Modelli organizzativi per l'Intelligenza Artificiale conformi al GDPR e all'AI Act

Data: 6 luglio 2025 | Autore: Redazione



L’Intelligenza Artificiale (IA) sta cambiando radicalmente il nostro modo di vivere e di lavorare, portando nuove opportunità in settori chiave come la sanità, la finanza e l’industria. Tuttavia, a fronte di benefici senza precedenti in termini di efficienza e produttività, emergono rischi significativi: discriminazioni algoritmiche, sistemi opachi ("black box"), violazioni della privacy e problemi di sicurezza complessi.

Per affrontare questi rischi in modo efficace, le organizzazioni devono dotarsi di **modelli organizzativi solidi e conformi alle normative europee**. Due sono oggi i pilastri di riferimento: il **Regolamento Generale sulla Protezione dei Dati (GDPR - Reg. UE 2016/679)** e il nuovissimo **AI Act (Reg. UE 2024/1689)**.

GDPR e AI Act: il binomio normativo per l’IA

Il **GDPR**rimane il principale riferimento per la protezione dei dati personali, applicandosi a tutte le situazioni in cui l’IA tratta dati identificabili. I suoi principi fondamentali, come **base giuridica valida**, **trasparenza algoritmica**, **minimizzazione dei dati** e **Data Protection by Design e by Default**(Art. 25 GDPR), si estendono su tutto il ciclo di vita dei sistemi IA. Cruciale è anche il rispetto del **diritto di opposizione alle decisioni automatizzate**(Art. 22 GDPR), riaffermando il ruolo centrale dell’essere umano.

Il **nuovo AI Act**, primo regolamento organico a livello europeo sull'intelligenza artificiale, introduce un approccio **risk-based** alla disciplina. L'obiettivo? Promuovere un'IA **antropocentrica** e **affidabile**, garantendo la tutela della salute, della sicurezza e dei diritti fondamentali. Il regolamento classifica i sistemi IA in quattro categorie:

- **Rischio inaccettabile**: pratiche vietate, come manipolazioni subliminali e social scoring.
- **Alto rischio**: sistemi utilizzati in settori critici (infrastrutture, istruzione, sanità, giustizia), soggetti a requisiti rigorosi tra cui **gestione continua del rischio**, **data governance**, **documentazione tecnica**, **logging**, **trasparenza**, **sorveglianza umana** e **sicurezza informatica**. La conformità richiede una **valutazione d'impatto** e la **marcatura CE** prima della commercializzazione.
- **Rischio limitato**: obblighi di trasparenza, ad esempio l'indicazione chiara che si sta interagendo con un sistema di IA.
- **Rischio minimo o nullo**: la maggior parte delle applicazioni IA, prive di obblighi specifici.

La sinergia tra GDPR e AI Act è chiara: entrambi promuovono un approccio **by design**, trasparente e responsabile. Le organizzazioni devono eseguire una **Valutazione d'Impatto sulla Protezione dei Dati (DPIA)** e una **Valutazione d'Impatto sui Diritti Fondamentali**, assicurando che l'innovazione tecnologica vada di pari passo con la tutela dei diritti umani.

Costruire modelli organizzativi efficaci

Per navigare la complessità normativa, è essenziale adottare **modelli organizzativi integrati** e **robusti**, basati su alcuni capisaldi:

- **Governance chiara** e leadership attiva, con l'istituzione di un **Comitato Etico per l'IA**.
- **Politiche e procedure documentate**, che regolino il ciclo di vita dei dati e la gestione dei rischi.
- **Misure tecniche e organizzative** orientate alla **Data Protection & AI Ethics by Design**.
- **Programmi di formazione continua** per tutti i livelli aziendali.
- **Monitoraggio e audit periodici**, per verificare costantemente la conformità.

Un **regolamento interno sull'uso dell'IA**, basato su un'accurata analisi dei rischi, deve guidare ogni processo decisionale. La gestione responsabile dell'IA non può essere demandata esclusivamente all'IT o al DPO. Serve un **team interdisciplinare**, composto da DPO, AI Compliance Officer, AI Risk Manager, sviluppatori IT, operatori e management.

L'esperienza umana è insostituibile: solo con una supervisione critica e competente si possono interpretare e validare gli output dei sistemi IA.

Il ruolo strategico del Project Management

Il **Project Management**è chiamato a un ruolo chiave: ogni progetto IA è un vettore di cambiamento organizzativo. Per questo è fondamentale integrare i requisiti dell'AI Act in ogni fase progettuale, dalla gestione dei dati alla produzione dei deliverables, fino ai test e alla validazione.

Un **PMO strutturato**aiuta ad allineare obiettivi di compliance e di business, garantendo che la trasformazione digitale proceda nel rispetto della normativa.

Le sfide e le opportunità

La strada non è priva di ostacoli: interpretare correttamente le norme, sostenere i costi di implementazione, gestire l'assenza di standard tecnici consolidati e affrontare il **model drift**sono

sfide concrete.

Tuttavia, un approccio **proattivo e strategico** trasforma queste sfide in opportunità per costruire una **fiducia solida**, **innovare responsabilmente** e sviluppare un'**IA sostenibile e antropocentrica**.

Investire oggi in **modelli organizzativi flessibili**, **pratiche di project management efficaci** e **una cultura della responsabilità**è fondamentale per guidare le organizzazioni verso un futuro in cui tecnologia e diritti umani convivono armoniosamente.

Vuoi restare sempre aggiornato con le notizie più importanti? Iscriviti al nostro canale WhatsApp InfoOggi e ricevi in tempo reale gli aggiornamenti direttamente sul tuo smartphone! Clicca qui per unirti

Articolo scaricato da www.infooggi.it
https://www.infooggi.it/articolo/modelli-organizzativi-per-l-intelligenza-artificiale-conformi-al-gdpr-e-all-ai-act/146209