

Nuove linee guida EDPS sull'IA generativa: titolare del trattamento, provider o deployer?



La rivoluzione silenziosa nella governance dei dati personali.

Una trasformazione paradigmatica sta ridefinendo l'architettura della protezione dei dati personali nell'ecosistema dell'intelligenza artificiale generativa. Le Linee Guida dell'EDPS del 28 ottobre 2025 hanno introdotto un principio dirompente che destabilizza certezze consolidate: le categorie tecniche dell'AI Act – *provider, developer, deployer* – non trovano corrispondenza automatica nelle figure giuridiche del Regolamento (UE) 2016/679 (GDPR).

Questo disallineamento ontologico tra lessico tecnologico e tassonomia giuridica impone una riflessione profonda sulla distribuzione delle responsabilità nel trattamento dei dati personali. La domanda che emerge con urgenza crescente – chi è realmente il titolare del trattamento? – non ammette più risposte aprioristiche.

Il framework normativo europeo: GDPR e AI Act a confronto

La grammatica giuridica del GDPR

Il GDPR articola un sistema tripartito di responsabilità fondato su criteri funzionali, non nominalistici. L'articolo 4, paragrafi 7 e 8, definisce con precisione:

Il *controller* (titolare del trattamento) è la persona fisica o

giuridica che determina le finalità e i mezzi del trattamento. Il *joint controller* (contitolare) opera quando due o più titolari determinano congiuntamente finalità e mezzi. Il *processor* (responsabile del trattamento) è chi tratta dati personali per conto del titolare.

La giurisprudenza della Corte di Giustizia dell'Unione Europea ha progressivamente affinato questi concetti attraverso pronunce fondamentali. Nella sentenza C-210/16 *Wirtschaftsakademie Schleswig-Holstein* del 5 giugno 2018, la Corte ha stabilito che la qualificazione di titolare dipende dall'effettivo potere decisionale, non dalla designazione contrattuale. L'amministratore di una fan page Facebook è stato considerato contitolare con la piattaforma per il trattamento dei dati dei visitatori, nonostante non avesse accesso diretto ai dati personali raccolti tramite cookie.

Tale principio è stato consolidato nella sentenza C-40/17 *Fashion ID* del 29 luglio 2019, dove l'integrazione del pulsante *Like* di Facebook in un sito web è stata ritenuta sufficiente a configurare una contitolarità limitata alla fase di raccolta e trasmissione dei dati.

Il lessico tecnico dell'AI Act

Il Regolamento (UE) 2024/1689 sull'Intelligenza Artificiale, entrato in vigore il 1° agosto 2024, introduce una terminologia funzionale alla catena del valore dell'IA. Il *provider* (fornitore) è chi sviluppa o fa sviluppare un sistema di IA e lo immette sul mercato. Il *deployer* (utilizzatore) è chi utilizza un sistema di IA sotto la propria autorità. Queste categorie rispondono a logiche di mercato e conformità tecnica, non a criteri di *accountability* sul trattamento dei dati personali.

Come chiarisce esplicitamente il documento EDPS: "I termini *provider*, *developer* e *deployer*, comunemente utilizzati nel settore tecnologico e in altri quadri normativi come l'AI Act,

non corrispondono ai concetti di protezione dei dati di *controller*, *processor* e *joint controller*.”

L'evoluzione interpretativa dell'EDPS: dal 2024 al 2025

Le Orientations del giugno 2024

Il 3 giugno 2024, l'EDPS ha pubblicato le prime Orientations sull'IA generativa, un documento destinato alle istituzioni europee soggette al Regolamento (UE) 2018/1725. Il testo riconosceva già l'autonomia concettuale tra categorie AI Act e ruoli GDPR, ma manteneva un approccio preliminare nell'analisi delle responsabilità.

Le Linee Guida del 28 ottobre 2025: il cambio di paradigma

Le Linee Guida aggiornate segnano una discontinuità interpretativa significativa. Il documento, strutturato in sedici sezioni operative, fornisce indicazioni dettagliate sulla determinazione dei ruoli in ogni fase del ciclo di vita dei sistemi di IA generativa.

L'EDPS introduce un'analisi più granulare, costruendo sulle Linee Guida EDPB 07/2020 sui concetti di titolare e responsabile, che distinguono tra *essential means* (mezzi essenziali) e *non-essential means* (mezzi non essenziali) del trattamento.

I mezzi essenziali includono la tipologia di dati trattati, le categorie di interessati, la durata del trattamento e i destinatari dei dati. Chi li determina è titolare o contitolare. I mezzi non essenziali comprendono invece misure tecniche e organizzative di sicurezza, piattaforme hardware e software specifici, che possono essere delegati al *processor*.

La svolta interpretativa riconosce che i provider di sistemi di IA generativa spesso determinano *de facto* mezzi essenziali del trattamento attraverso l'architettura del modello e i dati di addestramento, le modalità di elaborazione dei *prompt*, la conservazione e il riutilizzo degli input per il *fine-tuning*, e le politiche di *data retention* incorporate nel servizio.

