



**UNIMORE**

UNIVERSITÀ DEGLI STUDI DI  
MODENA E REGGIO EMILIA

## Dipartimento di Comunicazione ed Economia

### Corso di Laurea Magistrale in

MANAGEMENT E COMUNICAZIONE D'IMPRESA

A.A. 2025/2026

Lo sviluppo delle Intelligenze Artificiali,  
il loro utilizzo nel settore bancario e la  
mitigazione del rischio socioeconomico.  
L'importanza di una normativa cogente  
per regolamentare le Intelligenze Artificiali

Relatore: Prof. Giuliano Lemme

Laureanda: Eleonora Fontana

# **Lo sviluppo delle Intelligenze Artificiali, il loro utilizzo nel settore bancario e la mitigazione del rischio socioeconomico.**

## **L'importanza di una normativa cogente per regolamentare le Intelligenze Artificiali**

### Introduzione

#### Capitolo 1. Intelligenza Artificiale e settore bancario

##### 1.1 Breve storia e definizione delle AI

##### 1.2 Intelligenza artificiale e settore bancario

##### 1.3 Cyber crime finanziario, dati e stime

##### 1.4 Profili giuridici della regolamentazione dell'AI nel settore bancario

#### Capitolo 2. Normativa Europea

##### 2.1 La cornice giuridica dell'AI Act

##### 2.2 Analisi dell'AI Act e impatti specifici nel settore bancario

##### 2.3 Interpretazione della letteratura scientifica italiana dell'AI Act

##### 2.4 Considerazioni sulla Legge italiana recepimento AI Act

##### 2.5 Valutazione delle lacune normative

#### Capitolo 3 L'impatto dell'intelligenza artificiale sul settore bancario e sul lavoro

##### 3.1 Ambiti di applicazione dell'AI

##### 3.2 Impatti economici e strategici

##### 3.3 Uomo e intelligenza artificiale: modelli di collaborazione

##### 3.4 Scenari futuri del settore bancario

##### 3.5 L'ipotesi di una funzione di controllo basata su AI

#### Capitolo 4 Percezioni di clienti e dipendenti sull'utilizzo dell'Intelligenza Artificiale nel settore bancario

##### 4.1 Le principali indagini condotte a livello europeo

##### 4.2 Analisi empirica delle percezioni della clientela

##### 4.3 Percezione dell'intelligenza artificiale tra gli operatori del settore bancario

##### 4.4 Confronto tra percezione della clientela e degli operatori bancari

##### 4.5 Considerazioni conclusive dell'analisi empirica

### Conclusioni

Negli ultimi anni, l'intelligenza artificiale è progressivamente uscita dai confini della ricerca specialistica per entrare in modo pervasivo nella vita quotidiana. Ciò che fino a pochi decenni fa era oggetto di speculazione teorica o di rappresentazioni fantascientifiche è oggi parte integrante di pratiche ordinarie, spesso adottate in modo inconsapevole. In alcuni casi, tale integrazione assume una dimensione ancora più profonda, arrivando a incidere direttamente sulla gestione della salute e della vita personale. L'utilizzo di sistemi intelligenti in ambito medico, come nel caso di dispositivi in grado di mettere in comunicazione sensori per il monitoraggio della glicemia e microinfusori per la somministrazione di insulina, rappresenta un esempio emblematico di come l'intelligenza artificiale non sia più soltanto uno strumento di supporto, ma diventi parte attiva nei processi decisionali, contribuendo a migliorare la qualità della vita e a ridurre il margine di errore umano.

Questa crescente pervasività dell'intelligenza artificiale era stata, per certi versi, anticipata già nella riflessione letteraria e filosofica del Novecento. Le opere di Isaac Asimov, con la formulazione delle celebri leggi della robotica, rappresentano uno dei primi tentativi di immaginare un sistema normativo capace di governare il comportamento delle macchine intelligenti. Più recentemente, produzioni culturali come la serie Black Mirror hanno offerto rappresentazioni spesso distopiche degli effetti sociali della tecnologia, mettendo in luce i rischi connessi a un utilizzo non controllato degli algoritmi e alla progressiva erosione della dimensione umana nelle relazioni sociali.

Sul piano teorico, tali trasformazioni possono essere lette anche alla luce delle riflessioni di studiosi come Marshall McLuhan, secondo cui i media non si limitano a trasmettere contenuti, ma contribuiscono a ridefinire le strutture percettive e sociali, o di Zygmunt Bauman, che ha descritto la modernità come un contesto caratterizzato da crescente fluidità e incertezza. In modo analogo, l'intelligenza artificiale può essere interpretata non solo come un insieme di strumenti tecnologici, ma come un fattore capace di trasformare profondamente i modelli organizzativi, le dinamiche economiche e le modalità di esercizio del potere decisionale.

In questo scenario, il settore bancario rappresenta un ambito di particolare interesse.

Tradizionalmente fondato su relazioni fiduciarie e su un elevato grado di regolamentazione, esso è oggi interessato da un processo di trasformazione profonda, determinato dall'introduzione di tecnologie avanzate e dalla crescente centralità dei dati. L'intelligenza artificiale viene impiegata in una pluralità di funzioni, dalla valutazione del merito creditizio alla prevenzione delle frodi, fino alla gestione della relazione con la clientela, contribuendo a migliorare l'efficienza operativa, ma sollevando al contempo interrogativi rilevanti sul piano giuridico ed etico.

La presente tesi si inserisce in questo contesto di trasformazione, proponendosi di analizzare l'impatto dell'intelligenza artificiale nel settore bancario, con particolare attenzione ai profili giuridici e regolamentari. L'obiettivo è quello di comprendere in che modo l'innovazione tecnologica interagisca con il quadro normativo esistente e quali siano le principali criticità emergenti, sia sotto il profilo della tutela dei diritti fondamentali sia in relazione alla stabilità del sistema finanziario.

Il lavoro si articola in quattro capitoli.

Nel primo capitolo viene ricostruito il percorso evolutivo dell'intelligenza artificiale, a partire dalle sue origini fino alle più recenti applicazioni nel settore bancario, con particolare attenzione ai rischi connessi al cybercrime finanziario e ai primi interventi normativi.

Il secondo capitolo è dedicato all'analisi della cornice europea, con un approfondimento dell'AI Act, dei suoi contenuti e dei suoi impatti sul settore bancario, nonché delle principali interpretazioni offerte dalla letteratura scientifica, anche italiana, e delle questioni relative al recepimento nel contesto nazionale.

Il terzo capitolo esamina gli ambiti applicativi dell'intelligenza artificiale nel settore bancario, soffermandosi sugli impatti economici e strategici, sui modelli di interazione tra uomo e macchina e sui possibili scenari futuri, includendo anche riflessioni sulle nuove forme di controllo basate sull'utilizzo di sistemi algoritmici.

Infine, il quarto capitolo propone un'analisi empirica, basata sia su studi di settore sia su dati raccolti attraverso questionari, al fine di indagare la percezione dell'intelligenza artificiale da parte della clientela e degli operatori bancari.

Nel complesso, la ricerca intende contribuire alla comprensione di un fenomeno in continua evoluzione, mettendo in evidenza la necessità di un approccio equilibrato che sappia coniugare innovazione tecnologica e tutela dei diritti. La sfida principale, infatti, non consiste soltanto nell'introdurre nuove tecnologie, ma nel governarne gli effetti, evitando che il progresso tecnico si traduca in una riduzione delle garanzie e della fiducia che costituiscono il fondamento del sistema bancario.

## Capitolo 1. Intelligenza Artificiale e settore bancario

### 1.1 Breve storia e definizione delle AI

Nonostante il dibattito pubblico abbia riaperto i riflettori sull'intelligenza artificiale negli ultimi anni, non si tratta di uno sviluppo recente. Si inizia a parlare di "intelligenza artificiale" a partire dagli Anni 50 del 900, periodo caratterizzato da ricerche scientifiche pionieristiche su calcolatori elettronici e sul loro possibile utilizzo per dare vita a sistemi intelligenti, cioè sistemi capaci di agire razionalmente, ma anche in grado di simulare le facoltà cognitive e intellettive umane.

Sebbene i primi lavori comunemente considerati appartenenti all'AI risalgano al 1943, i primi entusiasmi si accesero tra il 1952 e il 1969.

Negli Anni quaranta alcuni biologi, impegnati a dimostrare come l'intelligenza e l'apprendimento fossero il risultato dei segnali trasmessi tra i neuroni nel cervello umano, diedero vita alla teoria, valida ancora oggi, che i collegamenti tra i neuroni si rafforzino attraverso la frequenza delle comunicazioni.

Già nel 1943, McCulloch e Walter Pitts dimostrarono che ogni funzione computabile poteva essere calcolata da una rete di neuroni collegati e che tutti gli operatori logici potevano essere implementati con semplici strutture a rete. Suggestarono, inoltre, che reti neurali adeguatamente definite potessero essere capaci di apprendere. Donald Hebb nel 1949 formulò una regola, chiamata apprendimento Hebbiano<sup>1</sup> e utilizzata ancora oggi, di aggiornamento per la modifica dei pesi delle connessioni tra i neuroni. Secondo lo psicologo statunitense il rafforzamento sinaptico ha conseguenze funzionali importanti e avviene attraverso l'attivazione contemporanea e frequente di un gruppo di neuroni. Anche attivando soltanto alcuni dei neuroni, si attiverà l'intero gruppo.

Unità funzionali, composte da diversi neuroni, formano una rete associativa chiamata corteccia in grado di generare un rafforzamento sinaptico. L'idea di insiemi distribuiti con topografie corticali definite è parte integrante delle teorie neuronali a grande scala del linguaggio e di altre funzioni cognitive.

Nel 1950, Edmonds e Minsky costruirono il primo computer basato su reti neurali, lo **SNARC**.

Utilizzava tremila tubi a vuoto e un sistema automatico di pilotaggio riciclato da un bombardiere B-24 per simulare una rete di quaranta neuroni.

Nello stesso anno Alan Turing pubblica un articolo sulla rivista Mind intitolato "*Computing Machinery and Intelligence*" in cui si chiese se le macchine potessero pensare. Il test di Turing introduce l'idea

---

<sup>1</sup> Regola di Hebb - Enciclopedia - Treccani

secondo cui se non siamo in grado di distinguere il comportamento di una macchina da quello di un essere umano, allora quella macchina può essere considerata intelligente<sup>2</sup>.

Già nel 1956 al Dartmouth College furono raccolti tutti i principali contributi in tema di intelligenza artificiale ponendo particolare attenzione sugli sviluppi futuri. Dieci ricercatori si riunirono per due mesi con il proposito di studiare le congetture di ogni aspetto dell'apprendimento, qualsiasi altra caratteristica dell'intelligenza che potesse in linea di principio essere descritta con una precisione tale da poter costruire una macchina in grado di simularla.

Nel 1958 Frank Rosenblatt, neurofisiologo e psicologo del Cornell Aeronautical Laboratory diede vita a una delle prime reti neurali artificiali, il Perceptron. Si trattava di un modello computazionale in grado di apprendere e risolvere problemi di classificazione lineare processando dei dati di input, attraverso delle connessioni tra i neuroni artificiali. Rosenblatt dimostrò che le macchine non solo potevano imparare un enorme quantità di dati, ma erano in grado di migliorare le loro performance nel tempo. Il Perceptron, per esempio, era in grado di distinguere le forme geometriche concave da quelle convesse.

