

ATTUALITÀ

L'Intelligenza Artificiale nel settore bancario, finanziario e assicurativo

7 Giugno 2024

Jacopo Liguori, Partner, Withers





Jacopo Liguori, Partner, Withers

> Jacopo Liguori

Jacopo Liguori è responsabile del team di proprietà intellettuale, tech e privacy negli uffici di Milano e Padova. Assiste primarie aziende italiane e internazionali e clienti privati, attivi in diversi settori quali: life science e pharma, fashion & luxury, automotive, food and beverage, sport, elettronica e software, entertainment e multimedia, assicurazioni, finanza e arte. Presta assistenza nel campo della proprietà intellettuale, delle nuove tecnologie, della privacy e della protezione dei dati e nel campo delle startup ad alto valore tecnologico.

1. Introduzione

L'intelligenza artificiale (IA) sta rivoluzionando vari settori, inclusi quello bancario, finanziario e assicurativo. La recente approvazione del regolamento sull'IA da parte del Parlamento Europeo e il disegno di legge italiano del Consiglio dei Ministri pongono l'accento sulla necessità di bilanciare innovazione e sicurezza. Questo articolo propone alcune riflessioni sull'applicazione dell'IA in questi settori, con esempi pratici di utilizzo e linee guida operative per conformarsi alla nuova normativa.

2. La normativa sull'Intelligenza Artificiale

Il regolamento approvato dal Parlamento Europeo mira a stabilire un quadro giuridico che garantisca lo sviluppo sicuro e etico dell'IA. Le principali caratteristiche del regolamento includono:

- 1. Classificazione dei Sistemi di IA:** la nuova normativa classifica i sistemi in base ai rischi associati al loro utilizzo (rischio minimo, limitato, alto e inaccettabile). I sistemi di IA ad alto rischio sono soggetti a requisiti più stringenti, mentre quelli a rischio minimo hanno obblighi normativi meno severi.
- 2. Requisiti di Sicurezza:** Per i sistemi di IA ad alto rischio il regolamento prevede obblighi di trasparenza e tracciabilità, come mantenere registri dettagliati delle operazioni dei sistemi di IA e garantire che gli utenti possano comprendere e contestare le decisioni automatizzate.
- 3. Sorveglianza del Mercato:** Per garantire il rispetto delle normative è stato previsto un rafforzamento delle autorità di vigilanza. Le autorità avranno il compito di monitorare l'uso dell'IA e di intervenire in caso di violazioni delle norme, con l'applicazione di sanzioni molto severe, fino a 35 milioni di euro, oppure, in caso di società, fino al 7% del fatturato globale annuale, se maggiore.

Queste misure mirano a prevenire l'uso improprio dell'IA, proteggendo i cittadini da abusi e discriminazioni e hanno allo stesso tempo l'obiettivo di promuovere l'innovazione responsabile, assicurando che i benefici dell'IA siano accessibili a tutti senza compromettere i diritti e le libertà fondamentali.

Accanto al regolamento è in discussione in questi giorni nel nostro paese un disegno di legge sull'Intelligenza Artificiale. Il disegno di legge italiano integra il regolamento europeo con disposizioni specifiche

per il contesto nazionale. Di seguito alcuni punti di interesse:

- 1. Strategia Nazionale:** il disegno di legge promuove la collaborazione tra pubblico e privato per lo sviluppo dell'IA. Questa strategia mira a creare un ecosistema favorevole all'innovazione, incentivando le startup e facilitando la ricerca e lo sviluppo, incoraggiando così la nascita di nuove soluzioni e applicazioni.
- 2. Autorità Nazionali:** si vogliono affidare compiti di controllo all'Agenzia per l'Italia digitale (AgID) e all'Agenzia per la cybersicurezza nazionale (ACN). Queste agenzie dovrebbero essere responsabili della supervisione e dell'implementazione delle normative sull'IA.
- 3. Formazione e Alfabetizzazione:** il disegno di legge prevede programmi educativi per cittadini e professionisti. Questi programmi mirano a colmare il divario di competenze digitali e a preparare la forza lavoro per le sfide del futuro, garantendo che i professionisti siano in grado di sfruttare appieno le potenzialità dell'IA. Le autorità di controllo avranno un ruolo decisivo nel diffondere linee guida e best practice per l'implementazione etica e responsabile dell'IA.
- 4. Norme di Sicurezza:** infine, si pone attenzione particolare ai temi di cybersicurezza e protezione dei dati personali. Le aziende dovranno adottare misure di sicurezza avanzate per proteggere i dati e garantire la conformità alle normative europee e nazionali.

