modifica dell'art. 4, n.1) del GDPR

In primo luogo, il Regolamento Digital Omnibus mira a ridefinire la nozione di dato personale di cui all'**art. 4**, **n. 1)** del **GDPR**, ancorandola a un criterio di valutazione più **soggettivo** e dipendente dalle capacità concrete del titolare del trattamento di identificare il destinatario oggetto del trattamento medesimo.

Il Regolamento Digital Omnibus si propone, invero, di considerare un'informazione come dato personale non sulla base di una definizione e/o un elenco predeterminato – come previsto dalla formulazione attuale dell'art. 4, n. 1) del GDPR[4] – bensì soltanto qualora le informazioni in possesso del titolare del trattamento consentano a quest'ultimo di **identificare** effettivamente la persona fisica alla quale tali dati si riferiscono, tenendo conto dei mezzi che il titolare del trattamento potrebbe ragionevolmente utilizzare per effettuare tale identificazione.

In particolare, viene precisato che le informazioni raccolte da un determinato titolare del trattamento non dovrebbero essere considerate dati personali per tale soggetto semplicemente perché un potenziale destinatario successivo dispone di mezzi che potrebbero ragionevolmente essere utilizzati per identificare la persona fisica a cui i dati stessi si riferiscono.

Di conseguenza, lo stesso *set* di informazioni potrebbe essere qualificato come dato personale per una grande piattaforma tecnologica, ma non per una piccola impresa teoricamente priva delle risorse per effettuare l'identificazione (*rectius*: la re-identificazione[5]) dell'interessato.

[4] Per << dato personale>> si intende "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale ma solo se il soggetto che la tratta possiede i mezzi ragionevolmente utilizzabili per ricondurla a una persona fisica identificata o identificabile*"

[5] Si rileva anche che il Regolamento Digital Omnibus si propone di introdurre il nuovo articolo art. 41a del GDPR, il quale prevede di affidare alla Commissione europea il compito di adottare atti di esecuzione per specificare quali siano i mezzi e i criteri per determinare se i dati risultanti dalla pseudonimizzazione non costituiscano più dati personali per determinati soggetti, nonché di elaborare criteri e/o categorie affinché il titolare del trattamento e ciascun destinatario valutino il rischio di re-identificazione in relazione ai destinatari tipici dei dati.

Da un punto di vista pratico, è evidente che la proposta di modifica dell'art. 4, n. 1) del GDPR, laddove confermata dal Parlamento europeo e dal Consiglio europeo, potrebbe rappresentare un punto di svolta rilevante per molte imprese operanti nel territorio dello Spazio Economico Europeo: queste potrebbero essere esentate, in tutto o in parte, dagli adempimenti in materia di *data protection* qualora i mezzi a loro disposizione non fossero tali da consentire di ricondurre un'informazione, direttamente o indirettamente, a un determinato interessato.

2.2. Il trattamento per finalità di archiviazione, ricerca e pubblico interesse: la proposta di modifica dell'art.5, par. 1, lett. b) del GDPR

Il Regolamento Digital Omnibus si propone, altresì, di intervenire sulle disposizioni del GDPR relative al trattamento dei dati personali posto in essere per fini di **archiviazione nel pubblico interesse**, **ricerca scientifica**, **storica** o a **fini statistici**, attualmente regolato dal combinato disposto degli artt. 5, par. 1, lett. b), 6, par., 4[6] e 89, par. 1[7] del GDPR.

Nello specifico, il Regolamento Digital Omnibus si prefigge di consolidare la regola già prevista dall'art. 5, par. 1, lett. b) del GDPR - secondo cui il trattamento dei dati per finalità di cui in parola beneficia di una presunzione di non incompatibilità rispetto agli scopi originari della raccolta dei dati - chiarendo esplicitamente che tale presunzione si applica indipendentemente dalla sussistenza o meno delle condizioni di cui all'art. 6, par. 4 del GDPR, fatto salvo, in ogni caso, il rispetto dell'art. 89, par. 1 del GDPR.

