Digeat N.6 - 19 Giugno 2025

Il dominio funzionale dell’intelligenza artificiale nelle aziende tra cybersecurity e tutela del patrimonio informativo

Di Anna Perut

Abstract

I sistemi di Intelligenza Artificiale generativa sono rientrati ormai a pieno titolo negli strumenti di lavoro della maggior parte delle realtà aziendali, laddove le esigenze di velocizzare processi e ottimizzare risultati ben vengono soddisfatte dai molteplici tool di IA disponibili sul mercato. Questa diffusione esponenziale, tuttavia, non può essere lasciata alla discrezionalità e alle iniziative del singolo dipendente, ma necessita di regole ben precise volte a tutelare il patrimonio informativo e la sicurezza aziendale, in modo da presidiare i possibili rischi insiti nell’utilizzo di tali strumenti. Le aziende dovranno quindi prendere cognizione effettiva dei sistemi in uso e stabilire policy in grado di orientare le proprie risorse in modo consapevole.

Indice

L’utilizzo dei sistemi di IA nelle aziende. Stato dell’arte

L’Intelligenza Artificiale sta diventando ormai un elemento di utilizzo sempre più diffuso, la troviamo integrata nelle varie piattaforme, nei provider di posta elettronica, nei chatbot presenti nei siti, oltre naturalmente nei sistemi di IA generativa (c.d. “GenIA”) accessibili liberamente. Fintanto che questi sistemi vengono utilizzati nell’ambito della vita privata l’unico soggetto responsabile è l’utente, sul quale ricadono le scelte sia in termini di tutela dei dati sia di utilizzo dei risultati generati dai sistemi.

> Quando i sistemi di IA vengono invece utilizzati in un **contesto aziendale**, come strumento di lavoro, le cose cambiano. Le valutazioni sui sistemi e sui contesti nei quali applicare i sistemi di IA non possono essere lasciate al singolo dipendente ma devono essere **presidiate dalla *governance* aziendale**, in modo da definire **perimetri e chiare regole** da condividere al proprio interno.

Recenti **studi di settore** hanno invece evidenziato dati piuttosto preoccupanti che dimostrano come **la tematica dell'IA sia ancora poco gestita in molte realtà aziendali.**

L'Enterprise GenAI Security Report 2025 pubblicato da LayerX Security e basato sui dati raccolti presso i propri clienti ha evidenziato come **l'89% di app e tool di Intelligenza Artificiale generativa utilizzate dai dipendenti sia fuori dal controllo delle aziende**.

Il 71% delle connessioni ai sistemi di GenAi avviene utilizzando account privati dei dipendenti, uscendo quindi dal perimetro dei sistemi aziendali e gli accessi effettuati tramite account aziendali avvengono per la maggior parte mediante sistemi di autenticazione non tracciati.

A questo si aggiunge la prassi per molti dipendenti di installare almeno un'estensione di IA nel proprio browser. Lo studio ha rilevato che **il 58% delle estensioni di IA ha permessi di accesso classificati come a rischio alto o critico**, in quanto in grado di monitorare le attività svolte dall'utente (es. dati di navigazione, cookie, ecc.).

Quanto alle modalità di utilizzo, è stato rilevato come **in più del 50% dei casi gli utenti copino nei sistemi di GenAI dati classificati come informazioni aziendali**.

> Lo stato dell'arte quindi non è dei più confortanti. La maggior parte delle organizzazioni non ha contezza su quali strumenti di IA siano utilizzati al loro interno, chi li utilizzi e con quali modalità.

Questo dato di fatto, di per sé difficile da concepire soprattutto per le realtà più strutturate, deve costituire **il punto di partenza** per costruire **modelli di governance** armonizzando le innovazioni tecnologiche portate dai sistemi di IA con la tutela dei dati e degli asset aziendali.

Diventerà quindi fondamentale gestire questi nuovi strumenti, definendo **chiare regole di utilizzo attraverso policy specifiche** volte a presidiare i vari rischi insiti dei sistemi di IA. Giova ricordare in ogni caso come **la formazione del personale** in materia **sia diventata un vero e proprio obbligo** per le aziende che utilizzino sistemi di IA, introdotto dal Regolamento UE 2024/1689 ("AI Act"), laddove si fa riferimento all'articolo 4 all'"*Alfabetizzazione in materia di IA*", obbligo peraltro già in vigore. Le regole e istruzioni non dovranno tuttavia essere viste come l'ennesima formalità necessaria destinata a rimanere un pezzo di carta fine a sé stesso, bensì **un'opportunità per un utilizzo consapevole e produttivo**.

