OSSERVATORIO
TMT · DATA PROTECTION
di Morri Rossetti & Franzosi

Monthly Roundup

Marzo - aprile 2026

Marzo - aprile 2026

I principali aggiornamenti in materia di TMT & Data Protection dei mesi di marzo e aprile.

NUOVI PROVVEDIMENTI LEGISLATIVI E REGOLATORI

GARANTE PRIVACY

- Prove d'esame e corsi a distanza, online le Faq del Garante privacy; [Link]
- Il Garante privacy sanziona Eni per 96mila euro; [Link]
- Garante: sì ad accesso proprie email dopo fine rapporto lavoro; [Link]
- Garante: non conforme al GDPR "FaceBoarding" di Milano Linate. [Link]

EDPB

- EDPB Annual Report 2025; [Link]
- EDPB DPIA Template; [Link]
- Guidelines 1/2026 on processing of personal data for scientific research purposes. [Link]

AGCOM

- Determinazione ACN 127437/2026 – Piattaforma, Punto di contatto e sostituto, aggiornamento delle informazioni e rappresentante NIS di cui all'articolo 7 del decreto NIS; [Link]
- Determinazione ACN 127434/2026 – Termini per i soggetti 2026 in relazione agli obblighi di cui agli articoli 23, 24, 25, 29 e 32 del decreto NIS; [Link]
- Determinazione 155238/2026 categorie di rilevanza nonché il processo, le modalità e i criteri per l'elencazione, caratterizzazione e categorizzazione delle attività e dei servizi; [Link]
- Linee Guida NIS Modello di categorizzazione Guida alla lettura. [Link]

Riutilizzo dei dati e responsabilità privacy: la qualificazione dell'agenzia nelle reti assicurative

Il Garante Privacy (Provv. 89/2026, doc. web. 10227039) è recentemente intervenuto sulla qualificazione dei ruoli privacy e sulle relative responsabilità nell'ambito dei rapporti tra compagnia assicurativa e agenzie mandatarie.

In particolare, l'Autorità ha sanzionato un'agenzia con una sanzione di Euro 15.000,00 per una pluralità di violazioni in materia di protezione dei dati personali, riconducibili, in ultima analisi, a un'errata qualificazione del proprio ruolo nel trattamento.

I fatti oggetto del provvedimento

Il caso tra origine da alcuni reclami con cui veniva lamentata la ricezione di e-mail promozionali senza consenso, nonché il mancato riscontro a una richiesta di accesso ai dati personali.

Le comunicazioni in questione promuovevano servizi riconducibili a una compagnia assicurativa per conto della quale l'agenzia operava in qualità di mandataria.

Nel corso dell'istruttoria, il Garante Privacy ha richiesto chiarimenti in merito alle modalità con cui l'agenzia assicurava il rispetto della normativa in relazione alle attività di marketing.

L'agenzia ha dichiarato di operare quale responsabile del trattamento della compagnia mandante, ritenendo conseguentemente che gli obblighi relativi, tra l'altro, alla gestione delle richieste degli interessati, alla predisposizione dell'informativa e all'eventuale acquisizione del consenso gravassero su quest'ultima, in qualità di titolare del trattamento.

La qualificazione del ruolo privacy: il rilievo delle modalità concrete di trattamento

Tale ricostruzione non è stata condivisa dall'Autorità, che ha invece valorizzato le modalità concrete di utilizzo dei dati.

In linea generale, la compagnia assicurativa dev'essere considerata titolare del trattamento dei dati dei clienti acquisiti tramite le agenzie che, tipicamente, operano in qualità di responsabili del trattamento sulla base di appositi accordi ai sensi dell'art. 28 del GDPR. In tale assetto, l'agenzia non dispone di autonomia decisionale rispetto alle finalità e ai mezzi del trattamento, limitandosi a trattare i dati per conto della compagnia.

Tuttavia, pur essendo stati originariamente raccolti nell'ambito di tale rapporto, il Garante Privacy ha sottolineato come i dati sono stati successivamente utilizzati dall'agenzia per finalità ulteriori, segnatamente di natura promozionale, riconducibili a una propria iniziativa.

In questo contesto, l'Autorità ha ritenuto che l'agenzia avesse agito in autonomia nella determinazione delle finalità e dei mezzi del trattamento, dovendo pertanto essere qualificata, per tali attività, quale autonomo titolare del trattamento[1].

[1] Nella propria memoria difensiva, l'agenzia chiarisce che l'essersi qualificata come mero responsabile del trattamento è stato un errore commesso in buona fede. Tale errore deriverebbe dall'aver fatto riferimento alla propria qualifica di "distributore" ai sensi dell'art. 82 del Regolamento IVASS 40/18. Questa norma prevede che i distributori, quando promuovono contratti assicurativi tramite tecniche di

Il Garante Privacy ha ribadito, di fatto, un principio fondamentale del GDPR: la qualificazione del ruolo privacy delle parti non discende automaticamente dalla previsione contrattuale, ma dev'essere verificato alla luce delle concrete modalità con cui vengono trattati i dati.

La gestione delle richieste di esercizio dei diritti degli interessati

La diversa qualificazione del ruolo assume rilievo anche con riferimento alla gestione dei diritti degli interessati. L'agenzia, infatti, non ha fornito riscontro alla richiesta di accesso, ritenendo che la stessa fosse già all'attenzione della compagnia assicurativa.

Il Garante Privacy ha censurato tale condotta, osservando come la qualifica di titolare comporti l'obbligo di fornire un riscontro diretto e tempestivo agli interessati.

Al contempo, l'Autorità ha ricordato che, anche nell'ipotesi in cui l'agenzia avesse correttamente operato quale responsabile del trattamento, sarebbe stata comunque tenuta a prestare assistenza al titolare nella gestione delle richieste, ai sensi dell'art. 28 GDPR.