2.3. Le nuove eccezioni al divieto di trattamento dei dati particolari: la proposta di modifica dell'art. 9 del GDPR

Un'altra revisione essenziale che la Commissione europea si propone di attuare è quella di estendere il novero delle eccezioni[8] al divieto di trattamento dei dati particolari di cui all'art. 9, par. 1, del GDPR, aggiungendo due lettere finali all'art. 9, par. 2, dello stesso, ovvero:

- la lett. k), per consentire il trattamento dei dati particolari ex art. 9, par. 1, del GDPR, nel contesto dello **sviluppo** e del

[6] Tale disposizione prescrive che, laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'UE, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento deve tener conto, tra l'altro: a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ex art. 9 del GDPR, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'art. 10 del GDPR.

[7] Tale previsione impone che il trattamento in parola sia attuato dal titolare del trattamento adottando misure tecniche e organizzative adeguate (quali la pseudonimizzazione) e nel rispetto dei diritti e delle libertà dell'interessato.

[8] Quelle attualmente in essere sono elencate all'art. 9, par. 2, lett. da a) a j) del GDPR.

funzionamento dei sistemi di intelligenza artificiale, per come definiti dall'art. 3, punto 1 dell'Ai Act, o di un modello di intelligenza artificiale (di seguito, i "**Sistemi AI**");

- la lett. l), per permettere al titolare del trattamento, con specifico riferimento ai **dati biometrici** di cui all'art. 4, par. 14 del GDPR, il trattamento dei detti dati qualora esso sia necessario per **verificare l'identità dell'interessato** nell'ambito delle finalità legittime perseguite dal titolare medesimo.

Per quanto riguarda l'eccezione di cui alla superiore lett. k), il Regolamento Digital Omnibus precisa[9] che essa si può applicare se il titolare del trattamento:

- una volta identificati i dati particolari coinvolti nel processo di sviluppo di un Sistema AI, si sia concretamente attivato per **rimuovere** tali dati, adottando **misure tecniche e organizzative** adeguate a tale fine;
- qualora la rimozione dei dati particolari richieda uno sforzo sproporzionato[10], abbia posto in essere misure appropriate per **proteggere** efficacemente e senza indebito ritardo i dati stessi dall'essere utilizzati per produrre risultati, dall'essere divulgati o altrimenti resi disponibili a terzi.

Con riferimento all'eccezione di cui al precedente punto l), la deroga al divieto di trattamento dei dati biometrici può essere invocata dal titolare del trattamento a patto che quest'ultimo abbia adottato misure congrue[11] per consentire all'interessato di avere il **controllo esclusivo** del processo di verifica dell'identità.

In tal modo, infatti, il trattamento non sarebbe suscettibile di creare **rischi significativi** per i diritti e le libertà fondamentali dell'interessato, in quanto il titolare del trattamento non verrebbe a conoscenza dei dati biometrici o ne verrebbe a conoscenza solo per un periodo di tempo molto limitato durante il processo di verifica dell'identità dell'interessato.

2.4. Informazioni e comunicazioni all'interessato: le proposte di modifica degli artt. 12, par. 5, e 13, par. 4 e 5, del GDPR

Il Regolamento Digital Omnibus mira, inoltre, a prevenire l'**abuso** da parte dell'interessato del diritto di ottenere le

[9] Introducendo un nuovo paragrafo, il n. 5, dell'art.9 del GDPR.
[10] Ad esempio, la riprogettazione del Sistema AI, come indicato dalla premessa n. (30) del COM (2025) 837.
[11] Ad esempio, come previsto dalla premessa n. (31) del COM (2025) 837, sono considerate misure congrue la conservazione dei dati biometrici in modo sicuro esclusivamente presso l'interessato o presso il titolare del trattamento in una forma crittografata all'avanguardia e la chiave o mezzi equivalenti siano detenuti esclusivamente dall'interessato.

informazioni di cui agli artt. 13 e 14 del GDPR, e le comunicazioni relative al diritto di accesso di cui all'art. 15 del GDPR, prevedendo una modifica dell'art. 12, par. 5, del GDPR, in presenza di richieste palesemente **infondate** o **eccessive**[12] – ovvero quando il titolare del trattamento possa dimostrare che l'interessato stia esercitando i diritti conferiti dagli artt. da 15 a 22 del GDPR per scopi diversi dalla protezione dei propri dati.