La nuova normativa sulla IA avrà un impatto significativo su diversi livelli. Le aziende dovranno investire in sistemi di compliance per garantire l'adesione alle nuove normative. Questo potrebbe comportare costi iniziali piuttosto rilevanti, ma a lungo termine contribuirà a creare un ambiente di maggiore fiducia e sicurezza. Nonostante le sfide, l'IA rappresenta una straordinaria opportunità di innovazione in tutti i settori. Le tecnologie emergenti, come l'apprendimento automatico e l'elaborazione del linguaggio naturale, possono trasformare profondamente il nostro modo di vivere e lavorare o di fare impresa, migliorando l'efficienza operativa e offrendo nuovi modi per interagire con i clienti.

3. Prime Linee Guida Operative per le Aziende

Per conformarsi alla nuova normativa sull'IA ed essere preparate ancor prima della sua effettiva applicazione, le aziende potranno adottare diverse linee guida operative, tra cui:

- 1. Mappatura dei sistemi di IA per identificare i sistemi vietati:** il primo passo fondamentale è la mappatura dei sistemi di IA attualmente in uso o che si prevede di utilizzare all'interno dell'UE, per classificarli in base ai livelli di rischio definiti dal regolamento. Se tra questi dovessero essere rinvenuti sistemi a "rischio inaccettabile", quali ad esempio quelli che permettono il riconoscimento delle emozioni nei luoghi di lavoro o i sistemi di c.d. social credit scoring, le aziende dovranno cessarne immediatamente l'uso o lo sviluppo.
- 2. Valutazione dei Rischi:** una volta mappati i sistemi, ed esclusi i sistemi inaccettabili, occorre identificare e valutare i rischi associati all'uso dell'IA, differenziando quelli a rischio alto (quali ad esempio quelli per la selezione del personale) dagli altri sistemi con minor impatto (ad esempio l'uso di un chatbot per semplificare il customer care). Si dovranno quindi implementare misure di mitigazione e assicurare che i sistemi di IA siano privi di bias e discriminazioni. Questo include l'analisi dei potenziali impatti negativi e la predisposizione di piani di emergenza. Il periodo per assicurare la conformità di questi sistemi è piuttosto ampio ma in strutture organizzative complesse occorre affrontare questi temi con la massima tempestività.
- 3. Trasparenza e Tracciabilità:** terminata l'analisi dei rischi è necessario garantire che i sistemi di IA siano trasparenti, con la possibilità di tracciare le decisioni algoritmiche (quali log di registrazione degli eventi). Le aziende devono essere in grado di spiegare come e perché vengono prese determinate decisioni. In questo modo si potrà garantire che le decisioni automatizzate possano essere comprese e contestate dagli utenti. Questo è essenziale per mantenere la fiducia nei sistemi di IA.
- 4. Protezione dei Dati:** l'IA può avere un impatto significativo sui dati personali. Occorre dunque implementare anche rigorose misure di protezione dei dati personali, in conformità con il GDPR. Questo include la crittografia dei dati, l'anonimizzazione e politiche di accesso rigorose.

5. Formazione Continua: per garantire l'uso responsabile dell'IA le imprese devono fornire formazione continua ai dipendenti. La formazione dovrebbe coprire aspetti tecnici, etici e normativi. Le aziende devono dunque stabilire chiare procedure interne per l'utilizzo dei sistemi di IA tese ad istruire i dipendenti sul corretto utilizzo dei sistemi.

6. Monitoraggio e Revisione: le imprese, con l'aiuto dei fornitori, devono infine stabilire procedure per il monitoraggio e la revisione periodica dei sistemi di IA, assicurando un'alta qualità e obiettività dei dati processati e l'allenamento continuo degli algoritmi per una risposta sempre più efficace e priva di rischi. Le aziende devono effettuare audit regolari per garantire che i sistemi funzionino come previsto e che siano conformi alle normative.

4. Applicazioni dell'IA nel Settore Bancario, Finanziario e Assicurativo

Di seguito, a puro titolo illustrativo, sono indicati alcuni esempi di utilizzo dei sistemi di IA nei settori bancario, finanziario e assicurativo e l'impatto che l'attuale normativa sulla tutela dei dati personali, in combinazione con la nuova, potrebbe avere:

1. Rilevazione delle Frodi: attraverso l'utilizzo di algoritmi di machine learning il sistema IA per la prevenzione frodi è in grado di identificare transazioni sospette. In particolare, il sistema analizza i comportamenti transazionali per rilevare attività fraudolente in tempo reale, utilizzando al contempo modelli predittivi basati su grandi quantità di dati storici per individuare anomalie e comportamenti insoliti. Il beneficio atteso è la riduzione delle perdite finanziarie e la protezione dei clienti. L'efficacia di questi sistemi permette infatti di prevenire frodi prima che possano causare danni significativi.