La base giuridica per l'invio di comunicazioni promozionali

L'agenzia aveva ritenuto di poter fondare l'invio delle comunicazioni promozionali dapprima sull'eccezione del c.d. soft spam di cui all'art. 130, comma 4, del Codice Privacy e, successivamente, sul legittimo interesse.

Entrambe le opzioni sono state escluse dal Garante Privacy. Da un lato, è stato ribadito come l'eccezione del soft spam sia applicabile esclusivamente al titolare che ha originariamente raccolto i dati nel contesto della vendita del prodotto o servizio; dall'altro lato, il ricorso al legittimo interesse non è praticabile in presenza della disciplina speciale dettata dall'art. 130 del Codice Privacy per l'invio di comunicazioni elettroniche a fini promozionali.

L'invio delle comunicazioni promozionali è stato dunque effettuato in assenza di uno specifico e autonomo consenso per finalità commerciali riconducibili esclusivamente all'agenzia.

Ne consegue che il trattamento deve ritenersi privo di un idoneo presupposto di liceità, non risultando acquisito un consenso valido riferibile all'agenzia e alle sua autonome finalità.

---

comunicazione a distanza (ad esempio per invio di materiale pubblicitario, vendita a distanza, ricerche di mercato o comunicazioni commerciali), debbano acquisire il previo consenso del contraente. Tuttavia, in assenza di opposizione e previa informazione sulla possibilità di opporsi, il consenso non è necessario se il contraente ha già fornito i propri recapiti in occasione della commercializzazione di un contratto assicurativo relativo allo stesso o ad altri rami, purché il prodotto sia distribuito dalla stessa impresa. Sulla base di tale disposizione, l'agenzia ha ritenuto (seppur erroneamente) che, in qualità di distributore, potesse qualificarsi come responsabile del trattamento nell'ambito delle attività di promozione commerciale, agendo nell'interesse esclusivo del titolare.
Il Garante Privacy ha confermato come l'art. 82 del Regolamento IVASS 40/18 non sia in contrasto con l'art. 130 del Codice Privacy. In linea con l'art. 130 del Codice, norma di rango primario, anche l'art. 82 citato stabilisce come regola generale il previo consenso del contraente per le attività di *marketing*. Solo in via eccezionale il distributore può effettuare comunicazioni commerciali senza consenso, salvo opposizione dell'interessato, quando questi abbia già fornito i propri recapiti nell'ambito della commercializzazione di un contratto assicurativo distribuito dalla stessa impresa. Ne consegue che la qualifica di "distributore" può coincidere con quella di "responsabile del trattamento" solo se il soggetto sia stato previamente autorizzato dal titolare. In mancanza di tale presupposto, il distributore deve essere qualificato, in base al caso concreto, come titolare o contitolare del trattamento, poiché il responsabile non può determinare autonomamente finalità e mezzi del trattamento senza assumere la veste di titolare.

Gli obblighi di trasparenza

In tale prospettiva, assume rilievo anche il profilo della trasparenza.

L'unica informativa resa all'interessato era quella fornita dalla compagnia assicurativa al momento della raccolta dei dati, mentre nessuna informativa ulteriore risultava essere stata predisposta dall'agenzia in relazione ai trattamenti successivi (c.d. secondari) effettuati in qualità di titolare autonomo.

Il trattamento per finalità ulteriori deve pertanto considerarsi avvenuto in assenza di un'adeguata informativa agli interessati, non essendo quella originaria idonea a coprire utilizzi dei dati ulteriori e autonomi.

Implicazioni pratiche

Il provvedimento in esame si presta a una lettura che va oltre il caso concreto e richiama l'attenzione su un profilo di frequente criticità nei modelli organizzativi complessi.

La qualificazione dei ruoli privacy non può essere considerata un elemento statico, definito sulla base della mera designazione formale (ad es., in un contratto), ma deve essere costantemente verificata alla luce delle attività effettivamente svolte.

In particolare, il riutilizzo dei dati da parte di un altro soggetto per finalità ulteriori rispetto a quelle originarie comporta una rivalutazione del ruolo privacy, con tutte le responsabilità che ne derivano.

In questa prospettiva, prima di procedere a qualsiasi trattamento di dati personali, si rende necessario un esame sostanziale delle attività svolte, che consenta di individuare correttamente i trattamenti effettuati.

Tale analisi costituisce infatti il presupposto per una corretta qualificazione dei ruoli privacy e per la conseguente definizione delle responsabilità.

* * *

NIS2: nuove Determinazioni ACN su scadenze, fornitori rilevanti e categorizzazione

Il 13 aprile 2026 l'Agenzia per la Cybersicurezza Nazionale ("**ACN**") ha adottato due nuove determinazioni – la n. 127434/2026 e la n. 127437/2026 – che intervengono su termini e modalità operative della disciplina NIS2.

Il loro impatto, tuttavia, non si esaurisce nell'aggiornamento degli adempimenti: tocca il modo in cui i soggetti NIS devono leggere e gestire il rischio operativo, soprattutto lungo la catena dei fornitori.

Nuovi termini per i soggetti NIS inseriti in elenco nel 2026

La Determinazione 127434/2026 (la "**Determinazione 127434**"), applicabile dal 30 aprile, definisce le scadenze per i soggetti inseriti per la prima volta nell'elenco dei soggetti NIS nel 2026 con riferimento agli obblighi relativi alle c.d.

specifiche di base (artt. 24 e 25 del Decreto NIS2 e Determinazione 379907/2025[2]).

Per tali soggetti, l'obbligo di notifica degli incidenti decorrerà dal **1° gennaio 2027**, con la conseguente necessità di designare il Referente CSIRT entro il 31 dicembre 2026[3]. Le misure di sicurezza dovranno invece essere adottate entro il **31 luglio 2027**.