Al ricorrere di tali ipotesi, secondo le modifiche proposte dal Regolamento Digital Omnibus, il titolare del trattamento potrebbe:

- addebitare all'interessato un **contributo spese ragionevole** tenuto conto dei costi amministrativi connessi alla fornitura delle informazioni o comunicazioni o all'esecuzione delle azioni da lui richieste; oppure
- **rifiutare** di dare seguito alla richiesta dell'interessato, fermo restando l'onere del titolare del trattamento di dimostrare che la richiesta sia manifestamente infondata o che vi sono motivi ragionevoli per ritenere che essa sia eccessiva.

L'obiettivo è chiaramente quello di destinare le risorse del titolare del trattamento alla gestione di istanze legittime, evitando utilizzi impropri delle previsioni del GDPR, come spesso si è visto fare nella pratica.

Il rischio è, tuttavia, quello per cui l'assenza di determinazione del "contributo ragionevole" potrebbe portare a un'eccessiva discrezionalità da parte del titolare del trattamento, creando così un effetto deterrente nei confronti dell'interessato a presentare richieste di accesso ai propri dati.

Sempre nel contesto di una limitazione degli obblighi del titolare del trattamento, ma senza compromettere la possibilità per l'interessato di esercitare i propri diritti ai sensi del Capo III del GDPR, il Regolamento Digital Omnibus si propone di modificare l'art. 13, par. 4 del GDPR[13], prevedendo che il titolare del trattamento non sia tenuto a fornire

[12] Secondo il Regolamento Digital Omnibus, esempi di abuso includono situazioni in cui l'interessato fa un uso eccessivo del diritto di accesso con l'unico intento di causare danni o pregiudizi al titolare del trattamento o quando un individuo presenta una richiesta, ma allo stesso tempo si offre di ritirarla in cambio di qualche forma di vantaggio da parte del titolare del trattamento. Peraltro, sempre secondo la premessa qui citata, anche le richieste eccessivamente generiche e indifferenziate dovrebbero essere considerate eccessive.

[13] Nella sua attuale formulazione, l'art. 13, par. 4 del GDPR, prevede semplicemente che l'obbligo di fornire l'informativa all'interessato non si applica qualora e nella misura in cui l'interessato disponga già delle informazioni di cui ai par. 1, 2 e 3 del GDPR.

all'interessato le informazioni di cui all'art. 13, par. 1, 2 e 3 dello stesso, qualora:

- i dati personali siano stati raccolti nel contesto di un rapporto **chiaro** e **circoscritto**[14] tra l'interessato e il titolare del trattamento, e quest'ultimo eserciti un'attività che non sia ad **alta intensità** di dati[15];
- vi siano motivi ragionevoli per ritenere che l'interessato **disponga già delle informazioni** relative all'identità e ai dati di contatto del titolare del trattamento, alle finalità e alla base giuridica del trattamento stesso.

Il Regolamento Digital Omnibus si propone, altresì, di introdurre un nuovo paragrafo (il par. 5) all'art. 13 del GDPR, prevedendo che il titolare del trattamento non sia tenuto a fornire le informazioni di cui ai par. 1, 2 e 3. dell'art. 13 del GPPR quando il trattamento sia effettuato a fini di ricerca scientifica e la fornitura delle dette informazioni risulti impossibile o comporterebbe uno **sforzo sproporzionato**[16].

2.5. I trattamenti automatizzati: la proposta di modifica dell'art. 22 del GDPR

L'art. 22, par. 1, del GDPR riconosce all'interessato un diritto di non essere sottoposto a decisioni generate unicamente da processi automatizzati, inclusi quelli di profilazione, qualora tali decisioni producano effetti giuridici o incidano in modo analogo significativamente sulla sua persona, salvo che la decisione sia necessaria per stipulare o eseguire un contratto, autorizzata dalla legge, o basata su consenso esplicito.

Il Regolamento Digital Omnibus non muta l'impostazione delineata dall'art. 22, par.1, del GDPR, ma interviene in modo deciso sulla prima delle sue eccezioni, chiarendo che essa si reputa soddisfatta indipendentemente dal fatto che la decisione possa essere assunta con mezzi diversi da quelli esclusivamente automatizzati, ovvero mediante l'intervento di un **essere umano**.

