IL RAPPORTO TRA INTELLIGENZA ARTIFICIALE E PROTEZIONE DEI DATI PERSONALI

20 novembre 2024

AUTORI

Aurora Agostini
Partner

Giulietta Minucci
Counsel

Jessica Giussani
Associate

Giovanni Lombardi
Associate

L'intelligenza artificiale (IA) ha trasformato profondamente vari settori, offrendo opportunità senza precedenti. Tuttavia, l'integrazione di sistemi IA solleva questioni complesse riguardo alla protezione dei dati personali. In Europa, il Regolamento Generale sulla Protezione dei Dati (GDPR) e il recente AI Act delineano il quadro normativo per garantire che l'innovazione tecnologica rispetti i diritti fondamentali degli individui.

IL QUADRO NORMATIVO

L'avvento e la progressiva diffusione dei sistemi di intelligenza artificiale nel tessuto economico e sociale contemporaneo hanno determinato una profonda trasformazione delle modalità attraverso cui vengono raccolti, elaborati e utilizzati i dati personali, ponendo sfide regolamentari di considerevole complessità che il legislatore europeo ha deciso di affrontare attraverso un approccio normativo multilivello, caratterizzato dall'interazione tra il Regolamento Generale sulla Protezione dei Dati (GDPR) e il nuovo Regolamento sull'intelligenza artificiale (AI Act), recentemente approvato dal Parlamento europeo nel quadro di una più ampia strategia digitale dell'Unione. Tale strategia, che trova le proprie fondamenta nella volontà di promuovere l'innovazione tecnologica nel rispetto dei diritti fondamentali dei cittadini europei, si articola attraverso un complesso sistema di norme interconnesse che comprende, oltre ai citati regolamenti, anche il Data Governance Act, il Data Act, il Digital Services Act e il Digital Markets Act, configurando un *framework* normativo organico finalizzato alla creazione di un mercato unico digitale europeo caratterizzato da elevati standard di tutela per i diritti degli individui.

In questo contesto normativo particolarmente articolato, l'interazione tra il GDPR e l'AI Act assume una rilevanza centrale, considerando come l'utilizzo dei sistemi di intelligenza artificiale sia intrinsecamente connesso al trattamento di ingenti quantità di dati personali, necessari tanto per l'addestramento degli algoritmi quanto per il loro funzionamento operativo. La complessità di tale interazione emerge con particolare evidenza nell'analisi delle modalità attraverso cui le due normative si integrano e si completano reciprocamente, delineando un sistema di tutele che, pur presentando alcuni elementi di potenziale sovrapposizione, si

caratterizza per una sostanziale complementarietà degli approcci regolatori adottati.

L'UE adotta un approccio multi-livello: GDPR e AI Act si integrano con DGA, Data Act, DSA e DMA

L'APPROCCIO RISK-BASED E I MECCANISMI DI VALUTAZIONE PREVENTIVA

La metodologia regolatoria adottata tanto dal GDPR quanto dall'AI Act si fonda su un approccio basato sul rischio che, pur presentando significative analogie nelle due normative, si declina secondo modalità peculiari in ciascuno dei due contesti regolamentari. Mentre il GDPR introduce un sistema di obblighi graduati in funzione della rischiosità dei trattamenti, affidando al titolare del trattamento la responsabilità di valutare preventivamente l'impatto delle operazioni sui diritti e le libertà degli interessati attraverso lo strumento della *Data Protection Impact Assessment* (DPIA), l'AI Act sviluppa un sistema di classificazione dei sistemi di intelligenza artificiale basato su quattro livelli di rischio (inaccettabile, alto, limitato e minimo), a ciascuno dei quali corrisponde un diverso regime di obblighi e responsabilità.

