Estratto della Politica in materia di sviluppo e utilizzo responsabile dei sistemi di intelligenza artificiale

Unipol

ESTRATTO DELLA POLITICA IN MATERIA DI SVILUPPO E UTILIZZO RESPONSABILE DEI SISTEMI DI INTELLIGENZA ARTIFICIALE

Milano, 7 agosto 2025

Sommario

Obiettivi del documento

La Politica ha l'obiettivo di definire le linee guida del Gruppo Unipol (il "**Gruppo**") in materia di sviluppo e utilizzo responsabile di sistemi di intelligenza artificiale ("**IA**").

A tal fine, la Politica stabilisce, con riguardo alle società del Gruppo che rientrano nel perimetro di applicazione:

- il modello organizzativo per il presidio del Rischio IA;
- le linee guida in materia di sviluppo e utilizzo responsabile dei Sistemi di IA, inclusi i principi fondamentali adottati dal Gruppo rispetto all'IA;
- il processo per lo sviluppo e utilizzo responsabile dei Sistemi di IA, gli adempimenti previsti per i Sistemi di IA ad Alto Rischio e gli obblighi di informativa;
- le disposizioni in materia di monitoraggio di Sistemi di IA, di selezione e gestione delle Terze Parti e di formazione in materia di IA;
- i ruoli e le responsabilità nell'ambito dell'utilizzo e sviluppo di Sistemi di IA e i relativi flussi di reporting.

Si precisa che, laddove non diversamente specificato, gli organi/aree/funzioni citati nella Politica si intendono riferiti ad Unipol Assicurazioni S.p.A. ("**Unipol**") e agli organi/aree/funzioni equivalenti, ove presenti, delle altre Società in perimetro anche qualora esternalizzati.

Riferimenti normativi

La Politica è stata redatta in conformità alla normativa in vigore e agli indirizzi di vigilanza di settore di seguito riportati.

Normativa europea:

- Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale (l'"AI Act");
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei Dati Personali, nonché alla libera circolazione di tali dati (il "GDPR");
- Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario (il "DORA") e relativa regolamentazione delegata;
- Report Artificial intelligence governance principles: towards ethical and trustworthy artificial intelligence in the European insurance sector, emanato dal Consultative Expert Group on Digital Ethics in Insurance di EIOPA (le "Linee Guida EIOPA").

Normativa nazionale:

- Decreto legislativo 24 febbraio 1998, n. 58: TUF - Testo unico delle disposizioni in materia di intermediazione finanziaria;
- Decreto legislativo 7 settembre 2005, n. 209 - Codice delle Assicurazioni private, e successive modifiche ("Codice delle Assicurazioni private");
- Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" (il "Codice Privacy") e ss. mm;
- Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica emanate da Banca d'Italia il 17 maggio 2016 e ss. mm.;
- Regolamento IVASS n. 38 del 3 luglio 2018, recante disposizioni in materia di sistema di governo societario e ss.mm.;
- Provvedimento Banca d'Italia 5 dicembre 2019 e s.m. di attuazione degli artt. 4-undecies e 6, co. 1, lett. b) e c-bis) del TUF.

La Politica inoltre è coerente ed integra il sistema di autoregolamentazione in vigore nel Gruppo.

Perimetro di applicazione

La Politica si applica alla Capogruppo e alle società del Gruppo da essa controllate con sede legale in Italia che sviluppano o utilizzano Sistemi di IA (collettivamente, le "Società in perimetro").

Con riguardo ai principi fondamentali identificati da Unipol, la Politica si applica altresì alle società del Gruppo non aventi sede legale in Italia, che in ogni caso si dotano di una propria politica in materia coerente con la Politica in oggetto.

