DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Dati personali e modelli di IA

Indicazioni operative per la compliance alla luce del parere EDPB 28/2024

9 Gennaio 2025

Aurora Agostini, Partner, Lexia

Aurora Agostini, Partner, Lexia

Aurora Agostini

Aurora Agostini è partner responsabile del team Data & Technology Innovation di Lexia Avvocati. Assiste clienti in tutti i settori del diritto dell'informatica, della proprietà intellettuale e delle nuove tecnologie, con un'ampia competenza sugli aspetti della protezione dei dati e della privacy. La sua attività si concentra sulle misure di compliance, come le procedure e la documentazione richieste dal GDPR, la valutazione della base giuridica del trattamento, la conformità digitale (ad esempio i cookie), le politiche sulla privacy, le risposte ai reclami e l'esercizio dei diritti, i trasferimenti transfrontalieri di dati.

Avvocati

Lexia

LEXIA LAW | TAX | INNOVATION

Il recente parere 28/2024 del Comitato Europeo per la Protezione dei Dati (EDPB) fornisce importanti chiarimenti sull'applicazione del Regolamento (UE) 2016/679 (GDPR) nel contesto dello sviluppo e dell'implementazione di modelli di intelligenza artificiale (IA): il parere si rivolge a tutti i soggetti coinvolti nella filiera dell'IA, e offre spunti particolarmente rilevanti per chi utilizza queste tecnologie in contesti regolamentati o con impatti significativi sui diritti degli interessati, delineando un quadro di adempimenti destinato ad incidere significativamente sulle scelte organizzative delle aziende.

Nel contesto bancario-assicurativo, l'utilizzo di modelli di IA interessa ormai numerosi **processi *core***, quali la valutazione del merito creditizio, il monitoraggio delle frodi, la profilazione della clientela, i controlli antiriciclaggio, nonché la gestione automatizzata delle relazioni con la clientela. Per ciascuno di questi ambiti, il parere EDPB richiede agli utilizzatori di assumere un ruolo attivo nella verifica della conformità dei modelli utilizzati, non potendo questi limitarsi a fare affidamento sulle dichiarazioni dei fornitori.

L'implementazione di modelli di intelligenza artificiale nelle istituzioni finanziarie comporta una serie di **responsabilità e adempimenti fondamentali per garantire la conformità al GDPR** e alle altre normative applicabili, ponendo particolare attenzione alla tutela dei diritti e delle libertà fondamentali degli interessati. In tale prospettiva, il parere EDPB delinea un quadro articolato di requisiti operativi che gli utilizzatori dei sistemi di IA sono chiamati ad implementare, con particolare riferimento a tre ambiti fondamentali: la verifica della base giuridica del trattamento, la predisposizione di adeguati presidi organizzativi e l'implementazione di un sistema strutturato di controlli continui:

1. La verifica della base giuridica

Il GDPR richiede che ogni trattamento di dati personali sia fondato su una **base giuridica** conforme all'art. 6 e, nel caso di categorie particolari di dati, all'art. 9. Nel contesto dell'utilizzo di modelli di IA, tale requisito assume particolare rilevanza e complessità per gli operatori del settore finanziario, richiedendo un'analisi articolata che deve essere condotta con specifico riferimento al contesto operativo di ciascun intermediario.

In fase di implementazione di un modello di IA, banche e assicurazioni dovranno innanzitutto individuare quale delle basi giuridiche previste dal GDPR sia più appropriata per il trattamento. Tale valutazio-

vedi l'articolo online

ne dovrà tenere conto della natura del trattamento e delle sue finalità: così, ad esempio, il consenso dell'interessato (art. 6(1)(a)) potrà risultare appropriato per trattamenti non essenziali, quali l'utilizzo di dati per il miglioramento di modelli predittivi di *marketing*; l'esecuzione del contratto (art. 6(1)(b)) potrà legittimare l'impiego di modelli destinati a fornire servizi contrattualmente previsti, come nel caso delle valutazioni creditizie; mentre il legittimo interesse (art. 6(1)(f)) potrà trovare applicazione in contesti quali il rilevamento delle frodi, ferma restando la necessità di un rigoroso bilanciamento con i diritti degli interessati.

