



La Cassa di Ravenna S.p.A.
Privata e Indipendente dal 1840

Gruppo Bancario  La Cassa di Ravenna

LINEE DI INDIRIZZO SULL'UTILIZZO E LA GESTIONE DEI SISTEMI DI INTELLIGENZA ARTIFICIALE E CLOUD

Estratto

Versione 1 del 10/12/2025

Approvato dal CDA nella seduta del 10/12/2025

INDICE

1. Premessa e obiettivi	3
1.1. Destinatari del documento	3
1.2. Gestione del documento.....	3
2. Fonti normative	3
2.1. Normativa sovranazionale e nazionale	3
2.2. Normativa interna	4
5. Aspetti generali dell'Intelligenza Artificiale (<i>Artificial Intelligence – AI</i>)	4
5.1. Definizione di Intelligenza Artificiale (AI)	4
5.2. Linee guida per l'adozione di sistemi AI	6
5.3. Classificazione delle soluzioni AI.....	7
5.3.1. AI ad impatto minimo o nullo	8
5.3.2. AI ad impatto limitato.....	8
5.3.3. AI ad impatto alto.....	8
5.3.4. AI vietate (impatto inaccettabile)	9
5.4. Requisiti normativi e di sicurezza dei sistemi AI	9
5.4.1. Spiegabilità e trasparenza	10
5.4.2. Supervisione umana per decisioni critiche	10
5.4.3. Protezione dei dati.....	10
5.4.4. Accesso e conservazione dei dati.....	11
5.4.5. Obblighi e Vincoli di Utilizzo per gli Utenti Finali.....	11
5.4.6. Processo decisionale	11
5.4.8. Obblighi di formazione in materia di Intelligenza Artificiale	12
5.4.9. Responsabilità e Sanzioni.....	12

1. Premessa e obiettivi

Il presente documento stabilisce i principi, le linee guida ed indica le migliori pratiche da seguire per l'adozione, lo sviluppo e l'utilizzo di soluzioni di Intelligenza Artificiale (di seguito anche "AI") [...] all'interno del Gruppo La Cassa di Ravenna (di seguito anche "il Gruppo").

Il presente documento è redatto per rispondere ai seguenti obiettivi:

- Proteggere la riservatezza, integrità, autenticità e disponibilità dei dati [...] gestiti mediante soluzioni di AI;
- Definire i requisiti minimi di sicurezza da rispettare quando si adottano soluzioni [...] che prevedono utilizzo di sistemi di AI;
- Garantire la conformità alle normative legali in materia di privacy e sicurezza e ai reati presupposto di cui al D.Lgs. 231/01.

L'obiettivo è garantire che soluzioni informatiche che adottino strumenti di AI [...] siano utilizzate in modo sicuro, trasparente ed equo, in conformità con le normative vigenti e con i valori del Gruppo Bancario La Cassa di Ravenna.

1.1. Destinatari del documento

Il presente documento è applicabile per quanto di competenza, a tutte le Unità Organizzative de La Cassa di Ravenna Spa (nel seguito "La Banca") e delle società del Gruppo Bancario.

1.2. Gestione del documento

Il presente documento, su proposta del Direttore Generale e previo parere della funzione di controllo: Compliance di Gruppo, è approvato dal Consiglio di Amministrazione.

L'Ufficio Organizzazione e IT di Gruppo propone, al Direttore Generale, qualora necessario, l'aggiornamento del presente documento, per rispondere alle evoluzioni nella normativa in materia di Intelligenza Artificiale e cloud computing ed alle evoluzioni nei servizi e prodotti forniti dal Gruppo, nonché in risposta alle attività di verifica ed audit condotte e di gestione dei rischi informatici.

2. Fonti normative

2.1. Normativa sovranazionale e nazionale

- Regolamento DORA (Digital Operational Resilience Act) – Regolamento (UE) 2022/2554;
 - GDPR – Regolamento (UE) 2016/679 sulla protezione dei dati personali;
 - AI Act (Regolamento Europeo sull'Intelligenza Artificiale) Regolamento UE 2024/1689;
 - Circolare Banca d'Italia n. 285/2013 – Disposizioni di Vigilanza per le Banche;
 - Regolamento IVASS n. 38/2018 – Esternalizzazione dei servizi IT nel settore assicurativo;
 - Piano Nazionale per la Cybersecurity 2022-2026;
 - Codice dell'Amministrazione Digitale (D.Lgs. 82/2005 e successive modifiche).
 - Decreto Legislativo 231/2011 – Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300;
 - Legge 23 settembre 2025 n.132/2025 – Disposizioni e deleghe al Governo in materia di intelligenza artificiale.
- [...]