L'espressione "Intelligenza Artificiale" (AI) in quegli anni descriveva accuratamente il sogno dei ricercatori di comprendere i principi e i meccanismi del funzionamento della mente umana allo scopo di riprodurre l'intelligenza umana su una macchina.

*"Nel 1956 lo scienziato informatico John McCarthy definì ulteriormente l'intelligenza artificiale come macchina capace di svolgere compiti che sono caratteristici dell'intelligenza umana. Da allora le definizioni dell'intelligenza artificiale formulate da Turing e McCarthy sono diventate veri e propri capisaldi, che hanno indirizzato la nostra attenzione verso la definizione dell'intelligenza sulla prestazione (un comportamento apparentemente intelligente) anziché sulle più profonde dimensioni filosofiche, cognitive o neuroscientifiche del termine. Sebbene negli ultimi cinquant'anni le macchine non siano sostanzialmente riuscite a dimostrare tale intelligenza, quello stallo sembra ormai in procinto di essere superato".<sup>3</sup>*

I ricercatori erano molto ottimisti in materia di sviluppo dei cosiddetti sistemi intelligenti, ma le circostanze socio-economiche e le ridotte conoscenze neuroscientifiche rallentarono il processo.

Nel 1969 Marvin Minsky e Seymour Papert, due matematici del Massachusetts Institute of Technology (MIT), pubblicarono "Perceptrons" un libro nel quale misero in evidenza i limiti del modello di Rosenblatt, contribuendo all'inizio di quel periodo buio per lo sviluppo delle intelligenze artificiali, che viene ricordato come "AI Winter".<sup>4</sup>

---

<sup>2</sup> Alan Turing, *Computing Machinery and Intelligence*, Mind, 1950, pp. 433-460

<sup>3</sup> H.A.Kissinger, E.Schmidt, D. Huttenlocher, *L'erA dell'Intelligenza artificiale. Il futuro dell'identità umana*. Mondadori, Milano. 2023 pag. 48

<sup>4</sup> Marvin Minsky & Seymour Papert, *Perceptrons: an introduction to computational Geometry*, 1969

In quegli anni 69-82 i ricercatori si scontrarono contro le insufficienti capacità di calcolo, nonché di memoria dei computer e con l'arresto delle ricerche nel campo delle neuroscienze, legato sia allo sconforto generato dalla pubblicazione di Perceptrons, ma anche e soprattutto per via degli elevati costi di ricerca.

La concomitanza di tali fattori portò gli studiosi a rinunciare alla ricerca nell'ambito dell'intelligenza artificiale già a partire dall'inizio degli anni '70. Lo studio di questa materia fu sostanzialmente abbandonato fino al 1990 quando lo sviluppo dei computer li rese capaci di prestazioni sempre più straordinarie, e soprattutto quando le neuroscienze resero disponibili i primi modelli delle funzioni neurali di base.

Una prima importante ripresa della ricerca neuroscientifica, però, avviene già nel 1982, quando alcuni studiosi propongono nuovi modelli di reti neurali capaci di apprendere, dando vita al Machine Learning. In questo campo possiamo citare le ricerche di Hopfield che propose un modello in grado di comportarsi come una memoria associativa<sup>5</sup>; i lavori di Kohonen che rese le reti neurali artificiali in grado di autorganizzarsi per formare delle mappe sensoriali<sup>6</sup> e Marr, che propose un modello a tre livelli del sistema visivo umano<sup>7</sup>.

Nel 1983 Barto, Sutton e Anderson integrarono gli studi sulle reti neurali a quelli sull'apprendimento sviluppando il Reinforcement Learning, un modello di reti neurali in grado di generare azioni di controllo attraverso un processo di apprendimento basato su premi e punizioni<sup>8</sup>. L'idea alla base di questo modello ricorda il condizionamento operante skinneriano per cui ad azione positiva corrisponde una ricompensa e ad azione negativa una punizione.

Questo periodo segna sostanzialmente il passaggio dalle intelligenze artificiali deboli a quelle forti, dal machine learning al deep learning.

Il cambio di prospettiva iniziò negli Anni '90, quando i ricercatori si resero conto che era necessario un nuovo approccio: non utilizzare gli esseri umani come modello, ma consentire alle macchine di imparare in modo autonomo. In poche parole, terminò in tentativo di instillare nelle macchine una perspicacia distillata dalla mente umana, per affidare loro lo stesso processo di apprendimento. I metodi che hanno funzionato meglio nella pratica estraggono modelli da vasti insiemi di dati utilizzando le reti neurali.

---

<sup>5</sup> John J. Hopfield, *Neural networks and physical systems with emergent collective computational abilities*, Proc. Natl. Acad. Sci. USA, Vol. 79, 1982, pp. 2554-2558

<sup>6</sup> Teuvo Kohonen, *Self-organized formation of topologically correct feature maps*, Biol. Cybern. 43, 1982, pp. 59-69

<sup>7</sup> David Marr, *Vision: a computational investigation into the human representation and processing of visual information*, San Francisco, 1982

<sup>8</sup> Andrew G. Barto, Richard S. Sutton & Charles W. Anderson, *Neuronlike adaptive elements that can solve difficult learning control problems*, IEEE Transactions on Systems, Man and Cybernetics, vol. SMC 13, 1983, pp. 834-846

Il termine deep learning si riferisce all'apprendimento automatico realizzato usando molteplici livelli di elementi computazionali semplici e regolabili. I primi esperimenti risalgono al 1970, ma soltanto nel 2011 hanno riscosso un successo reale con il riconoscimento vocale e visivo. Da allora, i sistemi di deep learning sono arrivati a superare le prestazioni umane in alcuni compiti di visione, sviluppando anche applicazioni per la traduzione automatica, di diagnostica medica e giochi.

*“Nel programma AlphaDogfight elaborato dalla DARPA (Defense Advanced Research Projects Agency) i piloti elettronici a intelligenza artificiale hanno ottenuto performance superiori rispetto ai piloti umani in combattimenti simulati, eseguendo manovre che superavano le capacità dei piloti umani. Che si tratti di pilotare jet per condurre operazioni belliche o droni per consegnare la spesa, l'intelligenza artificiale è destinata ad avere un significativo impatto sul futuro dell'aviazione militare e civile”.<sup>9</sup>*

I ricercatori del MIT hanno elaborato un algoritmo di apprendimento automatico che ha permesso di scoprire l'halicina<sup>10</sup>, il primo antibiotico scoperto dall' AI, il cui nome è stato scelto in onore dell'elaboratore di “2001 Odissea nello Spazio” HAL 9000. Per prevedere le proprietà antibatteriche i ricercatori hanno addestrato l'algoritmo con un dataset di molecole attive contro *Escherichia Coli* con una libreria di 1760 strutture molecolari approvate dalla FDA (Food and Drugs Administration) e 800 prodotti isolati da piante, animali e risorse microbiologiche. Gli scienziati hanno inserito le strutture chimiche nell'AI semplicemente come insieme di atomi uniti tra loro da una rete di legami chimici, così da facilitare al sistema la ricerca di analogie tra le sue molecole e quelle potenzialmente attive. Nessun essere umano era riuscito a comprendere le connessioni tra le proprietà di un composto e le sue proprietà antibiotiche. La tecnica utilizzata per ottenere questo importante risultato è chiamata apprendimento supervisionato, perchè gli sviluppatori hanno utilizzato un database contenente input d'esempio (strutture molecolari) che erano individualmente etichettate in base all'output o risultato desiderato (l'efficacia come antibiotico).

Nell'apprendimento non supervisionato mancano i dati di output, gli sviluppatori chiedono all'algoritmo di raggruppare i dati sulla base di indici specifici per la misurazione del grado di somiglianza. Per esempio i servizi di raccomandazione online utilizzati da Amazon, Netflix, etc, utilizzano algoritmi per identificare gruppi di clienti con gusti simili per promuovere nuove vendite. A oggi, i principali problemi tecnologici che incontra la AI sono:

- capacità di calcolo e memorizzazione

---

<sup>9</sup> H.A.Kissinger, E.Schmidt, D. Huttenlocher, L'erA dell'Intelligenza artificiale. Il futuro dell'identità umana. Mondadori, Milano. 2023 pag. 50

<sup>10</sup> Halicina (HAL): il potere del Machine Learning nella Farmaceutica da [www.microbiologiaitalia.it](http://www.microbiologiaitalia.it)

- disponibilità di dati per un apprendimento raffinato
- consumi energetici e disponibilità economica dei sistemi

Negli ultimi dieci anni, l'Intelligenza Artificiale è penetrata sempre più profondamente nella vita quotidiana di persone, imprese e, seppur più lentamente, istituzioni pubbliche, anche se probabilmente meno di quanto le compagnie che si occupano del loro sviluppo desidererebbero.

Ma è interessante notare come, a prescindere dagli avanzamenti scientifici e tecnologici, in questi decenni l'Intelligenza Artificiale sia stata un tema sempre presente nella cultura di massa.

È impressionante il numero di produzioni letterarie, cinematografiche, televisive e videoludiche che affrontano il tema dell'Intelligenza Artificiale, da quelle più distopiche, che immaginano un futuro, più o meno prossimo, in cui l'intera umanità è schiava di una tecnocrazia digitale governata dall'Intelligenza Artificiale, a quelle più speranzose dove le menti artificiali liberano l'uomo dalla fatica del lavoro e trasformano radicalmente la società, segnando il passaggio dall'era dei bisogni a quella del benessere diffuso.

### Intelligenza umana vs AI

Per definire l'intelligenza artificiale è necessario partire dalla definizione di intelligenza. Sebbene il dizionario Treccani la definisca come: *“Complesso di facoltà psichiche e mentali che consentono all'uomo di pensare, comprendere o spiegare i fatti o le azioni, elaborare modelli astratti della realtà, intendere e farsi intendere dagli altri, giudicare, e lo rendono insieme capace di adattarsi a situazioni nuove e di modificare la situazione stessa quando questa presenta ostacoli all'adattamento; propria dell'uomo, in cui si sviluppa gradualmente a partire dall'infanzia e in cui è accompagnata dalla consapevolezza e dall'autoconsapevolezza, è riconosciuta anche, entro certi limiti (memoria associativa, capacità di reagire a stimoli interni ed esterni, di comunicare in modo anche complesso, ecc.)... Nella terminologia filosofica, il termine equivale sostanzialmente a intelletto”*, sarebbe opportuno considerare che esistono diverse forme di intelligenza.

Il cervello umano, infatti, lavora mettendo in comunicazione specifiche sinapsi, ovvero circuiti neuronali specializzati, a seconda del tipo di ragionamento richiesto per svolgere una specifica azione.

Anatomicamente il cervello può essere diviso in due parti uguali: gli emisferi cerebrali, ciascuno dei quali è suddiviso in quattro lobi.

Lobo frontale: è una delle aree più ampie del cervello e svolge una funzione di convergenza dei dati relativi a sensazioni, emozioni e pensieri che arrivano dalle altre aree. Essendo connesso con la

zona motoria, risulta molto importante per la programmazione e la pianificazione delle decisioni nonché per il controllo del corpo.

Lobo occipitale: si trova nella parte posteriore del cervello e custodisce l'area visiva primaria fondamentale per l'attivazione emozionale e la spinta ad agire. Trasmette le informazioni primarie alla corteccia temporale e parietale che le elaborano per orientarsi nello spazio, identificare e riconoscere gli oggetti.

Lobo temporale: si trova tra la corteccia occipitale e quella frontale. Contiene al suo interno l'area di Broca e di Wernicke deputate rispettivamente all'espressione e alla comprensione del linguaggio.