Il principio di *accountability*, sancito dall'art. 5(2) del GDPR, richiede agli operatori vigilati di documentare accuratamente le proprie valutazioni. Tale documentazione dovrà includere, in particolare, un'analisi approfondita della necessità del trattamento, dimostrando perché l'utilizzo dell'IA rappresenti lo strumento più appropriato per il perseguimento degli obiettivi prefissati rispetto ad alternative meno invasive, quali analisi manuali o metodi aggregati. Nel caso di trattamenti fondati sul legittimo interesse, particolare attenzione dovrà essere dedicata al bilanciamento degli interessi richiesto dal Considerando 47, dovendo l'intermediario dimostrare che i benefici attesi dal trattamento superano i potenziali rischi per i diritti e le libertà degli interessati.

Tale valutazione, peraltro, non può considerarsi definitiva: l'art. 24 del GDPR richiede infatti un **aggiornamento continuo** dell'analisi della base giuridica, in considerazione dell'evoluzione delle finalità del trattamento o di eventuali modifiche nei modelli operativi. In tale prospettiva, risulta essenziale per i soggetti vigilati l'implementazione di procedure che garantiscano una rivalutazione periodica della base giuridica, con particolare attenzione ai casi in cui modifiche nel funzionamento del modello o nelle modalità del suo utilizzo possano incidere sulla validità delle valutazioni inizialmente effettuate.

Sul piano operativo, è fondamentale sottolineare come tali valutazioni non possano essere delegate ai fornitori dei modelli di IA: conformemente all'art. 24(1) del GDPR, gli intermediari finanziari devono infatti considerare le peculiarità del proprio contesto operativo e i rischi specifici per i diritti degli interessati. Ciò non esclude, naturalmente, l'opportunità di una collaborazione con i fornitori, che potrà concretizzarsi nella negoziazione di clausole contrattuali volte a garantire adeguati livelli di trasparenza sul trattamento e il necessario supporto nella documentazione delle valutazioni effettuate.

2. Presidi organizzativi

L'adozione di modelli di IA nel settore finanziario richiede l'implementazione di un'infrastruttura organizzativa articolata, che trova fondamento nelle disposizioni del GDPR in materia di *accountability* (art. 5(2)), *privacy by design* e *by default* (art. 25), e sicurezza del trattamento (art. 32). Tale infrastruttura si articola su tre livelli principali:

1. definizione di una ***policy* interna** che stabilisca linee guida chiare e vincolanti per la gestione dei modelli di IA: tale documento dovrà disciplinare, con adeguato livello di dettaglio, i criteri di selezione dei modelli, i requisiti di conformità normativa e le responsabilità delle diverse funzioni coinvolte. A titolo esemplificativo, una banca potrebbe prevedere nella propria *policy* l'obbligo di sottoporre preventivamente ogni nuovo modello alla validazione del Data Protection Officer (DPO), assicurando così una valutazione preliminare degli impatti sui diritti degli interessati;
2. un sistema di *governance* per la valutazione della confornità normativa e dei rischi oepratívi, che preveda, per le realtà di maggiori dimensioni, la costituzione di un **comitato interdisciplinare** che coingolga diverse professionalità: esperti di tecnologia, per valutare l'affidabilità dei modelli; giuristi, per verificare la conformità normativa; rappresentanti delle funzioni di *business* e di controllo, per garantire la coerenza con le finalità aziendali e presidiare i rischi;
3. procedure di ***due diligence* sui fornitori**, integrate da **presidi di secondo livello**: gli operatori finanziari devono verificare che i *provider* rispettino gli standard normativi e di sicurezza richiesti, con particolare attenzione alle modalità di trattamento dei dati e all'utilizzo di tecniche di protezione quali pseudonimizzazione e crittografia. In termini operativi, ciò comporta l'acquisizione di documentazione dettagliata e certificazioni di conformità, nonché la negoziazione di specifici impegni contrattuali. I controlli di secondo livello, complementari a tali verifiche, sono finalizzati a garantire l'allineamento costante al GDPR e alle policy aziendali attraverso *audit* periodici, monitoraggi continui per l'individuazione di eventuali bias algoritmici e procedure di escalation per la gestione tempestiva delle criticità.