Detto in altre parole, il titolare del trattamento potrebbe ricorrere a un trattamento automatizzato, avvalendosi

[14] Come indicato dalla premessa n. (36) del COM (2025) 837, si fa riferimento a casi ristretti, come ad esempio, il rapporto che intercorre tra un artigiano e i suoi clienti.
[15] Come indicato dalla premessa n. (36) del COM (2025) 837, per dati non ad "alta intensità" si intendono le ipotesi di raccolta di una quantità limitata di dati personali o di operazioni di trattamento, in sé, non complesse.
[16] Come previsto dalla premessa n. (37) del COM (2025) 837, la fornitura delle informazioni comporterebbe uno sforzo sproporzionato, in particolare, qualora il titolare del trattamento, al momento della raccolta dei dati personali, non sapesse o non prevedesse che avrebbe trattato i dati personali a fini di ricerca scientifica in una fase successiva, nel qual caso potrebbe non disporre di recapiti facilmente accessibili di ciascun interessato.

dell'eccezione contrattuale, laddove dimostri che il medesimo risultato sarebbe stato raggiunto anche con mezzi umani.

Da un lato, tale proposta di modifica potrebbe favorire la competitività delle imprese UE, velocizzandone il processo di assunzione di decisioni non critiche; dall'altro, il rischio è che l'interessato sia destinatario di decisioni automatizzate in contesti[17] sempre più delicati e incisivi.

Resta fermo, in ogni caso, il diritto dell'interessato di esprimere la propria opinione e contestare la decisione, ai sensi e per gli effetti dell'art. 22, par. 3, del GDPR.

2.6. I casi e i termini per la notifica del *data breach*: la proposta di modifica dell'art. 33 del GDPR

Il Regolamento Digital Omnibus si propone di modificare l'art. 33, par.1[18] del GDPR, sia in relazione ai casi in cui è necessario provvedere alla notifica della violazione dei dati personali (di seguito, il ***Data breach***), sia ai termini per la notifica dello stesso.

Quanto al primo punto, il Regolamento Digital Omnibus si prefigge di innalzare la soglia qualitativa per la notifica del Data breach all'autorità di controllo, sostituendo il concetto di "improbabilità" con quello di "**rischio elevato**[19]" per i diritti e le libertà dell'interessato.

Il Regolamento Digital Omnibus chiarisce, tuttavia, che la soglia qualitativa più elevata per la notifica del Data breach, non esonera il titolare del trattamento dall'**obbligo di documentare**[20], in ogni caso, la violazione a norma dell'art. 33, par. 5 del GDPR[21], né il suo obbligo di provare la propria conformità al GDPR, a norma dell'art. 5, par. 2, dello stesso regolamento.

Con riferimento ai termini per la notifica del Data breach, il "tetto" per la notifica di una violazione dei dati personali che presenti un rischio elevato per i diritti e le libertà

[17] Si pensi, ad esempio, al *rating* automatico per l'accesso al credito, alle decisioni automatizzate per l'assegnazione dei turni di lavoro, o al processo di selezione per una posizione lavorativa.

[18] L'art. 33, par. 1 del GDPR prevede che, in caso di violazione di dati personali, il titolare del trattamento debba notificare la violazione all'autorità competente ai sensi dell'art. 55 del GDPR senza ingiustificato ritardo e, comunque, entro 72 (settantadue) 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.

[19] Un elenco delle circostanze in cui una violazione dei dati personali può comportare un rischio elevato per i diritti e le libertà delle persone fisiche sarà presentato dall'EDPB. Oltre a tale elenco, l'EDPB si occuperà anche di trasmettere alla Commissione europea un modello comune per la denuncia da parte del titolare del trattamento del Data breach al punto unico di contatto, che sarà istituito a norma dell'art. 23a della Direttiva Nis2. La presentazione di tale elenco e del modello comune sarà effettuata dall'EDPB alla Commissione europea entro 9 (nove) mesi dall'entrata in vigore del Regolamento Digital Omnibus.

[20] Si tratta di un obbligo di documentazione interno, come previsto dall'art. 33, par. 5 del GDPR, il quale sancisce che "*il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio*".

dell'interessato dovrebbe essere innalzato da 72 (settantadue) a **96** (novantasei) **ore**.