Restano invece fermi i termini originariamente previsti dalla Determinazione 379907/2025 per i soggetti inseriti in elenco nel corso del 2025, che dovranno notificare gli incidenti a partire da gennaio 2026 e adottare le misure di sicurezza entro ottobre 2026.

Elencazione dei fornitori rilevanti NIS

La Determinazione n. 127437/2026 (la "**Determinazione 127437**") introduce l'obbligo di indicare i fornitori rilevanti NIS nell'ambito dell'aggiornamento annuale delle informazioni, da effettuarsi tra il 15 aprile e il 31 maggio.

Si tratta, in particolare, dei fornitori che erogano servizi o prodotti al soggetto NIS e che presentano un profilo di rilevanza qualificata. Tale rilevanza ricorre quando è soddisfatto almeno uno dei seguenti criteri:

a. **fornitura ICT**: rientrano in questa categoria le forniture riconducibili alle attività o ai servizi di cui all'Allegato I, punti 8 e 9, del Decreto NIS2 (D.Lgs. 138/2024). Si tratta, in concreto, di infrastrutture digitali e gestione dei servizi ICT (B2B), quali – a titolo esemplificativo – *internet exchange point*, servizi DNS, *cloud computing*, *data center*, nonché servizi gestiti o di sicurezza gestiti;
b. **fornitura non fungibile**: si tratta delle forniture la cui interruzione o compromissione è suscettibile di incidere in modo significativo sulla capacità del soggetto NIS di erogare i propri servizi. La non fungibilità va verificata in concreto e può dipendere anche dall'indisponibilità di fornitori alternativi. Nelle FAQ, l'ACN richiama casi tipici come la connettività (dati e voce, fissa e mobile) quando non adeguatamente ridondata, nonché la fornitura di energia elettrica.

Ne deriva che i soggetti NIS sono chiamati a individuare quei fornitori la cui eventuale indisponibilità sarebbe idonea a produrre un impatto concreto sull'operatività, incidendo sulla capacità di erogare i servizi rilevanti.

In particolare, in sede di aggiornamento annuale, occorrerà comunicare denominazione, codice fiscale e sede legale del fornitore, nonché i codici CPV (*Common Procurement Vocabulary*)[4] relativi alle forniture e il criterio di rilevanza che si ritiene soddisfatto.

Elencazione e categorizzazione delle attività e dei servizi NIS

Una delle principali novità operative riguarda l'obbligo, per i soggetti NIS, di comunicare l'elenco delle proprie attività e dei propri servizi, attribuendo a ciascuno la relativa categoria di rilevanza. L'adempimento, previsto dall'art. 30 del Decreto NIS2 e applicabile a partire dal 2026, dovrà essere svolto annualmente tra il 1° maggio e il 30 giugno, tramite la piattaforma dell'ACN, a seguito della comunicazione di inserimento nell'elenco dei soggetti NIS.

[2] Per maggiori approfondimenti, rinviamo al nostro precedente contributo "*NIS2: dalla compliance formale alla responsabilità operativa. Cosa cambia dopo le ultime Determinazioni e Linee Guida dell'ACN*".
[3] Per maggiori approfondimenti sulla figura del Referente CSIRT rinviano al nostro precedente contributo "*NIS2 e gestione degli incidenti: l'ACN introduce il Referente CSIRT*"
[4] Ai fini della definizione della fornitura si fa riferimento alla tassonomia contenuta nel vocabolario comune per gli appalti pubblici (*common procurement vocabulary* – CPV) adottato con Regolamento (CE) n. 2195/2002 e ss.mm.ii. L'ACN, all'interno nella FAQ FRN.4 illustra alcuni esempi di forniture con la relativa indicazione del CPV di riferimento.

Tale attività è rimessa al Punto di Contatto, attraverso il "*Servizio NIS/Categorizzazione*", che dovrà predisporre l'elenco e attribuire le categorie secondo il modello che sarà adottato dall'ACN, unitamente al materiale di supporto per la relativa analisi di impatto (BIA)[5].

Decorso il termine del 30 giugno, l'elenco categorizzato si intenderà acquisito in via definitiva e non più modificabile, salvo il caso in cui il ritardo sia dipeso da documentate criticità tecnico-operative non imputabili al soggetto NIS.

È inoltre previsto un meccanismo di verifica: l'ACN potrà effettuare controlli di conformità a campione, anche mediante confronto con soggetti comparabili, e dovrà fornire un riscontro entro 90 giorni, salvo proroga[6].

In caso di richieste di integrazione, chiarimento o modifica, il soggetto NIS dovrà rispondere entro 30 giorni; l'omesso o tardivo riscontro può condurre al rigetto dell'elenco. In assenza di esito negativo comunicato nei termini, la categorizzazione si intende convalidata.

La Determinazione 127437 precisa, infine, che le entità finanziarie soggette al DORA (Reg. UE 2554/2022), qualora rientrino anche nell'ambito applicazione del Decreto NIS2, sono esentate da tale adempimento, ferma restando la possibilità di aderirvi su base volontaria.

Ulteriori novità della Determinazione 127437

Rispetto alla disciplina previgente (Determinazione 37887/2025), la Determinazione 127437 introduce alcune ulteriori previsioni di rilievo operativo.

In primo luogo, è prevista la possibilità per il Punto di Contatto di procedere, in via eccezionale, alla notifica degli incidenti in caso di indisponibilità del Referente CSIRT e dei relativi sostituti.

La Determinazione 127437 introduce inoltre specifiche esenzioni per le entità finanziarie già soggette al DORA e rientranti anche nell'ambito di applicazione del Decreto NIS2.

