CAMERA DEI DEPUTATI
IX COMMISSIONE

PROPOSTA DI REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO CHE RIGUARDA LA SEMPLIFICAZIONE DEL QUADRO LEGISLATIVO NEL SETTORE DIGITALE
(COM(2026) 837 FINAL)

MEMORIA DEL PRESIDENTE DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
PROF. PASQUALE STANZIONE

Ringrazio, anzitutto, la Commissione, per aver inteso acquisire l'avviso del Garante in ordine alla proposta in esame, che si inserisce nel processo di razionalizzazione dell'acquis digitale dell'Unione europea, per ridurre gli oneri amministrativi gravanti sugli operatori economici, in particolare le piccole e medie imprese e quelle a media capitalizzazione, preservando un adeguato livello di tutela dei diritti fondamentali.

La proposta – parallelamente a quella COM (2026) 836, c.d. Omnibus AI- interviene, trasversalmente, su una pluralità di normative unionali: il "*data acquis*", il GDPR (Regolamento (UE) 2016/679), la direttiva e-privacy (.

La disciplina di protezione dei dati è interessata in modo profondo da queste novelle, che incidono sulle norme definitorie e i principi del GDPR, sulla disciplina dell'esercizio dei diritti degli interessati, delle decisioni automatizzate, specie in ambito contrattuale, di specifici adempimenti, nonché sul trattamento dei dati, anche particolari, per lo sviluppo e l'addestramento di sistemi di intelligenza artificiale. Positive sono, in particolare, le semplificazioni inerenti agli adempimenti correlati alla notifica di data breach e alla valutazione d'impatto sulla protezione dei dati, come le precisazioni in materia di ricerca scientifica e la legittimazione della verifica biometrica decentralizzata dell'identità.

Per esigenze di sintesi, tuttavia, ci si soffermerà sui soli aspetti della proposta inerenti alla protezione dati, meritevoli di riflessione, in particolare riguardo al principio di proporzionalità, in relazione a novelle che paiono trascendere obiettivi di mera semplificazione e riduzione degli oneri amministrativi, incidendo invece in maniera più profonda su norme fondative della disciplina di protezione dei dati, con una complessiva diminuzione degli standard di tutela. Si tratta di aspetti sottolineati anche dal parere congiunto del Comitato europeo per la protezione dei dati e dal Garante europeo, adottato l'11 febbraio.

Mi riferisco, in questo senso, alla modifica dell'articolo 4 del GDPR, che rimodula la nozione di dato personale (con effetti espansivi su tutte le norme, unionali e non, che la richiamino) secondo il criterio dell'identificabilità dell'interessato. Essa è valutata non più in astratto, bensì in relazione alla possibilità *effettiva* per il titolare o per il destinatario del dato, di reidentificarlo con mezzi ragionevolmente disponibili. Si esclude che un'informazione possa qualificarsi come dato personale per il solo fatto che un soggetto terzo disponga di strumenti idonei alla reidentificazione, introducendo un criterio soggettivo di "ragionevole potenzialità". Il baricentro della tutela si sposta, in altri termini, dalla natura (oggettiva, intrinseca e certa) del dato alla prospettiva (soggettiva, estrinseca e potenziale) dell'operatore che lo tratti.

La tutela accordata al diritto, fondamentale, alla protezione dei dati, sancita dall'art. 8 della CDFUE come universale rischia di divenire, così, relativa e frammentaria, condizionandosene l'operatività alla capacità del singolo titolare di identificare gli interessati in ragione dei mezzi a propria disposizione. Ne deriva il rischio *(*soprattutto in contesti delicati come i trasferimenti di dati all'estero*)* di interpretazioni arbitrarie e- per paradossale eterogenesi dei fini – di un'incertezza giuridica, potenzialmente foriera di contenziosi, certamente incoerente con i fini semplificatori sottesi alla proposta.

Il criterio proposto non è, peraltro, del tutto coerente con la giurisprudenza consolidata CGUE[1] richiamata, invece, a sostegno della novella. Essa, pur valorizzando il contesto in cui si svolge il trattamento, ha infatti utilizzato l'approccio in concreto in senso ampliativo (e non restrittivo) della nozione di dato personale, attraendovi anche i dati che tali diventino in ragione dei mezzi ragionevolmente utilizzabili, a fini reidentificativi, da un terzo e in particolare dal destinatario.

Peraltro, l'attribuzione alla Commissione del potere di adottare – sia pure su parere del Comitato europeo per la protezione dei dati - atti di esecuzione in materia di pseudonimizzazione incide, in misura rilevante, sull'ambito di applicazione oggettivo del diritto UE in materia di protezione dei dati, alterando il riparto di attribuzioni tra l'esecutivo dell'Unione e il ruolo di garanzia delle autorità di controllo, sancito dell'art. 8 della CDFUE, nonché dello stesso del Comitato.

