DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Sistemi di Intelligenza Artificiale: la gestione dei rischi

Gennaio 2025

Giulia Caja, Partner, KPMG Advisory
Andrea Ottini, Senior Manager, KPMG Advisory

Giulia Caja, Partner, KPMG Advisory

Andrea Ottini, Senior Manager, KPMG Advisory

Società di consulenza

KPMG Advisory

Negli ultimi anni, i **sistemi di Intelligenza Artificiale** sono diventati strumenti di rilievo in una moltitudine di settori, tra i quali quello bancario. Essi svolgono un ruolo fondamentale nel migliorare i processi decisionali, influenzare i risultati aziendali e aumentare l'efficienza operativa. Questi algoritmi sofisticati hanno consentito progressi senza precedenti in molti ambiti, tra cui la rilevazione delle frodi, l'automazione del servizio clienti, il monitoraggio e la valutazione dei rischi.

Tuttavia, accanto a questi benefici trasformativi, l'adozione dei sistemi di Intelligenza Artificiale ha introdotto **sfide** che potrebbero aumentare i **rischi** per le aziende lungo l'intero ciclo di vita di tali sistemi. Infatti, rispetto ai sistemi classici, quelli di intelligenza artificiale e machine learning hanno una complessità intrinseca dovuta alla loro natura non deterministica.

Pertanto, considerando il rapido ed inesorabile diffondersi di queste tecniche, il Parlamento Europeo si è adoperato negli ultimi anni, di concerto con altre regolamentazioni non EU, per istituire un quadro giuridico, che ha preso forma nel regolamento 2024/1689 (EU AI Act) pubblicato il 12 Luglio 2024 ed entrato in vigore il 2 Agosto 2024, con lo scopo di promuovere la diffusione di un'intelligenza artificiale antropocentrica ed affidabile.

Nonostante i dettami regolamentari dell'EU AI Act si applichino chiaramente ai sistemi ad alto rischio, il regolatore stesso incoraggia ad adottare i principi del regolamento anche ai sistemi AI non ad alto rischio.

Considerata la pervasività del fenomeno, è quindi essenziale dotarsi di un **metodo robusto** ed industrializzato con regole chiare ed un modello operativo resiliente. L'approccio osservato sul mercato è quello di far leva sul framework di model risk adottandone i processi e le metodologie adattate per gestire anche le specificità dei sistemi di AI.

Pertanto, successivamente alla comprensione approfondita dei principi regolatori, il primo passo da compiere è quello di dotarsi di un **modello di governance** adeguato rispondendo a domande come: *è stato scelto un approccio centralizzato o decentralizzato? Sono stati assegnati ruoli e responsabilità all'interno della banca? Sono state definite adeguate policy interne? È stato adottato un sistema di gestione dei rischi e della qualità?*

vedi l'articolo online

Attualmente, in risposta alla prima domanda, si osserva che il sistema bancario italiano è ancora in una fase di comprensione dell'intelligenza artificiale e delle conseguenze che questa può avere sul modello organizzativo. Pertanto, solo in alcuni contesti bancari trova adozione il **modello Hub&Spoke**, considerato il target a cui tendere, mentre, per gli altri operatori di mercato, si rileva un modello dove tutti fanno sistemi di intelligenza artificiale introducendo potenziali inefficienze e duplicazioni.

Il modello "Hub&Spoke" è costituito da un **presidio centrale** (l'Hub) che mette ordine dando le regole e da **unità distribuite** (gli Spoke) per valorizzare le competenze specifiche.

L'Hub è incaricato di dare una chiara strategia, stabilendo le regole per la gestione delle esigenze delle diverse unità della banca e di averne contezza, grazie ad una panoramica chiara del percorso attuale e futuro sui temi di intelligenza artificiale, evitando inutili duplicazioni ed indirizzando le esigenze nel modo migliore.

Gli Spoke presentano le adeguate competenze di settore e di processo per indirizzare al meglio le attività di sviluppo di soluzioni verticali.

Il secondo passo, dopo l'aver individuato il modello organizzativo, è quello di definire una **policy robusta** che declini ed instradi i principi guida e le modalità operative da adottare e seguire al fine di mantenere un adeguato presidio sull'AI.

Per essere efficace, la **policy** deve descrivere il modello organizzativo e le regole adottate a livello di gruppo, dare una chiara definizione di cosa si intende per sistema di Intelligenza Artificiale e assegnare correttamente i ruoli e le responsabilità coinvolgendo non solo le funzioni tecniche ma anche gli organi strategici e le funzioni di controllo per quanto di competenza.

La policy deve anche declinare le modalità di **censimento e classificazione** dei sistemi di intelligenza artificiale e regolamentare le modalità di scelta tra un'implementazione in house ("make") e l'adozione di una soluzione sviluppata da un fornitore esterno ("buy").

Poiché il regolatore impone requisiti più severi per il **rilascio in produzione** di sistemi di AI, è fondamentale dotarsi di un framework robusto per documentare come è stato costruito il sistema e in che modo è stato collaudato. Anche queste regole devono essere previste nella policy e declinate in standard documentali predefiniti.