In tali casi, vengono meno alcuni obblighi organizzativi e informativi, tra cui la nomina del Referente CSIRT e dei suoi sostituti, nonché la trasmissione dell'elenco dei componenti degli organi amministrativi e direttivi in sede di aggiornamento annuale.

Un ulteriore profilo riguarda la gestione delle ipotesi di registrazione tardiva. Pur restando ferma la possibile applicazione di sanzioni pecuniarie[7], viene riconosciuto un termine di 30 giorni dalla comunicazione di inserimento nell'elenco dei soggetti NIS per completare l'aggiornamento annuale delle informazioni.

Infine, per i soggetti già inclusi nell'elenco NIS 2025, l'avvio dell'aggiornamento per il 2026 avverrà sulla base di informazioni precompilate, elaborate a partire dai dati già trasmessi.

Conclusioni

A partire da metà aprile 2026, con l'avvio della fase di categorizzazione delle attività e dei servizi, la disciplina NIS2 entra in una fase attuativa più matura, caratterizzata dall'implementazione degli obblighi a lungo termine.

[5] https://www.acn.gov.it/portale/w/nis-online-le-determine-sugli-adempimenti-per-i-nuovi-soggetti-e-sulle-modalita-di-accesso-alla-piattaforma-acn

[6] In particolare, nel caso in cui sia necessario effettuare degli approfondimenti, tale termine potrà essere prorogato per una sola volta e fino a un massimo di ulteriori 60 giorni.

[7] In questi casi è prevista l'irrogazione di sanzioni amministrative pecuniarie fino a un massimo dello 0,01% (per i soggetti "essenziali") e dello 0,07% (per i soggetti "importanti") del totale del fatturato annuo, calcolato a livello di gruppo (art. 38, co. 10, lett. b) e l'art. 11 del Decreto NIS2).

Tra le novità introdotte, il profilo di maggiore impatto riguarda l'obbligo di identificare i fornitori rilevanti.

I soggetti qualificati come "essenziali" o "importanti" sono chiamati a ricostruire in modo strutturato la propria catena di approvvigionamento, individuando i fornitori in grado di incidere concretamente sulla continuità dei servizi NIS e verificando, per ciascuno di essi, l'effettiva esistenza di alternative operative o, al contrario, la natura non fungibile della fornitura.

Come evidenziato anche nelle FAQ dell'ACN, tale attività si inserisce nella logica del Decreto NIS2.

Il Decreto [art. 3, co. 9, lett. f)], prevede infatti che la disciplina trovi applicazione, indipendentemente dalle dimensioni, anche nei confronti di soggetti che risultino critici in quanto elementi sistemici della catena di approvvigionamento (anche digitale) di uno o più soggetti "*essenziali*" o "*importanti*".

In questa prospettiva, la raccolta e strutturazione delle informazioni sui fornitori rilevanti assume una funzione che va oltre il singolo adempimento.

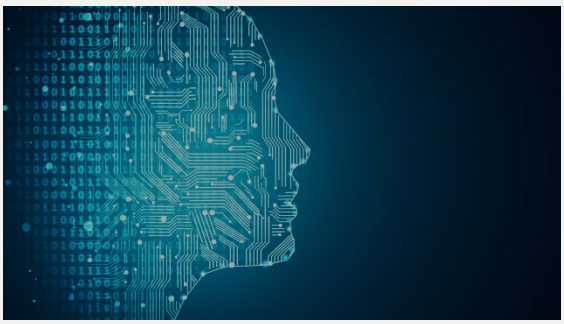
Tali informazioni consentono, anche d'intesa con le Autorità di settore, di individuare all'interno della *supply chain* quei fornitori che presentano un rilievo sistemico e che, proprio per questo, possono essere a loro volta qualificati come soggetti "essenziali" o "importanti".

In termini operativi, per i soggetti NIS tutto ciò si traduce in alcune attività difficilmente differibili:

- **mappare** (o eventualmente aggiornare) **i propri fornitori**, superando eventuali ricostruzioni parziali o stratificate nel tempo;
- **valutarne la criticità** in relazione ai servizi NIS e verificare, in concreto, la **fungibilità** delle forniture;
- **integrare la gestione della *supply chain*** nei processi di *compliance* NIS2, evitando che resti un ambito separato rispetto alle misure di sicurezza e alla gestione degli incidenti.

* * *

AI Act e Digital Omnibus: gli emendamenti del Parlamento europeo



Il 26 marzo 2026 il Parlamento europeo ha approvato una serie di emendamenti alla proposta della Commissione europea volta a modificare e semplificare l'AI Act (Regolamento UE 1689/2024) nell'ambito del c.d. Digital Omnibus (Proposta del 19 novembre 2025, COM(2025) 836), aprendo così la fase dei negoziati con Consiglio e Commissione europea.

Le modifiche incidono su alcuni snodi operativi della disciplina – dalle tempistiche di applicazione agli obblighi di trasparenza, fino al perimetro dei sistemi vietati – con effetti immediati sulle scelte organizzative e di *compliance* di fornitori e *deployer* coinvolti.

La posticipazione degli obblighi per i sistemi ad alto rischio

Il Parlamento interviene sul tema del rinvio degli obblighi per i sistemi di IA ad alto rischio introducendo un elemento che mancava nella proposta della Commissione: la certezza delle

scadenze. In particolare, vengono fissate due date chiave:

a. **2 dicembre 2027** per i sistemi di IA ad alto rischio esplicitamente elencati nell'AI Act nell'Allegato III, tra cui quelli relativi alla biometria, quelli utilizzati in infrastrutture critiche, istruzione, occupazione, servizi essenziali, giustizia e gestione delle frontiere;
b. **2 agosto 2028** per i sistemi di IA disciplinati da normative settoriali dell'UE in materia di sicurezza e vigilanza del mercato di cui all'Allegato I.