Il contributo dell'EDPB Opinion 28/2024

Il Parere 28/2024 dell'EDPB, adottato il 17 dicembre 2024 su richiesta dell'autorità irlandese per la protezione dei dati, affronta aspetti cruciali del trattamento di dati personali nel contesto dei modelli di IA.

Il parere chiarisce la distinzione tra fase di sviluppo (*development*) e fase di distribuzione (*deployment*) dei modelli. Lo sviluppo comprende tutte le fasi precedenti alla distribuzione, inclusi lo sviluppo del codice, la raccolta dei dati di addestramento, la loro pre-elaborazione e l'addestramento stesso. La distribuzione copre tutte le fasi relative all'utilizzo del modello.

L'EDPB stabilisce inoltre che un modello di IA può essere considerato anonimo solo quando sia la probabilità di estrazione diretta o probabilistica di dati personali, sia la probabilità di ottenere tali dati attraverso *query*, risultino insignificanti per qualsiasi interessato.

Il test di determinazione: chi decide davvero?

Anatomia del potere decisionale nell'IA generativa

L'applicazione del test funzionale di titolarità ai sistemi di IA generativa rivela una complessità inedita. Quando un'organizzazione integra un *Large Language Model* nei propri

processi, la mappa delle responsabilità non segue automaticamente i confini contrattuali.

Il documento EDPS propone un esempio illuminante. Un'istituzione europea (EUI-D) sviluppa uno strumento di IA generativa per supportare i dipartimenti risorse umane di altre istituzioni. Durante la fase di sviluppo, EUI-D si qualifica come titolare perché determina le finalità (creare uno strumento per ottimizzare i flussi di lavoro) e i mezzi del trattamento (selezionando i dati e definendo la struttura dei *prompt*). Il fornitore terzo del modello linguistico, pur essendo componente chiave dello sviluppo, non determina finalità né mezzi specifici di questo trattamento iniziale.

Quando un'altra istituzione (EUI-X) acquista e implementa lo strumento, si qualifica come titolare autonomo perché determina le proprie finalità e mezzi essenziali. EUI-D opera come titolare separato, non essendo coinvolto nel trattamento di EUI-X.

La situazione cambia radicalmente se le due istituzioni sviluppassero congiuntamente lo strumento per ottimizzare i rispettivi processi HR: in questo caso sarebbero contitolari per il trattamento nella fase di sviluppo.

La contitolarità emergente

Le nuove Linee Guida aprono alla possibilità che molti rapporti provider-deployer configurino una contitolarità ex articolo 26 GDPR, non una relazione titolare-responsabile ex articolo 28. Questa riqualificazione comporta conseguenze operative rilevanti: necessità di un accordo di contitolarità che definisca le rispettive responsabilità, obbligo di rendere disponibile agli interessati il contenuto essenziale dell'accordo, responsabilità solidale per i danni derivanti dal trattamento, e revisione delle informative privacy attualmente in uso.

Implicazioni operative per le organizzazioni

La *due diligence* rafforzata

Le organizzazioni che intendono implementare soluzioni di IA generativa devono sviluppare un processo di *Privacy by Design* potenziato. Le Linee Guida EDPS raccomandano di definire chiaramente finalità e base giuridica, determinare e documentare ruoli e responsabilità, garantire che le attività di trattamento siano registrate nei *records*, condurre una valutazione dei rischi specifica per l'IA generativa, effettuare una valutazione d'impatto sulla protezione dei dati (DPIA) quando richiesta, implementare i principi fondamentali di protezione dei dati, predisporre procedure robuste per gestire i diritti degli interessati, e svolgere una *due diligence* approfondita sui fornitori terzi.

Il ruolo del DPO

L'EDPS sottolinea che il *Data Protection Officer* deve avere una comprensione adeguata del ciclo di vita del sistema di IA generativa che l'organizzazione intende acquisire, progettare o implementare. Questo significa ottenere informazioni su quando e come questi sistemi trattano dati personali, come funzionano i meccanismi di input e output, e quali processi decisionali sono implementati attraverso il modello.

La responsabilità di garantire la conformità al regolamento rimane in capo al titolare. L'implementazione di sistemi di IA generativa in conformità con la normativa non dovrebbe essere uno sforzo individuale ma richiedere un dialogo continuo tra tutti gli *stakeholder* coinvolti nel ciclo di vita del prodotto.

Il web scraping: un terreno minato

Le Linee Guida affrontano con particolare attenzione l'uso di tecniche di *web scraping* per la raccolta di dati di addestramento. L'EDPS riconosce che questa pratica comporta rischi significativi, considerando che gli individui possono perdere il controllo delle proprie informazioni personali quando queste vengono raccolte senza la loro conoscenza, contro le loro aspettative, e per finalità diverse da quelle della raccolta originaria.