Le policy sull'utilizzo dei sistemi di IA in azienda

L'utilizzo dei sistemi di IA in azienda può avvenire in molteplici contesti e forme d'uso. Al di là dell'implementazione di soluzioni specifiche in processi aziendali definiti, che necessitano naturalmente di valutazioni *ad hoc*, uno degli **aspetti da presidiare** con attenzione è **l'utilizzo dei sistemi di GenAI da parte dei dipendenti**, anche tenuto conto che il mercato offre diverse soluzioni accessibili, con funzionalità diverse.

> Ogni realtà sarà tenuta ad effettuare un'attenta analisi del proprio contesto in modo da scegliere con accuratezza i sistemi di IA utilizzabili in azienda e modulare la policy sulle singole esigenze, valutando le possibili alternative tra sistemi totalmente controllati dall'azienda mediante account business, soluzione che offre maggior controllo e sicurezza, da soluzioni meno presidiate e che prestano il fianco a maggiori criticità, ove la responsabilizzazione degli utenti giocherà un ruolo determinante. È innegabile come ci sia in ogni caso un nucleo essenziale comune imprescindibile.

La protezione dei dati personali

Uno degli aspetti che devono essere necessariamente presidiati sono i **dati personali**. I sistemi di IA processano enormi moli di dati e va da sé che la tutela del dato sia un elemento fondamentale di qualsiasi policy. Nell'utilizzo dei sistemi di IA deve essere posta una **particolare attenzione alla protezione dei dati** personali, trattandosi peraltro di strumenti potenti e di nuova tecnologia, nel rispetto non solo del Regolamento UE 679/16 – GDPR, quadro normativo cardine in materia, ma anche dell'AI Act, che contempla una serie di disposizioni volte a rafforzare ulteriormente la tutela dei diritti degli interessati.

Come è noto, i sistemi di GenAI si basano sui Large Language Models (LLMs), modelli di fondazione in continuo apprendimento. **Uno dei potenziali rischi è quello che i dati inseriti nei vari sistemi possano finire nel calderone degli algoritmi ed essere elaborati in modo non conforme alla normativa in materia**, in assenza di valide basi giuridiche.

I vari sistemi di IA presenti sul mercato, a seconda del piano scelto, offrono maggiori o minori garanzie al riguardo ed è fondamentale che la policy stabilisca chiare regole in modo da evitare indebiti trattamenti di dati. Optare per **sistemi che non utilizzino nel processo di autoapprendimento i dati contenuti negli input** e che offrano adeguate **garanzie sulla protezione dei dati** nonché prescrivere agli utenti **appropriate tecniche di minimizzazione e sanitizzazione dei dati** costituiscono sicuramente **una buona prassi** per la gestione dei rischi privacy (ad esempio, eliminando i dati personali delle persone fisiche nei vari prompt/input, in particolare i dati particolari).

> Utili spunti a riguardo vengono forniti dal recente documento elaborato dal pool di esperti dell'EDPB "AI Privacy Risks & Mitigations Large Language Models (LLMs)", il quale costituisce una guida pratica non solo per gli sviluppatori ma anche per gli utilizzatori ("*deployer*") dei sistemi basati sui LLMs per gestire i rischi privacy connessi a queste tecnologie, fornendo supporto nelle valutazioni richieste ai sensi dell'articolo 25 GDPR sui principi di *privacy by design and by default* e dell'articolo 32 GDPR nell'ambito delle misure di sicurezza tecniche ed organizzative.

Il documento analizza il *data flow* e i connessi rischi privacy distinguendo tra tre tipologie di LLMs, quali le applicazioni di LLMs *as a service*, accessibili on line (es. ChatGPT), i così detti LLMs "*off the shelf*", ovvero le soluzioni che possono essere personalizzate dall'utilizzatore e i modelli di LLMs sviluppati all'interno dell'utilizzatore, fornendo molteplici esempi di misure di mitigazione dei rischi.