Lobo parietale: si sviluppa nella parte laterale e in quella mediale del cervello. Riceve input dalla corteccia occipitale ed è fondamentale per elaborare funzioni determinanti come la coscienza, l'autoconsapevolezza e l'empatia.

La struttura encefalica e le diverse aree che la compongono ci consentono di distinguere diversi tipi di ragionamento:

1. Logico-Matematico: le aree cerebrali come il lobo parietale e frontale elaborano informazioni numeriche e logiche, supportando la risoluzione di problemi complessi e il pensiero analitico.
2. Linguistico: le aree di Broca e Wernicke, situate nei lobi frontali e temporali, sono coinvolte nella produzione e comprensione del linguaggio, permettendo una comunicazione efficace.
3. Spaziale: le funzioni spaziali sono mediate da circuiti neuronali nel lobo occipitale e parietale posteriore, cruciali per la visualizzazione e manipolazione degli oggetti in tre dimensioni.
4. Cinestetico: il lobo parietale e i gangli della base coordinano il movimento e la sensibilità corporea, supportando le abilità motorie e la coordinazione.
5. Interpersonale e Intrapersonale: le aree frontali e il sistema limbico gestiscono le emozioni e le interazioni sociali, facilitando la comprensione e la regolazione delle emozioni personali e altrui.

L'intelligenza artificiale analizza i processi mentali per riprodurli ed emularli affinché siano applicabili a elaboratori informatici. Una materia scientifica complessa che affonda le sue radici nella fusione di diverse discipline, tra cui informatica, ingegneria, robotica, neuroscienze e psicologia.

Il dizionario Treccani recita: *“In cibernetica, intelligenza artificiale (traduzione dell'inglese. artificial intelligence), riproduzione parziale dell'attività intellettuale propria dell'uomo (con particolare riguardo ai processi di apprendimento, di riconoscimento, di scelta) realizzata o attraverso l'elaborazione di modelli ideali, o, concretamente, con la messa a punto di macchine che utilizzano per lo più a tale fine elaboratori elettronici (per questo detti cervelli elettronici)”*.

L'Intelligenza Artificiale, funziona grazie agli algoritmi. Un algoritmo è uno schema di passaggi che semplifica una sequenza di istruzioni per portare al compimento di un'operazione specifica, suddividendola in operazioni più semplici che portano alla creazione dello schema.

L'intelligenza artificiale è quindi in grado di elaborare dati e di decifrare codici per svolgere il compito richiesto. Inoltre, è capace di apprendere codifiche non fornite in precedenza per svolgere nuove funzioni.

Le intelligenze artificiali (AI) vengono generalmente classificate in base a diversi criteri.

Gli studiosi parlano di AI Deboli nel caso di macchine capaci di svolgere compiti specifici e limitati senza capacità di coscienza o comprensione al di fuori dei compiti per i quali sono state progettate. Siri e Alexa, i famosi assistenti vocali e i motori di raccomandazione sono esempi di intelligenza artificiale debole, ma il vero obiettivo dello sviluppo tecnologico è la realizzazione di sistemi di AI forti, dotati di capacità di comprendere, apprendere e applicare conoscenze in vari ambiti, simulando o addirittura superando l'intelligenza umana.

Una distinzione importante è rappresentata dal metodo di apprendimento. Esistono AI basate sull'apprendimento automatico (Machine Learning), che utilizzano algoritmi per apprendere dai dati e migliorare le prestazioni nel tempo, senza essere esplicitamente programmata per ogni compito. Includono sottocategorie come apprendimento supervisionato, non supervisionato e rinforzato. Quando, invece, si utilizzano reti neurali artificiali complesse per simulare il funzionamento del cervello umano, per compiti come il riconoscimento delle immagini e il processamento del linguaggio naturale siamo di fronte a AI basate sull'apprendimento profondo (Deep Learning).

Le intelligenze artificiali deboli funzionano in un contesto delimitato e astratto, le regole devono essere chiare e inderogabili, come avviene per esempio nel gioco degli scacchi. Oggi neanche i più grandi scacchisti al mondo riescono a battere l'intelligenza artificiale. *“Alla fine del 2017 AlphaZero, un algoritmo di intelligenza artificiale sviluppato da Google DeepMind, ha sconfitto Stockfish, fino a quel momento il programma di scacchi più potente al mondo... Di solito la vittoria di un programma di scacchi contro un altro programma di scacchi suscita l'interesse soltanto di qualche appassionato. Ma AlphaZero non era un programma di scacchi ordinario. Tutti i programmi precedenti erano basati su mosse concepite, eseguite e caricate da giocatori umani: in altre parole, si fondavano sull'esperienza, la conoscenza e la strategia di esseri umani... Al contrario AlphaZero non operava sulla base di mosse, combinazioni e strategie derivanti da partite giocate da giocatori in carne e ossa. Lo stile di gioco di AlphaZero era esclusivamente il frutto dell'addestramento di un'intelligenza*

*artificiale: i suoi creatori gli avevano fornito le regole degli scacchi impartendo l'istruzione di sviluppare una strategia per ottenere il massimo numero di vittorie e ridurre quello delle sconfitte".<sup>11</sup>*

### Considerazioni Filosofiche e Sociologiche

L'AI solleva interrogativi riguardo la natura dell'intelligenza e della coscienza. Una macchina può essere dotata di coscienza o autoconsapevolezza? Può raggiungere un'intelligenza comparabile a quella umana o superarla? Queste domande stimolano dibattiti sulla definizione stessa di intelligenza e sul suo significato.

L'AI influisce sul modo in cui percepiamo e utilizziamo le capacità intellettive. L'automazione e l'AI stanno cambiando il mercato del lavoro, riducendo il bisogno di alcune competenze mentre ne creano di nuove. Inoltre, l'AI solleva questioni etiche riguardo alla privacy, al controllo e alla responsabilità, poiché le decisioni automatizzate possono avere impatti significativi sulle vite umane. Già all'alba dell'era degli home/personal computer vi fu chi, come Sherry Turkle<sup>12</sup>, cercò di capire come i computer stessero influenzando la cognizione umana e la socialità. Dai suoi studi emerse che, già 40 anni fa, la nostra tendenza a definire e descrivere l'operatore elettronico in termini di caratteristiche umane e usando termini umanizzanti (ad esempio, descrivendo i computer come "cervelli elettronici") stava spingendo verso la definizione e la descrizione degli esseri umani in termini di caratteristiche performative dei computer, con un ampio ricorso alle analogie informatiche per parlare metaforicamente di capacità e condizioni dell'essere umano.

Questo ci avverte che la diffusione culturale dell'AI in assenza di un discorso "umano" che le faccia da contraltare potrebbe avere un effetto colonizzante sulla società umana, qualcosa che trasformerebbe le metafore cui ricorriamo per parlare delle nostre società in termini tecnocratici, e quelle circa il ruolo che vi svolgiamo come individui in termini stranianti, da "ingranaggio del meccanismo".

Il sociologo Bruce Berman sostiene che discutere delle capacità umane usando metafore ispirate ai computer contribuisce a giustificare le condizioni sociali ed economiche alienanti nelle democrazie avanzate segnate da robuste componenti tecnocratiche. Mentre le narrazioni generaliste sull'AI, che ne illuminano solo gli aspetti performativi, di aumentata produttività e di iper-efficienza, possono creare nei decisori politici un'acquiescenza verso lo sviluppo tecnologico che rischia di inibire la capacità di leggere le trasformazioni del lavoro e della distribuzione del reddito che inevitabilmente s'accompagnano e s'accompagneranno alla diffusione sempre maggiore dell'Intelligenza Artificiale in

---

<sup>11</sup> H.A.Kissinger, E.Schmidt, D. Huttenlocher, *L'erA dell'Intelligenza artificiale. Il futuro dell'identità umana*. Mondadori, Milano. 2023 pag. 55

<sup>12</sup> Sherry Turkle, *Insieme ma soli*, 2019, pp 350

ogni ambito produttivo, con una sostanziale abdicazione dei soggetti democratici nei confronti dei gruppi scientifici, economici e politici che controllano la tecnologia informatica.

La diffusione di una cultura dell'Intelligenza Artificiale priva di intermediazione politica potrebbe quindi contribuire ad ampliare le diseguaglianze sociali e economiche nella società invece di attenuarle.

Rainer Mühlhoff<sup>13</sup> ha esaminato l'attività compiuta dalle deep learning machine di estrazione di dati generati dagli esseri umani. Lo studio evidenzia come questi algoritmi sfruttino regolarmente l'input di dati generati dagli utenti per il loro stesso addestramento, o per quello di altri algoritmi, e che per questo i loro progressi siano strutturalmente dipendenti dallo sfruttamento di capacità umane sostanzialmente fornite a titolo gratuito e inconsapevole.

Anche l'antropologia e le scienze della comunicazione si stanno interessando sempre di più agli aspetti culturali dell'AI quali costrutti socioculturali e linguistici, con l'obiettivo di comprendere come diversi gruppi sfruttino risorse e tradizioni culturali differenti per sviluppare narrazioni sull'AI coerenti con le rispettive agende sociali, culturali e politiche.

Eynon e Young hanno esaminato come accademici, professionisti dell'industria e responsabili politici inquadrano l'AI per fini didattico/educativi, e hanno individuato che questi gruppi esprimono interpretazioni divergenti dell'AI e tendono a definire e caratterizzarla in modi che avvantaggiano il lavoro e gli obiettivi dei rispettivi settori. Questi attori sociali e economici non solo comprendono diversamente l'Intelligenza Artificiale, ma la inquadrano con strategie differenti per influenzare come l'AI educativa debba essere utilizzata, finanziata, regolamentata e commercializzata a lungo termine.

Forse ancora più interessante è lo studio che Selma Sabanovic ha condotto sulla cultura dei robot in Giappone. La studiosa ha mostrato che, incorporando immagini popolari, valori, tradizioni culturali locali nei loro progetti, i progettisti di robotica giapponesi stanno istituendo dei fondamenti epistemologici e di profonda legittimazione sociale per i robot, suscitando un forte consenso culturale.

Questa strategia di sfruttamento delle risorse culturali per innescare un interesse sociale più ampio e l'accettazione dell'AI è stata osservata anche da altri antropologi, che esaminando la nascita e lo sviluppo dell'AI dagli anni '50 agli anni '70, hanno mostrato che inquadrare la nuova tecnologia in termini di una sorta di mito tecnologico in riedizione del mito classico di Prometeo (l'AI che "ruba" la

---

<sup>13</sup> Rainer Mühlhoff, *Intelligenza artificiale assistita dall'uomo: ovvero come eseguire calcoli complessi nel cervello umano?*  
In: *New Media & Society* - 2020

scintilla dell'intelligenza all'uomo) ha contribuito fortemente alla popolarizzazione dell'Intelligenza Artificiale nella cultura di massa, soprattutto in ambito letterario, cinematografico e televisivo.

Non si può negare la rilevanza dell'inquadramento culturale per la penetrazione dell'Intelligenza Artificiale nella cultura di massa.

Inquadramento culturale che può essere inteso, e questa è una riflessione davvero sorprendente, quale "parte socio-culturale" del design dell'AI.

Analisi scientifiche mettono in luce come i ricercatori sociali, gli utenti, i regolatori e altre parti rilevanti possano contribuire a creare un'AI socialmente benefica, sia influenzando la percezione degli sviluppatori su ciò che la rende socialmente accettabile, sia - e questo è ancora più importante - influenzando la progettazione sociale dell'AI attraverso un suo inquadramento culturale positivo, umano.