2.2. Normativa interna

- SVRGR1051 - Codice Etico di Gruppo;
- SVP002202 - Politica in materia di protezione dei dati personali;
- SVP001868 - Politiche per l'esternalizzazione di funzioni aziendali;
- SVR003654 - Regolamento - Procedura di gestione dei progetti ICT;
- SVR001681 - Regolamento - Procedura di gestione dei cambiamenti delle applicazioni e risorse ICT;
- SVR003838 - Regolamento di gestione dei fornitori ICT;
- SVR003839 - Regolamento di gestione delle risorse ICT;
- SVR002203 - Regolamento in materia di protezione dei dati personali;
- SVC001222 - Procedure di sicurezza informatica componenti ICT interne al Gruppo;
- Responsabilità Amministrative delle Persone Giuridiche - Modello Organizzativo con Delega delle funzioni di Sicurezza - Regolamento dell'Organismo di Vigilanza - Regolamento Whistleblowing - Politiche di Gruppo in materia di Anticorruzione per le Società del Gruppo.

[OMISSIS]

5. Aspetti generali dell'Intelligenza Artificiale (Artificial Intelligence – AI)

5.1. Definizione di Intelligenza Artificiale (AI)

L'Intelligenza Artificiale (d'ora in avanti anche AI) è un insieme di tecnologie che consentono a sistemi informatici di eseguire attività tipicamente associate all'intelligenza umana, come l'apprendimento, il ragionamento, la percezione e il processo decisionale. In ambito bancario, l'AI viene utilizzata per analisi predittiva, automazione, gestione del rischio e personalizzazione dei servizi finanziari.

L'art. 3 del Regolamento (UE) 2024/1689 (AI Act Europeo), definisce una soluzione di AI come un *“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”*.

Una soluzione informatica è quindi qualificata come AI quando presenta le seguenti caratteristiche:

- È basata su macchine (insieme di software e hardware);
- È autonoma, nel senso che opera con un certo grado di indipendenza dall'umano;
- È adattabile, nel senso che dispone di capacità di apprendimento post produzione, anche se si tratta di una condizione facoltativa;
- Persegue obiettivi impliciti o espliciti;
- È capace di inferire, ossia dedurre, quali risultati produrre dai dati di input;
- Produce determinati risultati (previsioni, contenuti, raccomandazioni e decisioni).

Quadro delle definizioni:

Deployer	È un soggetto che utilizza un sistema di AI sotto la propria autorità (salvo un utilizzo personale non professionale).
Machine Learning	È una sottocategoria dell'AI che consente ai sistemi di apprendere da dati senza essere esplicitamente programmati. Gli algoritmi di Machine Learning migliorano le proprie prestazioni nel tempo attraverso l'analisi di pattern e correlazioni nei dati.

Deep Learning	Tecnica avanzata di Machine Learning basata su reti neurali artificiali con più livelli. Il Deep Learning è usato in applicazioni AI complesse come elaborazione del linguaggio naturale (NLP) e riconoscimento delle immagini.
Modelli Generativi (AI Generativa)	Tecnologie AI in grado di creare nuovi contenuti, come testi, immagini o dati sintetici, basandosi su modelli pre-addestrati.
Explainability (Spiegabilità)	Principio secondo cui un sistema AI deve essere in grado di fornire spiegazioni comprensibili sui propri processi decisionali.
Black Box AI (AI a Scatola Nera)	Modelli AI che prendono decisioni senza fornire una spiegazione chiara del processo sottostante. La "black box" è particolarmente critica nei sistemi bancari, dove la trasparenza è essenziale.
Supervisione Umana (Human-in-the-loop)	Strategia che prevede un intervento umano in determinati passaggi decisionali di un sistema AI.
Bias Algoritmico	Distorsione nei risultati di un algoritmo AI causata da dati di training non rappresentativi o sbilanciati. Il bias può portare a decisioni discriminatorie.
Dati sintetici	Dati generati artificialmente per addestrare modelli AI, evitando l'uso di dati sensibili reali.
Anonimizzazione	L'anonimizzazione è il processo che rende i dati irriconoscibili e non riconducibili a una persona fisica.
Pseudonimizzazione	La pseudonimizzazione consiste nella sostituzione di informazioni identificative con pseudonimi, mantenendo la possibilità di riconnettere i dati originali.
Deriva algoritmica	Fenomeno per cui le prestazioni di un modello AI diminuiscono nel tempo a causa di cambiamenti nei dati.
AI Act (Regolamento Europeo sull'Intelligenza Artificiale)	Normativa UE che classifica le applicazioni AI in quattro categorie di rischio: AI Proibita (es. manipolazione cognitiva, social scoring); AI ad Alto Rischio (es. credito e identificazione biometrica); AI a Rischio Limitato (es. chatbot, assistenti virtuali); AI a Rischio Minimo (es. sistemi di automazione interna).
Attacco Adversarial (Adversarial Attack):	Tecnica usata per ingannare i modelli AI, manipolando i dati di input in modo impercettibile per gli umani, ma rilevante per l'algoritmo.
Audit AI	Processo di verifica dei modelli AI per assicurare conformità, trasparenza e assenza di bias algoritmico.
Watermarking	Pratica che consiste nell'incorporare informazioni visibili o invisibili all'interno dei contenuti generati da un'intelligenza artificiale, al fine di garantire trasparenza e tracciabilità. Consiste in una tecnica usata per rendere evidente che un'opera non è completamente naturale o umana, ma è il risultato dell'intervento di un sistema automatizzato.

