Nei provvedimenti del Garante per la protezione dei dati le istruzioni per un utilizzo in regola

Sistemi di IA, policy d'obbligo

Imprese e p.a. devono redigere atti sulle scelte adottate

Pagina a cura di
ANTONIO CICCIA MESSINA

Addestramento continuo dell'intelligenza artificiale (IA) usata da aziende e pubbliche amministrazioni: è una misura che deve essere inserita nelle policy con cui imprese ed enti pubblici devono documentare la scelta di avvalersi di questa innovativa tecnologia. A fronte di una ormai disponibilità diffusa di sistemi di IA e nelle more della definitiva approvazione e operatività del Regolamento Ue sull'IA, imprese e pa non devono farsi prendere la mano e, prima di ricorrere all'IA, devono redigere appositi atti di documentazione della scelta effettuata.

Una verifica della congruità e completezza delle policy può essere svolta mediante confronto con alcuni provvedimenti del Garante della privacy. Al riguardo si segnala il Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di IA, il quale seppure rispetto a un comparto specifico (quello sanitario) ha indicazioni generali e trasversali per tutti i settori pubblici e privati. Peraltro, va anche citato il provvedimento n. 78/2022, con il quale il Garante ha dato parere favorevole al regolamento della Banca d'Italia che disciplina l'uso di uno specifico sistema di IA, e cioè quello per l'istruttoria degli esposti di utenti bancari. Quest'ultimo provvedimento scende in dettagli operativi e, quindi, è una fonte alla quale attingere consigli concreti per la stesura di una policy interna sull'IA, di cui passiamo ad analizzare i passaggi più rilevanti.

Dichiarazione generale. L'atto di documentazione delle scelte deve contenere una dichiarazione di impegno al rispetto dei principi privacy. Una formula utilizzabile può attestare che, nell'ambito del principio della responsabilizzazione, l'utilizzo di IA e tecnologie correlate risponde a principi di liceità, correttezza, trasparenza, limitazione della finalità e della conservazione, minimizzazione dei dati, esattezza, integrità e riservatezza.

Descrizione della logica. Nell'atto di documentazione delle scelte è necessario descrivere la logica del trattamento realizzato con i sistemi di IA. Occorre dettagliare le tecniche di analisi e algoritmi (ad esempio machine learning), arricchendo tale descrizione con ulteriori dettagli. Nel regolamento della Banca d'Italia, ad esempio, si espone che la logica alla base delle tecniche attualmente utilizzate consiste nell' aggregare i documenti in cluster, per similitudine semantica, così da consentire l'apprendimento di elementi informativi e rappresentazioni gerarchiche dall'aggregazione dei dati, previa assegnazione di tag esemplificativi del contenuto.

Clusterizzazione. Un elemento valutato molto positivamente dal Garante con riferimento al caso della Banca d'Italia è stata l'esclusione della clusterizzazione sulla base dei dati personali analizzati dall'IA. Rispetto a questo profilo ci possono essere esiti diversi, se assistiti da una idonea base giuridica e da un quadro di adeguate tutele per gli interessati.

Descrizione dell'impatto. La descrizione dell'impatto rispetto ai diritti e alle libertà individuale è un passaggio obbligato dell'atto di documentazione delle scelte. Occorre mettere in evidenza gli effetti giuridici conseguenza dei trattamenti con l'IA.

Nel precedente del regolamento di Banca d'Italia, ad esempio, si escludono profilazioni o conseguenze sanzionatorie o decisioni automatiche su persone fisiche. Per una pubblica amministrazione, a legislazione vigente, i provvedimenti sanzionatori, rientrano infatti nell'esercizio discrezionale delle funzioni di vigilanza e non possono essere la risultante di procedure automatiche.

In ambiti diversi si può giungere a risultati differenti, nel rispetto dell'articolo 22 del regolamento Ue sulla privacy n. 2016/679 e, quindi, in casi di necessità contrattuale o di consenso esplicito dell'interessato. Peraltro, la descrizione dell'impatto dovrà essere tanto più approfondita quanto maggiore sarà lo spazio di manovra autonoma da parte dell'IA.

Tempi di conservazione. L'atto di documentazione delle scelte deve precisare il periodo di conservazione delle informazioni acquisite in relazione alle operazioni svolte tramite strumenti di IA. Ad esempio, nel regolamento della Banca d'Italia, avallato dal Garante, si prevede che negli applicativi che utilizzano tecniche di analisi e algoritmi di machine learning, i dati vengono conservati per dieci anni, come documentazione di supporto alle attività svolte e per garantire la correlazione esistente tra la performance dei sistemi di IA e la lunghezza delle serie storiche sottostanti e consentire così la verifica e la replicabilità dei risultati delle analisi, utile a stabilire le corrette interazioni tra i dati contenuti nei documenti esaminati dall'IA. Ciò fermo restando il diritto dell'interessato di opporsi in qualsiasi momento al trattamento dei dati personali.

Finalità. Anche la finalità perseguita dal titolare del trattamento va inserita nell'atto di documentazione delle scelte. Si può, ad esempio, fare riferimento, in relazione alle operazioni effettuate strumenti di IA, allo scopo di ottimizzare il patrimonio informativo raccolto, per poterne ricavare elementi utili su fenomeni d'interesse per l'attività del titolare del trattamento.