Definizioni e terminologia

Dati di addestramento	I dati utilizzati per addestrare un Sistema di IA adattandone i parametri che può apprendere.
Dati di convalida	I dati utilizzati per fornire una valutazione del Sistema di IA addestrato e per metterne a punto, tra l'altro, i parametri che non può apprendere e il processo di apprendimento, al fine tra l'altro di evitare lo scarso (*underfitting*) o l'eccessivo (*overfitting*) adattamento ai Dati di addestramento.
Dati di prova	I dati utilizzati per fornire una valutazione indipendente del Sistema di IA al fine di

	confermarne le prestazioni attese prima della sua immissione sul mercato o messa in servizio.
Dato Personale (o Dati Personali)	Qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Destinatario	Persona fisica o giuridica che subisce gli effetti del Sistema di IA, anche senza interagire direttamente con esso. Può incidere con l'utente.
DPIA o *Data Protection Impact Assessment*	Valutazione d'impatto sulla protezione dei Dati Personali.
IA Room	*Team* coordinato dal Presidio IA e composto dalle funzioni aziendali della Capogruppo e dalle omologhe funzioni presso le Società in perimetro coinvolte, a cui è affidato il compito di coadiuvare la Funzione Proponente nella valutazione del Rischio IA: *area Compliance*, area *Information*, area *Innovation*, area *Risk,* funzione *Corporate Social Responsability*, funzione *Organisation* (o, laddove nominato, il BC Manager) ed *Ethics Officer.* Il Presidio IA può avvalersi della consulenza di altre funzioni aziendali sulla base delle esigenze di valutazione rilevate.
Incidente Grave	Un incidente o un malfunzionamento di un Sistema di IA che, direttamente o indirettamente, causa una delle conseguenze seguenti: (i) il decesso di una persona o gravi danni alla salute di una persona, (ii) la violazione degli obblighi a norma del diritto

	dell'Unione intesi a proteggere i diritti fondamentali, (iii) gravi danni alle cose o all'ambiente.
IT Incident	Singolo evento o serie di Eventi collegati non pianificati con impatto negativo su Integrità, Autenticità, Disponibilità e/o Riservatezza dei sistemi e Servizi ICT e relativi dati.
Modello di IA	La rappresentazione fisica, matematica o altrimenti logica che sottostà a un Sistema di IA. Include, tra gli altri, i modelli statistici e vari tipi di funzioni di *input-output* (come alberi decisionali e reti neurali).
Pratiche di IA vietate	L'emissione sul mercato, la messa in servizio o l'uso di Sistemi di IA che comportano un rischio inaccettabile per i diritti e le libertà degli Utenti ai sensi dell'AI Act.
Profilazione	Qualsiasi forma di Trattamento automatizzato di Dati Personali consistente nell'utilizzo di tali Dati Personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.
Registro dei Sistemi di IA, o Registro	Piattaforma informatica di Gruppo che consente il censimento dei Sistemi di IA sviluppati/ in uso nel Gruppo, nonché della relativa documentazione tecnica, supervisionata dal Presidio IA e manutenuta nel continuo dalle Funzioni Proponenti.
Requisiti di accessibilità	Requisiti tecnici che il Sistema di IA deve possedere per essere utilizzabile da tutte le persone fisiche, comprese quelle con disabilità.

Requisiti per la gestione del Rischio IA	Requisiti per la gestione del Rischio IA dei Sistemi di IA, distinti secondo un approccio risk-based.
Rischio IA	S'intende l'insieme dei rischi derivanti dallo sviluppo e utilizzo di un Sistema di IA (es. rischio di non conformità alle norme, rischio operativo, rischio reputazionale, rischio strategico, etc.).
Sistema di IA	Sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali. Più Sistemi di IA possono essere sorretti dal medesimo Modello di IA.
Sistema di IA ad Alto Rischio	Sistema di IA che presenta un rischio significativo per i diritti e le libertà degli Utenti secondo i criteri definiti nell'AI Act..
Sistema di IA a Rischio Medio-Alto	Sistema di IA che, pur non essendo classificabile come Sistema di IA ad Alto Rischio, può presentare rischi significativi per i Destinatari e/o per le Società in perimetro.
Sistema di IA a Rischio Basso o Medio	Sistema di IA che non presenta rischi significativi per i Destinatari né per le Società in perimetro.
Sistema di IA generativa	Sistema di IA che genera contenuti audio, immagine, video o testuali in risposta al prompt o alla richiesta di un utente.
Utente	Persona fisica che materialmente utilizza o interagisce direttamente con il Sistema di IA. Si considerano Utenti anche i Destinatari, quando i Sistemi di IA sono progettati anche per interagire direttamente con loro.

