



ERSEL

Policy Intelligenza Artificiale - IA -

Documento N°	121
Data	26/06/2025
Approvato da	Consiglio di Amministrazione
Società Interessate	Ersel Banca Privata S.p.A., Ersel Asset Management S.p.A., Online Sim S.p.A., Simon Fiduciaria S.p.A.
Decorrenza	26/06/2025
Versione	01
Pubblicazione su sito Internet	SI'

SOMMARIO

1. DEFINIZIONI E AMBITO NORMATIVO	3
1.1 DEFINIZIONI.....	3
1.2 SCOPO DELLA POLICY	3
1.3 AMBITO NORMATIVO DI RIFERIMENTO.....	3
1.3.1 REQUISITI INTERNAZIONALI.....	3
1.3.2 REQUISITI NAZIONALI.....	5
2. PRINCIPI GENERALI	5
2.1 ETICA E TRASPARENZA	5
2.2 RESPONSABILITA' E DIRITTI UMANI	5
2.3 RUOLO DELL' INTELLIGENZA ARTIFICIALE.....	6
2.4 GESTIONE DEL RISCHIO	6
3. GOVERNANCE DELL'INTELLIGENZA ARTIFICIALE	6
4. AMBITO DI APPLICAZIONE	7
5. SICUREZZA E CYBERSECURITY	8
5.1 PROTEZIONE DEI DATI	8
5.2 MISURE DI SICUREZZA.....	9

1. DEFINIZIONI E AMBITO NORMATIVO

1.1 DEFINIZIONI

- a) intelligenza artificiale – di seguito IA: è un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione. Questo sistema, 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;
- b) machine Learning: processo di apprendimento automatico effettuato da parte dell'IA che impara dai dati forniti riuscendo a ottenere output (previsioni, contenuti, raccomandazioni o decisioni), ricavandone inoltre modelli e algoritmi atti a modificare nel continuo in modalità adattiva le piattaforme che li utilizzano;
- c) chatbot di IA: sono definiti come modelli di IA caratterizzati da una generalità significativa e in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato; esso, inoltre, si presenta in forma di chat digitale e fornisce risposte, chiarimenti o raccomandazioni ai quesiti ad esso proposti;
- d) robot process automation: si tratta di una tecnologia che utilizza software "robot" per automatizzare attività ripetitive e regolari svolte da persone utilizzando i sistemi informatici strutturati o meno. Le tecnologie di RPA sostituiscono quindi l'intervento umano in questi compiti, consentendo di risparmiare tempo, ridurre gli errori e liberare gli addetti per attività a maggior valore aggiunto.

1.2 SCOPO DELLA POLICY

La presente policy mira a stabilire un quadro chiaro e coerente per l'uso dell'IA all'interno del Gruppo Ersel, garantendo che tutte le applicazioni di IA siano conformi alle normative vigenti, nazionali ed europee, e che rispettino i principi etici fondamentali in modo da garantire un utilizzo proficuo dell'IA non andando incontro a rischi reputazionali e di non compliance. La policy supporta la strategia aziendale promuovendo un'innovazione responsabile e la gestione dei rischi associati all'IA.

1.3 AMBITO NORMATIVO DI RIFERIMENTO

Una policy IA, per garantire la sua efficacia e applicabilità, deve essere conforme a stringenti requisiti normativi internazionali e nazionali.

1.3.1 REQUISITI INTERNAZIONALI

La policy si conforma al Regolamento UE 2024/1689 sull'IA, che stabilisce requisiti per la sicurezza, affidabilità e trasparenza dei sistemi di IA. Inoltre, integra i principi etici promossi dalle linee guida OCSE e UNESCO.

Il Regolamento UE 2024/1689 si basa su regole armonizzate per lo sviluppo e l'immissione sul mercato di sistemi sull'IA nell'Unione Europea con l'obiettivo di promuovere un'IA

antropocentrica e affidabile, proteggendo al contempo la salute, la sicurezza e i diritti fondamentali dei cittadini europei. Tale norma, che sfrutta un risk based approach, si applica a fornitori, distributori e utilizzatori di sistemi IA garantendo un suo uso etico e vietando alcune pratiche scorrette come la manipolazione subliminale, lo sfruttamento delle vulnerabilità delle persone, il social scoring, la valutazione del rischio basata sulla profilazione e l'uso di sistemi di IA per provocare emozioni sul luogo di lavoro. Questo regolamento prevede anche la promozione dell'utilizzo etico dell'IA, stabilisce sanzioni in caso di uso scorretto e viene esaminato periodicamente dalla Commissione Europea per garantirne la sua adeguatezza e attualità.