Fornitori e *deployer* avranno quindi più tempo per adeguarsi (gli obblighi erano inizialmente previsti rispettivamente per il 2 agosto 2026 e il 2 agosto 2027). Tuttavia, questo tempo aggiuntivo dovrà essere sfruttato per strutturare processi, responsabilità, controlli e dotarsi di una *governance* adeguata.

Analoga logica si ritrova nella proroga degli obblighi di trasparenza, applicabili anche per quei sistemi che presentano un rischio limitato (es., *chatbot*).

I fornitori avranno tempo di conformarsi all'obbligo di apporre una filigrana (*watermarking*) ai contenuti generati dall'IA quali audio, immagini, video o testi, al fine di indicarne l'origine fino al **2 novembre 2026**. Tali obblighi avrebbero dovuto applicarsi a partire dal prossimo 2 agosto 2026.

Il divieto dei "*deep nude*"

Tra le modifiche più discusse vi è l'inclusione tra i sistemi vietati (Art. 5 dell'AI Act) di quelli in grado di generare o manipolare contenuti realistici sessualmente espliciti o intimi di persone fisiche identificabili senza il loro consenso.

Tuttavia, la formulazione adottata dal Parlamento specifica che lo sviluppo di tali funzionalità non è di per sé vietato: il divieto non si applicherebbe, infatti, a quei sistemi che incorporano misure efficaci per impedire tali utilizzi.

Questa modifica sposta l'attenzione su un piano operativo: progettazione, controlli, limitazioni tecniche e monitoraggio diventano elementi determinanti per la liceità del sistema.

In tale ottica, dunque, la valutazione dell'adeguatezza delle misure tecniche di sicurezza adottate dai *provider* diventa essenziale alla luce del regime sanzionatorio applicabile, in base al quale l'ACN (Autorità per la Cybersicurezza Nazionale)[8] per queste violazioni può applicare sanzioni pecuniarie fino a 35 milioni di euro o al 7% del fatturato annuo globale.

AI *literacy*: la formazione in materia di AI

L'obbligo di garantire una formazione al personale coinvolto nel funzionamento e nell'uso dei sistemi di AI rappresenta uno dei primi obblighi ad essere entrato in vigore dell'AI Act (il 2 febbraio 2025).

Il Parlamento riscrive la norma in un'ottica di "supporto", con un'intensità inferiore rispetto alla versione corrente: fornitori e *deployer* dovranno supportare il miglioramento dell'alfabetizzazione in materia di IA per i propri dipendenti e le altre figure coinvolte.

Viene, quindi, cassata la proposta iniziale della Commissione che prevedeva che l'alfabetizzazione dovesse essere considerata non

[8] L'ACN è stata designata, con la L. 132/2025, come Autorità di vigilanza del mercato, responsabile della ricezione dei reclami relativi alle violazioni dell'AI Act, nonché dell'irrogazione delle sanzioni in caso di mancato rispetto delle disposizioni.

più come obbligo, ma come un incoraggiamento[9].

La modifica proposta dal Parlamento non riduce infatti la rilevanza operativa del tema. La capacità delle persone coinvolte di comprendere e gestire i sistemi di AI incide direttamente sulla possibilità di rispettare obblighi più strutturati: dalla gestione del rischio alla supervisione umana, fino alla qualità dei dati.

L'intervento della Commissione, chiamata – come previsto nel nuovo testo dell'Art. 4 dell'AI Act proposto dal Parlamento – a fornire orientamenti sull'attuazione di questo obbligo, conferma che il tema è destinato a incidere sulle scelte organizzative interne delle società.

Registrazione dei sistemi ad alto rischio e trattamento dei dati "sensibili"

Gli emendamenti intervengono anche su due ambiti operativi rilevanti. Sul fronte della registrazione, il Parlamento propone di mantenere l'obbligo di iscrizione nella banca dati UE dei sistemi ad alto rischio anche nei casi in cui il *provider* ritenga che il sistema non rientri in tale categoria.

È una scelta che privilegia la trasparenza nelle situazioni di incertezza, riducendo i margini di autovalutazione non verificabile.

Quanto al trattamento di categorie particolari di dati per il rilevamento e la correzione dei *bias*, viene ampliata la platea dei soggetti autorizzati, ma solo per il rilevamento e la correzione di *bias* che possano incidere negativamente sulla salute, sicurezza, diritti fondamentali delle persone o portare a discriminazione e fermo restando il criterio della stretta necessità.

Ne emerge un'impostazione coerente con l'approccio europeo in materia di protezione dei dati[10]: apertura funzionale, ma accompagnata da un elevato livello di *accountability*.

Conclusioni

Il rinvio delle scadenze offre una finestra temporale che deve essere utilizzata per rafforzare i modelli di *governance* dell'AI.

Allo stesso tempo, l'attenzione crescente sulla qualità delle misure tecniche e organizzative adottate rende sempre meno sostenibile un approccio meramente formale alla *compliance*.

Infine, i margini di discrezionalità lasciati agli operatori – dalla valutazione dei rischi alla gestione dei dati – richiedono competenze interne adeguate e processi decisionali strutturati.

In questa fase, dunque, *provider*, *deployer* e *stakeholder* coinvolti sono chiamati a utilizzare il tempo del trilogo non per attendere, ma per consolidare fin da ora modelli di governance coerenti con il quadro in evoluzione.

* * *

[9] Il testo della proposta iniziale del Digital Omnibus prevedeva infatti che la Commissione e gli Stati membri avrebbero dovuto incoraggiare fornitori e *deployer* ad adottare misure volte a garantire un livello sufficiente di alfabetizzazione in materi di Ai per il personale e qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di AI per loro conto.