5.2. Linee guida per l'adozione di sistemi AI

Il Gruppo Bancario La Cassa dei Ravenna dispone che le eventuali tecnologie AI utilizzate delle Banche/Società del Gruppo devono essere conformi alle normative internazionali, europee e nazionali e alla normativa interna di settore, rispettando i seguenti richiamati dall'AI Act Europeo:

- a) **Principio di legalità e conformità normativa:** l'uso dell'AI deve essere conforme a tutte le normative vigenti, incluse le leggi nazionali, europee e internazionali;
- b) **Principio di etica e responsabilità:** l'uso dell'AI deve essere etico, equo, evitando discriminazioni, pratiche sleali o usi impropri. L'obiettivo è garantire che i sistemi AI non generino decisioni discriminatorie, prevenendo bias algoritmici, lo scopo è quello di promuovere un uso responsabile della tecnologia nella gestione dei servizi bancari per evitare manipolazioni o influenze indebite di qualsiasi natura.
- c) **Principio di trasparenza:** la trasparenza è un principio fondamentale per promuovere la fiducia degli utenti nei contenuti e nelle tecnologie basate sull'AI. Gli algoritmi AI devono essere trasparenti e quando richiesto dalle normative spiegabili, affinché gli utenti possano comprenderne i risultati.

Secondo l'art. 50 dell'AI Act, le informazioni sulle opere generate tramite AI devono essere chiaramente identificabili, affinché gli utenti possano riconoscere facilmente se un contenuto è stato creato, modificato o influenzato da una tecnologia di intelligenza artificiale. Secondo l'articolo citato è previsto che, quando un sistema di AI produce contenuti che potrebbero essere confusi con quelli creati da persone, occorre specificarne l'origine (c.d. Watermarking).

Il Watermarking può consistere in vari metodi e tecniche e applicato in diversi modi ad esempio avvisi con parole o frasi visibili oppure incorporazione di un logo o simbolo.