Le linee guida OCSE garantiscono il rispetto di alcuni principi etici fondamentali fra cui:

- a) crescita inclusiva, sviluppo sostenibile e benessere: le parti interessate devono impegnarsi in modo proattivo a promuovere la gestione responsabile di una IA affidabile, al fine di aumentare le capacità umane, la creatività, l'inclusione e ridurre le disuguaglianze, incentivando la crescita economica e la sostenibilità ambientale;
- b) rispetto per lo stato di diritto, i diritti umani e i valori democratici: gli operatori del settore dovrebbero garantire, per l'intero ciclo di vita del sistema di IA, la tutela dello stato di diritto, dei diritti umani e i valori democratici. A tal fine, i vari operatori dovrebbero implementare meccanismi e salvaguardie, come la sorveglianza umana, anche per affrontare i rischi derivanti da utilizzi al di fuori dello scopo previsto, o da un uso improprio (intenzionale o meno). Tra i valori da rispettare rientrano, tra gli altri, l'uguaglianza e la non discriminazione, la libertà, la dignità e l'autonomia umana, la tutela della vita privata e la protezione dei dati personali, la diversità e l'equità, la giustizia sociale e la tutela dei diritti dei lavoratori promossa a livello internazionale. Si sottolinea anche la necessità di affrontare l'amplificazione della disinformazione da parte dell'IA, nel rispetto della libertà di espressione e degli altri diritti umani fondamentali;
- c) trasparenza: è necessario garantire la trasparenza della comunicazione in relazione ai sistemi di IA;
- d) sicurezza e affidabilità: le applicazioni di IA dovrebbero essere sicure e affidabili in condizioni di normale utilizzo, uso prevedibile o uso improprio. Inoltre, bisognerebbe assicurare la presenza di meccanismi per annullare, riparare o disattivare i sistemi se causano danni o manifestano comportamenti indesiderati;
- e) accountability: gli operatori sono responsabili del funzionamento dell'IA; è necessario garantirne la tracciabilità per permettere l'analisi delle decisioni del sistema IA.

L'Unesco propone linee guida basate su:

- a) principi etici fondamentali: rispetto dei diritti umani, inclusività, sostenibilità ambientale, privacy e protezione dei dati e trasparenza. Per garantire il rispetto di questi principi etici fondamentali è necessario stabilire normative e leggi a protezione della privacy, promuovere l'educazione e l'alfabetizzazione in materia di IA e assicurarsi che l'IA promuova l'uguaglianza di genere e non perpetui stereotipi discriminatori;
- b) principali sfide: creare programmi di formazione, garantire la protezione dei dati sensibili garantendo la privacy. Per garantire ciò è necessario promuovere l'equità e l'inclusione, garantendo la formazione sull'uso dell'IA e favorendo la diversità di idee e l'inclusione.

Da citare infine il Regolamento UE No 575/2013 (CRR) e gli orientamenti dell'EBA, che definiscono le aspettative sulla governance e il controllo dei rischi.

Gli orientamenti EBA sull'IA sono stati emanati per stabilire aspettative comuni riguardo alle politiche aziendali e ai controlli interni necessari per l'implementazione efficace delle tecnologie di IA in modo da garantire una corretta gestione dei rischi associati all'IA, promuovendo comunque l'innovazione e la competitività nel settore.

1.3.2 REQUISITI NAZIONALI

La policy rispetta il precitato Regolamento UE 2024/1689 nonché il Regolamento UE 2016/679 (GDPR) assicurando altresì che l'uso dell'IA sia conforme alle leggi nazionali; infatti, nonostante non ci siano ancora normative precise a livello nazionale sull'IA (sono presenti linee guida e disegni di legge a riguardo), è evidente che l'IA debba operare garantendo il rispetto dei principi etici base e il rispetto dei diritti dell'uomo e dei lavoratori.