Analoga incertezza giuridica – anche qui, con paradossale eterogenesi dei fini – rischia di determinarsi in relazione al concetto di sproporzione dello sforzo connesso alla rimozione dei dati appartenenti a categorie particolari, che ne legittima il trattamento 'incidentale' e 'residuale' per lo sviluppo o il funzionamento di sistemi di i.a.. Sarebbe opportuno precisare almeno dei parametri di valutazione di tale concetto,

[1] In particolare in materia di indirizzi IP (sentenze Breyer (C-582/14) e Nowak (Causa C-434/16), nonché SRB (C-413/23): quest'ultima, peraltro, neppure resa su rinvio pregiudiziale

richiedendo la documentazione della ritenuta sproporzione, tenendo conto dello stato dell'arte della tecnologia e dell'impatto sugli interessati, imponendo comunque l'adozione di garanzie adeguate durante l'intero trattamento.

Ancora, in relazione alla prevista possibilità di ricorrere al legittimo interesse quale presupposto di liceità del trattamento funzionale allo sviluppo e al funzionamento di sistemi di i.a., andrebbe chiarito che il previsto "diritto incondizionato di opposizione" va oltre il diritto generale di opposizione di cui all'articolo 21 del GDPR , così come gli obblighi di maggiore trasparenza richiesti verso gli interessati, devono ritenersi ulteriori rispetto a quelli già imposti dagli artt. 13 e 14 del GDPR.

Su materia affine, il parere congiunto Edpb-Edps sul Digital Omnibus AI, in relazione alla prevista possibilità di trattamento di dati appartenenti a categorie particolari, pseudonimizzati, per la mitigazione dei bias nei sistemi e modelli di i.a. ha raccomandato un'interpretazione restrittiva per evitare potenziali abusi, limitando tale facoltà alle ipotesi in cui il rischio di discriminazione sia sufficientemente grave da giustificare l'uso di informazioni così delicate. La posizione raggiunta con l'accordo del 7 maggio scorso sull'Omnibus AI tra i colegislatori (che, per altro verso, introduce un condivisibile divieto rispetto ai deepfake sessuali e agli algoritmi di nudificazione) va, correttamente, in questo senso.

Un rischio di incertezza giuridica, con vanificazione degli effetti di riduzione degli oneri amministrativi potrebbe inoltre derivare dalle modifiche- contenuta nel Digital Omnibus- in tema di esercizio (abusivo) dei diritti degli interessati, che consentono il rifiuto o la subordinazione a un corrispettivo ragionevole delle istanze, tra le altre, funzionali a fini estranei alla protezione dei dati. Dal momento che il GDPR, come riconosciuto dalla giurisprudenza della CGUE, mira a tutelare, con il diritto alla protezione dati, anche altri diritti e libertà fondamentali, tale requisito non concorre a delineare correttamente il carattere abusivo delle istanze e dovrebbe essere, più correttamente, sostituito dal riferimento a intenti emulativi o, comunque, di carattere abusivo (ad esempio, l'evidente intenzione pregiudizievole nei confronti del titolare del trattamento). Ulteriori precisazioni merita anche la deroga all'obbligo di informativa per i trattamenti non intensivi nei rapporti chiari e circoscritti, la cui definizione piuttosto ambigua rischia di ingenerare interpretazioni disomogenee.

Per altro verso, la previsione della legittimità del trattamento funzionale a decisioni automatizzate necessarie per la conclusione o l'esecuzione di un contratto, anche qualora la decisione potrebbe essere adottata da un essere umano, rischia di prestarsi a interpretazioni arbitrarie, in virtù di tale ultimo inciso, eccessivamente ampio, che potrebbe invece rifluire in un Considerando. Alternativamente, si potrebbe sostituire

tale norma legittimante con la previsione di una deroga più puntuale a un più generale divieto, secondo una formulazione più simile all'attuale.

La disciplina del tracciamento online e dei cookie è riformulata introducendo il principio del consenso *"once only",* volto a prevenire la c.d. *consent fatigue*, con la previsione di deroghe al consenso per fini di sicurezza, misurazione dell'utenza e fornitura del servizio richiesto, individuati tuttavia in maniera ancora troppo ampia e generica da evitare interpretazioni discrezionali.

Complessivamente, la proposta ha certamente il merito di introdurre talune semplificazioni e riduzioni di oneri amministrativi e regolatori, ma esige alcuni correttivi, quali quelli illustrati, tali da evitare il rischio, paradossale, di incertezze in sede applicativa, con anche conseguenti maggiori oneri per imprese, pubbliche amministrazioni e, in ulteriore analisi, per le Autorità di protezione dei dati. E' peraltro necessario che il livello delle garanzie non sia affievolito, non potendo in alcun modo ammettersi un *aut aut* tra innovazione e diritti, la cui sinergia va invece, sempre più, promossa.

Ringrazio la Commissione per l'attenzione.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Pasquale Stanzione