Il Regolamento Digital Omnibus prevede, in ultimo, che la notifica in esame non dovrà più essere effettuata dal titolare del trattamento a ciascuna autorità competente, ma al **punto di contatto unico**[22] che sarà istituito a norma dell'art. 23a della Direttiva Nis2.

Fino all'istituzione del punto di accesso unico a norma dell'art. 23a della Direttiva Nis2, il Regolamento Digital Omnibus propone che il titolare del trattamento continui a notificare il Data breach direttamente all'autorità di controllo competente a norma degli artt. 55 e 56 del GDPR.

2.7. La Valutazione d'impatto di cui all'art. 35 del GDPR: i nuovi modelli a livello UE

Per quanto riguarda l'obbligo del titolare del trattamento di effettuare una **valutazione d'impatto** sulla protezione dei dati personali qualora il trattamento degli stessi possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche (art. 35 del GDPR), le modifiche proposte dal Regolamento Digital Omnibus sono più marginali rispetto alle altre sin qui analizzate.

A tal proposito, il Regolamento Digital Omnibus si limita a prevedere che l'**elenco unico**[23] delle operazioni che comportano un rischio elevato per i diritti e le libertà degli interessati, dovrebbe essere fornito a **livello UE** dal Comitato europeo per la protezione dei dati (l'*European Data Protection Board* – di seguito, l'"**EDPB**"), in sostituzione degli elenchi nazionali attualmente predisposti dalle autorità di controllo nazionali.

Inoltre, la pubblicazione di un elenco dei tipi di operazioni di trattamento per i quali non è richiesta una valutazione

[22] L'art. 23a della Direttiva Nis2 prevede, in particolare, la costituzione dell'ENISA come punto di accesso unico per la segnalazione degli incidenti. L'ENISA potrà garantire che il punto di accesso unico si basi sulla piattaforma di segnalazione unica, che sarà istituita a norma del Regolamento Digital Omnibus. L'ENISA sarà competente, tra l'altro, a garantire che le autorità competenti abbiano accesso alle informazioni e le trattino come richiesto dagli atti giuridici dell'UE. Per quanto riguarda le tempistiche, entro 18 (diciotto) mesi dall'entrata in vigore del Regolamento Digital Omnibus (il quale dovrà prima passare all'esame del Parlamento europeo e del Consiglio europeo), l'ENISA avvierà una fase "pilota" per il funzionamento del punto di accesso unico per ciascun atto giuridico dell'UE. La Commissione europea, in cooperazione con l'ENISA, valuterà successivamente il corretto funzionamento, l'affidabilità, l'integrità e la riservatezza del punto di accesso unico. Quando la Commissione europea, previa consultazione della rete CSIRT e delle autorità competenti ai sensi degli atti giuridici dell'UE, constaterà che il punto di accesso unico garantisce il corretto funzionamento, l'affidabilità, l'integrità e la riservatezza, pubblicherà un avviso in tal senso nella Gazzetta ufficiale dell'UE.

[23] Le proposte relative a tale elenco saranno presentate dall'EDPB alla Commissione europea entro 9 (nove) mesi dall'entrata in vigore del Regolamento Digital Omnibus, con l'elenco stesso che, una volta approvato, dovrà essere aggiornato ogni 3 (tre) anni o quando vi sarà la necessità.

d'impatto sulla protezione dei dati, attualmente facoltativa, dovrebbe essere resa obbligatoria.

2.8. I *cookie* e gli strumenti di tracciamento: la proposta dei nuovi artt. 88a e 88b del GDPR, e le conseguenti modifiche alla Direttiva ePrivacy

Una particolarità del Regolamento Digital Omnibus è la proposta di coordinamento tra il GDPR e la Direttiva ePrivacy, normativa comunitaria che costituisce la disciplina cardine in materia di tutela dei dati personali nell'ambito delle comunicazioni elettroniche e **tracciamento *online***[24] dell'interessato.