Anche nell'ambito delle scienze economiche, politiche e del diritto si è esaminato lo sviluppo dell'AI, e in particolare il suo collegamento con la rivoluzione digitale. Il testo del 2019 di Anthony Elliott, *The Culture of AI*, è fra i più rilevanti in tal senso, poiché si propone di esplorare gli impatti sociali più ampi e a lungo termine dell'AI nell'era digitale.

Lo studio di Anthony Elliott esamina i diversi ambiti socioeconomici che stanno subendo forti trasformazioni indotte dalle tecnologie dell'AI, tra cui:

- il sé e l'identità;
- la globalizzazione e deglobalizzazione dell'economia;
- l'interazione sociale;
- la mobilità;
- le politiche pubbliche.

Elliott connette lo studio specifico della sociologia dell'AI alle preoccupazioni classiche della sociologia e arriva a reimmaginare una nuova sociologia alla luce dello sviluppo dell'Intelligenza Artificiale nell'era digitale.

In linea generale, tuttavia, al netto dei brillanti contributi illustrati, rispetto alla ricerca sull'AI scientifica e quella tecnica, la ricerca su quella culturale va ancora considerata un campo emergente, per quanto assai promettente e, in prospettiva, indispensabile per lo sviluppo di una cultura umana dell'AI, contrapposta al rischio di torsioni tecnocratiche.

Lo sbaglio più grande che si può commettere di fronte alla diffusione dell'AI è considerarla alla stregua di qualsiasi altra tecnologia, per quanto evoluta. Pensare, cioè, che si tratti di uno strumento tecnologico/informatico dal carattere “neutro”, e che quindi tutte le possibili problematiche connesse al suo uso dipendano solo dalla buona o cattiva volontà di chi le utilizza.

In realtà, già l'ascesa di internet a partire dagli anni '90 ci ha mostrato che le tecnologie sono in grado di indurre trasformazioni sociologiche, linguistiche, culturali ed economiche che prescindono dalla volontà dei singoli.

Per capire meglio la vastità delle implicazioni dell'AI, partiamo dalla definizione tecnico-scientifica che ne ha dato, nel 2020, l'High Level Expert Group istituito dalla Commissione europea.

“L'Intelligenza Artificiale è un sistema (e possibilmente anche hardware) progettato da esseri umani che, assegnato un obiettivo complesso, agisce nella dimensione fisica o digitale percependo l'ambiente circostante attraverso l'acquisizione di dati, interpretando i dati raccolti, siano essi strutturati o non strutturati, ragionando sulla conoscenza o elaborando le informazioni derivate da questi dati, e decidendo le azioni migliori da intraprendere per raggiungere l'obiettivo assegnato.

I sistemi di AI possono utilizzare regole simboliche o apprendere un modello numerico e possono anche adattare il loro comportamento analizzando come l'ambiente è influenzato dalle loro azioni precedenti”.

Già questa definizione si riferisce con sufficiente chiarezza non a un mero strumento, ma a un soggetto, per quanto artificiale, in grado di intervenire sul mondo che lo circonda con ampi gradi di autonomia, le cui azioni non sono predicibili in modo integralmente deterministico.

## **1.2 Intelligenza artificiale e settore bancario**

Indubbiamente l'Intelligenza Artificiale sta rivoluzionando il mondo della finanza. Può analizzare enormi quantità di dati, prendere decisioni in frazioni di secondo, ridefinendo il modo in cui investiamo, risparmiamo e assicuriamo il nostro futuro. Una rivoluzione digitale promettente che, tuttavia, nasconde parecchie ombre: da un lato, offre strumenti potenti per prendere decisioni finanziarie più consapevoli; dall'altro, solleva interrogativi importanti.

Storicamente i modelli tradizionali di valutazione del merito creditizio si sono basati su indicatori finanziari standardizzati e su metriche statiche, come il reddito e lo storico dei pagamenti. L'AI grazie a big data e apprendimento automatico permette di elaborare un volume maggiore di informazioni

come il comportamento online o le transazioni atipiche<sup>14</sup>.

Tutto ciò solleva criticità sotto il profilo della discriminazione algoritmica. Alcuni modelli possono penalizzare categorie di soggetti già svantaggiati. Questo avviene perché l'AI, elaborando dati generati dagli esseri umani, assorbe anche i pregiudizi. Famoso è diventato il caso del sistema di machine learning per il recruitment online testato da Amazon che selezionava solo candidature maschili per ruoli da sviluppatore<sup>15</sup>. Il caso ha aperto interrogativi importanti sulla possibilità che anche gli algoritmi possano sviluppare "pregiudizi". Si rende pertanto necessario che gli input forniti alla macchina siano il più possibile liberi da preconcetti. La regolamentazione di questi strumenti risulta, pertanto, fondamentale per garantire equità e trasparenza nelle decisioni.

L'impiego di decisioni automatizzate solleva interrogativi giuridici e rende complesso rispettare l'articolo 22 del Regolamento Generale sulla Protezione dei Dati (GDPR)<sup>16</sup> che vuole garantire la piena spiegabilità delle decisioni.

Essendo in grado di analizzare in tempo reale milioni di transazioni, l'intelligenza artificiale è utilizzata dalle banche anche per prevenire e rilevare attività fraudolente. Gli algoritmi di anomaly detection individuano schemi di comportamento sospetti, permettendo di bloccare transazioni potenzialmente fraudolente prima che vengano completate<sup>17</sup>.

Oggi si sente parlare sempre più spesso di Operational Excellence.

L'Eccellenza Operativa è una visione aziendale focalizzata sull'ottimizzazione di processi, strumenti e metodologie, che unisce all'efficacia produttiva una forte spinta verso l'innovazione<sup>18</sup>. In linea con i nuovi modelli di business delle Fintech e dei principali operatori digitali, le Banche tradizionali stanno adottando delle strategie di efficienza per innovarsi e ottimizzare le attività interne.

Per esempio in Credit Agricole, dal mese di luglio 2025 è disponibile in fase pilota il nuovo processo di consulenza su servizi di investimento Robo4Advisory e Storytelling.

RoboAdvisory, intesa come servizio di consulenza finanziaria automatizzato, utilizza algoritmi e sistemi statistici per gestire i portafogli degli investitori, viene utilizzata dagli operatori per supportare

---

<sup>14</sup> Fuster et al., *Predictably Unequal? The Effects of Machine Learning on Credit Markets*, NBER, 2022, p. 5

<sup>15</sup> Federica Meta, articolo di *CorCom* 10 ottobre 2018

<sup>16</sup> L'art. 22 del GDPR prevede il diritto degli utenti a ottenere una spiegazione chiara delle decisioni automatizzate che li riguardano

<sup>17</sup> European Banking Authority, *Report on Big Data and Advanced Analytics*, 2022, p. 30

<sup>18</sup> Operational Excellence – Bonfiglioli Consulting

il segmento di clientela Mass e Affluent, costituito da risparmiatori in cerca di soluzioni di investimento precostituite ma efficaci.

La Robo4Advisor, invece, sfrutta l'utilizzo degli strumenti automatizzati per supportare l'attività del Consulente Finanziario o del Private Banker e viene utilizzata prevalentemente per ottimizzarne ed evolvere il servizio di consulenza offerto alla clientela di elevato standing che presenta esigenze più complesse e sofisticate.

Robo4Advisor è un motore di Intelligenza Artificiale tradizionale che mette a disposizione del gestore strumenti automatici atti a rendere il processo di consulenza più veloce ed efficiente grazie all'analisi massiva effettuata ogni notte che consente di individuare i clienti prioritari da contattare generando contestualmente una proposta di investimento personalizzata sulla base delle loro specifiche esigenze. Viene prodotto anche lo Storytelling, uno speech testuale che fornisce al gestore una visione chiara dei razionali sottostanti alla proposta e alla visione di mercato, utili per la discussione della consulenza insieme al cliente.

La nuova piattaforma permette di selezionare automaticamente, sulla base di criteri strategici, normativi e commerciali, i clienti che richiedono prioritariamente una consulenza su servizi di investimento. Per esempio: individuando i clienti meno conosciuti e con portafogli non adeguati o portafogli con opportunità commerciali attive. Consente, inoltre, una formulazione rapida della proposta di investimento riducendo notevolmente i tempi di analisi del portafoglio e studio della soluzione da parte del gestore. La proposta viene creata sulla base delle richieste del cliente nel pieno rispetto delle normative MIFID. Grazie a una user experience semplice la tecnologia consentirà di semplificare l'attuale processo di consulenza supportando il gestore fornendo elementi chiave per migliorare la relazione con i clienti, anche con quelli meno conosciuti!

Il mercato del RoboAdvisory sta registrando una forte crescita in tutto il mondo, con importanti asset in gestione e un numero crescente di utilizzatori. Secondo Statista<sup>19</sup>, si prevede che il mercato mondiale dei RoboAdvisor vedrà un aumento significativo del patrimonio gestito, raggiungendo oltre 2.200 miliardi di dollari entro la fine del 2027. Una simile crescita è guidata da molteplici fattori, tra cui il risparmio dei costi, lo sviluppo di un concetto di finanza democratica e una maggiore accettazione da parte del mercato.

---

<sup>19</sup> [www.statista.com/](http://www.statista.com/) Statista è una piattaforma globale di dati e business intelligence con un'ampia raccolta di statistiche, report e approfondimenti su oltre 80.000 argomenti provenienti da 22.500 fonti in 170 settori. Fondata in Germania nel 2007, Statista opera in 8 sedi in tutto il mondo e impiega circa 1.450 professionisti.

Guardando al mercato italiano, il segmento RoboAdvisory è ancora poco sviluppato anche se presenta tassi di crescita molto interessanti. Le aspettative di crescita prevedono che possa crescere a un tasso annuo del 7% da qui al 2027.

L'aumento dell'interesse per il RoboAdvisory riflette sicuramente la tendenza verso la digitalizzazione dei servizi finanziari, particolarmente ricercata dai giovani in cerca di soluzioni di investimento innovative. In considerazione di questo trend, anche banche private e family office, che sono tradizionalmente più lenti nell'adozione delle nuove tecnologie, stanno innovando la Value Proposition per rimanere competitivi. Alcuni lo fanno acquisendo piattaforme di RoboAdvisory, altri optando per soluzioni ibride che integrano la consulenza tradizionale con strumenti digitali, mantenendo il consulente al centro del processo, assistito da tecnologie avanzate per l'analisi e la gestione degli investimenti.

L'intelligenza artificiale in questo si configura come un acceleratore, offrendo un supporto agli utenti nell'automatizzazione delle attività, con una riduzione di costi, tempi e rischi, e aprendo a nuove opportunità. Infatti, secondo uno studio di Deloitte, pubblicato nel 2023, che investiga i principali trend in ambito Wealth Management attualmente ben il 44% delle Banche si propone di contenere i costi operativi nei prossimi tre anni grazie all'adozione di innovazioni digitali.

Tra le aree del settore bancario maggiormente impattate dall'innovazione digitale vi sono la Direzione Operativa, il Dipartimento di Information Technology, le Funzioni di Controllo e tra queste Legale, Risk Management e Compliance, l'Audit, i Servizi di Assistenza e Supporto interno o esterno alla clientela.