- d) **Principio di affidabilità e robustezza:** i sistemi AI devono essere affidabili, resilienti agli errori e progettati per ridurre il rischio di guasti e vulnerabilità. Occorre prevedere l'implementazione di misure per garantire la sicurezza informatica e prevenire ogni tipo di attacco esterno. Il monitoraggio nel continuo è fondamentale per evitare la c.d. deriva algoritmica, ossia che il sistema diventi meno preciso nel tempo.
- e) **Principio di protezione dei dati e privacy:** l'AI deve essere conforme al GDPR e alla normativa interna relativa alla privacy e al trattamento dei dati personali, garantendo il trattamento etico dei dati personali e il rispetto della privacy. Gli utenti utilizzatori di sistemi AI devono minimizzare l'uso dei dati personali ai soli scopi necessari utilizzando quando possibile meccanismi di anonimizzazione e pseudonimizzazione nei dati di training dell'AI.
- f) **Principio di non discriminazione ed equità:** l'AI deve essere sviluppata e utilizzata in modo equo e imparziale, evitando discriminazioni basate su razza, genere, età o altri fattori sensibili. Occorre quindi creare modelli AI che minimizzino devianze algoritmiche, pregiudizi sistemici e monitorare costantemente gli output dell'AI per correggere eventuali distorsioni nei dati. Si deve garantire che gli algoritmi siano addestrati su dataset rappresentativi e diversificati.
- g) **Principio di supervisione umana e accountability:** le decisioni critiche prese dall'AI devono sempre prevedere una supervisione umana, evitando la totale automatizzazione in processi sensibili. Ogni sistema AI può proporre una soluzione ma la decisione deve essere sempre presa dall'utente persona fisica.
- h) **Principio di innovazione e proporzionalità:** l'uso dell'AI deve essere bilanciato tra innovazione tecnologica e prudenza operativa, evitando soluzioni troppo complesse o non adeguate al contesto bancario. È quindi opportuno valutare i benefici dell'AI rispetto ai rischi operativi e reputazionali, implementare soluzioni AI che siano proporzionate alle necessità della banca e dei clienti e adottare un approccio risk-based per l'uso dell'AI in ambiti regolati (es. concessione del credito).
- i) **Principio di sostenibilità e impatto sociale:** le soluzioni AI devono essere sviluppate in ottica sostenibile, riducendo l'impatto ambientale e garantendo un utilizzo responsabile delle risorse.
- j) **Principio di audit e monitoraggio continuo:** il Gruppo Bancario La Cassa di Ravenna prevede meccanismi di controllo sui sistemi AI, per garantirne la correttezza nel tempo.

- k) **Diritti di Proprietà intellettuale:** il Gruppo Bancario La Cassa di Ravenna garantisce che l'utilizzo dei dati e l'addestramento dei modelli di intelligenza artificiale non violi brevetti, marchi o diritti d'autore di altre parti.
- l) **Formazione e alfabetizzazione:** il Gruppo Bancario La Cassa di Ravenna assicura la trasparenza nell'interazione tra AI e utenti e garantisce la formazione del personale, affinché tutti i dipendenti abbiano una conoscenza adeguata delle opportunità e dei limiti dell'AI. L'art. 4 dell'AI ACT indica che "i fornitori e i deployer dei sistemi di IA adottano misure per garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto". Per alfabetizzazione si intendono le competenze, le conoscenze e la comprensione che consentono ai fornitori, ai deployer e alle persone interessate, tenendo conto dei loro rispettivi diritti e obblighi nel contesto del regolamento, di procedere a una diffusione informata dei sistemi di IA, nonché di acquisire consapevolezza in merito alle opportunità e ai rischi dell'IA e ai possibili danni che essa può causare.

5.3. Classificazione delle soluzioni AI

Le soluzioni AI sono classificate secondo livelli di impatto sui diritti fondamentali tutelati dall'AI Act che sono:

- **Diritto alla privacy e alla protezione dei dati personali** (Art. 7 e 8): i sistemi AI non devono trattare dati in modo sproporzionato, opaco o discriminatorio, risulta pertanto importante assicurare (in funzione della tipologia di soluzione AI) che i sistemi AI garantiscano trasparenza, finalità lecite, minimizzazione e sicurezza del trattamento;
- **Diritto alla non discriminazione** (Art. 21): i sistemi AI non devono portare ad azioni/decisioni discriminatorie in funzione di sesso, etnia, religione, ed altri aspetti rilevanti.
- **Diritto alla dignità umana** (Art. 1): nessun sistema AI deve umiliare, strumentalizzare o ridurre la persona a oggetto di manipolazione o controllo (es. sistemi subliminali o di sorveglianza invasiva).
- **Diritto alla libertà di espressione e informazione** (Art. 11): gli utenti devono essere informati quando interagiscono con un sistema AI che fornisce informazioni desunte da auto-generazione di dati e/o raccomandazioni automatizzate.
- **Diritto alla libertà individuale, autodeterminazione e autonomia** (Art. 6 e 7): gli utenti devono poter prendere decisioni informate, non essere manipolati o indotti in errore da sistemi opachi o coercitivi. La supervisione umana è essenziale nei sistemi ad alto impatto.
- **Diritto alla revisione e ad un equo processo** (Art. 47): particolarmente importante per i sistemi decisionali automatizzati (es. nella concessione di credito o nella selezione del personale). Le persone devono poter comprendere e contestare decisioni prese o supportate da sistemi di AI.
- **Diritti dei minori e delle persone vulnerabili** (Art. 24): è previsto il divieto di utilizzo di AI che sfrutta vulnerabilità, età, condizioni psicologiche, sociali o economiche.
- **Altri diritti rilevanti contemplati dall'AI Act in modo indiretto:** in generale le soluzioni AI devono assicurare: la libertà di impresa (Art. 16); la protezione dei consumatori (Art. 38); la libertà religiosa e di pensiero (Art. 10); la libertà di movimento e di riunione (Art. 12 e 45)

In funzione della rilevanza dell'impatto che i sistemi AI possono avere sui diritti sopra citati, l'AI Act individua le seguenti quattro categorie di impatto:

- 1) minimo o nullo;
- 2) limitato;
- 3) alto
- 4) inaccettabile.