Tale approccio si manifesta con particolare evidenza nell'introduzione, da parte dell'AI Act, della *Fundamental Rights Impact Assessment* (FRIA), uno strumento di valutazione preventiva che, pur presentando alcune similitudini con la DPIA prevista dal GDPR, se ne differenzia per ambito di applicazione e finalità. Mentre la DPIA si concentra specificamente sulla valutazione dei rischi connessi al trattamento dei dati personali, la FRIA adotta una prospettiva più ampia, considerando l'impatto potenziale dei sistemi di intelligenza artificiale sull'intero spettro dei diritti fondamentali tutelati dall'ordinamento europeo. Questa apparente sovrapposizione tra DPIA e FRIA riflette in realtà una precisa scelta del legislatore europeo di costruire un sistema di tutele complementari e sinergiche. Mentre la DPIA si concentra specificamente sugli impatti privacy del trattamento dei dati personali (come la valutazione dei rischi di *data breach*, la proporzionalità della raccolta dati o l'adeguatezza delle misure di sicurezza), la FRIA allarga lo sguardo a un più ampio spettro di diritti fondamentali potenzialmente impattati dai sistemi di IA, quali la non discriminazione, la libertà di espressione, la dignità umana o i diritti dei minori. Le due valutazioni, dunque, più che duplicare gli oneri amministrativi, permettono di catturare rischi di natura diversa che potrebbero sfuggire a un'analisi concentrata su un solo aspetto: un sistema di IA potrebbe infatti essere *privacy compliant* ma comunque discriminatorio, o viceversa rispettoso dei diritti fondamentali ma carente sotto il profilo della protezione dei dati.

Inoltre, il legislatore europeo ha previsto specifici meccanismi di coordinamento tra le due valutazioni: quando un sistema di IA ad alto rischio implica il trattamento di dati personali, la FRIA può incorporare elementi della DPIA già svolta, evitando così duplicazioni non necessarie. Questo approccio integrato permette di

ottimizzare gli sforzi di *compliance* garantendo al contempo una valutazione esaustiva dei rischi sotto molteplici profili di tutela.

LE CRITICITÀ APPLICATIVE NELLA GESTIONE INTEGRATA DELLE DUE NORMATIVE

L'implementazione coordinata del GDPR e dell'AI Act presenta numerose sfide operative che richiedono un'attenta analisi delle modalità attraverso cui le due normative possono essere efficacemente integrate nei processi aziendali e istituzionali. Una delle principali criticità emerge in relazione al principio di trasparenza, che assume declinazioni differenti nelle due normative: mentre il GDPR richiede una trasparenza completa e dettagliata relativamente alle modalità di trattamento dei dati personali, l'AI Act deve confrontarsi con le limitazioni tecniche intrinseche ai sistemi di intelligenza artificiale, in particolare quelli basati su reti neurali profonde, la cui natura "*black box*" può rendere particolarmente complessa la spiegabilità dei processi decisionali.

Tale tensione si manifesta con particolare evidenza nel contesto dei processi decisionali automatizzati, dove l'articolo 22 del GDPR, che sancisce il diritto degli interessati a non essere sottoposti a decisioni basate unicamente su trattamenti automatizzati che producano effetti giuridici significativi, deve essere interpretato alla luce delle previsioni dell'AI Act relative ai sistemi di intelligenza artificiale ad alto rischio. La necessità di garantire una supervisione umana significativa su tali sistemi, prevista dall'AI Act, si interseca infatti con le garanzie procedurali richieste dal GDPR, richiedendo lo sviluppo di procedure operative integrate che permettano di soddisfare contemporaneamente i requisiti di entrambe le normative.

▼▼

La natura 'black box' di alcuni sistemi AI crea tensioni con gli obblighi di trasparenza del GDPR

Particolarmente complessa risulta inoltre la gestione dei diritti degli interessati previsti dal GDPR nel contesto dei sistemi di intelligenza artificiale, specialmente per quanto riguarda il diritto alla cancellazione e alla rettifica dei dati personali. La natura degli algoritmi di *machine learning*, che incorporano le informazioni utilizzate per il loro addestramento in modo difficilmente reversibile, pone infatti significative sfide tecniche nell'implementazione di tali diritti, richiedendo lo sviluppo di soluzioni innovative che permettano di bilanciare le esigenze di tutela degli interessati con le caratteristiche intrinseche dei sistemi di intelligenza artificiale.

LA GOVERNANCE DEI SISTEMI DI INTELLIGENZA ARTIFICIALE: VERSO UN MODELLO INTEGRATO DI SUPERVISIONE

La complessità delle interazioni tra protezione dei dati personali e regolamentazione dell'intelligenza artificiale si riflette nella necessità di sviluppare

un sistema di *governance* in grado di garantire un'efficace supervisione dell'applicazione coordinata delle due normative. L'AI Act introduce un modello di *governance* multilivello che si articola attraverso l'istituzione di nuovi organismi di supervisione a livello europeo, tra cui il Comitato europeo per l'Intelligenza artificiale, e l'attribuzione di specifiche competenze alle autorità nazionali di controllo. Tale sistema si interseca con quello già esistente in materia di protezione dei dati personali, caratterizzato dal ruolo centrale del Comitato europeo per la protezione dei dati (EDPB) e delle autorità nazionali di controllo previste dal GDPR.