Secondo lo studio di Deloitte, oggi:

- il 37% dei player utilizza l'AI per la gestione del rischio e della cybersecurity
- il 32% per le attività di prevenzione, scouting e identificazione delle frodi
- il 31% per il monitoraggio e l'analisi della clientela
- abbiamo poi un 20% per le attività di pianificazione strategica e finanziaria
- e solo il 18% dei player utilizza l'AI per semplificare le attività dei consulenti finanziari e meno del 10% per il supporto alle vendite, lo sviluppo del prodotto, i processi di back-office e l'analisi di scenari. Tuttavia, entro il 2027 si prevede che l'AI svolgerà un ruolo significativo anche in queste aree.

Con l'AI sono realizzabili soluzioni avanzate di lettura e processing dati e documenti attraverso le funzionalità di estrazione metadati, classificazione degli argomenti, sintesi dei contenuti e analisi delle serie storiche.

Molti istituti bancari italiani, infatti, si avvalgono già dell'Intelligenza Artificiale per snellire il processo di analisi dei tre principali documenti delle pratiche di mutuo: delibera, perizia e relazione notarile preliminare. Un passo significativo verso la trasformazione digitale, volto a migliorare l'efficienza operativa, la qualità del servizio e i tempi di risposta al cliente. L'iniziativa nasce con l'obiettivo di ottimizzare i processi più ripetitivi legati alla gestione dei mutui, attraverso soluzioni intelligenti capaci di interpretare i documenti e validare informazioni in tempo reale.

Questi sistemi sono capaci di fornire ai consulenti e agli utenti Banca, gli strumenti di supporto alle operazioni quotidiane con un servizio di assistenza informativa e in alcuni casi esecutiva, disponibile 24/7.

Credit Agricole, per esempio, ha avviato il Progetto di Digitalizzazione dei Processi Creditizi, focalizzandosi sull'automazione e digitalizzazione dei processi nel mondo credito retail e small business. L'obiettivo principale è migliorare l'efficienza, ridurre la manualità e il rischio operativo, accelerando il processo decisionale.

Il progetto si articola in tre fasi distinte, ognuna con specifici obiettivi tecnologici e operativi.

La Fase 1 prevede lo sviluppo di un tool che, mediante l'utilizzo di tecnologie di OCR (Riconoscimento Ottico dei Caratteri) e Machine Learning, automatizzerà la lettura dei documenti reddituali delle persone fisiche (siano essi richiedenti o garanti) consentendo la compilazione automatica dei relativi campi in PEF (Piattaforma di Istruttoria Fido), riducendo così il bisogno di intervento manuale da parte degli operatori di filiale e il relativo rischio di errori.

La Fase 2 si concentra sullo sviluppo di un algoritmo di pre-delibera che supporterà i deliberanti nel processo decisionale per il segmento POE/Affari, fornendo un'indicazione preliminare corredata dalle informazioni che hanno prevalentemente impattato sulla formulazione della decisione finale. Tra i vantaggi rientrano il supporto alle concessioni di credito e l'ottimizzazione dei tempi.

Infine, la Fase 3 esplora l'acquisizione dei dati dal cassetto fiscale del cliente per identificare nuovi casi d'uso e migliorare la predittività dei processi decisionali.

Il progetto rappresenta, dunque, una parte fondamentale della strategia di digitalizzazione dei processi e segna un passo rilevante verso l'ottimizzazione delle attività di delibera del credito. Non si

ridurranno solo i tempi di gestione, ma anche i rischi legati agli errori manuali, migliorando nel contempo l'efficienza complessiva del lavoro.

Nell'ambito delle funzionalità AI dedicate al supporto operativo, molti investimenti riguardano l'implementazione di assistenti virtuali o chatbot interni.

Il Virtual Network Assistant sfrutta le avanzate capacità di Natural Language Processing (NLP) per interagire in modo efficace con i consulenti o gli utenti banca, offrendo assistenza informativa e, in certi casi, anche esecutiva, disponibile 24 ore su 24.

Questo approccio permette di migliorare l'accessibilità alle informazioni contenute nei documenti bancari interni come procedure o normative, in una nuova logica dialogica semplice e intuitiva.

Morgan Stanley ha adottato un nuovo assistente virtuale basato su AI generativa chiamato «AI @ Morgan Stanley Assistant». Questo strumento consente ai consulenti finanziari e al personale di supporto di accedere a oltre 100.000 rapporti e documenti di ricerca con l'obiettivo di risparmiare tempo su attività amministrative e di ricerca riguardanti domande sui mercati, processi interni e raccomandazioni.

Per i consulenti il maggiore vantaggio dell'uso di chatbot virtuali è la disponibilità 24/7 e la possibilità di una interazione semplificata.

#### Evoluzione e logiche del servizio

Se da un lato le banche stanno traendo benefici tangibili dall'implementazione di sistemi innovativi basati sull'intelligenza artificiale, dall'altro i benefici sono sempre di più anche per il cliente finale, con un impatto differenziato per ciascun segmento di clientela.

Nel Wealth Management dedicato ai clienti ad alto valore (come gli High-Net-Worth Individuals), per esempio, l'Artificial Intelligence non sta disintermediando la relazione tra gestore e cliente, ma permette piuttosto di evolvere il livello di servizio offerto. Un esempio concreto di offerta custom resa possibile tramite l'Artificial Intelligence è la Dynamic Asset Allocation, pensata per l'investitore che vuole ottimizzare il proprio portafoglio a fronte delle fluttuazioni di mercato. La soluzione effettua le attività di monitoraggio e analisi continua delle condizioni di mercato, apportando modifiche in tempo reale al portafoglio di investimenti per massimizzare i rendimenti, adattandosi alle esigenze personalizzate del cliente. Naturalmente, le esigenze cambiano da cliente a cliente. Le famiglie Wealth richiedono sempre di più soluzioni di investimento per proteggere il proprio patrimonio; mentre imprenditori e titolari di aziende mostrano necessità finanziarie personali e aziendali spesso

interconnesse. L'intelligenza artificiale è in grado di offrire una risposta personalizzata per singola esigenza anche su larga scala, e questo sicuramente rappresenta uno dei suoi punti vincenti. Secondo stime recenti sull'evoluzione della ricchezza demografica<sup>20</sup>, più di 15 trilioni di dollari di ricchezza a livello globale verranno trasferiti dalle Silent Generation (nati tra il 1928 e il 1945) alle generazioni più giovani entro il 2030. In particolare, diventeranno sempre più rilevanti nei prossimi anni le generazioni X (nati tra il 1965 e il 1979), Y/Millennials (1980-1994) e Z (dal 1995).

Aspettative simili si applicano anche allo scenario italiano del Private Banking che oggi gestisce oltre 1.000 miliardi di euro e riguarda contemporaneamente diverse generazioni di clienti con pesi molto diversi tra loro. Gli over 65 detengono oltre il 50% della ricchezza gestita, una quota di mercato nettamente superiore rispetto a quella attualmente nelle mani degli under 55 (in totale pari circa al 20% e di cui l'11% è detenuta da coloro che hanno una età compresa tra i 45 e i 55 anni). Nei prossimi anni, tuttavia, l'industria italiana assisterà a ingenti passaggi di ricchezza da parte dell'attuale generazione di clienti (over 65) verso le successive. In particolare, entro la fine di quest'anno si prevede che 22 miliardi di euro passeranno alle generazioni più giovani, cifra che è destinata a salire a 180 miliardi di euro entro il 2028 e a 300 miliardi di euro entro il 2033. Di conseguenza, l'attenzione degli operatori del Private Banking nei prossimi tre anni è destinata a spostarsi in modo significativo verso i segmenti di clientela più giovane, come Millennials e Generazione Z. Questi ultimi, dunque, saranno i protagonisti della crescita maggiore, rispettivamente pari a +13% e +24% se paragonati alla Generazione X. Gli altri segmenti di clientela resteranno stabili o, in modo inverso rispetto a quello che accadrà alle generazioni più giovani, si ridurranno progressivamente nel tempo.

Gli investitori più giovani hanno aspettative diverse rispetto agli investitori senior: sono più aperti all'utilizzo di strumenti innovativi quali l'intelligenza artificiale, più attenti alla tutela della propria privacy e alla sicurezza dei dati condivisi. Tale evoluzione demografica impone quindi cambiamenti su larga scala in tutto il settore.

In particolare, secondo lo studio Deloitte Global Wealth Megatrends, oltre il 75% degli investitori a livello globale si aspetta delle esperienze digitali in linea con quelle offerte dalle aziende native digitali, tanto che oltre il 50% del campione prenderebbe in considerazione l'idea di investire tramite fintech o Banche Digitali.

I cambiamenti della base clienti e i trasferimenti di ricchezza in atto determinano nuovi bisogni. In particolare, il passaggio di ricchezza determina la ricerca di un servizio di consulenza olistica multigenerazionale, il cui obiettivo principale sarà quello di fornire supporto alle esigenze dell'intero

---

<sup>20</sup> Guido Bolaffi, Nel mondo cambia la distribuzione della ricchezza, Fondazione Med-Or, settembre 2023

nucleo familiare del cliente. Un consulente finanziario che adotta questo approccio lavora infatti con più membri della stessa famiglia, appartenenti a generazioni diverse, per sviluppare una strategia finanziaria che tenga conto nel complesso delle esigenze immediate e a lungo termine di tutti i membri della famiglia. Questo tipo di consulenza tende a essere più complessa e coinvolge la gestione di vari aspetti finanziari, come investimenti, piani pensionistici, pianificazione fiscale, ma anche pianificazione patrimoniale e successoria.

La combinazione di fattori demografici, tecnologici, economici e culturali porta all'aumento del peso di segmenti di clientela relativamente nuovi, come le donne (che oggi detengono circa al 30% della ricchezza Private), i nativi digitali e le nuove generazioni, che impongono di ripensare i modelli di servizio in logica sempre più personalizzata in base al profilo del cliente (età, contesto di riferimento, tipologia di cliente). Occorre essere flessibili e innovativi nel rispondere alle esigenze mutevoli dei clienti, così da rimanere competitivi e rilevanti nel mercato.

### **1.3 Cybercrime finanziario, dati e stime**

Il cybercrime finanziario continua a evolversi, dominato da gruppi internazionali ben strutturati e organizzati. Per alcuni anni il settore finanziario è stato il più attaccato a livello mondiale, alternando recentemente il podio con il settore manifatturiero. Anche limitando l'analisi alla sola Europa, è stato il settore finanziario il più attaccato nel corso del 2022, con l'Italia che ha attratto circa l'8% degli attacchi verso l'Europa, dietro Regno Unito, Germania e Portogallo<sup>21</sup>.

Il financial fraud, frode bancaria o finanziaria, passa quasi sempre attraverso il furto delle credenziali d'accesso ai sistemi bancari o di pagamento, e riutilizzate per transazioni fraudolente all'insaputa del titolare. Invece di attaccare direttamente l'istituzione finanziaria si preferisce attaccarne i clienti in quanto obiettivo indubbiamente più permeabile.

La frode avviene prevalentemente attraverso i seguenti vettori:

- phishing per il furto iniziale di credenziali di accesso (credential theft) oppure di altri dati personali (telefono, codice fiscale, e-mail) sempre combinata con una successiva interazione con un finto operatore per il furto dei fattori mancanti, ad esempio i fattori di autenticazione forte o codici dispositivi;
- malware per il furto di credenziali o fattori addizionali di autenticazione o manipolazione di una transazione;
- manipolazione dell'utente, ad esempio convincendolo a recarsi allo sportello e fare un'operazione dispositiva;
- hacking del dispositivo mobile tramite SIM Swap, emulazione software dello smartphone;

---

<sup>21</sup> Pier Luigi Rotondo, Elementi sul cybercrime nel settore finanziario in Europa, Rapporto Clusit 2024, pag 127

- e infine, ma in misura inferiore, con l'attacco diretto all'infrastruttura dell'istituzione finanziaria sfruttando vulnerabilità spesso note ma ancora non fissate.