Modello organizzativo per il presidio dei rischi derivanti dall'impiego dell'IA

Al fine di conseguire un efficace presidio del Rischio IA, sia in fase di sviluppo che di utilizzo di un Sistema di IA, è necessario che, presso la Capogruppo e le Società in perimetro, il processo di *governance* sia chiaramente e coerentemente stabilito.

Il Gruppo ha definito ruoli e responsabilità, sia a livello di Capogruppo sia a livello di società controllate, che garantiscono l'indirizzo e governo, l'esecuzione e il controllo del modello per il presidio dei rischi derivanti dall'impiego dell'IA (il "**Modello**").

Area	**Obiettivo**
Indirizzo e governo	Garantire la definizione e favorire la diffusione e la corretta implementazione del Modello, nonché delle strategie per uno sviluppo e utilizzo etico e responsabile dell'IA.
Esecuzione	Garantire l'implementazione del Modello definito, nel rispetto delle disposizioni interne ed esterne applicabili.
Controllo	Identificare, valutare, gestire e monitorare i rischi derivanti dall'impiego dell'IA.

Linee guida in materia di sviluppo e utilizzo responsabile dei Sistemi di IA

La normativa in tema di IA mira a promuovere uno sviluppo etico, responsabile e sicuro dei Sistemi di IA, garantendo la protezione dei diritti fondamentali e la sicurezza degli Utenti e dei Destinatari.

L'approccio del Gruppo Unipol allo sviluppo e all'utilizzo dell'Intelligenza Artificiale si fonda su principi etici, normativi e di responsabilità sociale, che assicurano che le tecnologie siano impiegate a beneficio delle persone e della collettività.

I seguenti principi fondamentali guidano tutte le fasi del ciclo di vita dei Sistemi di IA sviluppati e utilizzati all'interno del Gruppo:

Trasparenza, spiegabilità, sicurezza ed affidabilità

Il Gruppo riconosce che la trasparenza è fondamentale per costruire la fiducia nell'uso dell'Intelligenza Artificiale. Il Gruppo si impegna a garantire che i Sistemi di IA siano sviluppati e

utilizzati in modo da renderne comprensibili agli Utenti e ai Destinatari gli obiettivi, il funzionamento generale e le principali logiche decisionali. Dove applicabile, i clienti saranno informati in modo chiaro e accessibile sull'impiego dell'IA nei servizi e nei prodotti offerti.

Sotto il profilo della trasparenza assume rilevanza la spiegabilità di quanto prodotto dai Sistemi di IA. Pertanto, tra le soluzioni adottate dal Gruppo sono previsti metodi e strumenti che, in particolare laddove la trasparenza a tutela dei destinatari sia ritenuta necessaria, consentono di ricostruire come sia stato prodotto un determinato *output* a partire dagli *input* forniti.

Inoltre, il Gruppo considera la sicurezza e l'affidabilità aspetti imprescindibili nello sviluppo e nell'adozione dei Sistemi di IA, per cui i Modelli di IA sono progettati per garantire la robustezza tecnica e riducendo al minimo il rischio di errori imprevisti o comportamenti inattesi. A tal fine il Gruppo adotta processi di validazione, *testing* e monitoraggio continuo per assicurare il rispetto di elevati standard di qualità, sicurezza informatica e resilienza.

