ANDERSEN®

marzo 2026

&Compliance Risk Management

Novità normative e pratiche di governance dei dati e di gestione di rischi d'impresa

Paola Finetto
Partner
paola.finetto@it.andersen.com

Luca Rigotti
Partner
luca.rigotti@it.andersen.com

Hanno collaborato: **Nicolò Bottura**, **Elisa D'Arrigo**

D.Lgs. 231/2001

La responsabilità 231 in caso di reati connessi all'uso di sistemi AI-based

L'impiego di sistemi di Intelligenza Artificiale nei processi aziendali – dalla selezione del personale all'analisi predittiva, fino alla gestione della supply chain – apre nuove frontiere di efficienza, ma anche inediti profili di rischio ai sensi del D.Lgs 231/2001.

La **responsabilità** dell'ente può emergere quando l'utilizzo di sistemi AI-based diventa strumento per la commissione di reati-presupposto: si pensi ai delitti informatici (accesso abusivo, trattamento illecito di dati), ai reati in materia di privacy, alle falsità informatiche, fino alle ipotesi di frode, manipolazione del mercato o violazioni in ambito sicurezza sul lavoro qualora algoritmi mal configurati incidano su processi produttivi.

L'adozione di soluzioni automatizzate non attenua la **colpa organizzativa**: al contrario, impone un rafforzamento dei presidi. L'ente è chiamato a dimostrare di aver valutato i **rischi connessi all'AI**, di aver definito responsabilità chiare nella **governance** dei sistemi, di aver previsto **controlli** sui dataset, sulla qualità degli output e sulla tracciabilità delle decisioni algoritmiche.

In questo scenario, il Modello 231 deve essere aggiornato integrando: mappatura dei processi "AI-driven", protocolli di validazione tecnica e legale, segregazione delle funzioni tra sviluppo, implementazione e controllo, flussi informativi verso l'OdV. Centrale è anche la **formazione** del personale sull'uso consapevole degli strumenti.

L'innovazione tecnologica non esonera dall'obbligo di controllo: la vera compliance passa dalla capacità di governare l'algoritmo, non di subirlo.

Privacy | AI | Cyber

GDPR e AI ACT: un approccio integrato per proteggere i dati personali

Nel panorama digitale europeo, la protezione dei dati personali richiede oggi un approccio sempre più integrato. L'interazione tra **GDPR** e **AI Act** rappresenta un punto cruciale per lo sviluppo responsabile ed etico dell'intelligenza artificiale in quanto volta a garantire che la tecnologia, in particolare quella basata sui sistemi di intelligenza artificiale (IA), si sviluppi nel rispetto dei diritti fondamentali delle persone.

Dalla sua entrata in vigore, il Regolamento UE n. 2016/679 (noto come GDPR) rappresenta il quadro normativo essenziale ai fini della tutela dei dati personali. Prevede infatti il rispetto di principi fondamentali come quelli di **minimizzazione, trasparenza, accountability e proporzionalità** e stabilisce regole specifiche nel caso in cui un sistema di IA possa assumere **decisioni in modo automatizzato** (ad es. sistemi di credit scoring).
Ciò tuttavia non basta.

La rapida evoluzione dell'IA ha reso necessario un ulteriore intervento del legislatore europeo. Il Regolamento UE 2024/1689 (noto come AI Act), entrato in vigore il 1° agosto 2024, introduce infatti **criteri di classificazione dei sistemi di IA in base al rischio**, obblighi di governance e requisiti di qualità dei dati per garantire che gli algoritmi operino in modo sicuro, equo e verificabile.

Una gestione integrata di queste due normative consente quindi di affrontare le criticità legate ai sistemi automatizzati: dalla necessità di **spiegabilità delle decisioni** alla prevenzione di bias, dalla corretta valutazione d'impatto alla definizione di ruoli e responsabilità tra sviluppatori, fornitori e utilizzatori.
In termini operativi, per le organizzazioni, ciò implica il rafforzamento della **governance**, tramite lo svolgimento di **risk assessment** specifici, la definizione di **procedure** interne chiare e trasparenti e la **formazione** del personale in materia di data protection, cybersecurity e IA.

L'integrazione tra GDPR e AI Act diventa così una leva strategica per aumentare la fiducia negli stakeholders, garantire la sostenibilità digitale e l'utilizzo della tecnologia nel rispetto dei diritti fondamentali.

Risk Management

La classificazione dei sistemi di IA in base al rischio: i sistemi IA ad alto rischio.

Il regolamento europeo sull'intelligenza artificiale (**AI Act**) identifica i sistemi di IA ad alto rischio in considerazione del loro potenziale impatto su salute, sicurezza e diritti fondamentali degli individui.

Questi sistemi non sono vietati, ma la loro immissione sul mercato è soggetta a rigorosi **obblighi di conformità**.

Tra i sistemi di IA ad alto rischio vi sono giocattoli, ascensori, apparecchiature radio, attrezzature a pressione, attrezzature per imbarcazioni da diporto, impianti a fune, dispositivi medici, dispositivi medico-diagnostici in vitro, veicoli automobilistici e aeronautici, oltre che sistemi destinati a essere utilizzati come componenti di sicurezza delle infrastrutture digitali critiche e di infrastrutture per la fornitura di acqua, gas, riscaldamento ed elettricità.

Inoltre, rientrano nella categoria in esame i sistemi di IA utilizzati nell'istruzione o nella formazione professionale, ad esempio per valutare i risultati dell'apprendimento oppure i sistemi utilizzati nel settore dell'occupazione, in particolare per la selezione del personale o per il monitoraggio o la valutazione dei lavoratori.

Si pensi, poi, ai sistemi di IA utilizzati per determinare l'accesso o la sospensione di servizi o prestazioni essenziali di assistenza pubblica, quali servizi sanitari, prestazioni di sicurezza sociale, servizi sociali.

L'AI Act stabilisce specifici requisiti per lo sviluppo, la commercializzazione e l'utilizzo di tali sistemi, con l'obiettivo di bilanciare **innovazione** e **tutela** delle persone. Questi sistemi devono essere progettati e sviluppati in modo tale da poter essere utilizzati sotto la costante **supervisione** di persone fisiche.

Inoltre, sono previsti controlli periodici per verificare che essi garantiscano standard elevati di **sicurezza**, in linea con gli obiettivi della strategia digitale europea tendenti a rendere l'IA tanto innovativa quanto affidabile.