Il trattamento di dati personali pubblicamente disponibili rimane soggetto alla normativa europea sulla protezione dei dati. Se viene identificata una base giuridica per il *web scraping*, le organizzazioni devono comunque garantire il rispetto degli obblighi di trasparenza. Considerando le difficoltà nel garantire che la raccolta di dati personali tramite *web scraping* sia conforme al regolamento, l'EDPS raccomanda di utilizzare fonti alternative di dati personali, ove possibile.

Il problema delle allucinazioni e dell'accuratezza

I sistemi di IA generativa possono produrre output contenenti informazioni inesatte o false, inclusi dati personali: le cosiddette "allucinazioni". L'EDPS richiede che le organizzazioni valutino attentamente l'accuratezza dei dati durante l'intero ciclo di vita dei sistemi di IA generativa e riconsiderino l'uso di tali sistemi se l'accuratezza non può essere mantenuta.

Le Linee Guida propongono un esempio pratico: un'istituzione utilizza un sistema di IA generativa per analizzare le candidature di lavoro, creando sintesi standardizzate delle qualifiche dei candidati. Per mitigare le allucinazioni e le imprecisioni, l'istituzione implementa una fase di verifica

manuale per ogni sintesi generata dall'IA, assicurandosi che rifletta accuratamente i dati forniti dai candidati.

Sicurezza: nuove vulnerabilità, nuove responsabilità

L'uso di sistemi di IA generativa può amplificare rischi di sicurezza esistenti o crearne di nuovi. L'EDPS identifica vulnerabilità specifiche: *model inversion attacks* (attacchi che estraggono informazioni dal modello attraverso *reverse-engineering*), *prompt injection* (iniezione di istruzioni malevole mascherate da input innocui), e *jailbreaks* (tecniche per aggirare le protezioni del modello).

Il documento raccomanda l'uso di tecniche di *red teaming* per scoprire ed esporre vulnerabilità sconosciute, e avverte che quando si utilizza la *Retrieval Augmented Generation*, è necessario verificare che il sistema non stia diffondendo dati personali dalla base di conoscenza.

Scenari prospettici: verso un nuovo equilibrio

L'ipotesi di coordinamento normativo

Il disallineamento sistematico tra categorie AI Act e ruoli GDPR richiederà probabilmente interventi di raccordo. Il Parere congiunto EDPB-EDPS 5/2021 sulla proposta di AI Act aveva già sottolineato la necessità di chiarire il rapporto tra i due quadri normativi.

L'EDPB ha inoltre adottato la Dichiarazione 3/2024 sul ruolo delle autorità di protezione dei dati nel framework dell'AI Act, raccomandando che le DPA siano designate come autorità di vigilanza del mercato per i sistemi di IA ad alto rischio che incidono sui diritti e le libertà delle persone fisiche in relazione al trattamento dei dati personali.

L'autodeterminazione algoritmica come frontiera

Un'evoluzione particolarmente rilevante riguarda i sistemi di IA con capacità di apprendimento continuo. Quando un modello generativo modifica autonomamente i propri parametri sulla base delle interazioni – determinando di fatto nuovi mezzi di trattamento – chi è il titolare di questo trattamento evolutivo?

L'EDPS riconosce che alcune di queste domande rimangono aperte e che ulteriori questioni emergeranno probabilmente con l'aumento dell'uso di questi sistemi e l'evoluzione della tecnologia.

Conclusioni: dalla presunzione alla verifica

Le Linee Guida EDPS del 28 ottobre 2025 sull'IA generativa codificano un principio metodologico fondamentale: la qualificazione dei ruoli privacy richiede un'analisi fattuale, non presuntiva. Il contratto è un indizio, non una prova. La denominazione commerciale è un'etichetta, non una qualificazione giuridica.

Per le organizzazioni, questo significa abbandonare l'approccio *checkbox* alla compliance e sviluppare competenze di analisi sostanziale dei flussi di dati e dei centri decisionali. Per i provider, implica una maggiore trasparenza sulle effettive operazioni di trattamento e la disponibilità a negoziare architetture contrattuali coerenti con la realtà operativa.

La domanda "il titolare sei tu o il provider?" non ammette una risposta universale. Ammette solo un metodo: guardare oltre le etichette, analizzare chi decide cosa, documentare questa analisi, e costruire accordi contrattuali che riflettano la

distribuzione reale del potere sui dati personali.

In un ecosistema dove i *Large Language Model* elaborano miliardi di *prompt* quotidianamente, la corretta attribuzione della titolarità non è un esercizio teorico. È la condizione per garantire che il diritto alla protezione dei dati personali – pietra angolare della Carta dei Diritti Fondamentali dell'Unione Europea – mantenga effettività nell'era dell'intelligenza artificiale generativa.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/linee-guida-edps/>