Inoltre, nei sistemi di Intelligenza Artificiale che prevedono un'interazione diretta con le persone – come ad esempio *chatbot*, assistenti virtuali e generatori di contenuti - il Gruppo si impegna ad assicurare che l'Utente sia informato in modo chiaro e inequivocabile del fatto che sta interagendo con un Sistema IA. Tali sistemi sono progettati per fornire risposte accurate, pertinenti, verificabili e complete. Le Società in perimetro rendono, in ogni caso, sempre disponibile per l'Utente la possibilità di un confronto con l'operatore umano.

Equità e non discriminazione algoritmica

Nell'utilizzo dell'Intelligenza Artificiale, il Gruppo si impegna a prevenire la creazione o l'amplificazione di discriminazioni ingiustificate, adottando misure volte a garantire imparzialità e correttezza dei dati utilizzati e a monitorare l'equità degli *output* generati dai modelli.

Particolare attenzione è riservata alla rilevazione e mitigazione di eventuali *bias3*, ossia orientamenti indesiderati nei risultati prodotti dalla tecnologia. Tali deviazioni possono infatti produrre effetti negativi sia rispetto agli obiettivi che si intendono perseguire con l'utilizzo della tecnologia, sia, potenzialmente, ledere i principi di inclusività, uguaglianza e non discriminazione.

Supervisione e presidio umano

Il Gruppo riconosce l'importanza della supervisione e del presidio umano nella progettazione, realizzazione e controllo dei Sistemi di IA. I processi decisionali automatizzati prevedono la possibilità di monitorare, comprendere e, se necessario, intervenire sul funzionamento dei Sistemi di IA e, ove possibile, sull'*output* prodotto attraverso un controllo umano. Il presidio umano contribuisce a garantire che l'IA operi nel rispetto dei principi etici, dei diritti fondamentali e delle normative vigenti, mantenendo il controllo e la responsabilità ultima in capo agli operatori umani designati.

Privacy e protezione dei dati

L'adozione di Sistemi di IA deve avvenire secondo i principi rappresentati nella Politica in materia di protezione e valorizzazione dei Dati Personali tempo per tempo in vigore, garantendo il rispetto dei diritti, delle libertà fondamentali e della dignità degli Interessati, la minimizzazione dei dati trattati, la trasparenza nei confronti degli interessati e la sicurezza dei dati lungo tutto il ciclo di vita dei Sistemi di IA.

In coerenza con tale impianto, il Gruppo conferma il proprio impegno a:

- garantire che ogni trattamento di Dati Personali avvenga nel rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati;
- implementare misure tecniche e organizzative adeguate a prevenire accessi non autorizzati, perdite, alterazioni o trattamenti illeciti dei Dati Personali;
- assicurare una comunicazione chiara, completa e facilmente accessibile agli interessati sulle modalità e finalità di trattamento dei dati;
- promuovere l'uso responsabile dei Dati Personali, favorendo la consapevolezza e la comprensione degli impatti che le tecnologie di IA possono generare sulle persone;
- utilizzare i dati in modo da creare valore per clienti, stakeholder e collettività, senza mai compromettere i diritti e le aspettative legittime degli interessati;
- garantire, ove applicabile, che l'utilizzo di categorie particolari di dati (es. biometrici, sanitari, sensibili) avvenga solo in presenza di una base giuridica adeguata e in condizioni di stretta necessità, secondo quanto previsto dall'articolo 9(2)(g) del GDPR e dall'articolo 10, paragrafo 5, dell'AI Act;
- garantire che i set di dati utilizzati per l'addestramento, la convalida e la prova dei Sistemi di IA ad Alto Rischio siano selezionati e trattati in modo tale da essere pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi rispetto alla finalità prevista, come previsto dall'articolo 10, paragrafo 3, dell'AI Act.

Sostenibilità ambientale e innovazione responsabile

Consapevole dell'impatto ambientale legato allo sviluppo e all'utilizzo dell'IA, il Gruppo promuove un approccio orientato a pratiche responsabili che tengano conto della sostenibilità ambientale, favorendo l'adozione di soluzioni tecnologiche a ridotto consumo energetico e a minore impatto ambientale, in linea con la propria Politica in materia di Sostenibilità e con la Strategia del Gruppo sul Cambiamento Climatico.

