Data Manager Online
il portale dell'ICT professionale

09/12/2025

SB Italia, AI sotto controllo con AI-Docs

Data Manager Online
il portale dell'ICT professionale

09/12/2025

Shadow AI e chatbot esterni: il rischio si estende oltre la cybersecurity. SB Italia definisce un framework di utilizzo, è SB Italia certificata per dati protetti e governance trasparente dei modelli AI

L'ingresso dell'intelligenza generativa e predittiva nelle piattaforme di business process e content management segna un triplo salto in avanti nell'evoluzione di tutti i processi aziendali. L'integrazione dei sistemi comporta una serie di sfide: sicurezza dei dati, conformità e governance etica. Man mano che l'AI si espande finisce per amplificare le criticità esistenti, per esempio in termini di correttezza delle procedure interne, di accesso alle informazioni sensibili, di controllo degli automatismi decisionali. Uno scenario che impone una riflessione anche da parte di fornitori di tecnologia, come **SB Italia**, chiamati a progettare piattaforme trasparenti e affidabili, capaci di bilanciare velocità e governance dell'innovazione. «L'AI pervade i processi aziendali, anche quelli più sensibili» – spiega **Luca Rodolfi, Bu manager AI & Analytics di SB Italia**.

«Questo cambia anche il profilo di rischio per le imprese: non si tratta solo di cybersecurity e compliance, ma anche di tutela della fiducia. In Europa, l'*AI Act* ci indica la strada da seguire». Ma non basta: «L'utilizzo di servizi disponibili online amplia ulteriormente la superficie di rischio». Soprattutto con il fenomeno della shadow AI: «Quando ci si affida a chatbot esterni inserendo informazioni aziendali, ci si espone non solo alla dispersione dei dati, ma anche a potenziali errori e bias».

REGOLE E GESTIONE CONTINUA

Alle nuove esigenze di innovazione e security, SB Italia risponde con la piattaforma proprietaria *AI-Docs*, un vero e proprio acceleratore di soluzioni AI, che integra più modelli (anche open source), ma con un livello più elevato di controllo sul dato, evitando il trasferimento di dati su cloud pubblici e la possibile perdita di informazioni critiche. «I dati restano all'interno del perimetro aziendale, gli accessi sono tracciati e l'utilizzo dei modelli è monitorato in modalità continua» – prosegue Rodolfi. «Anche la fase di inferenza è personalizzabile, potendo essere eseguita sia su cloud privati sia in ambienti on-premise».

A rafforzare ulteriormente l'affidabilità di AI-Docs contribuisce la certificazione ISO/IEC 42001, ottenuta da SB Italia, che attesta l'adozione di un framework trasparente e sicuro. «Vuol dire che mettiamo a disposizione non solo una piattaforma sicura ma un vero e proprio sistema di gestione per l'uso di modelli e algoritmi inseriti in un flusso governato in ogni sua parte». Secondo Rodolfi, la protezione del dato richiede due elementi: tecnologie adeguate e regole organizzative chiare. «Sul piano tecnologico è indispensabile evitare che informazioni sensibili finiscano in mani terze, non controllate, che potrebbero utilizzarle per scopi diversi da quelli previsti o dichiarati. Servono architetture dedicate, capaci di mantenere il governo delle fonti. In SB Italia possiamo mantenere i modelli "entro i binari", costruendo intorno a loro le necessarie barriere di sicurezza, così da limitarne le risposte a domini specifici. Dal punto di vista organizzativo, invece, è fondamentale definire policy da seguire con rigore, così da arginare gli utilizzi opachi di strumenti che, pur essendo comodi e immediati, non sempre sono compatibili con i requisiti di sicurezza».

INTEGRAZIONE SENZA INTOPPI

Ma quali competenze specifiche deve sviluppare un'azienda per gestire la cosiddetta AI-governance? «Le grandi organizzazioni di tipo enterprise dispongono di strutture adatte a gestire questi temi, con competenze tecnologiche ma anche legali. Diverso è il caso delle PMI, dove il consiglio è costituire un comitato AI coinvolgendo le figure disponibili in azienda – dal CISO al DPO, fino al responsabile delle applicazioni. Un comitato in grado di sollevare i dubbi più urgenti e, al tempo stesso, proporre percorsi formativi da introdurre in azienda».

Secondo Rodolfi, quando si parla di AI è necessario coniugare innovazione e controllo. «Il modo migliore per non rallentare lo sviluppo delle applicazioni è integrare la governance by design, lavorando su sandbox protette, classificando i progetti in base al rischio e accorciando i tempi di go-live. In questo modo, riusciamo ad anticipare gli eventuali intoppi di compliance e sicurezza, garantendo progetti con basi solide e durevoli nel tempo. All'inizio, ciò che sembra un ostacolo può diventare fattore abilitante, anche per le tecnologie più dirompenti».