In questo contesto, la sfida principale consiste nella necessità di sviluppare interpretazioni armonizzate delle disposizioni contenute nelle due normative, evitando sovrapposizioni inefficienti e garantendo al contempo una tutela completa dei diritti fondamentali. Risulta quindi fondamentale il ruolo delle linee guida interpretative che dovranno essere sviluppate dalle autorità competenti, con particolare riferimento alle modalità di integrazione tra DPIA e FRIA, alla gestione dei diritti degli interessati nel contesto dei sistemi di intelligenza artificiale e all'implementazione dei requisiti di trasparenza e spiegabilità.

La scelta degli Stati membri circa l'individuazione delle autorità nazionali competenti per la supervisione dell'AI Act rappresenta un elemento cruciale per l'efficacia del sistema di governance. In questo contesto, emerge con particolare evidenza il dibattito circa l'opportunità di attribuire tali competenze alle autorità garanti per la protezione dei dati personali, che già dispongono di significativa esperienza nella supervisione di questioni tecnologiche complesse, o di istituire nuove autorità specificatamente dedicate alla regolamentazione dell'intelligenza artificiale. Tale decisione, che dovrà essere assunta tenendo conto delle specificità dei diversi ordinamenti nazionali, avrà un impatto significativo sull'efficacia complessiva del sistema di governance e sulla capacità di garantire un'interpretazione armonica delle due normative.

LE SFIDE TECNICHE E OPERATIVE NELL'IMPLEMENTAZIONE COORDINATA DELLE DUE NORMATIVE

L'implementazione pratica delle disposizioni contenute nel GDPR e nell'AI Act pone significative sfide tecniche e operative che richiedono lo sviluppo di soluzioni innovative e l'adozione di approcci integrati alla compliance normativa. La necessità di garantire contemporaneamente il rispetto dei principi di protezione dei dati personali e dei requisiti specifici previsti per i sistemi di intelligenza artificiale richiede infatti lo sviluppo di architetture tecniche e processi organizzativi in grado di soddisfare simultaneamente le esigenze di entrambe le normative.

Un esempio paradigmatico di queste sfide si riscontra nel **settore bancario**, dove l'utilizzo di sistemi di IA per la valutazione del merito creditizio deve confrontarsi tanto con i requisiti di trasparenza e non discriminazione previsti dall'AI Act, quanto con le tutele in materia di trattamento dei dati personali stabilite dal GDPR. In questo contesto, le banche devono implementare sistemi che siano in grado non solo di giustificare in modo comprensibile le decisioni di credito (explainable AI), ma anche di garantire che i dati utilizzati per l'addestramento degli algoritmi siano stati raccolti e trattati nel rispetto dei principi di minimizzazione e finalità limitata.

Analogamente, nel **settore sanitario**, l'utilizzo di sistemi di IA per la diagnostica medica solleva complesse questioni di implementazione. Un sistema di diagnosi assistita basato su reti neurali profonde deve essere progettato per garantire non solo l'accuratezza delle previsioni mediche, ma anche la protezione delle categorie particolari di dati personali utilizzati per il suo addestramento. Ciò richiede l'implementazione di sofisticate misure tecniche e organizzative, come la pseudonimizzazione dei dati di addestramento, la segregazione degli ambienti di sviluppo e produzione, e la predisposizione di meccanismi di audit trail che permettano di tracciare l'intero ciclo di vita del dato.

La sfida della trasparenza algoritmica si manifesta con particolare evidenza nei **sistemi di *recruitment*** basati su IA, dove l'opacità dei processi decisionali deve confrontarsi con il diritto degli interessati di comprendere la logica sottesa alle decisioni che li riguardano. Un sistema che valuti automaticamente i curriculum vitae deve essere in grado di spiegare in modo comprensibile i criteri di selezione utilizzati, dimostrando al contempo l'assenza di bias discriminatori e il rispetto dei principi di protezione dei dati. Questo richiede lo sviluppo di approcci innovativi che bilancino la complessità degli algoritmi con la necessità di fornire spiegazioni significative, ad esempio attraverso l'utilizzo di tecniche di local interpretable model-agnostic explanations (LIME) o di Shapley additive explanations (SHAP).