In quest'ottica, il Gruppo incoraggia l'adozione volontaria di requisiti aggiuntivi che contribuiscano alla sostenibilità dell'IA, tra cui la progettazione ecocompatibile dei modelli, l'ottimizzazione del consumo computazionale, la misurazione e il contenimento dell'impronta ambientale delle soluzioni

sviluppate o adottate. Particolare attenzione è rivolta all'integrazione di criteri ambientali anche nei processi di innovazione e sperimentazione tecnologica, con il coinvolgimento di *stakeholder* esterni quali organizzazioni di ricerca, accademiche o civiche, per promuovere una visione sistemica dell'innovazione responsabile.

Collaborazione e partecipazione degli stakeholder

Il Gruppo valorizza il dialogo e il coinvolgimento degli *stakeholder* come elemento essenziale per uno sviluppo dell'Intelligenza Artificiale che sia sostenibile, responsabile e in linea con le aspettative della società civile.

Nello sviluppo, utilizzo e monitoraggio dei Sistemi di IA, il Gruppo si impegna a:

- considerare, laddove applicabile, le esigenze e le aspettative dei clienti, dei partner commerciali, dei dipendenti e della collettività;
- garantire il rispetto dei diritti dei clienti, dei partner commerciali, dei dipendenti e degli altri stakeholder;
- promuovere - ove opportuno - la partecipazione attiva di stakeholder interni ed esterni nella definizione di linee guida, policy e pratiche operative sull'IA;
- mantenere un confronto aperto con enti regolatori, associazioni di settore, comunità scientifica e organizzazioni della società civile per condividere buone pratiche in relazione ai modelli di governance dell'IA.

Questa impostazione mira a indirizzare l'adozione dell'IA da parte del Gruppo in modo che sia integrata con il contesto economico, sociale e ambientale in cui opera.

Il Gruppo riconosce che il successo nell'adozione responsabile dell'Intelligenza Artificiale dipende in modo decisivo dalla consapevolezza e dalla competenza delle proprie persone.

A tal fine, il Gruppo promuove iniziative continuative di comunicazione e ingaggio per sensibilizzare i dipendenti e di formazione, con l'obiettivo di:

- diffondere una cultura aziendale orientata all'uso etico e responsabile dell'IA attraverso l'uso della Intranet Futura e di tutti i canali digitali interni (Communty di pratica, UniDuello, brochure, incontri di ingaggio, etc.);
- fornire conoscenze di base sui principi di trasparenza, equità, sicurezza e protezione dei dati applicabili ai Sistemi di IA;
- rendere i dipendenti consapevoli dei rischi potenziali connessi all'uso dell'IA e dei comportamenti da adottare per prevenirli o segnalarli;
- supportare lo sviluppo di competenze tecniche e gestionali funzionali alla progettazione, allo sviluppo, alla realizzazione e al monitoraggio dei Sistemi di IA.

I programmi formativi sono calibrati in funzione dei diversi ruoli e livelli di responsabilità, garantendo un'adeguata preparazione di tutti coloro che intervengono, direttamente o indirettamente, nei processi legati all'IA.

Fundamental Rights Impact Assessment (FRIA)

Qualora il Sistema di IA ad Alto Rischio che si intende sviluppare e utilizzare sia destinato a essere utilizzato per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito o per la valutazione dei rischi e la determinazione dei prezzi di assicurazioni sulla vita e assicurazioni sanitarie, è effettuata una valutazione dell'impatto che l'uso di tale Sistema può produrre sui diritti fondamentali degli Utenti (*Fundamental Rights Impact Assessment* o "**FRIA**") secondo le modalità illustrate nel DCA di Gruppo.