Sempre seguendo il dettame normativo, la policy deve riportare chiare regole per il **monitoraggio periodico** di questi sistemi onde evitare il diffondersi di pratiche scorrette di utilizzo o l'incorrere in eventuali errori dovuti ad un possibile deterioramento del sistema in seguito alla sua evoluzione.

La messa a terra del modello operativo target deve prevedere anche la **promozione** interna alla banca della **cultura** sull'Intelligenza Artificiale. Dopo un'attenta valutazione del livello di alfabetizzazione di tutti gli stakeholder, sia interni che esterni, è fondamentale predisporre un programma formativo solido. Sarà necessario pianificare sessioni di induction specifiche per il top management e, parallelamente, sviluppare un piano formativo per l'upskilling e il reskilling del personale. Questo piano dovrà essere basato sui cambiamenti introdotti dall'intelligenza artificiale nei processi operativi e nel modus operandi delle persone, al fine di superare la naturale paura di essere sostituiti dai sistemi intelligenti.

Altro aspetto fondamentale da indirizzare è il corretto coinvolgimento delle funzioni aziendali. Viene spontaneo pensare alle funzioni Innovation, Data & Technology ma sempre più devono assumere un ruolo rilevante anche le funzioni di controllo ed Organizzazione & People. In questo contesto l'area del Chief Risk Officer ha il compito di integrare l'appetito al rischio della banca considerando la propensione all'intelligenza artificiale, di declinarne i limiti di utilizzo, ma soprattutto di classificare, in accordo con la norma, i sistemi e di assegnare loro un indice di rischiosità puntuale e calibrato.

Pertanto, grazie al coinvolgimento della funzione di organizzazione, deve essere disegnato un processo strutturato per la raccolta e la catalogazione dei sistemi di AI, possibilmente predisponendo dei questionari sintetici ed efficaci da adottare a livello di gruppo.

Una buona prassi osservata sul mercato è quella di responsabilizzare lo sponsor del sistema di intelligenza artificiale nella fase di censimento dello stesso che, per agevolare la gestione del ciclo di vita del sistema, può avvenire tramite l'utilizzo di uno strumento informatico. Sul mercato esistono infatti, soluzioni IT che consentono di **gestire il workflow** con agilità, in modo che le funzioni coinvolte possano collaborare e tutti siano al corrente della natura del modello, dello stato di approvazione ed utilizzo, evidenziando la necessità di revisione e agevolando la pianificazione degli interventi correttivi. All'atto

vedi l'articolo online

del censimento è importante che lo sponsor si faccia promotore di assegnare al sistema una **prima valutazione di rischiosità,** il così detto rischio sintetico, che sarà in seguito opportunamente controllato e, se del caso, avvallato dall'area del Chief Risk Officer. A questo punto, il sistema può essere classificato in coerenza con la governance interna e soprattutto in linea con quanto richiesto dall'AI Act.

Con il rischio sintetico si possono escludere immediatamente i casi non accettabili come da normativa e, aggiungendo altre due dimensioni di analisi, attribuire una valutazione di rischio specifico che prenda in considerazione l'**impatto** che un errore del sistema potrebbe causare alla realtà bancaria, combinato alla **complessità** del sistema.

A titolo di esempio, la dimensione **impatto** deve prendere in considerazione le possibili implicazioni regolamentari, reputazionali ed economiche che si possono riverberare sia internamente che su soggetti terzi e clienti.

La seconda dimensione da considerare è la **complessità** del sistema, ovvero sono da valutare aspetti quali l'obiettivo che il sistema si pone, le metodologie e le tecnologie che adotta, eventuali interconnessioni e dipendenze che ha in essere con altri sistemi, la natura dei dati che utilizza, le implicazioni etiche e di fairness e, ultimo ma non ultimo, quanto interagisce con l'essere umano nello spiegare le scelte fatte.

A questo punto, considerando il rischio sintetico, la complessità e gli impatti, il sistema può essere posizionato all'interno di una **matrice di conformità**.

La priorità deve essere posta sui modelli ad alto impatto, alta complessità e poco conformi ai dettami regolamentari, sui quali **avviare un processo di validazione** ed un continuo monitoraggio nel tempo.

Nonostante l'importanza del processo di monitoraggio nel tempo, i sistemi posizionati nella parte più rischiosa della matrice di conformità sarebbero da sottoporre anche a **revisione e validazione periodica** con frequenza dipendente dal livello di rischiosità specifica e pianificata ex-ante.

In conclusione, la gestione dei sistemi di intelligenza artificiale richiede un approccio multidisciplinare e una governance robusta che consentano di monitorare costantemente i rischi e le opportunità che queste tecnologie comportano. Solo attraverso una politica ben definita, una formazione adeguata e una gestione continua dei rischi, le banche possono sfruttare appieno il potenziale dell'AI, garantendo al contempo la conformità alle regolamentazioni e la salvaguardia della salute, della sicurezza e dei diritti fondamentali degli utenti. L'adozione di buone pratiche di gestione del rischio e una cultura aziendale aperta all'innovazione saranno elementi chiave per il successo nel lungo termine.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it