Solo le soluzioni classificate a impatto minimo o limitato possono essere adottate con approvazione semplificata. Le soluzioni ad alto impatto richiedono supervisione umana, documentazione, controllo e approvazione specifica da parte del Consiglio di Amministrazione, previo preventivo parere del Comitato Endoconsiliare Rischi e Sostenibilità e delle funzioni di controllo: Risk Management di Gruppo e Compliance di Gruppo.

Di seguito nel dettaglio si riporta la classificazione delle quattro categorie di impatto sopra indicate.

5.3.1. AI ad impatto minimo o nullo

Includono sistemi AI con impatto minimo o nullo, che non influiscono sui diritti fondamentali tutelati dall'AI Act o sulla sicurezza. Esempi di AI ad impatto minimo sono ad esempio:

- Motori di ricerca documentale interni per recuperare policy o manuali;
- Classificatori automatici di e-mail (es. inbox condivise del contact center);
- Completamento automatico di moduli (es. IBAN, codice fiscale);
- Analisi statistica aggregata delle richieste ricevute dai clienti;
- Chatbot statici per FAQ tecniche interne (es. login, reset password, orari filiali).

L'adozione di soluzioni ad impatto minimo o nullo per le società del Gruppo La Cassa di Ravenna deve seguire gli ordinari iter di approvazione e di gestione dei cambiamenti ICT.

5.3.2. AI ad impatto limitato

Includono applicazioni AI che interagiscono direttamente con gli utenti, ma senza impatti sui diritti fondamentali. Questi sistemi devono rispettare alcuni requisiti di trasparenza ed informazione. Rientrano in questa categoria ad esempio:

- Chatbot che forniscono informazioni su conti, carte, mutui o Chatbot conversazionale su normative o processi operativi interni;
- Traduttori automatici AI di contenuti bancari multilingue per clienti o dipendenti;
- Assistenti virtuali per onboarding digitale (es. guida all'apertura conto online);
- Sistemi di generazione automatica di risposte e-mail predefinite per l'assistenza;
- Avatar virtuali che spiegano normative o servizi all'interno di portali informativi.

L'adozione di soluzioni ad impatto limitato per le società del Gruppo La Cassa di Ravenna deve seguire gli ordinari iter di approvazione e di gestione dei cambiamenti ICT.

5.3.3. AI ad impatto alto

Comprendono i sistemi AI che possono avere impatti significativi sui diritti fondamentali o sulla sicurezza delle persone. L'AI Act richiede requisiti di conformità più stringenti per queste soluzioni. Esempi di AI ad alto impatto possono essere soluzioni AI che generano: lo scoring del credito e la valutazione di affidabilità finanziaria (es. concessione di mutui o prestiti); modelli AI per la prevenzione del riciclaggio di denaro (AML) e rilevamento frodi; AI per l'identificazione biometrica remota dei clienti (es. onboarding digitale con riconoscimento facciale).

Per questa tipologia di sistemi sono previste oltre che agli ordinari processi di change management anche misure di conformità più stringenti quali:

- Registrazione: ogni AI ad alto impatto deve essere registrata in un database dell'UE con rilascio marchiatura CE;
- Spiegabilità e supervisione umana: l'output AI deve essere comprensibile e deve sempre essere possibile una revisione umana.
- Test e audit periodici: i modelli devono essere sottoposti a verifiche per garantire accuratezza, equità e affidabilità
- Monitoraggio continuo: l'AI deve essere testata in condizioni reali per prevenire deviazioni/derivate algoritmiche.
- Documentazione: l'art. 27 del Regolamento (UE) n. 1689/2024 (AI Act) introduce nei confronti dei deployer l'obbligo di condurre una valutazione d'impatto sui diritti fondamentali (FRIA). Tale adempimento presenta carattere preventivo e va svolto solo in particolari ipotesi. L'obbligo di compilare la FRIA è limitato ai casi di utilizzo di sistemi di IA ad alto impatto destinati ad essere impiegati in particolari settori, e più specificamente:
 - Istruzione e formazione;
 - Occupazione;