La FRIA, una volta effettuata, è sottoposta alla firma dell'Amministratore Delegato o, ove non presente, del Direttore Generale della Società e trasmessa alle Authorities nelle modalità dalle stesse indicate.

Se, durante l'uso del Sistema di IA, è ritenuto che uno qualsiasi degli elementi analizzati in sede di FRIA sia cambiato o non sia più aggiornato, il Gruppo adotta le misure necessarie per aggiornare le informazioni.

Monitoraggio dei Sistemi di IA

I Sistemi di IA in uso presso le Società in perimetro sono soggetti, secondo un approccio *risk-based*, a un sistema di monitoraggio per tutto il ciclo di vita dei medesimi, finalizzato a:

verificare che i dati siano trattati in conformità alle normative vigenti, con particolare attenzione alla protezione dei dati personali, al diritto d'autore e a eventuali ulteriori normative di settore;

- garantire l'aggiornamento continuo della documentazione tecnica a supporto del Sistema di IA;
- identificare potenziali errori o malfunzionamenti del Sistema di IA;
- garantire la qualità e il miglioramento delle performance del Sistema di IA;
- con particolare riferimento ai Sistemi di IA generativa, prevenire la generazione e/o la diffusione di contenuti dannosi, violenti, ingannevoli o illegali;
- verificare quali Utenti utilizzano i Sistemi di IA, garantendo la coerenza rispetto a quanto riportato nel Registro.

A tal fine, il Gruppo si dota di strumenti che consentono il controllo automatizzato dei Sistemi di IA sulla base di KPIs definiti in sede di progettazione, sviluppo, convalida o valutazione dei Sistemi di IA.

Le Società in perimetro che assumono il ruolo di *Developer* di Sistemi di IA ad Alto Rischio elaborano un piano per il monitoraggio degli stessi successivo alla loro messa in produzione, che costituisce parte integrante della documentazione tecnica e tale da consentirne in modo costante la verifica

della conformità rispetto ai requisiti normativi, anche sulla base delle informazioni fornite dai *Deployer*, lungo tutto il loro ciclo di vita.

Comunicazione e formazione in materia di IA

Ciascun dipendente, in relazione al proprio ruolo e ambito aziendale, sviluppa e utilizza solo i Sistemi di IA a cui è stato abilitato, attenendosi alla normativa tempo per tempo vigente e garantendo un efficace presidio del Rischio IA.

A tal fine sono pianificati e predisposti piani di comunicazione e appositi corsi di formazione per garantire un livello sufficiente di alfabetizzazione in materia di IA, e un'adeguata consapevolezza in merito al rischio di utilizzo di Sistemi di IA non sottoposti al processo di governo, anche in termini di potenziale compromissione o diffusione di dati aziendali riservati, anche non personali.

I percorsi di formazione istituiti, al fine di garantire una formazione adeguata dei *Deployer*, comprendono:

- elementi di base sull'IA e sulla sua capacità di influenzare i processi aziendali (*AI Awareness*), nonché sulle modalità e ragioni di tale influenza, inclusa la conoscenza degli aspetti normativi e operativi associati all'IA (*AI Literacy*);
- piani formativi appositamente dedicati alle funzioni aziendali dedicate alla progettazione e allo sviluppo di Sistemi di IA.

Inoltre, sono riservate al Consiglio di Amministrazione apposite sessioni di *induction*.

I corsi di formazione tengono conto:

- del ruolo ricoperto dalle diverse funzioni aziendali, nonché dei singoli Sistemi di IA cui sono state eventualmente abilitate;
- ove applicabile, dei compiti di supervisione umana eventualmente demandati;
- delle conoscenze tecniche, esperienza, istruzione e formazione delle diverse funzioni aziendali;
- del contesto in cui i Sistemi di IA devono essere utilizzati e, ove applicabile, dei Destinatari.

In caso di violazione delle modalità e dei limiti di utilizzo dei Sistemi di IA, potranno essere applicate sanzioni disciplinari, secondo le modalità e nel rispetto di quanto definito dai CCNL di settore.