▼▼

Banche, Sanità, HR e Marketing sono i settori più impattati dalla doppia compliance

Nel contesto del ***marketing*** **personalizzato**, le aziende che utilizzano sistemi di IA per la profilazione dei clienti devono implementare architetture che garantiscano non solo la compliance con i requisiti di consenso e trasparenza del GDPR, ma anche con le nuove disposizioni dell'AI Act in materia di sistemi di raccomandazione. Questo può richiedere, ad esempio, l'implementazione di *dashboard* interattive che permettano agli utenti di comprendere e controllare i parametri utilizzati per la personalizzazione, insieme a sistemi di logging avanzati che documentino ogni fase del processo decisionale.

La soluzione a queste sfide richiede un approccio olistico che integri:

architetture tecniche *privacy-by-design* che incorporino nativamente i requisiti di entrambe le normative;

processi di governance dei dati che garantiscano la tracciabilità e l'accountability dell'intero ciclo di vita dell'informazione;

framework di testing e validazione che permettano di verificare continuamente la compliance con entrambe le normative;

sistemi di monitoraggio continuo che identifichino tempestivamente potenziali violazioni o derive algoritmiche;

programmi di formazione che mantengano aggiornate le competenze del personale su entrambi gli ambiti normativi.

IL SISTEMA SANZIONATORIO: UN'ANALISI COMPARATA TRA GDPR E AI ACT

L'impianto sanzionatorio delineato dall'AI Act presenta significative analogie strutturali con quello già previsto dal GDPR, pur caratterizzandosi per una maggiore articolazione delle fattispecie sanzionatorie e per l'introduzione di soglie economiche più elevate, che riflettono la particolare rilevanza attribuita dal legislatore europeo alla regolamentazione dei sistemi di intelligenza artificiale. Tale sistema si fonda sul principio di proporzionalità, declinato attraverso una graduazione delle sanzioni che tiene conto non solo della gravità delle violazioni, ma anche delle dimensioni e del fatturato degli operatori economici coinvolti, in

una prospettiva che mira a garantire l'effettività deterrente delle misure sanzionatorie senza compromettere la sostenibilità economica delle imprese, con particolare attenzione alle specificità delle piccole e medie imprese.

▼▼

Le sanzioni AI Act possono arrivare al 7% del fatturato globale vs 4% GDPR

La particolare complessità del sistema sanzionatorio emerge con evidenza nell'analisi delle diverse soglie previste dall'AI Act, che possono raggiungere il 7% del fatturato globale annuo per le violazioni più gravi, superando significativamente i limiti massimi del 4% previsti dal GDPR. Tale inasprimento delle sanzioni pecuniarie massime riflette la consapevolezza del legislatore europeo circa la particolare delicatezza delle questioni regolate dall'AI Act e la necessità di garantire un elevato livello di *compliance* attraverso un apparato sanzionatorio particolarmente incisivo. La sovrapposizione dei due regimi sanzionatori, che può verificarsi quando una violazione dell'AI Act comporti anche una violazione delle disposizioni in materia di protezione dei dati personali, pone significative questioni interpretative circa i criteri di coordinamento tra le diverse autorità competenti e le modalità di determinazione delle sanzioni applicabili.

In primo luogo, si pone il problema del possibile cumulo delle sanzioni: nel caso in cui una singola condotta violi contemporaneamente entrambe le normative - si pensi, ad esempio, all'utilizzo di un sistema di IA ad alto rischio che effettui profilazione senza adeguate basi giuridiche e in violazione dei requisiti di trasparenza previsti da entrambi i regolamenti - ci si chiede se le sanzioni debbano essere applicate cumulativamente o se debba prevalere il principio del ne bis in idem, con l'applicazione del solo regime sanzionatorio più severo.

La questione si complica ulteriormente considerando la possibile diversità delle autorità competenti all'irrogazione delle sanzioni: mentre per il GDPR il potere sanzionatorio è chiaramente attribuito alle autorità di protezione dei dati, per l'AI Act la scelta dell'autorità competente è rimessa agli Stati membri, con la possibilità che vengano designati organismi diversi dai Garanti privacy. In tale scenario, si rende necessario stabilire meccanismi di coordinamento tra le diverse autorità, non solo per evitare duplicazioni procedimentali, ma anche per garantire un'interpretazione uniforme delle disposizioni normative e una coerente quantificazione delle sanzioni. Tale coordinamento risulta particolarmente critico nei casi transfrontalieri, dove potrebbero essere coinvolte autorità di diversi Stati membri, ciascuna con le proprie competenze e procedure.