Poiché questo sistema di IA potrebbe essere classificato come ad alto rischio, potrebbe rendersi necessaria una analisi preliminare con indicazioni dettagliate sui dati di addestramento e i processi decisionali e quindi l'implementazione di un sistema di governance dei dati che assicuri la qualità e la integrità dei dati utilizzati per l'addestramento e il funzionamento del sistema IA. Al contempo si rende necessaria anche una valutazione d'impatto sulla protezione dei dati per valutare i rischi per i diritti e le libertà delle persone coinvolte. Le entità che utilizzano questi sistemi devono inoltre informare gli utenti su come i dati vengono raccolti, elaborati e utilizzati,

garantendo trasparenza, ed implementare misure di sicurezza adeguate per proteggere i dati da accessi non autorizzati e perdite di dati, comprese tecniche di pseudonimizzazione e crittografia. Dovrebbe poi essere assicurato un monitoraggio continuo delle prestazioni del sistema per garantire accuratezza e affidabilità nel tempo. In caso di contestazioni, ma non solo, occorre mantenere anche una documentazione dettagliata dei modelli predittivi utilizzati e delle metriche di performance per garantire la trasparenza e la rendicontabilità.

2. Servizi di Consulenza Finanziaria: il sistema IA utilizza un robo-advisor per la gestione degli investimenti. La piattaforma fornisce una consulenza personalizzata basata su algoritmi di IA. Analizza il profilo di rischio e gli obiettivi finanziari degli utenti per offrire raccomandazioni di investimento su misura. Il sistema mira a garantire accessibilità ai servizi finanziari e ottimizzazione dei portafogli di investimento. Questi strumenti democratizzano l'accesso alla consulenza finanziaria, rendendola disponibile anche a chi non può permettersi un consulente tradizionale.

Considerando che il sistema può influenzare significativamente le decisioni finanziarie degli utenti, una DPIA è raccomandata per identificare e mitigare i potenziali rischi associati alle decisioni di investimento automatizzate, in particolare per valutare il rischio di bias algoritmico e le sue potenziali conseguenze sugli utenti. Gli utenti devono essere informati in modo chiaro e comprensibile riguardo al funzionamento del sistema, ai dati utilizzati e alle implicazioni delle raccomandazioni fornite. Devono inoltre essere intraprese misure di sicurezza robuste per proteggere i dati finanziari e personali degli utenti, prevenendo accessi non autorizzati e usi impropri. Il sistema dovrebbe tenere conto di pratiche riconosciute per lo sviluppo e il monitoraggio dei robo-advisor e il fornitore dovrebbe garantire un monitoraggio continuo della precisione e affidabilità delle raccomandazioni di investimento. Infine, il sistema dovrebbe offrire la possibilità agli utenti di contestare le raccomandazioni e di ottenere un intervento umano in caso di decisioni automatizzate critiche.

3. Gestione dei Rischi: il sistema di IA prevede modelli predittivi per valutare il rischio di credito. Sono analizzati grandi volumi di dati per prevedere la probabilità di default dei clienti. Il sistema utilizza variabili macroeconomiche, storici di credito e altri dati rilevanti per fornire valutazioni accurate del rischio. Attraverso questo strumento si ottiene un miglioramento delle decisioni di

credito e una significativa riduzione dei rischi. Le istituzioni finanziarie possono offrire prestiti in modo più sicuro e responsabile, riducendo il rischio di insolvenze.

Essendo un sistema che può avere impatti significativi sulla vita degli individui, una DPIA è necessaria per valutare i rischi associati. Le istituzioni finanziarie devono inoltre fornire informazioni chiare ai clienti su come vengono valutati i loro rischi di credito e su come vengono utilizzati i loro dati. Sono poi implementate misure di sicurezza per proteggere i dati dei clienti, assicurando che solo personale autorizzato possa accedere ai dati e che ci siano audit regolari per prevenire abusi. Soprattutto in sistemi di questo tipo è poi fondamentale assicurare che i modelli predittivi siano regolarmente aggiornati e validati per mantenere la loro accuratezza e rilevanza. A tal fine le aziende dovrebbero stabilire audit periodici e meccanismi di accountability per monitorare l'uso del sistema e prevenire discriminazioni o altri impatti negativi sui clienti.