- Accesso a servizi privati essenziali (es.: concessione di credito al consumo, prestiti, mutui mediante AI (es. credit scoring automatizzato; valutazione dell'affidabilità creditizia attraverso modelli predittivi AI);
- Attività di contrasto al crimine (es.: sistemi di AML avanzati);
- Migrazione;
- Biometria;
- Amministrazione della giustizia;

5.3.4. AI vietate (impatto inaccettabile)

Si tratta di sistemi AI che presentano un impatto elevato ed inaccettabile per i diritti fondamentali delle persone, la sicurezza e la democrazia. L'AI Act ne vieta l'uso, salvo eccezioni specifiche per motivi di sicurezza nazionale o ordine pubblico.

Un esempio di AI vietata consiste nella manipolazione cognitiva e subliminale, ossia in AI che influenzano il comportamento umano in modo dannoso (es. pubblicità manipolative).

Il Gruppo Bancario La Cassa di Ravenna si impegna ad escludere qualsiasi utilizzo di AI rientrante nelle pratiche vietate dall'AI Act (art. 5), tra cui:

- Sistemi AI per manipolazione cognitiva o comportamentale che possano indurre danni;
- Sistemi di punteggio sociale che valutano le persone per finalità discriminatorie;
- Giustizia predittiva: una decisione giudiziaria possa essere resa da un sistema di AI in autonomia, senza alcun intervento di un giudice umano. Oltre a questo, l'AI Act stabilisce anche che le persone devono essere sempre giudicate sulla base del loro comportamento effettivo, senza poter effettuare valutazioni in relazione ad altri elementi che nulla hanno a che vedere con la condotta posta in essere (come la cittadinanza, il luogo di residenza, il livello di indebitamento, etc.). La norma consente invece di utilizzare sistemi di AI a sostegno di una valutazione umana che deve fondarsi su fatti oggettivi e verificabili collegati alla condotta.
- AI per il riconoscimento facciale in tempo reale (salvo eccezioni previste dalla legge);
- Inferenza di emozioni: sistemi di AI possono riconoscere lo stato emozionale di una persona basandosi sulle espressioni del viso, sulla base di classificazioni precedentemente effettuate. Tali classificazioni, però, possono includere errori, in quanto non tengono conto delle diverse culture e delle particolari situazioni in cui una persona può trovarsi. Per tali motivi l'AI ACT vieta l'utilizzo di sistemi di inferenza delle emozioni quando utilizzati in ambito lavorativo o scolastico. Il divieto non comprende quei sistemi utilizzati per motivi medici o di sicurezza: questo significa che un sistema che controlli se un autista sia in condizioni di poter guidare, monitorando le sue espressioni, non deve ritenersi vietato, così come non sono vietati i sistemi che controllano gli stati fisici, come dolore, affaticamento, etc.
- Sistemi di classificazione biometrica: alcuni casi possono essere utilizzati per classificare una persona al fine di trarre conclusioni su appartenenza religiosa, razza, orientamento sessuale, opinioni politiche. Tali pratiche, se attuate con un sistema di intelligenza artificiale, sono considerate vietate perché potrebbero creare delle discriminazioni contro specifici insiemi della popolazione.

5.4. Requisiti normativi e di sicurezza dei sistemi AI

Come precisato al precedente paragrafo, per i sistemi di AI ad impatto alto, l'articolo 43 del Regolamento (UE) 2024/1689, prevede una serie di prerequisiti prima della loro immissione sul mercato o messa in servizio nell'Unione Europea. Tali attività sono predisposte dal fornitore del sistema AI che prima del rilascio deve assicurare:

- 1) La rispondenza del sistema AI ad impatto alto ai requisiti dell'AI Act;
- 2) la responsabilità di mantenere la conformità del sistema anche dopo la sua immissione sul mercato, attraverso un monitoraggio continuo e, se necessario, aggiornamenti o modifiche;

- 3) la registrazione e documentazione del sistema AI ad impatto alto che deve essere registrata in un database dell'UE con rilascio marchiatura CE.
- 4) La spiegabilità e supervisione umana: l'output AI deve essere comprensibile e deve sempre essere possibile una revisione umana.