Base giuridica. A riguardo della condizione di liceità nel trattamento dei dati per le pubbliche amministrazioni, l'atto di documentazione delle scelte deve indicare leggi e regolamenti posti a base dell'attività realizzata con l'IA. Per i trattamenti non fondati su presupposti normativi si ritiene che, quando vi siano decisioni interamente automatizzate, si applichi l'articolo 22 e, pertanto, le basi giuridiche utilizzabili sono il consenso esplicito e le necessità contrattuali. Non è chiaro se possa esserci attività svolta da IA che non comporti una decisione automatizzata: in caso affermativo si applicano le basi giuridiche previste dagli articoli da 6 a 11 del Gdpr.

Tipi di dati. Nell'uso delle informazioni tramite strumenti di IA, occorre rispettare il principio di minimizzazione rispetto alle finalità e descrivere, nell'atto di documentazione delle scelte, i tipi di dati analizzabili dai sistemi di IA.

Operazioni eseguibili. L'esposizione delle operazioni eseguibili con l'ausilio di sistemi di IA deve essere analitica. Ad esempio, si possono elencare le seguenti attività: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento, estrazione, consultazione, uso, raffronto, interconnessione, limitazione, cancellazione. Con riferimento specifico all'IA si può, ad esempio, sottolineare l'attività di analisi attraverso la ricerca di elementi rilevanti e la valutazione delle eventuali iniziative da intraprendere.

Misure di sicurezza. Una misura che ha rilevanza trasversale è l'addestramento continuo dei sistemi di IA. Nel regolamento della Banca d'Italia si prevede un processo continuo di riaddestramento, con periodico monitoraggio e aggiornamento degli algoritmi, i quali sono in grado di apprendere le logiche di analisi e di ricerca da un insieme di dati (training dataset).

A ciò si aggiunge che, per assicurare la qualità dei risultati delle analisi effettuate tramite strumenti di IA e monitorare l'obsolescenza delle relazioni apprese dai modelli di machine learning, nel processo di riaddestramento vengono coinvolti componenti di esperti appartenenti all'area di gestione degli esposti e al profilo tecnico (data scientist). Sempre nel regolamento della Banca d'Itala si attesta che l'algoritmo viene, periodicamente riaddestrato non appena si ritiene che il set di informazioni o l'interpretazione ad essi associata stia per rendere "obsolete" le relazioni apprese dal modello, a causa di fattori di variazione, anche esogeni, che possono impattare sui risultati delle analisi.

Sempre, quale misura di sicurezza, si afferma che l'applicazione del machine learning si avvale di tecniche in grado di fornire una rappresentazione del funzionamento interno dell'algoritmo, finalizzata alla spiegabilità dei risultati prodotti.

A ciò si aggiunge la conservazione della documentazione che dà conto del continuo perfezionamento dell'algoritmo al solo fine di "versioning" del modello e di monitoraggio dello sviluppo nel corso del tempo.

Adempimenti. L'uso di sistemi di IA nei trattamenti di dati personali impone la redazione della valutazione di impatto privacy, l'aggiornamento del registro del trattamento, delle informative agli interessati, designazione ad hoc degli autorizzati al trattamento, clausole specifiche negli accordi con contitolari e responsabili del trattamento.

I capitoli della policy sull'IA

Dichiarazione generale	Rispetto principi di responsabilizzazione, liceità, correttezza, trasparenza, limitazione della finalità e della conservazione, minimizzazione dei dati, esattezza, integrità e riservatezza
Descrizione della logica	Dettagliare le tecniche di analisi e algoritmi (ad esempio machine learning), arricchendo tale descrizione con ulteriori profili (ad esempio: aggregazione di documenti in cluster, per similitudine semantica, previa assegnazione di tag esemplificativi del contenuto)
Descrizione dell'impatto	Evidenziare effetti giuridici conseguenza dei trattamenti con l'IA (ad esempio profilazioni, sanzioni o decisioni automatiche)
Conservazione	Indicare termine di conservazione dei dati (ad esempio, termine relativo a garantire verifica e la replicabilità dei risultati delle analisi)
Finalità	Ad esempio: ottimizzare il patrimonio informativo raccolto
Base giuridica	Per le p.a. indicare leggi e regolamenti posti a base dell'attività istituzionale; per i soggetti privati, in caso di decisioni interamente automatizzate, non fondate su presupposti normativi si applica l'articolo 22 Gdpr (consenso esplicito, necessità contrattuale)
Tipi di dati	Rispettare il principio di minimizzazione rispetto alle finalità
Operazioni eseguibili	Ad esempio: analisi attraverso la ricerca di elementi rilevanti e valutazione delle iniziative da assumere
Misure di sicurezza	Addestramento continuo dei sistemi di IA (oltre a quelle previste dall'articolo 32 Gdpr)
Adempimenti	Redazione della valutazione di impatto privacy, aggiornamento del registro del trattamento, delle informative agli interessati, designazione ad hoc degli autorizzati al trattamento, clausole specifiche negli accordi con contitolari e responsabili del trattamento