Con specifico riferimento al tracciamento dell'interessato, la regolamentazione di tale attività opera, ad oggi, su un doppio binario normativo: da un lato, il GDPR detta la nozione di profilazione/tracciamento e stabilisce i principi generali per il trattamento dei dati personali; dall'altro, l'art. 5, par. 3, della Direttiva ePrivacy prescrive la base giuridica (**consenso**) generalmente richiesta per l'accesso alle informazioni presenti nell'apparecchio terminale di un utente/interessato, salvo le eccezioni[25] molto restrittive previste dalla detta norma.

Tale meccanismo, di continui rinvii tra le due normative, ha spesso generato confusione negli operatori, motivo per cui la Commissione europea si propone di apportare le seguenti modifiche:

- alla Direttiva ePrivacy, chiarendo[26] che l'art. 5, par. 3, della stessa non si applica se l'abbonato o l'utente è una **persona fisica** e le informazioni memorizzate o consultate costituiscono o comportano il trattamento di dati personali;
- al GDPR, introducendo l'art. **88a**, per affidare esclusivamente a quest'ultimo la disciplina del trattamento dei dati personali memorizzati nelle apparecchiature terminali delle persone fisiche.

Nello specifico, l'art. 88a del GDPR conferma la regola del consenso come base giuridica per il tracciamento *online* dell'utente, ma ciò che si propone di mutare rispetto all'art. 5, par. 3, della Direttiva ePrivacy sono i casi in cui esso potrebbe essere derogato.

[24] Tracciamento effettuato attraverso diversi strumenti, come ad esempio i *cookies*.
[25] Le uniche eccezioni previste dall'art. 5, par. 3 della Direttiva ePrivacy sono relative: (a) alla memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica; (b) o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente.
[26] A tal fine, viene introdotto un nuovo paragrafo, il par. 4, dell'art. 5 della Direttiva ePrivacy.

In aggiunta alla trasmissione di una comunicazione elettronica su una rete di comunicazione elettronica e alla fornitura di un servizio richiesto esplicitamente dall'utente – eccezioni già previste dall'art. 5, par. 3, della Direttiva ePrivacy – l'art.88a, par. 3 del GDPR stabilisce, invero, che la memorizzazione di dati personali o l'accesso a dati personali già memorizzati nell'apparecchiatura terminale di una persona fisica dovrebbero essere possibili senza il suo consenso per:

- creare **informazioni aggregate** sull'utilizzo di un servizio *online* e **misurare l'*audience*** di tale servizio, qualora ciò sia effettuato dal titolare del trattamento di tale servizio esclusivamente per proprio uso;
- mantenere o ripristinare la **sicurezza** di un servizio fornito dal titolare del trattamento e richiesto dall'interessato o per la fornitura del servizio stesso.

Ciò detto, altra previsione innovativa del Regolamento Digital Omnibus si rinviene nella proposta di introduzione dell'art. 88a, par. 4, lett. (a)[27] del GDPR[28], il quale prevede, nelle ipotesi in cui la conservazione di dati personali o l'accesso a dati personali già conservati nell'apparecchiatura terminale di una persona fisica sia basata sul consenso, il diritto dell'interessato di poter rifiutare le richieste di consenso in modo **facile** e **comprensibile** con un pulsante a ***clic* singolo** o tramite mezzi equivalenti.

Per quanto riguarda l'istituzione dell'art. 88b del GDPR, tramite quest'ultimo il Regolamento Digital Omnibus intende confermare a carico del titolare del trattamento l'obbligo[29], previsto dalla Direttiva ePrivacy, di mettere a disposizione dell'interessato/utente interfacce *online* che gli permettano di esprimere, rifiutare o revocare il consenso al trattamento dei propri dati personali.

La differenza rispetto all'attuale disciplina risiede, tuttavia, nella volontà di mettere a disposizione dell'interessato strumenti tecnologici centralizzati e "*machine-readable*" che gli consentano di impostare le proprie preferenze di consenso in via preventiva e **leggibili automaticamente**, superando così il meccanismo dei ***banner*** di consenso ripetitivi.