Il Gruppo Bancario La Cassa di Ravenna si impegna ad adottare soluzioni AI adottate che siano rispondenti ai requisiti normativi tempo per tempo vigenti.

5.4.1. Spiegabilità e trasparenza

Il Gruppo Bancario La Cassa di Ravenna adotta un approccio proporzionato ai requisiti di trasparenza e spiegabilità delle soluzioni di Intelligenza Artificiale (AI), in conformità con quanto previsto dal Regolamento (UE) 2024/1689 ("AI Act"). Tali requisiti si applicano a tutte le tipologie di AI, classificati come "ad impatto alto" o, in determinati casi, per i sistemi a impatto limitato in relazione a specifici obblighi di informazione.

In particolare:

- Per i sistemi AI ad impatto alto, conformemente all'AI Act, si prevede l'obbligo di rispettare :
 - I requisiti di trasparenza: l'utente deve essere chiaramente informato quando interagisce con un sistema automatizzato.
 - L'obbligo di spiegabilità ("explainability"): i modelli devono essere accompagnati da documentazione tecnica che consenta la comprensione del funzionamento dell'algoritmo, delle sue variabili rilevanti, dei margini di errore e delle limitazioni.
 - La predisposizione di audit trail e registri delle decisioni critiche per consentire controlli e verifiche.
 - L'implementazione di marcature (watermarking) per rendere evidente quando un contenuto è stato generato da un sistema di AI;
- Per i sistemi AI ad impatto limitato, è richiesto un livello di trasparenza proporzionato, come ad esempio l'inserimento di un disclaimer informativo che avvisi l'utente che sta interagendo con un sistema AI.
- Per i sistemi AI a rischio minimo o nullo, non sussistono obblighi normativi specifici in materia di trasparenza e spiegabilità, fermo restando l'impegno del Gruppo a garantire un utilizzo responsabile, monitorato e conforme alle policy interne.

In ogni caso, il Gruppo La Cassa di Ravenna garantisce che:

- le soluzioni AI adottate siano regolarmente censite tra le risorse ICT.
- vengano effettuati audit periodici sugli algoritmi delle soluzioni AI ad alto impatto con attenzione a deviazioni, accuratezza, robustezza e deriva algoritmica;

5.4.2. Supervisione umana per decisioni critiche

Le soluzioni AI non possono sostituire il giudizio umano nei processi bancari ad impatto alto, in particolare nelle decisioni che riguardano aspetti finanziari dei clienti. Per questo motivo, le società del Gruppo Bancario La Cassa di Ravenna adottano il principio di supervisione ed approvazione umana obbligatoria in tutti i processi ed ancora più nei processi critici in cui vi possa essere l'utilizzo di soluzioni AI quali ad esempio: concessione del credito; scoring del rischio; segnalazioni di operazioni sospette.

5.4.3. Protezione dei dati

Per garantire la sicurezza e la privacy dei dati utilizzati nei modelli AI, il Gruppo adotta rigorose misure di protezione, in conformità con il Regolamento Generale sulla Protezione dei Dati (GDPR).

In particolare, il Gruppo Bancario La Cassa di Ravenna impone a tutti gli utenti utilizzatori di sistemi AI la minimizzazione nell'uso dei dati personali ai soli scopi necessari utilizzando quando possibile meccanismi di anonimizzazione e pseudonimizzazione nei dati di training dell'AI.

L'insieme dei dati utilizzati per il training e la validazione degli algoritmi AI contengono solo i dati strettamente necessari all'addestramento.

Per il testing e l'addestramento dei modelli AI, si privilegia l'uso di dati sintetici generati artificialmente, in modo da ridurre la dipendenza da dati reali sensibili.

5.4.4. Accesso e conservazione dei dati

L'accesso ai dati utilizzati dall'AI è limitato al personale autorizzato e regolato da sistemi di controllo avanzati. I dati sono conservati per il tempo minimo indicato all'interno della normativa interna e in conformità con le politiche aziendali.