La tutela delle informazioni aziendali e della proprietà intellettuale

Analoghe problematiche possono presentarsi per le **informazioni aziendali** diverse dai dati personali ma che sono parimenti di notevole importanza per il business dell'organizzazione, quali dati strategici, finanziari, o relativi al know-how aziendale. È opportuno stabilire delle **metriche di utilizzo dei sistemi di IA in modo da evitare la divulgazione di informazioni riservate** (si pensi a contenuti coperti da accordi di riservatezza, informazioni confidenziali, ecc.), così come è necessario **rispettare i diritti di proprietà intellettuale altrui**.

La sicurezza informatica

Le aziende dovranno adottare adeguate **misure di sicurezza informatica** per **ridurre i possibili rischi collegati all'utilizzo dei sistemi di IA**, alle sue configurazioni e alle modalità di accesso da parte degli utenti, prevedendo **misure di autenticazione robuste** per prevenire accessi non

autorizzati e proteggere le sessioni di dati. È fondamentale **aumentare la consapevolezza del personale** sull'importanza del rispetto delle password policy aziendali, anche in questo ambito che in prima battuta può sembrare avulso dal contesto aziendale, ma che in realtà non lo è affatto, soprattutto qualora si utilizzino strumenti di IA mediante account lavorativi.

È chiaro che in caso di utilizzo di sistemi di IA di terze parti molti oneri in termini di cybersecurity gravino sul *provider*, ma **è importante che gli utilizzatori**, oltre ad effettuare una verifica delle garanzie offerte dai fornitori, **adottino in modo proattivo idonee misure di sicurezza per proteggere i propri sistemi e i dati trattati**.

Il presidio umano

> **I sistemi di IA** sono utili e con innumerevoli potenzialità, ma **sono strumenti a supporto dell'uomo**. Lo stesso AI Act promuove "*la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile*" (vd. Considerando 1), mantenendo quindi il ruolo centrale degli individui (si pensi anche alla previsione esplicita della sorveglianza umana nei sistemi ad alto rischio).

Questo principio fondamentale deve essere declinato anche nell'ambito lavorativo, prevedendo **l'obbligo per gli utilizzatori di controllare gli output generati e di assicurarsi sulla qualità ed affidabilità del contenuto** prima del loro utilizzo, soprattutto nel caso in cui debbano essere impiegati in contesti decisionali critici o riprodotti su documenti ufficiali, **evitando di riporre una fiducia eccessiva e acritica sulla nuova tecnologia**. È risaputo come i sistemi di IA possano generare contenuti non sempre corretti (le c.d. "allucinazioni" dell'IA) né tantomeno adeguati al contesto. L'IA può infatti elaborare di per sé un buon prodotto che tuttavia non tiene conto di quella che è la realtà aziendale o dell'ambito in cui il documento deve essere utilizzato. Ecco perché **è opportuno sensibilizzare il personale** anche **sulla corretta formulazione dei prompt/input,** i quali giocano un ruolo chiave ai fini del risultato finale.

> **Responsabilizzazione** e **consapevolezza** degli operatori sono due aspetti su cui le aziende devono necessariamente far leva, tenendo bene in mente che, laddove tali sistemi vengano utilizzati ad ausilio di funzioni aziendali complesse, gli eventuali errori di valutazione potrebbero non essere sempre monitorabili o prevedibili dall'uomo. Sarà quindi necessario **integrare i sistemi di controllo interno con le nuove tecnologie,** al fine di evitare epiloghi deleteri per l'organizzazione in termini di danni economici o reputazionali.

Conclusioni

Appare chiaro che le realtà aziendali dovranno prendere coscienza della sempre più pervasiva diffusione dei sistemi di IA e dell'utilizzo esponenziale che ne verrà fatto.

Affidare all'autonomia del singolo dipendente le scelte su tipologie e contesti di utilizzo di questi strumenti non è una strada percorribile.

L'unica soluzione è la **definizione di un modello di governance funzionale alla propria realtà**, da tenere costantemente aggiornato, tenuto conto del settore di appartenenza e delle tipologie di dati trattati, in modo da abbracciare l'innovazione tecnologica e potenziare il business, gestendo i rischi connessi in modo consapevole, etico e trasparente.