2. PRINCIPI GENERALI

2.1 ETICA E TRASPARENZA

Le Società del Gruppo si impegnano a garantire che tutte le applicazioni di IA siano sviluppate e utilizzate in modo etico e trasparente, rispettando i diritti umani e promuovendo la fiducia dei clienti.

L'utilizzo di soluzioni di IA deve garantire la trasparenza (ad esempio comunicando ai clienti quando interagiscono con un sistema chatbot IA), proteggere la privacy dei clienti e garantire che l'IA non applichi comportamenti discriminatori favorendo alcuni clienti piuttosto che altri.

Inoltre, è importante garantire e sviluppare la ricerca sull'IA con partnership strategiche e collaborazioni con poli universitari e centri di ricerca contribuendo a garantire e a sviluppare standard etici e regolamentari per l'utilizzo dell'IA.

2.2 RESPONSABILITA' E DIRITTI UMANI

È fondamentale che l'IA sia utilizzata in modo da rispettare i diritti umani e promuovere il benessere sociale, favorendo l'integrazione sociale, finanziaria, lavorativa e riuscendo a ridurre l'asimmetria informativa fra le Società del Gruppo e i clienti.

Infatti, l'utilizzo dell'IA può certamente garantire un miglioramento dell'ambiente lavorativo migliorando l'efficienza e l'efficacia del lavoro e svolgendo le attività più operative analizzando per esempio in brevi periodi grandi quantità di dati.

Può anche rappresentare una minaccia se non viene gestita correttamente; infatti, l'IA può perpetuare o ampliare pregiudizi esistenti favorendo comportamenti discriminatori ed essere

utilizzata per intensificare alcune dinamiche di controllo e di violazione della privacy di dipendenti e collaboratori.

2.3 RUOLO DELL' INTELLIGENZA ARTIFICIALE

È necessario che l'IA offra supporto ai lavoratori in modo da semplificarne le attività, senza però arrivare alla sostituzione di questi ultimi in modo da non violarne i diritti. Infatti, l'IA deve essere sviluppata in modo antropocentrico garantendo che quest'ultima favorisca il benessere umano.

L'IA deve operare sempre sotto controllo umano, verificando che sia sempre un essere umano a supervisionare o a controllare le decisioni prese da modelli di IA, garantendo e verificando la qualità e l'affidabilità degli output di risposta forniti dall'IA.

È importante formare i lavoratori permettendo loro una collaborazione più proficua con l'IA e garantendo che questi abbiano le competenze per lavorare in un contesto di questo tipo.

2.4 GESTIONE DEL RISCHIO

Un sistema di gestione del rischio interattivo e continuo è essenziale per identificare, valutare e mitigare i rischi per la salute, la sicurezza e i diritti fondamentali dei lavoratori derivanti dall'uso dell'IA.

Il sistema di gestione dei rischi è inteso come un processo interattivo continuo, pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA, che richiede riesami e aggiornamenti costanti e sistematici.

Esso comprende le seguenti fasi:

- a) identificazione e analisi dei rischi noti e ragionevolmente prevedibili che il sistema di IA potrebbe causare alla salute, alla sicurezza e ai diritti fondamentali dei lavoratori;
- b) stima e valutazione dei rischi che possono emergere quando il sistema di IA è usato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibili;
- c) valutazione di altri eventuali rischi derivanti dall'analisi dei dati raccolti;
- d) adozione di misure di gestione dei rischi opportune e mirate intese ad affrontare i rischi legati all'utilizzo dell'IA.

3. GOVERNANCE DELL'INTELLIGENZA ARTIFICIALE

La governance dell'IA si riferisce ai processi, agli standard e alle misure di sicurezza che contribuiscono a garantire che i sistemi e gli strumenti di IA siano sicuri ed etici. I framework di governance dell'IA orientano la ricerca, lo sviluppo e le applicazioni di IA per garantire sicurezza, equità e rispetto dei diritti umani.