5.4.5. Obblighi e Vincoli di Utilizzo per gli Utenti Finali

Gli utenti delle soluzioni AI sono tenuti a rispettare rigorosamente le seguenti regole di condotta:

- Uso esclusivamente professionale e autorizzato: l'accesso e l'utilizzo sono consentiti solo per scopi aziendali e nei limiti del ruolo assegnato. È vietato qualsiasi uso personale o non autorizzato.
- Divieto di utilizzo di strumenti AI generativi pubblici (es. ChatGPT, Bard, Copilot, Gemini) per trattare dati personali o sensibili.
- Riservatezza: le credenziali di accesso e le informazioni trattate devono essere custodite in modo sicuro e non condivise con soggetti non autorizzati.
- Sicurezza delle credenziali: devono essere usate password complesse, aggiornate periodicamente, e attivata l'autenticazione a più fattori (MFA) per l'accesso alle piattaforme che adottano soluzioni AI ad impatto elevato.
- Segnalazione tempestiva: ogni sospetta violazione, anomalia, accesso improprio o tentativo di phishing deve essere immediatamente comunicato all'Ufficio Organizzazione ed IT di Gruppo.

5.4.6. Processo decisionale

Prima dell'adozione o sostituzione di una soluzione basata su Intelligenza Artificiale (AI), è necessario identificare e valutare in modo preventivo i seguenti elementi:

- la tipologia della soluzione AI (es. machine learning, regole esperte, AI generativa, LLM);
- il livello di impatto della soluzione AI secondo la classificazione dell'AI Act (minimo, limitato, alto, vietato);
- la tipologia di dati trattati (personali, sensibili, bancari, sintetici, anonimi);
- le finalità e i processi aziendali supportati (es. credito, onboarding, AML, customer care);
- il grado di automazione e di impatto su utenti/clienti (decisioni automatizzate, suggerimenti, contenuti generati);
- la necessità di supervisione umana nei punti critici;
- la trasparenza e spiegabilità del modello (black-box o interpretabile);
- la compatibilità con la normativa vigente (AI Act, GDPR, DORA, BCE, EBA);
- eventuali conflitti di interesse nella selezione o utilizzo del sistema.

L'adozione di sistemi AI ad alto rischio o con finalità critiche richiede valutazione preventiva da parte delle Funzioni di Controllo e del Comitato Endoconsiliare Rischi e Sostenibilità. Le soluzioni AI vietate ex art. 5 AI Act sono escluse a priori.

[OMISSIS]

5.4.8. Obblighi di formazione in materia di Intelligenza Artificiale

In conformità con quanto previsto dall'articolo 4 del Regolamento (UE) 2024/1689 ("AI Act"), le società del Gruppo Bancario La Cassa di Ravenna sono tenute a garantire un adeguato livello di alfabetizzazione e formazione continua in materia di Intelligenza Artificiale per tutto il personale coinvolto a vario titolo nei processi di adozione, utilizzo o supervisione di sistemi di AI.

In particolare, il Gruppo assicura che:

- il personale direttamente coinvolto nell'utilizzo o nella supervisione di soluzioni AI (utenti, referenti di progetto, validatori, ecc.) sia adeguatamente formato sui principi generali dell'AI Act, con focus su: categorie di rischio AI, spiegabilità, responsabilità, trasparenza e sicurezza;
- siano attivati percorsi formativi specifici per gli utenti finali che interagiscono con sistemi AI ad impatto medio o alto, in particolare nei casi in cui siano previsti suggerimenti automatizzati, decisioni supportate da AI o interazioni dirette con modelli generativi;
- per le soluzioni AI classificate ad impatto elevato, sia prevista una formazione obbligatoria e tracciata, che comprenda: i meccanismi di supervisione umana, la gestione delle anomalie, il principio di accountability e i canali per la segnalazione di malfunzionamenti o distorsioni algoritmiche;
- l'Ufficio Personale con il supporto dell'Ufficio Organizzazione e IT di Gruppo predisponga piani formativi aggiornati con cadenza annuale, garantendo l'integrazione dei temi AI nei percorsi di aggiornamento continuo del personale;

Le attività formative sono considerate presidio obbligatorio per l'adozione di soluzioni AI. Le funzioni di controllo verificano l'adempimento degli obblighi formativi e suggeriscono eventuali integrazioni ai loro contenuti.

5.4.9. Responsabilità e Sanzioni

Il mancato rispetto delle regole di utilizzo delle soluzioni Cloud e di intelligenza artificiale può comportare conseguenze disciplinari e legali.

Ogni uso improprio delle soluzioni Cloud e AI è considerato una violazione del Codice Etico e del Modello Organizzativo 231.

In caso di gravi infrazioni (es. violazioni della privacy, uso illecito di AI, accesso abusivo a dati sensibili), la Banca potrà segnalare il fatto alle autorità competenti.

L'Organismo di Vigilanza (OdV) monitora il rispetto delle disposizioni e può attivare controlli e verifiche in caso di sospette violazioni.