[27] Tale disposizione, laddove confermata dal Parlamento europeo e Consiglio europeo, si applicherà 6 (sei) mesi dopo la data di entrata del Regolamento Digital Omnibus.
[28] Alle lett. (b) e (c) dell'art. 88b del GDPR, il Regolamento Digital Omnibus chiarisce che, laddove l'interessato abbia prestato il proprio consenso, il titolare del trattamento non potrebbe presentare una nuova richiesta di consenso per lo stesso scopo durante il periodo in cui esso può legittimamente fare affidamento sul consenso dell'interessato; qualora l'interessato avesse rifiutato la richiesta di consenso, il titolare del trattamento non potrebbe presentare una nuova richiesta di consenso per lo stesso scopo per un periodo di almeno 6 (sei) mesi.
[29] Tale obbligo è previsto che non si applichi ai fornitori *media* e limitatamente a tali servizi, come sancito dal Regolamento Digital Omnibus.

L'obiettivo è quello di semplificare le procedure di rilascio del consenso e tutelare l'interessato dal fenomeno del c.d. "*consent fatigue*", consistente nella proliferazione dei *banner pop-up* e dei continui avvisi che appaiono all'utente durante la navigazione sui siti *web* per fini non sempre legittimi[30].

Con l'introduzione del nuovo art. 88b del GDPR, invece, il Regolamento Digital Omnibus si prefigge di consentire all'interessato di esprimere il consenso al trattamento dei propri dati (c.d. *opt-in*) o la revoca dello stesso (c.d. *opt-out*) con un solo *clic* e salvare le proprie preferenze sui *cookie* attraverso le **impostazioni centrali** delle preferenze nei *browser* e nel sistema operativo.

La piena operatività di tale disposizione è legata, tuttavia, alla richiesta da parte della Commissione europea agli organismi europei di normalizzazione di elaborare **nuovi *standard***[31] per l'interpretazione delle indicazioni leggibili da dispositivi automatici delle scelte dell'interessato.

In tema di *cookie* e strumenti di tracciamento, il Regolamento Digital Omnibus propone, infine, di abrogare l'art. 4 della Direttiva ePrivacy, con riferimento all'obbligo del fornitore di servizi di comunicazione elettronica di adottare misure adeguate a garantire la sicurezza della rete e informare l'utente in caso di rischi specifici non completamente mitigabili indicando possibili rimedi e i relativi costi, in quanto gli stessi obblighi sono oggi disciplinati dal GDPR e della Direttiva Nis2.

2.9. Il legittimo interesse come base giuridica per il trattamento dei dati personali nell'ambito dello sviluppo e dell'addestramento dei Sistemi AI: il nuovo art. 88c del GDPR

Un'ultima novità fondamentale prevista dal Regolamento Digital Omnibus è l'introduzione del nuovo art. (l'88c) al GDPR, al fine di prevedere la possibilità per il titolare del trattamento di effettuare il trattamento dei dati personali nell'ambito dello sviluppo dei Sistemi AI avvalendosi della base giuridica del **legittimo interesse** di cui all'art. 6, par. 1, lett. f) del GDPR.

Il Regolamento Digital Omnibus chiarisce espressamente che lo sviluppo, l'**addestramento** e il miglioramento dei **Sistemi AI** possano fondarsi sul legittimo interesse del titolare del

[30] Come indicato dalle premesse n. (45) e (46) del COM (2025) 837, i *banner pop-up* spesso vengono mostrati dal fornitore del servizio – titolare o responsabile del trattamento – per "spingere" l'interessato a proseguire la navigazione e rendere meno comprensibili le scelte da lui compiute.

[31] Per questo motivo, l'art. 88b, par. 1 e 2 del GDPR è previsto che si applichi 24 (ventiquattro) mesi dopo l'entrata in vigore del Regolamento Digital Omnibus, con tale termine innalzato a 48 (quarantotto) mesi per le PMI.

trattamento, salvo i casi in cui il consenso dell'interessato è obbligatorio e fermo restando l'obbligo di effettuare il *test* di bilanciamento richiesto dall'art. 6, par. 1, lett. f) del GDPR.

Rimane fermo, inoltre, che trattamento in parola deve essere attuto nel rispetto dei principi di liceità, trasparenza, necessità e minimizzazione di cui all'art. 5 del GDPR, nonché dei diritti riconosciuti all'interessato dagli artt. da 15 a 22 del GDPR, compreso quello di opposizione.

