

Roma, 07/10/2026

Prot. 0007787

Com. n. 39

Oggetto: AI Act e protezione dei dati personali – Profili di coordinamento con il GDPR

AI Act e GDPR devono essere applicati congiuntamente. Il GDPR continua a disciplinare il trattamento dei dati personali e ogni sistema di IA che utilizza tali dati deve avere una valida base giuridica. L'adozione dell'IA non elimina gli obblighi del GDPR, ma richiede di integrare la governance dell'IA con quella della protezione dei dati personali.

AI Act e protezione dei dati personali – Profili di coordinamento con il GDPR

Il Regolamento (UE) 2024/1689 sull'intelligenza artificiale ("AI Act") disciplina in maniera organica lo sviluppo, l'immissione sul mercato e l'utilizzo dei sistemi di intelligenza artificiale, introducendo un quadro normativo basato sul livello di rischio associato ai diversi sistemi.

La disciplina della protezione dei dati personali resta tuttavia primariamente affidata al Regolamento (UE) 2016/679 ("GDPR"), che continua a trovare piena applicazione anche nell'ambito dei sistemi di intelligenza artificiale.

L'interazione tra le due normative impone pertanto ai soggetti che sviluppano o utilizzano sistemi di intelligenza artificiale di considerare congiuntamente gli obblighi derivanti dall'AI Act e quelli previsti dalla normativa in materia di protezione dei dati personali.

Gli obblighi di trasparenza nell'AI Act

Il principio di trasparenza costituisce uno degli elementi centrali dell'AI Act (cfr. [nota del 6 febbraio 2025](#) e [nota del 23 settembre 2026](#) del Settore Marketing, Innovazione e Internazionalizzazione) e mira a garantire che lo sviluppo e l'utilizzo dei sistemi di intelligenza artificiale avvengano in condizioni tali da consentire un'adeguata tracciabilità e comprensibilità del loro funzionamento.

In particolare, **l'articolo 50 dell'AI Act** introduce specifici obblighi di trasparenza con riguardo a determinate categorie di sistemi di intelligenza artificiale, tenendo conto dei rischi di manipolazione che tali sistemi possono comportare per le persone fisiche.

Nel caso di sistemi che interagiscono direttamente con le persone fisiche, deve essere garantito che queste siano informate del fatto di interagire con un sistema di intelligenza artificiale, salvo che ciò risulti evidente dalle circostanze e dal contesto.

Analogamente, devono essere rese note le circostanze in cui i contenuti visualizzati siano stati generati o manipolati artificialmente.

Le informazioni devono essere fornite in maniera chiara e distinguibile, al più tardi al momento della prima interazione o esposizione della persona fisica al sistema.

Esempio: il chatbot del negozio

Si pensi a un negozio online che utilizzi un chatbot basato sull'intelligenza artificiale – ovvero un'applicazione software che comunica con le persone tramite testo o voce – per rispondere alle domande dei clienti su prodotti, disponibilità, tempi di consegna e modalità di reso.

Il cliente dovrebbe essere messo nella condizione di comprendere che sta interagendo con un sistema di IA e non necessariamente con un operatore umano.

Una formulazione semplice potrebbe essere, ad esempio:

"Stai interagendo con un assistente virtuale basato sull'intelligenza artificiale. Le risposte sono generate automaticamente. Per assistenza personalizzata puoi richiedere l'intervento di un operatore."

La trasparenza richiesta dall'AI Act *non deve tuttavia essere confusa con l'informativa privacy prevista dal GDPR*. La prima riguarda il fatto che l'interessato interagisca con un sistema di IA e, nei casi previsti, le caratteristiche del contenuto generato o manipolato; la seconda riguarda le modalità di trattamento dei dati personali.

La trasparenza prevista dal GDPR

Il GDPR continua a imporre specifici obblighi informativi nei confronti degli interessati e integra la disciplina dell'AI Act per tutti gli aspetti non espressamente regolati da quest'ultimo.