Una governance efficace dell'IA include meccanismi di supervisione che trattano rischi quali distorsioni, violazioni della privacy e uso improprio, promuovendo al contempo l'innovazione e aumentando la fiducia. Un approccio etico alla governance dell'IA richiede quindi il coinvolgimento di un'ampia gamma di stakeholder, tra cui sviluppatori di IA, utenti, funzioni di direzione e di controllo, in modo da garantire che i sistemi legati all'IA siano sviluppati e utilizzati in linea con i valori dell'impresa.

I presidi di governance che l'impresa dovrà mettere in atto mirano quindi a definire la matrice di supervisione necessaria per allineare i comportamenti dei sistemi di IA in uso all'azienda agli standard etici sopra descritti.

4. AMBITO DI APPLICAZIONE

La presente policy si applica a tutte le società del Gruppo Ersel, alle unità aziendali e ai dipendenti coinvolti nello sviluppo, nell'implementazione e nella gestione di sistemi di IA. Include anche i fornitori esterni che forniscono soluzioni di IA alla Banca.

Gli ambiti di applicazione per l'IA possono essere vari in quanto può essere utilizzata per un'ampia gamma di attività semplificando svariati processi, fra cui:

- a) automazione dei processi;
- b) assistenti virtuali IA;
- c) Data Governance: controllo della qualità del dato.
- d) Data Strategy: indirizzo delle scelte tecnologiche e applicative influenzate dalle informazioni fornite dall'IA;
- e) svolgimento di attività amministrative ripetitive, di processi operativi e di back office e lo svolgimento di analisi predittive per effettuare assistenza clienti;
- f) trading algoritmico: sfrutta l'apprendimento automatico per sviluppare sistemi di trading ad alta frequenza in grado di analizzare i big data di mercato e identificare opportunità di investimento in tempo reale;
- g) Robo-Advisory: utile per offrire una consulenza di investimento personalizzata e conveniente attraverso robo-advisor alimentati dall'IA che analizzano il profilo di rischio, gli obiettivi e le preferenze dei clienti;
- h) prevenzione delle frodi: implementa algoritmi di machine learning per monitorare le transazioni e rilevare modelli di attività sospette, proteggendo clienti e istituzioni finanziarie dalle frodi;
- i) gestione del rischio: sfruttare l'IA per valutare e mitigare i rischi, dalle analisi predittive al monitoraggio delle minacce informatiche;
- j) esperienza del cliente potenziata: migliora l'esperienza del cliente con assistenti virtuali alimentati dall'IA, onboarding automatizzato e raccomandazioni personalizzate.

k) utilizzo dell'IA in operazioni di valutazione del merito creditizio.

Le soluzioni IA attualmente rese disponibili all'interno del Gruppo sono le seguenti:

- a) Copilot: assistente IA per il pacchetto office (Word, Excel, Outlook, Teams...);
- b) Aptus AI: IA funzionante in modalità di chatbot utilizzata come consulto in termini di normativa vigente;
- c) Document Search Assistant: una soluzione di IA in fase di prossimo rilascio che supporta l'utente nella ricerca intelligente all'interno del patrimonio informativo documentale dell'azienda.

Inoltre, le soluzioni di cybersecurity implementate in azienda sfruttano al loro interno motori di machine learning volti ad individuare comportamenti anomali che possono potenzialmente ricondursi ad un attacco informatico.

5. SICUREZZA E CYBERSECURITY

5.1 PROTEZIONE DEI DATI

Sono previste misure rigorose per la protezione dei dati personali e sensibili, in conformità con il GDPR e con le altre normative pertinenti.

Il GDPR stabilisce in linea generale un quadro normativo atto a proteggere i dati personali di clienti e dipendenti.

I dispositivi di IA devono essere conformi a questi principi, in particolare:

- a) trasparenza e informazione: gli interessati devono essere informati in modo chiaro e comprensibile sul trattamento dei loro dati da parte di sistemi IA, inclusi eventuali processi decisionali automatizzati;
- b) consenso e liceità: il trattamento dei dati personali da parte di IA deve basarsi su una base giuridica valida, spesso in forma di consenso esplicito;
- c) diritti degli interessati: gli interessati hanno il diritto di accedere ai dati, rettificarli, cancellarli, opporsi al trattamento e non essere soggetti a decisioni automatizzate senza intervento umano;
- d) valutazione d'impatto: per i trattamenti IA che presentano rischi elevati, è obbligatoria una valutazione d'impatto sulla protezione dei dati.