4. Automazione dei Processi: il sistema IA è costituito da un chatbot per l'assistenza clienti, che gestisce le loro richieste, riducendo i tempi di attesa. Il sistema permette di rispondere a domande frequenti, eseguire operazioni di base e indirizzare le richieste complesse a operatori umani. Le imprese che lo utilizzano aumentano l'efficienza operativa, riducendo i costi, e migliorano la soddisfazione del cliente. L'IA può infatti automatizzare compiti ripetitivi e a basso valore aggiunto, liberando risorse per attività più strategiche e a maggior valore aggiunto.

In questo caso la valutazione di impatto potrebbe non essere necessaria, anche se è sempre consigliabile per garantire che non ci siano impatti non previsti sui dati personali. Gli utenti devono essere in ogni caso informati che stanno interagendo con un sistema automatizzato e devono essere forniti dettagli su come vengono trattati i loro dati. Devono poi essere adottati meccanismi di fallback per garantire che gli utenti possano sempre accedere a un operatore umano in caso di necessità o insoddisfazione con il chatbot. Rimane ferma la necessità di misure di sicurezza per proteggere i dati personali gestiti dal chatbot, inclusi accessi limitati e registrazione delle interazioni per garantire la trasparenza. Occorre infine monitorare l'utilizzo dei chatbot e verificare in modo continuo le prestazioni e la precisione delle risposte.

5. Analisi dei Dati: in questo esempio il sistema permette la personalizzazione dei servizi attra-

verso l'utilizzo di algoritmi di IA per analizzare i dati dei clienti e offrire prodotti su misura. Le aziende possono sfruttare i dati raccolti per capire meglio le esigenze dei clienti e creare offerte personalizzate. L'IA può infatti prevedere tendenze future e comportamenti dei clienti, permettendo alle aziende di anticipare le esigenze del mercato e adattare le loro strategie di conseguenza. I benefici attesi mirano all'aumento delle vendite e la fidelizzazione dei clienti. La personalizzazione migliora l'esperienza del cliente e promuove la lealtà a lungo termine.

Pur non apparendo un sistema ad alto rischio potrebbe essere necessaria una valutazione di impatto se l'analisi dei dati implica un trattamento su larga scala di dati personali o sensibili, per assicurare che i rischi siano correttamente identificati e mitigati. I clienti devono essere chiaramente informati su come i loro dati vengono raccolti, utilizzati e per quali finalità specifiche, oltre ad avere la possibilità di opt-out. Il sistema di IA deve infatti garantire che i dati utilizzati per l'analisi siano pertinenti, limitati a ciò che è necessario e ottenuti in modo legale e trasparente. La creazione di politiche chiare di gestione dei dati che includano periodi di conservazione, misure di minimizzazione dei dati e procedure di eliminazione sicura dei dati contribuiscono a mantenere il sistema conforme alla normativa. Devono essere inoltre implementate adeguate misure di sicurezza per proteggere i dati dei clienti da accessi non autorizzati, perdite o altre violazioni, comprese tecniche di anonimizzazione quando possibile. Infine, il sistema deve tenere conto di pratiche riconosciute per l'analisi dei dati e la personalizzazione dei servizi e deve essere assicurato un monitoraggio continuo dell'accuratezza e affidabilità dei risultati delle analisi.

Il regolamento europeo e il disegno di legge italiano sull'intelligenza artificiale rappresentano passi fondamentali per garantire uno sviluppo etico e sicuro dell'IA. L'applicazione nel settore bancario, finanziario e assicurativo offre numerose opportunità, ma richiede anche un'attenta gestione dei rischi e una stretta aderenza alle normative. Le linee guida operative e l'impatto del nuovo quadro normativo delineano un futuro in cui l'IA potrà essere utilizzata in modo responsabile e sostenibile, migliorando la qualità dei servizi offerti e proteggendo i diritti dei cittadini. Per le aziende questo significa navigare un panorama regolamentare complesso, ma anche sfruttare le straordinarie opportunità offerte dall'IA. Con l'adozione di pratiche etiche, trasparenti e sicure, l'IA può diventare un potente alleato nella trasformazione digitale, migliorando i servizi offerti e rafforzando la fiducia dei clienti.

DB non solo
diritto
bancario

A NEW DIGITAL EXPERIENCE

 **dirittobancario.it**