Lo stesso articolo 50, paragrafo 6, dell'AI Act stabilisce, infatti, che restano impregiudicati gli ulteriori obblighi di trasparenza previsti da altre disposizioni del diritto dell'Unione o nazionale.

In base al GDPR, l'informativa deve comprendere, tra l'altro, informazioni relative:

- all'identità e ai dati di contatto del titolare del trattamento;
- alle finalità del trattamento e alle relative basi giuridiche;
- ai tempi di conservazione dei dati personali;
- agli eventuali destinatari o categorie di destinatari dei dati;
- agli eventuali trasferimenti di dati personali verso Paesi terzi o organizzazioni internazionali.

Per l'impresa, ciò significa che **l'aggiunta di uno strumento di IA non rende sufficiente un generico riferimento all'intelligenza artificiale nell'informativa privacy**. Occorre verificare quale trattamento di dati personali venga concretamente effettuato e aggiornare l'informativa quando necessario.

Esempio: programma fedeltà e offerte personalizzate

Si consideri un supermercato o un negozio di abbigliamento che utilizzi l'IA per analizzare gli acquisti effettuati dai clienti iscritti al programma fedeltà e proporre automaticamente prodotti o sconti personalizzati.

Il sistema potrebbe, ad esempio, rilevare che un cliente acquista frequentemente determinati prodotti e utilizzare tali informazioni per inviargli offerte mirate.

In questo caso occorre distinguere almeno due aspetti:

- **l'utilizzo dell'IA**, che deve essere valutato alla luce dell'AI Act e degli eventuali obblighi di trasparenza applicabili;
- **il trattamento dei dati personali del cliente**, che deve rispettare il GDPR, compresi gli obblighi relativi alla base giuridica, all'informativa, alla minimizzazione dei dati e, ove applicabile, alla profilazione.
-

Non è quindi sufficiente comunicare al cliente che "le offerte sono personalizzate tramite intelligenza artificiale": l'informativa deve consentire di comprendere anche quali dati vengono utilizzati, per quali finalità e secondo quale presupposto di liceità.

Un'ulteriore questione riguarda l'individuazione degli interessati ai quali deve essere resa l'informativa sul trattamento dei dati personali.

Un sistema di intelligenza artificiale può, infatti, trattare dati personali riferibili a un numero potenzialmente molto elevato e indeterminato di interessati, acquisendoli da fonti diverse. In tali circostanze, informare individualmente ciascun interessato può risultare impossibile o richiedere uno sforzo sproporzionato.

Come chiarito dallo *European Data Protection Board* ("EDPB"), può trovare applicazione l'esenzione prevista dall'articolo 14 par.5 lett.b) del GDPR, purché ne siano soddisfatti i relativi presupposti. Resta, tuttavia, necessario assicurare la disponibilità delle informazioni rilevanti sul trattamento, anche mediante la loro diffusione pubblica, incluse, in particolare, le indicazioni relative alle fonti dalle quali il sistema di intelligenza artificiale acquisisce i dati personali e alle modalità attraverso cui gli interessati possono esercitare il diritto di opposizione al trattamento.

Diversamente, quando i dati personali sono raccolti direttamente dall'interessato nel corso dell'interazione con il sistema di intelligenza artificiale, trovano applicazione gli obblighi informativi previsti dall'articolo 13 del GDPR e l'informativa deve essere resa direttamente all'interessato.

Particolare rilevanza assume inoltre la disciplina degli articoli 13, paragrafo 2, lettera f), e 14, paragrafo 2, lettera g), del GDPR, applicabile quando il trattamento comporti

processi decisionali automatizzati, compresa la profilazione, idonei a produrre effetti giuridici o ad incidere significativamente sull'interessato.

In tali ipotesi, l'interessato deve ricevere informazioni significative sulla logica utilizzata, nonché sull'importanza e sulle conseguenze previste del trattamento.