La fase di implementazione dei modelli richiede poi un approccio metodologico strutturato, che preveda innanzitutto lo svolgimento di test approfonditi prima del rilascio in produzione, opportunamente

vedi l'articolo online

documentati e condotti con il coinvolgimento di tutte le funzioni interessate, incluse quelle di controllo. Parallelamente, particolare attenzione deve essere dedicata alla predisposizione di adeguate **informative** per la clientela, che illustrino in modo chiaro e comprensibile le modalità di utilizzo dei modelli di IA e le finalità perseguite. Di fondamentale importanza risulta, inoltre, la **formazione** del personale coinvolto, che dovrà essere adeguatamente istruito non solo sugli aspetti tecnici ma anche sui profili di compliance e sui rischi connessi all'utilizzo dei modelli, prevedendo aggiornamenti periodici in considerazione della rapida evoluzione delle tecnologie e del quadro normativo di riferimento.

3. Obblighi di verifica continua

La conformità nell'utilizzo di modelli di IA non può essere considerata un obiettivo statico, richiedendosi, piuttosto, l'implementazione di un sistema di **monitoraggio** continuo che garantisca il costante allineamento ai requisiti del GDPR (in particolare, quanto ai principi di accountability e di limitazione delle finalità ex art. 5, nonché agli obblighi di sicurezza e di valutazione d'impatto di cui agli artt. 32 e 35) e l'efficacia operativa nel tempo.

Sul piano operativo, gli intermediari del settore finanziario sono chiamati, innanzitutto, a verificare periodicamente la persistenza dei presupposti di **liceità del trattamento**; tale verifica assume particolare rilevanza laddove il trattamento si fondi sul consenso dell'interessato - dovendo essere costantemente monitorata la validità dello stesso e l'eventuale esercizio del diritto di revoca - ovvero sul legittimo interesse, richiedendosi, in tal caso, una rivalutazione periodica del bilanciamento degli interessi alla luce dell'evoluzione delle circostanze.

Di non minor rilievo risulta il monitoraggio dell'accuratezza e dell'affidabilità dei modelli, da attuarsi mediante **test regolari delle prestazioni** e valutazioni sulla **qualità dei dati** in ingresso: un'attività cruciale nel contesto dei servizi finanziari, ove si consideri, ad esempio, la necessità di sottoporre a verifiche periodiche i modelli utilizzati per l'assegnazione di punteggi creditizi.

Specifica attenzione deve essere dedicata, inoltre, alla valutazione periodica dei **rischi di re-identificazione**, considerato che l'evoluzione delle tecnologie di analisi dei dati, ovvero l'aggregazione di informazioni provenienti da diverse fonti, potrebbe compromettere l'efficacia delle misure di anonimizzazione originariamente adottate: in tale prospettiva, gli operatori dovranno considerare l'implementazione di tecniche avanzate, quali la "*differential privacy*".

Il sistema di monitoraggio deve, infine, prevedere: procedure di escalation strutturate per la gestione delle anomalie; KPI specifici per la valutazione dell'efficacia dei modelli, nonché un registro dettagliato delle criticità riscontrate e delle conseguenti azioni intraprese, il tutto nell'ottica di un costante aggiornamento delle valutazioni d'impatto sulla protezione dei dati.

4. Considerazioni conclusive e prospettive operative

Il parere EDPB impone agli operatori del settore finanziario l'avvio di un articolato percorso di adeguamento che, muovendo da una preliminare mappatura dei modelli di IA in uso - con particolare riguardo alle tipologie di dati trattati, alle finalità perseguite e ai fornitori coinvolti -, richiede l'implementazione di un *framework* di *governance* integrato nei processi di gestione del rischio. Tale *framework* assume particolare criticità alla luce del regime sanzionatorio previsto dall'art. 83 del GDPR, che, come noto, prevede sanzioni fino a 20 milioni di euro ovvero al 4% del fatturato globale annuo.

Le principali aree di rischio attengono, in particolare, all'assenza di valide basi giuridiche per il trattamento, alla mancata dimostrazione dell'adozione di misure tecniche e organizzative adeguate, nonché alla gestione non conforme dei reclami degli interessati, profili questi che, oltre alle conseguenze sanzionatorie, possono determinare significativi impatti reputazionali.

Il settore bancario e assicurativo, forte della propria consolidata esperienza nella gestione di requisiti regolamentari complessi, è chiamato, pertanto, a cogliere l'opportunità di tale adeguamento normativo per rafforzare i propri presidi di controllo e promuovere un utilizzo etico e responsabile dell'IA, nell'ottica di coniugare l'innovazione tecnologica con un'efficace tutela dei diritti degli interessati e trasformando, così, un adempimento normativo in un potenziale vantaggio competitivo.

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it