La tecnica, o la combinazione di tecniche, varia in base alla tipologia di vittima, con differenze tra il cliente finale (retail) oppure aziendale (corporate) che vanno ad affievolirsi nel corso degli anni.

Limitandosi al settore finanziario italiano, in tutto il 2023 è stata osservata una media di circa 3,6 nuove pagine di phishing al giorno attivate e perfettamente funzionanti.

Il 43% di questi siti di phishing è stato ospitato negli Stati Uniti. Provider Italiani hanno ospitato il 6% delle pagine di phishing, un valore quasi dimezzato rispetto all'anno precedente nel quale era stato dell'11%.

Una delle novità recenti del panorama phishing verso l'Italia è che circa una pagina su cinque è ospitata su Amazon.

Un dato che deve farci riflettere è che ormai il 99,5% delle URL di phishing usa il protocollo HTTPS, il cosiddetto HTTP "sicuro" che quindi non è più un'indicazione sull'affidabilità o meno del sito.

Il phishing verso il settore finanziario italiano è veicolato principalmente tramite e-mail e SMS. In generale il phishing finanziario mira al furto delle credenziali di accesso, come il codice cliente in tutte le sue denominazioni, la password o PIN, e la OTP di accesso e tutti i suoi equivalenti, ma anche altre informazioni utili a rendere più facile un accesso fraudolento, come numero di telefono dell'utente, il codice fiscale e l'indirizzo e-mail. Ogni informazione, anche quella apparentemente meno critica, può essere utile quando combinata con altre, per mettere a punto uno schema di attacco ripetibile su più utenti. La frode è normalmente realizzata attraverso una sequenza di passi successivi, non necessariamente tutti nella stessa sessione, in ciascuno dei quali vengono rubate solo alcune credenziali, o altre informazioni, per poi ricomporre tutto assieme per perpetrare l'accesso fraudolento.

Il semplice furto delle credenziali di accesso, intese come nome utente e password, da solo non basta a portare a termine un attacco ad un sistema finanziario. La direttiva europea PSD2 [19] ha introdotto dal 2019 l'utilizzo di un ulteriore fattore di autenticazione forte del cliente (SCA – Strong Customer Authentication), spesso nella forma di una OTP (One Time Password – Password valida solo 1 volta) inviata via SMS o generati da una App, da reinserire in un form per verificare l'utente e completare l'autenticazione. Questi meccanismi sono anche noti come MFA – Multi-Factor Authentication, o autenticazione a più fattori. La cattiva notizia è che ben presto la Multi-Factor Authentication è diventata a sua volta vittima di phishing o social engineering. All'atto pratico, lo strumento messo a punto per scongiurare il furto delle credenziali, si è dimostrato vulnerabile allo stesso tipo di attacco. Anzi, tutte le frodi che hanno successo, e sono molte, sono riuscite a aggirare la protezione introdotta dalla Multi-Factor Authentication.

Da tenere monitorato l'utilizzo che la comunità dei cyber criminali ha iniziato a fare della AI per selezionare i target, scansionarli per trovare falle (es. vulnerabilità note), analizzare il codice per trovare nuove vulnerabilità (es. 0 day) e produrre contenuti per phishing o codice per malware. Questo è un trend in rapida ascesa di cui sarà possibile osservare gli effetti solo in un prossimo futuro<sup>22</sup>.

La situazione nazionale è preoccupante se confrontata, in termini di percentuali di crescita, rispetto al dato globale: all'aumento del 65% segnato dagli attacchi italiani nel 2023, corrisponde infatti un molto più contenuto +12% complessivo. Gli attacchi in Italia stanno quindi crescendo a un ritmo singolarmente elevato che può essere indice tanto di una tendenza da parte dei cybercriminali a bersagliare in particolare vittime italiane, quanto più probabilmente di una scarsa capacità delle stesse di proteggersi in maniera adeguata: un dato particolarmente grave, se si considera che gli investimenti in sicurezza in Italia continuano a crescere, come riscontrato dall'Osservatorio Cybersecurity e Data Protection del Politecnico di Milano<sup>23</sup>.

Il tema della Cybersecurity va quindi oggi declinato con un focus importante sul dato, sull'uso che se ne fa, sulla sua produzione, condivisione e conservazione e, non da ultimo, della sua protezione. Il dato, infatti, è l'oro nel nuovo ordine mondiale affermatosi con l'avvento della Società dell'Informazione, in cui la capacità di elaborare e trasmettere informazioni digitalizzate è diventata il fattore chiave per lo sviluppo economico, sociale e culturale<sup>24</sup>.

La data governance non è più una mera pratica aziendale, ma il baluardo cruciale contro le tempeste digitali, un faro che guida attraverso i flutti pericolosi della cybersicurezza, assicurando la continuità operativa e la fiducia dei soggetti coinvolti; più spesso di quanto immaginiamo anche la vita delle persone<sup>25</sup>.

## Prevenzione dei rischi

Secondo il rapporto 2024 del Clusit (Associazione Italiana per la sicurezza informatica), nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, che oggi rappresenta oltre 700 organizzazioni, appartenenti a tutti i settori del Sistema-Paese, il 47% delle aziende è stata vittima di reati finanziari negli ultimi 12 mesi e questi tipi di reati risultano interconnessi e non sempre scindibili. In particolare, possono essere identificati cinque principali reati finanziari: frode, corruzione, riciclaggio, furto di identità e cybercrime.

---

<sup>22</sup> Rapporto 2024 sulla Sicurezza ICT in Italia

<sup>23</sup> Lo scenario della cybersecurity in Italia nel 2023 - POLIMI

<sup>24</sup> Società dell'informazione - Wikipedia

<sup>25</sup> Patrizio Rinaldi, Strategie di data security nell'era dell'AI Generativa, Rapporto Clusit 2024, pag 298

1. La frode può essere descritta come un comportamento volto a ottenere un vantaggio economico attraverso pratiche ingannevoli, spesso a danno di altri soggetti. Essa può assumere forme diverse, tra cui frodi fiscali, bancarie o digitali, a seconda del contesto in cui si manifesta. I tipi di frode includono la frode fiscale, la frode con carta di credito, la frode telematica, la frode sui titoli, la frode fallimentare, assicurativa e bancaria.

20 miliardi di dollari è il fatturato globale medio delle aziende colpite e 0,5 miliardi di dollari è la cifra di fatturato medio perso (pari al 3% circa).

2. La corruzione si articola in una serie di comportamenti tra loro diversificati come il dare o accettare tangenti e regali inappropriati, le transazioni non tracciate, la manipolazione dei dati, il dirottamento di fondi e il riciclaggio di denaro.

25,3 miliardi di dollari è il fatturato globale medio delle aziende colpite e 0,81 miliardi di dollari è la cifra di fatturato medio perso (pari al 3% circa).

3. Il riciclaggio di denaro è il processo illegale attraverso il quale grandi quantità di denaro generate da attività criminali sembrano provenire da una fonte legittima.

25,1 miliardi di dollari è il fatturato globale medio delle aziende colpite e 0,75 miliardi di dollari è la cifra di fatturato medio perso (pari al 3% circa).

4. Il furto di identità viene commesso in molti modi diversi e le sue vittime in genere subiscono danni al credito, alle finanze e alla reputazione.

20,3 miliardi è il fatturato globale medio delle aziende colpite e 0,47 miliardi di dollari è la cifra di fatturato medio perso (pari al 2% circa).

5. Infine, il cybercrime fa leva sull'uso di un computer come strumento per fini illegali, come ad esempio commettere frodi, traffico di proprietà intellettuale, furto di identità o violazione della privacy.

21,6 miliardi è il fatturato globale medio delle aziende colpite e 0,5 miliardi di dollari è la cifra di fatturato medio (2% circa).

La gestione del rischio tradizionale deve essere integrata per far fronte all'evoluzione e allo sviluppo di sistemi sempre più sofisticati e potenti, anche grazie al ricorso all'intelligenza artificiale. Le aziende faticano infatti ad adottare soluzioni antifrode adatte alla natura dinamica dei rischi moderni. Le soluzioni antifrode avanguardistiche richiedono investimenti significativi in termini di denaro, risorse umane e tempo, inoltre l'integrazione di nuove soluzioni potrebbe essere complessa a livello tecnico, specialmente se richiede modifiche ai sistemi e ai processi esistenti dell'organizzazione. Anche il numero di risorse in grado di gestire e affrontare nel modo corretto le diverse forme di rischio è sempre inferiore rispetto alle esigenze dichiarate. Infine, la mancanza di consenso da parte della leadership è un altro fattore limitante. Questo perché il costo reale delle frodi va oltre le perdite di

fatturato e ha un impatto profondo sui pilastri fondamentali della funzionalità aziendale, come l'efficienza operativa, la conformità, l'esperienza del cliente.

L'utilizzo dell'intelligenza artificiale nei sistemi di controllo consente di individuare anomalie e schemi ricorrenti con un livello di precisione difficilmente raggiungibile attraverso metodi tradizionali. Questo permette alle imprese di intervenire in modo più tempestivo nella prevenzione delle frodi.

A inizio 2024 è stata condotta una indagine internazionale da ACFE in collaborazione con Sasche e pubblicata con il titolo di "AntiFraud Technology Benchmarking Report" dalla quale è emerso che il 59% delle aziende prevede di incrementare il budget per lo sviluppo di nuovi sistemi antifrode. In futuro, è probabile che i temi relativi alla biometria fisica, all'analisi della visione artificiale, alla robotica e alla biometria comportamentale diventino sempre più rilevanti e diffusi all'interno dei sistemi antifrode, interessando una buona parte del mercato. Sfruttando la potenza dell'intelligenza artificiale, le aziende possono dunque adattare le strategie di gestione del rischio ai singoli clienti con una precisione senza pari. Attraverso sofisticati algoritmi, i modelli di AI analizzano vasti set di dati per identificare sottili deviazioni dal comportamento normale, consentendo un intervento proattivo prima che le minacce si intensifichino.

I modelli di prevenzione delle frodi basati sull'intelligenza artificiale, sfruttando tecniche di analisi avanzate e apprendimento automatico, svolgono un ruolo fondamentale nel contenere le minacce di frode nel panorama digitale odierno e consentono alle aziende di rilevare e prevenire le frodi in modo più efficace, riducendo al minimo i falsi positivi e ottimizzando la user experience.

#### **1.4 Profili giuridici della regolamentazione dell'AI nel settore bancario**

La crescente diffusione dell'intelligenza artificiale nel settore bancario ha reso necessario un intervento normativo volto a disciplinarne l'utilizzo. In ambito europeo, tale esigenza ha trovato risposta nell'introduzione dell'AI Act da parte della Commissione Europea, che propone una classificazione dei sistemi di intelligenza artificiale basata sul livello di rischio.<sup>26</sup>

- Le applicazioni in ambito finanziario sono generalmente considerate ad alto rischio, con conseguente previsione di obblighi più stringenti in termini di trasparenza, sicurezza e controllo. L'obiettivo della normativa è duplice: da un lato, garantire un utilizzo affidabile delle tecnologie; dall'altro, favorire l'innovazione riducendo gli oneri eccessivi per le imprese, in particolare per le piccole e medie realtà.