Il GDPR pone inoltre particolare attenzione sul trattamento automatizzato dei dati personali. L'Art. 22 del GDPR (Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione) ribadisce, come principio generale, che l'interessato ha il diritto di non essere sottoposto a una decisione basata esclusivamente sul trattamento automatizzato dei propri dati, a cominciare dalla profilazione, che produca effetti giuridici che lo riguardano o che incida allo stesso modo sulla sua persona in modo significativo.

Ciò che viene infatti richiesto a chi utilizza Sistemi di IA per acquisire ed elaborare dati personali è:

- a) definire le finalità del trattamento;
- b) informare sull'utilizzo che si fa della tecnologia IA;
- c) raccogliere il consenso al trattamento automatizzato e alla profilazione;
- d) determinare la base giuridica;
- e) valutare l'impatto che l'uso dell'IA esercita sugli individui (DPIA);
- f) dare prospetto compiuto e completo del funzionamento della tecnologia, per individuarne i criteri di ragionamento (ed eventualmente anche alcuni bias di partenza);
- g) intervenire nel caso in cui si presentino possibili occasioni di violazione dei diritti degli interessati;
- h) comunicare e informare in caso di data breach;
- i) implementare sistemi di logging e tracciabilità per i sistemi di IA ad alto rischio;
- j) adottare misure di sicurezza rafforzate contro attacchi adversarial e tentativi di manipolazione.

5.2 MISURE DI SICUREZZA

Sono adottate misure di sicurezza avanzate per proteggere i sistemi di IA da minacce cibernetiche e garantire la continuità operativa; ciò è fondamentale per permettere il regolare svolgimento delle attività di IA e per proteggere sia i dati sensibili di personale e clienti sia le informazioni confidenziali delle Società del Gruppo.

Le minacce principali sono:

- a) data poisoning: manipolazione dei dati utilizzati per addestrare i modelli di IA, ciò fa sì che l'output fornito dall'IA sia incompleto o errato; oltre a ciò, può portare ad avere incombenze significative in termini di privacy, sicurezza e danno reputazionale. Per mitigare i rischi è necessario implementare rigorose pratiche per garantire la qualità dei dati necessari ad addestrare i modelli di IA; per ottenere ciò bisogna verificare l'affidabilità delle fonti dei dati usati come input stabilendo una politica di gestione dei dati robusta, affidabile e basata su crittografia e protezione del dato. È importante anche controllare periodicamente i sistemi di IA in modo da individuare potenziali attacchi di data poisoning mitigando il più possibile i danni e rilevando eventuali anomalie;
- b) adversarial attacks: ingannare i sistemi di IA manipolando input in modo impercettibile per gli esseri umani ma in modo altamente influente per l'algoritmo; il risultato resta comunque un output incompleto o errato; oltre a ciò, può portare ad avere incombenze significative in termini di privacy, sicurezza e danno reputazionale. Per mitigare i rischi è necessario svolgere una verifica e una pulizia dei dati utilizzati come input nel modello; in questo modo è possibile identificare per tempo anomalie ed effettuare azioni correttive. Un'altra strategia utile per mitigare tale rischio è quella di addestrare l'IA usando dati volontariamente alterati in modo da aumentare le sue capacità di riconoscimento di errori, la sua resilienza e diminuendo la sua vulnerabilità. È cruciale inoltre monitorare gli output del modello in modo da intervenire tempestivamente in caso di errori, omissioni o alterazioni;
- c) esfiltrazione dei dati messi a disposizione del motore di IA: processo non autorizzato con

cui informazioni sensibili o riservate vengono sottratte da un sistema informatico o da una rete.

Per garantire la sicurezza dei dati è indispensabile adottare le seguenti misure:

- a) autenticazione a più fattori per accessi dall'esterno;
- b) monitoraggio delle intrusioni;
- c) backup e ripristino;
- d) formazione del personale;
- e) algoritmi di autoapprendimento per rilevare e rispondere alle minacce informatiche in tempo reale;
- f) protezione da phishing e deepfake.