Un ulteriore elemento di complessità deriva dalla necessità di determinare i criteri per la quantificazione delle sanzioni in caso di violazioni "ibride". Se infatti entrambi i regolamenti prevedono criteri simili per la determinazione dell'ammontare delle sanzioni (come la natura, gravità e durata della violazione, il carattere doloso o colposo della condotta, le misure adottate per attenuare il danno), la loro applicazione congiunta richiede un'attenta valutazione per evitare che l'effetto combinato risulti sproporzionato rispetto alla gravità della violazione. In questo contesto, particolare attenzione dovrà essere prestata anche alle dimensioni dell'operatore economico e alla sua capacità di sostenere l'onere sanzionatorio, specialmente nel caso delle PMI.

Queste problematiche richiedono un intervento chiarificatore, auspicabilmente attraverso linee guida congiunte delle autorità competenti a livello europeo. Tali linee guida dovranno necessariamente affrontare molteplici aspetti cruciali per l'efficace implementazione del sistema sanzionatorio: dalla definizione di criteri oggettivi per determinare la natura unitaria o plurima delle violazioni, all'elaborazione di meccanismi di coordinamento procedurale tra le diverse autorità coinvolte. Particolare attenzione dovrà essere dedicata anche allo sviluppo di metodologie condivise per la quantificazione delle sanzioni nei casi di violazioni che interessino entrambe le normative, nonché alla definizione di specifiche salvaguardie volte a garantire la proporzionalità del trattamento sanzionatorio complessivo. Solo attraverso un simile intervento di armonizzazione interpretativa sarà possibile assicurare un'applicazione coerente ed efficace del duplice apparato sanzionatorio, preservando al contempo gli obiettivi di deterrenza e proporzionalità perseguiti dal legislatore europeo.

CONCLUSIONI E PROSPETTIVE FUTURE

L'analisi delle interazioni tra GDPR e AI Act evidenzia sfide concrete che le organizzazioni dovranno affrontare nei prossimi anni. Le aziende che sviluppano o utilizzano sistemi di IA si troveranno a dover implementare nuovi processi di compliance che tengano conto di entrambe le normative. Ad esempio, un'azienda che sviluppa software di recruitment basati su IA dovrà non solo garantire la conformità al GDPR per il trattamento dei dati dei candidati, ma anche soddisfare

i requisiti dell'AI Act in termini di trasparenza algoritmica e non discriminazione. Questo richiederà la creazione di team specializzati che combinino expertise in privacy, intelligenza artificiale e compliance normativa.

Le sfide operative si estenderanno anche agli aspetti documentali e procedurali: le organizzazioni dovranno ripensare i propri modelli di valutazione del rischio, integrando DPIA e FRIA in un processo unitario ed efficiente. Gli attuali template e procedure dovranno essere aggiornati per catturare sia gli aspetti privacy sia quelli specifici dell'IA, come la robustezza degli algoritmi o i potenziali bias. Sarà inoltre necessario implementare sistemi di monitoraggio continuo che permettano di verificare il mantenimento della compliance nel tempo, considerando che entrambe le normative richiedono un approccio dinamico alla gestione del rischio.

Il successo nell'implementazione di questi requisiti dipenderà in larga misura dalla capacità delle organizzazioni di sviluppare procedure pratiche e strumenti operativi efficaci: dalla predisposizione di checklist integrate per la valutazione preliminare dei progetti, alla definizione di workflow approvativi che coinvolgano tutte le funzioni rilevanti, fino all'implementazione di sistemi di logging e documentazione che soddisfino i requisiti di entrambe le normative. Solo attraverso questo approccio pragmatico sarà possibile trasformare le sfide regolamentari in opportunità di innovazione responsabile.

* * *

Per approfondimenti sulla regolamentazione dell'intelligenza artificiale, si rimanda ai precedenti articoli:

- AI Generativa e AI Act
- AI policy in azienda
- NIST AI Framework
- AI e proprietà intellettuale
- Strategia italiana AI

AUTORI

Aurora Agostini

Partner

Giulietta Minucci

Counsel

Jessica Giussani

Associate

Giovanni Lombardi

Associate