---

<sup>26</sup> Commissione Europea, *Proposal for a Regulation Laying Down Harmonized Rules on AI*, 2021, art. 5

- Il quadro normativo europeo individua alcune aree di intervento prioritarie, tra cui il divieto di pratiche particolarmente invasive, la regolamentazione dell'uso dei dati biometrici, l'introduzione di requisiti specifici per sistemi ad alto impatto e la promozione di ambienti di sperimentazione controllata (sandbox) per lo sviluppo di nuove soluzioni.

Parallelamente, l'Autorità Bancaria Europea ha evidenziato la necessità di garantire equità e non discriminazione nei processi decisionali automatizzati, soprattutto nell'ambito della concessione del credito. Il rischio di distorsioni nei modelli algoritmici rappresenta infatti una delle principali criticità legate all'impiego dell'intelligenza artificiale.<sup>27</sup>

Le decisioni automatizzate possono riflettere bias presenti nei dati utilizzati per l'addestramento, con possibili effetti discriminatori nei confronti di determinate categorie di soggetti. In ambito creditizio, ciò può tradursi in un accesso diseguale ai finanziamenti, penalizzando in particolare individui con profili non standardizzati o appartenenti a gruppi socioeconomici più vulnerabili.<sup>28</sup>

La distorsione dei giudizi nei processi decisionali è uno dei temi caldi quando si parla dell'utilizzo dell'Intelligenza Artificiale, nonché una delle sue principali problematiche. Inevitabilmente, il discorso coinvolge anche le valutazioni in merito all'opportunità di concedere o meno mutui o opportunità di credito. Storicamente la possibilità di ottenere una casa di proprietà è stata spesso influenzata da fattori come razza, etnia e altri pregiudizi, con o senza processi decisionali automatizzati. Anche in Europa, recenti ricerche hanno evidenziato come la riduzione della disuguaglianza razziale nella concessione dei mutui finalizzati all'acquisto di immobili sia lenta, squilibrata e fragile. In particolare, i fenomeni degli ultimi anni come la grande crisi economica iniziata nel 2008 e la pandemia Covid-19, hanno ridotto i tassi di proprietà immobiliare ottenuta tramite la concessione di finanziamenti per l'acquisto della casa tra le minoranze. In sostanza, gli algoritmi distorcono il processo decisionale automatizzato a svantaggio dei gruppi a basso reddito e delle minoranze.

Molti non riescono a ottenere crediti perché non rientrano nella casistica standardizzata prevista dagli algoritmi finanziari, e ciò porta inevitabilmente a soffermarsi sul fatto che nella vita reale esistono

---

<sup>27</sup> L'Autorità bancaria europea (ABE) è un'autorità indipendente dell'Unione europea (UE), che opera per assicurare un livello di regolamentazione e di vigilanza prudenziale efficace e uniforme nel settore bancario europeo. Gli obiettivi generali dell'Autorità sono assicurare la stabilità finanziaria nell'UE e garantire l'integrità, l'efficienza e il regolare funzionamento del settore bancario.

<sup>28</sup> Andrea Benedetti, Agenda Digitale 2020

<https://www.agendadigitale.eu/cultura-digitale/ai-e-finanza-tra-discriminazioni-e-imprecisioni-rischi-e-contromisure/>

situazioni particolari che solo una mente umana, dotata della capacità di individuare tante sfaccettature e di buon senso, può valutare correttamente<sup>29</sup>.

Quando l'algoritmo comprime una serie di dati socioeconomici, come la storia lavorativa, i dati finanziari e le abitudini di acquisto, li traduce in un unico numero. Questo unico numero dipende dalla quantità e dalla qualità dei dati utilizzati, e porta addirittura a decisioni che coinvolgono non solo le domande di prestito, ma anzi, il credit score viene utilizzato anche per prendere molte decisioni che cambiano la vita, comprese quelle su assicurazione, assunzione e alloggio.

Risolvere il problema non sarà facile. Un'opzione a breve termine potrebbe essere che i governi spingano i finanziatori ad accettare il rischio di emettere prestiti ai richiedenti appartenenti a una minoranza che vengono respinti dai loro algoritmi. Ciò consentirebbe ai finanziatori di iniziare quantomeno a raccogliere dati accurati su questi gruppi per la prima volta, il che andrebbe a beneficio sia dei richiedenti che dei finanziatori nel lungo periodo. Alcuni istituti di credito più piccoli stanno già iniziando a farlo, ma senza l'intervento dei maggiori attori del settore è difficile modificare le tendenze ed evitare che a causa della sfiducia nei confronti degli istituti bancari, alcuni utenti si affidino a soggetti poco raccomandabili, non inclini a trattare eventuali posticipazioni dei pagamenti e con tassi d'interesse elevatissimi.

Dal punto di vista della responsabilità giuridica, uno degli aspetti più complessi riguarda l'attribuzione delle responsabilità in caso di errori algoritmici o discriminazioni nei modelli di AI. Attualmente, il dibattito giuridico è orientato verso una maggiore responsabilizzazione delle banche nell'uso etico e conforme delle tecnologie intelligenti. Inoltre, il principio di **auditability** suggerisce l'adozione di strumenti di controllo interno per garantire l'aderenza agli standard normativi.

Tra le regolamentazioni più rilevanti in questo ambito, possiamo citare<sup>30</sup>:

- il Regolamento Generale sulla Protezione dei Dati (GDPR), entrato in vigore nell'Unione Europea nel 2018, che stabilisce principi e obblighi per il trattamento dei dati personali, come la liceità, la trasparenza, la limitazione della finalità, la minimizzazione dei dati, l'esattezza, la limitazione della conservazione, l'integrità, la riservatezza, la responsabilizzazione, il consenso, il diritto di accesso, il diritto di rettifica, il diritto all'oblio, il diritto alla portabilità, il diritto di opposizione, il diritto alla limitazione del trattamento, il diritto di non essere sottoposti a decisioni automatizzate, ecc. Il GDPR

---

<sup>29</sup> Andrea Benedetti, Agenda Digitale 2020

<https://www.agendadigitale.eu/cultura-digitale/ai-e-finanza-tra-discriminazioni-e-imprecisioni-rischi-e-contromisure/>

<sup>30</sup> Patrizio Rinaldi, *Strategie di data security nell'era dell'AI Generativa*, Rapporto Clusit 2024, pag 299

prevede anche sanzioni severe per le violazioni, che possono arrivare fino al 4% del fatturato annuo globale o a 20 milioni di euro, a seconda del caso più grave;

- la Convenzione di Budapest sulla criminalità informatica, entrata in vigore nel 2004, che è il primo trattato internazionale che definisce e sanziona i reati informatici, come l'accesso illecito, l'intercettazione illecita, l'interferenza con i dati, l'interferenza con i sistemi, l'abuso di dispositivi, la falsificazione informatica, la frode informatica, la pornografia infantile, le violazioni della proprietà intellettuale, ecc. La Convenzione di Budapest prevede anche la cooperazione tra le parti contraenti per la prevenzione, l'investigazione e la persecuzione dei reati informatici, attraverso lo scambio di informazioni, l'assistenza reciproca, l'estradizione, ecc.;
- l'European Data Strategy, che punta a far dell'Unione Europea un punto di riferimento di società basata sui dati, creando un mercato unico per consentire il libero flusso dei dati tra settori e Stati membri. L'accesso e l'utilizzo dei dati sono fondamentali per stimolare l'innovazione e la crescita, con benefici tangibili come la medicina personalizzata, una migliore mobilità e politiche più efficaci. Il Data Governance Act facilita la condivisione dei dati e mira a generare valore per la società, garantendo allo stesso tempo il controllo ai cittadini e la fiducia alle aziende.
- il Digital Operational Resilience Act (DORA), entrato in vigore nell'Unione Europea nel 2023, che stabilisce standard e requisiti per la gestione e la mitigazione dei rischi informatici e di sicurezza per il settore finanziario, come il risk management, il testing, il reporting, l'oversight, ecc. Il DORA si applica a 20 tipi diversi di entità finanziarie e a fornitori di servizi informatici di terze parti critici e prevede sanzioni per le violazioni, che possono arrivare fino al 2% del fatturato annuo globale o a 10 milioni di euro, nei casi più gravi.

Nel settore finanziario, il sistema di Screening Regulatory Agenda si occupa di analizzare l'agenda regolamentare per valutare l'impatto delle nuove disposizioni normative. Questo è fondamentale per garantire che le istituzioni finanziarie siano conformi alle normative vigenti e per pianificare eventuali adeguamenti strategici. Questo sistema, che si avvale dell'intelligenza artificiale tradizionale per affinare lo screening e l'analisi dell'agenda regolamentare, offre una panoramica dettagliata e aggiornata, dotando le istituzioni finanziarie degli strumenti necessari per interpretare con precisione le nuove norme e per adattarsi proattivamente ai cambiamenti in atto. Una soluzione che assicura alle banche una comprensione immediata e approfondita delle evoluzioni regolamentari, agevolando l'interpretazione delle implicazioni. Il sistema di allerta in tempo reale e l'accesso a un repository personalizzato aumentano l'efficienza nel monitoraggio delle novità legislative, garantendo che

nessun aggiornamento di rilevanza passi inosservato. La possibilità di visualizzare dinamicamente i contenuti normativi e di analizzare l'impatto potenziale consente di pianificare in modo proattivo le azioni di adeguamento, riducendo i rischi di non conformità.

Il quadro istituzionale e normativo nel quale si inserisce il ricorso a modelli di AI/ML per il credit scoring da parte degli intermediari<sup>31</sup> rileva sia la normativa prudenziale sia quella di tutela della clientela, inclusa quella più generale di tutela della riservatezza dei dati. Sono inoltre riportati i principali orientamenti emersi nei consessi internazionali e nazionali sull'applicazione di tecniche di AI/ML al credit scoring.

Nel quadro della normativa prudenziale vigente non si rinvengono disposizioni specificamente dedicate all'impiego di tecniche di intelligenza artificiale o di machine learning, né risultano previste limitazioni esplicite al loro utilizzo. Tuttavia, i principi generali stabiliti dalla disciplina mantengono piena validità a prescindere dalle metodologie adottate dagli intermediari per la costruzione dei modelli di valutazione.

Con riferimento al rischio di credito, il sistema regolamentare si fonda innanzitutto sulle disposizioni in materia di governo societario, controlli interni e gestione dei rischi, le quali delineano i criteri necessari a garantire l'efficacia e l'affidabilità dei processi decisionali. Nell'ambito dell'attività di concessione del credito, gli intermediari sono tenuti, in fase istruttoria, a raccogliere un insieme adeguato e completo di informazioni, funzionali alla valutazione del merito creditizio, anche mediante l'impiego di sistemi di scoring o rating.

Banca d'Italia sottolinea che i modelli utilizzati devono essere in grado di fornire una rappresentazione sufficientemente dettagliata e attendibile del grado di affidabilità del cliente, assicurando così la coerenza e la solidità delle decisioni adottate.<sup>32</sup>

Un quadro normativo più articolato e prescrittivo è invece definito per gli intermediari che chiedono all'autorità di Vigilanza l'autorizzazione all'utilizzo per il calcolo dei requisiti patrimoniali dei modelli interni per la misurazione del rischio di credito.