Ciò non significa, tuttavia, che l'informativa debba necessariamente descrivere gli aspetti tecnici degli algoritmi o dell'architettura del sistema. L'articolo 12, paragrafo 1, del GDPR richiede infatti che le informazioni siano fornite in forma concisa, trasparente, intelligibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

L'obiettivo deve pertanto essere quello di fornire agli interessati informazioni effettivamente comprensibili e utili per comprendere il trattamento, il ruolo dell'intelligenza artificiale e le relative conseguenze.

La base giuridica del trattamento

L'utilizzo di sistemi di intelligenza artificiale che comportino il trattamento di dati personali deve essere sorretto da una valida base giuridica ai sensi dell'articolo 6 del GDPR.

La scelta della base giuridica deve essere effettuata in relazione allo specifico trattamento e alle concrete finalità perseguite, senza che l'utilizzo dell'intelligenza artificiale possa costituire, di per sé, una base di liceità.

In determinate circostanze, il trattamento può essere necessario per l'esecuzione di un contratto di cui l'interessato è parte o per l'adozione di misure precontrattuali richieste dall'interessato, ai sensi dell'articolo 6, paragrafo 1, lettera b), del GDPR. Ciò può verificarsi, ad esempio, nell'ambito di servizi basati sull'intelligenza artificiale, quali chatbot o altri strumenti interattivi, qualora il trattamento dei dati personali sia effettivamente necessario per fornire il servizio richiesto.

La base giuridica potrà tuttavia essere utilizzata soltanto quando sussista un effettivo nesso di necessità tra il trattamento dei dati e l'esecuzione del contratto.

In presenza dei presupposti previsti dalla normativa, il trattamento può fondarsi anche sulla necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, ai sensi dell'articolo 6, paragrafo 1, lettera e), del GDPR.

In altri casi, il trattamento dovrà essere fondato sul consenso dell'interessato, ai sensi dell'articolo 6, paragrafo 1, lettera a), del GDPR. L'interessato deve poter revocare il consenso in qualsiasi momento, fermo restando che la revoca non pregiudica la liceità dei trattamenti effettuati prima della stessa.

Un'ulteriore base giuridica potenzialmente rilevante è costituita dal legittimo interesse del titolare del trattamento o di un terzo, previsto dall'articolo 6, paragrafo 1, lettera f), del GDPR.

Il ricorso a tale base giuridica richiede tuttavia un'attenta valutazione degli interessi, dei diritti e delle libertà fondamentali degli interessati, verificando che questi ultimi non prevalgano sul legittimo interesse perseguito.

L'importanza del principio di accountability

L'integrazione tra AI Act e GDPR evidenzia come la conformità normativa nell'ambito dell'intelligenza artificiale non possa essere perseguita attraverso l'applicazione isolata di singole disposizioni.

Il principio di *accountability*, previsto dagli articoli 5, paragrafo 2, e 24 del GDPR, assume pertanto un ruolo centrale.

I titolari del trattamento che utilizzano sistemi di intelligenza artificiale devono essere in grado di dimostrare di avere valutato preventivamente i rischi connessi ai trattamenti e di avere adottato misure tecniche e organizzative adeguate a garantire il rispetto della normativa.

L'*accountability* richiede quindi un approccio preventivo e documentato, che non si limiti ad attendere specifiche prescrizioni delle autorità di controllo.

L'adozione di un sistema di intelligenza artificiale non comporta quindi un superamento degli obblighi previsti dal GDPR. Al contrario, rende necessario integrare i processi di *governance* dell'intelligenza artificiale con quelli già previsti dalla normativa in materia di protezione dei dati personali.

Per ulteriori approfondimenti si rinvia alle disposizioni di riferimento dell'AI Act e del GDPR, alle [Linee guida](#) della Commissione, nonché agli orientamenti e alle indicazioni delle autorità europee in materia di protezione dei dati personali e intelligenza artificiale.

Cordiali saluti

IL RESPONSABILE
Roberto Cerminara