[10] Per maggiori approfondimenti sulle proposte di modifica al GDPR e alla direttiva e-Privacy e al Parere Congiunto di EDPB e EDPS sul punto, si rinvia al nostro precedente contributo "*Digital Omnibus e protezione dei dati: il parere congiunto di EDPB e EDPS tra semplificazione e rischi di incertezza*".

Digital Omnibus e protezione dei dati: il parere congiunto di EDPB e EDPS tra semplificazione e rischi di incertezza

Il 19 novembre 2025 la Commissione europea (la "**Commissione**") ha presentato il Digital Omnibus [11], una proposta di riforma che interviene su un ampio *corpus* della legislazione digitale dell'Unione europea (la "**Proposta**").

L'obiettivo dichiarato è quello di semplificare il quadro normativo e ridurre gli oneri di compliance per le imprese, intervenendo su strumenti chiave quali il GDPR, il Data Act, la direttiva e-Privacy, la direttiva NIS2 e il Data Governance Act.

In questo contesto si inserisce il parere congiunto adottato l'11 febbraio 2026 dall'EDPB (*European Data Protection Board*) e dall'EDPS (*European Data Protection Supervisor*) (il "**Parere Congiunto**").

Le due Autorità accolgono positivamente l'intento della Commissione di rendere più coerente e gestibile il quadro regolatorio digitale europeo.

Tuttavia, il Parere Congiunto evidenza anche una tensione di fondo: alcune delle semplificazioni proposte rischiano di incidere su elementi strutturali del sistema della protezione dei dati, generando nuove incertezze giuridiche e riducendo potenzialmente il livello di tutela degli interessati.

Le semplificazioni accolte positivamente dalle Autorità

Il Parere Congiunto riconosce come alcune misure di semplificazione possano contribuire in maniera positiva alla coerenza dell'impianto normativo europeo. Si tratta, in particolare, di proposte di modifica che incidono sui seguenti ambiti:

- **ricerca scientifica**. La Proposta introduce una definizione esplicita di ricerca scientifica[12], chiarisce che l'art. 6(4) del GDPR (relativo a trattamenti per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti) non dovrebbe essere applicato in questo contesto [13] e prevede una deroga (limitata) all'obbligo di fornire

[11] Il Digital Omnibus si compone di tre diverse proposte normative (COM(2025) 837, 836 e 835, volte a semplificare la disciplina in materia di dati, personali e non (Data Act, GDPR, Data Governance Act, etc.), le norme sui cookie e le altre tecnologie di tracciamento previste dalla Direttiva e-Privacy, gli obblighi di segnalazione degli incidenti connessi alla cybersicurezza (NIS2), la corretta applicazione delle norme dell'AI Act, nonché altri aspetti relativi all'identificazione elettronica e ai servizi fiduciari nell'ambito del quadro europeo relativo a un'identità digitale.

[12] La Proposta prevede l'inserimento del n. 38) all'interno dell'art. 4 del GDPR, contenente la definizione di "ricerca scientifica", intendendosi con la stessa "*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 modo 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*".

[13] In particolare, EDPB e EDPS accolgono con favore che la Proposta chiarisca l'applicazione del principio di limitazione delle finalità (art. 5(1)(b) del GDPR), prevedendo che il trattamento ulteriore per scopi di archiviazione nel pubblico interesse, per scopi di ricerca scientifica o storica o per scopi statistici, debba essere considerato compatibile con le finalità iniziali, indipendentemente dalle condizioni dell'art. 6(4) del GDPR. Quest'ultimo, riguardante il trattamento ulteriore dei dati personali per finalità diverse da quelle per cui sono stati raccolti, stabilisce che, se il nuovo scopo non è compatibile con quello iniziale e non si basa sul consenso o sul diritto UE/Stato membro, il titolare deve verificare la compatibilità della nuova finalità con quella originaria, considerando il legame tra le finalità, il contesto, la natura dei dati, le conseguenze e le garanzie.

l'informativa privacy[14]. Secondo le Autorità, questi chiarimenti potrebbero facilitare l'utilizzo dei dati a fini di ricerca senza compromettere le garanzie fondamentali previste dal GDPR.

- **Autenticazione biometrica**. La Proposta introduce una nuova eccezione al divieto di trattamento di categorie particolari di dati quando i mezzi di verifica sono sotto il controllo esclusivo dell'interessato. In termini pratici, si tratta di scenari in cui i modelli biometrici non sono conservati nei sistemi del titolare del trattamento, ma rimangono memorizzati su un dispositivo detenuto dall'utente – come un *badge* o una *smart card* – oppure sono protetti da una chiave segreta accessibile solo all'interessato.

- ***Data breach***[15] e **DPIA**. La proposta estende il termine per la notifica alle autorità di controllo da 72 a 96 ore e modifica la soglia di notifica, prevedendo l'obbligo solo nei casi in cui la violazione comporti un "rischio elevato" per i diritti degli interessati. Parallelamente, si propone di introdurre modelli comuni per la notifica dei *data breach* e per lo svolgimento delle DPIA[16]. Le Autorità accolgono inoltre con favore la previsione di un punto di accesso unico per la segnalazione degli incidenti, attraverso il quale le imprese potrebbero adempiere contemporaneamente agli obblighi di notifica previsti da diverse normative europee – ad esempio NIS2 o DORA – mediante un'unica interfaccia.

Le modifiche che rischiano di creare nuove incertezze

Accanto agli elementi positivi, il Parere Congiunto esprime forti riserve su alcune modifiche che potrebbero incidere negativamente sul livello di protezione e/o rendere più difficile per gli interessati esercitare i propri diritti.

La questione più delicata riguarda la proposta di modificare la definizione di "**dato personale**". La Commissione propone di codificare una lettura più "soggettiva" del concetto, secondo la quale un'informazione non dovrebbe essere considerata dato personale per una determinata impresa se quest'ultima non è in grado di identificare la persona fisica cui l'informazione si riferisce.