3. Conclusioni e primi commenti

Il Regolamento Digital Omnibus segna un punto di svolta nella regolazione digitale UE, in quanto tenta di riorganizzare un sistema normativo cresciuto nel tempo in modo stratificato e non sempre armonico.

Il Regolamento Digital Omnibus si propone di introdurre modifiche che, se confermate, dovrebbero rendere più semplice la gestione dei dati per imprese e amministrazioni, riducendo adempimenti quando non necessari e fornendo nuove basi giuridiche per attività oggi difficili da inquadrare, come quelle relative allo sviluppo e al funzionamento dei Sistemi AI.

La ridefinizione della nozione di dato personale in base alla capacità effettiva di identificazione, l'alleggerimento degli obblighi informativi e il riconoscimento del legittimo interesse nello sviluppo dei Sistemi AI sono segnali chiari della volontà del legislatore UE di favorire processi innovativi senza rinunciare alle garanzie fondamentali.

Allo stesso tempo, la scelta di concentrare in un unico quadro legislativo ambiti normativi fino a questo momento autonomi richiederà una particolare attenzione: il rischio di perdere livelli di tutela o specificità settoriali rimane un "nodo" delicato.

Anche l'introduzione di sistemi di gestione del consenso più snelli e centralizzati potrà effettivamente ridurre la complessità per cittadini e operatori, ma solo se l'interoperabilità tecnica sarà garantita e se gli *standard* europei verranno recepiti in modo uniforme.

In prospettiva, il vero "banco di prova" sarà la fase legislativa che coinvolgerà il Parlamento europeo e il Consiglio europeo: trasformare queste proposte in un regolamento realmente funzionale richiederà compromessi, valutazioni sull'impatto operativo e un dialogo costante con imprese, autorità e Stati membri.

Compromessi che dovranno probabilmente tener conto anche di dinamiche più ampie che stanno progressivamente entrando nel dibattito pubblico.

Il Regolamento Digital Omnibus si inserisce, infatti, in un contesto complesso, caratterizzato da esortazioni – esplicite e implicite – da parte dell'attuale amministrazione americana, volte a rendere più flessibili le regole europee (anche in materia di *data protection*) per mantenere la competitività globale, soprattutto nei confronti dei grandi *player* statunitensi.

A tali esortazioni fanno da contraltare coloro[32] che evidenziano il pericolo che la spinta alla semplificazione possa, di fatto, aprire la strada a un indebolimento delle tutele previste dal GDPR, in un momento in cui la dipendenza tecnologica dell'UE richiederebbe invece crescente prudenza strategica.

Secondo costoro, il Regolamento Digital Omnibus rischia di tradursi in un ripensamento profondo delle regole sulla protezione dei dati, sulla trasparenza nell'uso dei Sistemi AI e sulle garanzie contro il tracciamento pervasivo degli interessati, con potenziali impatti sulla capacità degli individui di esercitare adeguati controlli sulle tecnologie che li riguardano.

Tali preoccupazioni non negano la necessità di una semplificazione, ma evidenziano come la velocità del processo e la mancanza di un confronto strutturato possano incidere sulla qualità delle tutele oggi garantite dal diritto UE in materia di protezione dei dati personali.

Anche per questi motivi, il successo del Regolamento Digital Omnibus dipenderà dalla capacità dell'UE di mantenere l'equilibrio tra semplificazione e tutela, evitando che l'innovazione diventi un fattore di erosione dei diritti o, al contrario, che la protezione dei diritti diventi un ostacolo alla competitività tecnologica.

Per ora, il Regolamento Digital Omnibus rappresenta un'opportunità: un tentativo ambizioso di portare il diritto digitale UE in una fase più matura, capace di rispondere alle trasformazioni tecnologiche senza inseguirle, ma orientandole.

Avv. Giovanni Vidal

giovanni.vidal@gvalex.it

Avv. Kristjan Gjinaj

kristjan.gjinaj@gvalex.it

Dott. Pietro Borelli

pietro.borelli@gvalex.it

[32] In particolare, una coalizione di 127 sindacati e gruppi della società civile, tra cui NOYB, EDRi ed Access Now - Forthcoming Digital Omnibus would mark point of no return - European Digital Rights (EDRi), ha espresso più volte i loro timori sul punto.

GRECO VITALI
ASSOCIATI

gvalex.it