Secondo EDPB e EDPS, questa modifica andrebbe ben oltre una semplice precisazione tecnica del GDPR. Essa restringerebbe significativamente la nozione di dato personale e potrebbe incoraggiare interpretazioni opportunistiche da parte dei titolari del trattamento.

In particolare, le Autorità osservano che la Proposta non tiene adeguatamente conto di elementi centrali dell'attuale interpretazione del concetto di dato personale, come la possibilità di "*singling out*", ossia la capacità di isolare o distinguere un individuo all'interno di un insieme di dati anche senza identificarlo direttamente[17].

[14] La Proposta prevede che l'informativa non sarà necessaria se la fornitura delle informazioni si riveli impossibile o implichi uno sforzo sproporzionato, oppure se è probabile che ciò renda impossibile o pregiudichi gravemente il conseguimento delle finalità. In ogni caso, il titolare dovrà adottare misure appropriate per tutelare diritti e libertà degli interessati, anche rendendo pubbliche le informazioni.

[15] Per maggiori approfondimenti sulle modifiche previste nella Proposta in riferimento ai *data breach*, si rinvia a un nostro precedente contributo, disponibile qui.

[16] La Proposta attribuisce inoltre alla Commissione europea il compito di approvare e rivedere o modificare tali modelli. L'EDPB e l'EDPS ritengono invece che l'EDPB dovrebbe essere pienamente responsabile sia della preparazione sia dell'approvazione di tali documenti, mentre all'EDPS dovrebbero essere attribuite competenze corrispondenti nell'ambito dell'EUDPR (Reg. 2018/1725, ossia la normativa sulla protezione dei dati personali applicabile alle istituzioni, organi e organismi dell'UE).

[17] Tale principio viene espresso all'interno del Considerando 26 del GDPR, quale prevede espressamente che: "*[…]. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare*

Per queste ragioni, il Parere Congiunto invita esplicitamente i co-legislatori a non adottare le modifiche proposte.

Una criticità analoga emerge in relazione alla **pseudonimizzazione**. La Proposta introduce un nuovo art. 41-*bis* del GDPR che attribuirebbe alla Commissione il potere di adottare atti di esecuzione per stabilire quando i dati pseudonimizzati possano non essere più considerati dati personali per determinate entità.

Anche in questo caso le Autorità esprimono forti perplessità: stabilire quando un'informazione cessa di essere dato personale incide direttamente sull'ambito di applicazione del GDPR e, secondo EDPB ed EDPS, una decisione di tale portata non dovrebbe essere delegata a un atto di esecuzione della Commissione.

***Cookie*, consenso e nuove regole per i dati nei dispositivi**

Un altro aspetto rilevante riguarda il tentativo della Commissione di affrontare il problema della "***consent fatigue***" generata dalla proliferazione dei *cookie banner*.

La Proposta mira a trasferire parte della disciplina prevista dalla direttiva e-Privacy all'interno del GDPR. In particolare, verrebbe introdotto un nuovo art. 88-*bis* relativo alla protezione dei dati memorizzati nelle apparecchiature terminali degli utenti.

L'obiettivo è semplificare il quadro normativo, ma secondo il Parere Congiunto la soluzione proposta rischia di produrre l'effetto opposto. La disciplina verrebbe infatti divisa tra GDPR (per i dati personali) e direttiva ePrivacy (per i dati non personali), mentre nella pratica le informazioni presenti nei dispositivi degli utenti possono includere entrambe le tipologie.

Questo renderebbe spesso necessario un esame caso per caso per determinare quale regime applicare, mantenendo inoltre una frammentazione della supervisione tra autorità diverse.

La Proposta amplia inoltre le **eccezioni al consenso** per l'accesso ai dati memorizzati nell'apparecchiatura terminale[18], includendo – tra le altre – la fornitura di servizi esplicitamente richiesti, la misurazione dell'*audience* e finalità di sicurezza.

Le Autorità ritengono necessario introdurre limiti più stringenti, soprattutto nel caso dell'*audience measurement*, che dovrebbe basarsi su dati aggregati anonimi e non essere utilizzato per altre finalità né combinato con dati provenienti da altri servizi (del fornitore o di terzi), né tantomeno i dati dovrebbero essere condivisi con terzi.

Interessante è invece il suggerimento avanzato nel Parere Congiunto di prevedere una specifica eccezione per la **pubblicità contestuale**, considerata generalmente meno invasiva rispetto alla pubblicità comportamentale perché basata esclusivamente sulla visita corrente a una pagina *web* o su una singola *query* di ricerca e priva di collegamenti con l'attività passata o futura dell'utente.

del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. […]"

[18] Il nuovo art. 88-*bis* prevede che il trattamento è consentito per effettuare la trasmissione di una comunicazione elettronica su una rete di comunicazione elettronica; per fornire un servizio esplicitamente richiesto dall'interessato; per generare informazioni aggregate sull'uso di un servizio online per misurare l'*audience* di tale servizio (solo uso interno del titolare); per mantenere o ripristinare la sicurezza di un servizio o del terminale.

Intelligenza artificiale e basi giuridiche del trattamento

La Proposta interviene anche sul rapporto tra GDPR e sviluppo/funzionamento di sistemi e modelli di intelligenza artificiale ("**IA**"). In particolare, riconosce esplicitamente il **legittimo interesse** possa costituire, in determinate circostanze, una base giuridica per lo sviluppo o il funzionamento di sistemi o modelli di IA.

EDPB e EDPS concordano sul principio, ma osservano che la formulazione proposta non introduce chiarimenti sostanziali rispetto all'interpretazione già fornita dall'EDPB nel Parere 28/2024[19].

Le Autorità suggeriscono quindi di esplicitare alcuni aspetti operativi, tra cui la necessità di effettuare una **LIA** (*legitimate interest assessment*) e verificare, dunque, che gli interessi e i diritti fondamentali degli interessati non prevalgano su quelli del titolare.

Un tema analogo emerge con riferimento al **trattamento incidentale di categorie particolari di dati durante l'addestramento di sistemi di IA**, ad esempio nel caso dei modelli di IA generativa.

Le Autorità riconoscono che in tali contesti può essere difficile evitare completamente il trattamento di dati "sensibili", ma raccomandano di limitare espressamente l'eccezione ai casi in cui tale trattamento sia effettivamente incidentale e residuale e di prevedere adeguate garanzie lungo l'intero ciclo di vita del sistema di IA.

Diritto di accesso e decisioni automatizzate

La Proposta affronta anche due temi operativi particolarmente rilevanti: l'abuso del diritto di accesso e il processo decisionale automatizzato.

Nel primo caso, la Commissione propone che il titolare del trattamento possa rifiutare una richiesta di accesso o richiedere un corrispettivo ragionevole qualora l'interessato eserciti tale diritto per finalità diverse dalla tutela dei propri dati personali.

EDPB e EDPS ritengono positivo chiarire cosa possa costituisce un abuso, ma sottolineano che ciò non dovrebbe essere collegato all'esercizio del diritto di accesso per finalità diverse dalla protezione dei dati in quanto il GDPR contribuisce anche alla tutela di altri diritti fondamentali.

Secondo il Parere Congiunto, il concetto di "abuso di diritti" dovrebbe essere collegato piuttosto alla presenza di un intento abusivo evidente, come l'intenzione di causare un danno al titolare.

Per quanto riguarda il processo decisionale automatizzato, le Autorità accolgono con favore l'obiettivo di chiarire le eccezioni al divieto previsto dal GDPR[20], ma raccomandano di evitare formulazioni che possano suggerire che tali decisioni siano automaticamente ammissibili ogni volta che esiste un rapporto contrattuale, indipendentemente dal requisito della necessità.

Conclusioni

Il Parere Congiunto dell'EDPB e dell'EDPS mette in luce un nodo centrale nel dibattito europeo sulla regolazione digitale: semplificare è necessario per ridurre gli oneri amministrativi e

[19] Per maggiori approfondimenti su tale parere, rinviamo al nostro precedente contributo "*Protezione dei dati personali nell'IA: il Parere dell'EDPB su anonimizzazione, interesse legittimo e conseguenze di un trattamento illecito*".

[20] Il nuovo testo dell'art. 22 del GDPR consente l'adozione di decisioni interamente automatizzate qualora le stesse siano necessarie all'esecuzione di un contratto tra titolare e interessato, anche se tali decisioni potrebbero teoricamente essere ottenute in modo manuale.

rafforzare la competitività dell'Unione europea, ma la semplificazione non può tradursi in una riduzione del livello di tutela dei diritti fondamentali.

Se alcune delle modifiche proposte dalla Commissione sembrano effettivamente idonee a razionalizzare obblighi e procedure – ad esempio in materia di notifiche di *data breach* o coordinamento tra normative europee – altre incidono su concetti cardine del diritto della protezione dei dati e rischiano di generare nuove incertezze interpretative.

Il Digital Omnibus è ora all'esame del Parlamento europeo e del Consiglio. Solo nelle prossime fasi del processo legislativo sarà possibile comprendere se (e in quale misura) le raccomandazioni delle Autorità saranno recepite dal legislatore.

* * *

Adozione dell'IA in azienda: roadmap MLPS e impatti sul lavoro

L'irruzione dell'intelligenza artificiale ("**IA**") nell'ecosistema lavorativo non costituisce un mero fenomeno di innovazione tecnologica, ma rappresenta un punto di snodo che interroga le fondamenta stesse del **diritto del lavoro**. Al centro vi sono i **processi decisionali**, i meccanismi di **accountability** e la capacità dell'ordinamento di orientare l'innovazione nel rispetto dei principi costituzionali di **dignità del lavoratore** e di tutela della persona.

È proprio per rispondere a questa esigenza che il **Ministero del Lavoro e delle Politiche Sociali (MPLS)** ha adottato, con Decreto del 20 dicembre 2025, n. 180, le **Linee Guida per l'implementazione dell'intelligenza artificiale nel mondo del lavoro**.

Le Linee Guida del MLPS si configurano come strumento di traduzione operativa di un quadro normativo che, pur ambizioso nei principi, necessita di essere reso **accessibile** e praticabile per il tessuto produttivo nazionale.

Esse propongono una roadmap metodologica per un'adozione dell'IA strutturata e sostenibile, fondata su trasparenza, equità, sicurezza e controllo umano, valorizzando soprattutto il "come" implementare l'innovazione.

L'obiettivo è garantire che l'adozione dell'IA non produca **esternalità negative** .

Tra queste ultime, assume particolare rilevanza il tema delle riorganizzazioni aziendali e dei licenziamenti, come di recente sottolineato anche dalla sentenza del **Tribunale di Roma del 19 novembre 2025**, la quale – pur non affrontando direttamente il tema dell'intelligenza artificiale – offre spunti interpretativi rilevanti, ma solleva anche interrogativi critici.

L'Avv. Carlo Impalà e l'Avv. Polliani ne hanno parlato su Agenda Digitale – Network360.

Per maggiori informazioni e approfondimenti

Carlo Impalà
Partner e Responsabile Osservatorio TMT&DP

Carlo.Impala@MorriRossetti.it

Morri Rossetti & Franzosi **Osservatorio TMT&DP**

OSSERVATORIO
TMT·DATA PROTECTION
di Morri Rossetti & Franzosi

Piazza Eleonora Duse, 2
20122 Milano
MorriRossetti.it

Osservatorio-dataprotection.it