Le relative prescrizioni, per quanto non vincolanti per modelli che non sono destinati al calcolo dei requisiti patrimoniali, possono rappresentare comunque un utile riferimento per individuare migliori prassi da seguire anche per lo sviluppo e la gestione dei modelli di AI/ML. Tra le prescrizioni che hanno una valenza più diretta in relazione alle caratteristiche dei modelli di ML si segnala l'esigenza

---

<sup>31</sup> Emilia Bonaccorsi di Patti, Filippo Calabresi, Biagio De Varti, Fabrizio Federico, Massimiliano Affinito, Marco Antolini, Francesco Lorizzo, Sabina Marchetti, Ilaria Masiani, Mirko Moscatelli, Francesco Privitera e Giovanni Rinna - *Intelligenza artificiale nel credit scoring. Analisi di alcune esperienze nel sistema finanziario italiano* - Occasional Papers Banca d'Italia - Numero 721 – Ottobre 2022

<sup>32</sup> Circ. 285 e 288 della Banca d'Italia

che l'intermediario disponga di “un processo per vagliare i dati immessi nel modello di previsione che contempli una valutazione dell'accuratezza, completezza e pertinenza dei dati” (art. 174 CRR). Di rilievo anche il richiamo all'esigenza che l'intermediario combini “il modello statistico con la valutazione e la revisione umana in modo da verificare le assegnazioni effettuate in base al modello e da assicurare che i modelli siano utilizzati in modo appropriato”. L'intento è che l'intermediario sia in condizioni di scoprire e limitare gli errori derivanti da carenze del modello.

In relazione alla tematica dei dati, è rilevante quanto si richiede in tema di documentazione dei sistemi di rating (art. 175 CRR): la stessa deve in ogni caso assicurare “una descrizione dettagliata della teoria, delle ipotesi e delle basi matematiche ed empiriche su cui si fonda l'assegnazione delle stime a classi, singoli debitori, esposizioni o aggregati, nonché le fonti dei dati, una o più, utilizzate per costruire il modello”.

Con riferimento alla tematica dei modelli forniti da terze parti si ribadisce poi l'esigenza che i principi relativi alla documentazione dei sistemi di rating siano in ogni caso soddisfatti anche ove il fornitore “rifiuti o limiti l'accesso dell'ente ad informazioni relative alla metodologia di tale sistema di rating o modello, o ai dati di base utilizzati per elaborare tale metodologia o modello, vantando un diritto di proprietà su tali informazioni”.

Nel Testo Unico Bancario e nelle disposizioni di trasparenza sono contenuti dei riferimenti generali alla discriminazione che, pur limitati ai temi dell'accesso ai servizi di pagamento, introducono una definizione di ciò che può essere reputato discriminatorio nel contesto bancario-finanziario e riaffermano la connessione fra l'inclusione finanziaria e la non discriminazione. Nel TUB (comma 2 dell'art. 126-noviesdecies) è detto che “Tutti i consumatori soggiornanti legalmente nell'Unione europea, senza discriminazioni e a prescindere dal luogo di residenza, hanno diritto all'apertura di un conto di base ...”.

Le disposizioni di trasparenza in materia di servizi di pagamento (par. 5.2 della sezione VI) recitano: “Tutte le modifiche dei tassi di interesse o di cambio sono applicate e calcolate in modo tale da non creare discriminazioni tra clienti. Le modalità di applicazione e di calcolo di queste modifiche si presumono non discriminatorie quando gli intermediari le adottano sulla base di criteri oggettivi e motivati che applicano a tutti i clienti, a parità di condizioni”.

Con specifico riferimento alle normative di trasparenza in materia di credito immobiliare ai consumatori, l'art. 120-undecies del TUB, relativo alla verifica del merito creditizio, afferma al comma 1 che “...La valutazione del merito creditizio è effettuata sulla base delle informazioni sulla situazione

economica e finanziaria del consumatore necessarie, sufficienti e proporzionate e opportunamente verificate”, ponendo dunque dei requisiti alle caratteristiche dei dati utilizzati dall’intermediario ai fini del credit scoring.

Il comma 5 del medesimo articolo stabilisce inoltre che “Quando la domanda di credito è respinta, il finanziatore informa il consumatore senza indugio del rifiuto e, se del caso, del fatto che la decisione è basata sul trattamento automatico di dati”, evidenziando un diritto del consumatore ad essere informato qualora il rifiuto della sua domanda di credito immobiliare sia stato basato sull’utilizzo di forme di algorithmic credit scoring. La proposta di revisione della Consumer Credit Directive, pubblicata a luglio 2021 dalla Commissione Europea, introduce delle previsioni simili anche in materia di credito al consumo. L’obbligo di informazione ai consumatori dovrebbe valere anche in caso di offerte personalizzate basate su tecniche di profilazione. Anche se “non sussiste un obbligo per gli intermediari di concedere credito o di rivedere le condizioni alle quali è stato concesso, fatto salvo il dovere, in fase di valutazione e riscontro di eventuali richieste di rinegoziazione, di rispettare il principio di correttezza nei rapporti contrattuali...la valutazione del merito creditizio rientra infatti nell’autonomia gestionale degli intermediari”.

## **Capitolo 2. Normativa Europea**

Il rapido sviluppo delle tecnologie di intelligenza artificiale ha determinato una trasformazione profonda del settore finanziario, incidendo in modo significativo sia sui modelli operativi degli intermediari, sia sulle modalità di regolazione e vigilanza. I sistemi automatizzati nei processi decisionali, che vanno dalla valutazione del merito creditizio alla gestione del rischio, hanno posto nuove sfide per il diritto. Nuovi strumenti con elevata complessità tecnica richiedono un lungo lavoro per adattarsi alle tradizionali esigenze di trasparenza e accountability. L'Unione europea, in questo scenario ha assunto un ruolo primario nello sviluppo di un quadro normativo volto a disciplinare l'utilizzo dell'intelligenza artificiale, con l'obiettivo di coniugare innovazione tecnologica e tutela dei diritti fondamentali. L'adozione del Regolamento sull'intelligenza artificiale (AI Act) rappresenta un passaggio di particolare rilevanza, in quanto introduce un approccio basato sul rischio, destinato a incidere in modo significativo anche sul settore bancario e finanziario. Il presente capitolo si propone di analizzare l'impatto dell'AI Act sul sistema bancario, esaminando, in primo luogo, i principi e gli obiettivi della regolazione europea in materia di intelligenza artificiale, anche alla luce delle principali iniziative internazionali che hanno contribuito alla definizione di un quadro di riferimento condiviso. L'analisi si concentrerà poi sugli effetti concreti della normativa nei confronti degli operatori finanziari, con particolare attenzione agli obblighi di compliance e alle implicazioni in termini di gestione del rischio. Verranno evidenziate nel corso del capitolo quelle che sono le criticità emergenti, per esempio, il rischio di discriminazione algoritmica e le possibili implicazioni nel sistema finanziario. Il capitolo non intende offrire solo una ricostruzione del quadro normativo vigente, ma anche una riflessione critica sulle principali sfide che il legislatore e le autorità di vigilanza sono chiamati ad affrontare in un contesto caratterizzato da una rapida evoluzione. L'analisi si propone di studiare la correlazione tra diritto, tecnologia e finanza, con l'obiettivo di evidenziare come la regolazione dell'intelligenza artificiale nel settore bancario sia in continua evoluzione. La necessità di un approccio flessibile e dinamico, capace di adattarsi ai mutamenti del contesto economico e tecnologico, risulta determinante.

### **2.1 La cornice giuridica dell'AI Act e il settore bancario**

Negli ultimi due decenni l'evoluzione dell'Intelligenza Artificiale (AI) si è spinta oltre i confini accademici e sperimentali, trovando applicazione concreta in molti settori economici. Attualmente è considerata uno strumento centrale nei processi di modernizzazione, in particolare in contesti ad alta intensità di dati, come per esempio quello bancario. Gli strumenti AI più utilizzati nel settore bancario

vanno dai sistemi antifrode a sistemi per la valutazione del merito creditizio. Tuttavia, restano aperte questioni circa la reale trasparenza dei processi decisionali automatizzati e circa la comprensibilità e la spiegabilità di tali processi. Già a partire dalla seconda metà degli anni 2010, diversi organismi internazionali hanno elaborato principi etici e raccomandazioni al fine di guidare lo sviluppo e l'uso dell'AI, consapevoli del potenziale innovativo, ma anche dei rischi che tale tecnologia comporta. Tra le preoccupazioni vi sono temi come la protezione dei diritti fondamentali, la trasparenza dei sistemi, l'attribuzione di responsabilità in caso di danni, e la tutela della privacy. Questi temi sono diventati centrali per il dibattito giuridico internazionale, al punto da spingere le istituzioni a elaborare normative ad hoc, che mirano per esempio a garantire un adeguato livello di trasparenza e, ove possibile, la spiegabilità delle decisioni automatizzate, soprattutto quando queste incidono sui diritti dei cittadini.

Nel 2019 l'OCSE (Organizzazione intergovernativa con 38 paesi membri per la Cooperazione e lo Sviluppo Economico) ha emanato gli OECD Principles On Artificial Intelligence<sup>33</sup>. Si tratta del primo insieme di principi approvato da un'organizzazione intergovernativa con valore quasi universale. Questi principi sono stati fatti propri non soltanto dai 38 paesi membri dell'OCSE, ma anche dai paesi del G20, conferendo a tali standard un rilievo globale. Obiettivo preponderante, delineare un riferimento comune per promuovere un'AI innovativa, affidabile e rispettosa dei diritti umani. I principi si fondano, infatti, su una visione antropocentrica della tecnologia che considera l'Intelligenza Artificiale come strumento funzionale al progresso umano ed economico, ma la cui diffusione deve essere governata da criteri di sicurezza, equità e trasparenza.

I cinque principi cardine definiti dall'OCSE risultano di particolare rilevanza anche per il settore bancario e finanziario, che fa ampio uso di sistemi automatizzati ad alto impatto su individui e imprese.

#### 1. Principio di beneficio per le persone e il pianeta

Questo principio dell'OCSE si basa sul presupposto che i sistemi di Intelligenza Artificiale dovrebbero essere sviluppati in modo da generare benefici per la società, così che possano contribuire al progresso sostenibile. L'uso della tecnologia, secondo questa prospettiva, non dovrebbe limitarsi all'efficienza, ma contribuire concretamente al benessere delle persone e al miglioramento della qualità della vita.<sup>34</sup>

#### 2. Principio di trasparenza e spiegabilità

Secondo l'OCSE i sistemi di AI dovrebbero essere "comprensibili" e per quanto possibile "spiegabili". Ciò è particolarmente rilevante quando le decisioni automatizzate incidono direttamente sugli

---

<sup>33</sup> OECD Principles on Artificial Intelligence (2019), OECD <https://www.oecd.org/ai/>

<sup>34</sup> Ibidem, Principle 1

individui. Chiunque dovrebbe essere messo nelle condizioni di comprendere almeno i criteri base che determinano l'esito dell'algoritmo.<sup>35</sup> Nel settore bancario, questo aspetto assume particolare rilievo, infatti l'utilizzo di algoritmi complessi, come quelli usati per la valutazione del credito, può rendere difficile giustificare al cliente il motivo di un rifiuto per un finanziamento o l'attribuzione di un determinato punteggio di rischio. In questi casi la mancanza di spiegabilità rischia non solo di compromettere la fiducia del cliente, ma anche di aumentare il rischio di discriminazioni indirette, difficili da individuare.

### 3. Principio di robustezza sicurezza e accuratezza tecnica

Un ulteriore principio riguarda la necessità che i sistemi di intelligenza artificiale debbano essere progettati in modo affidabile, riducendo al minimo errori, vulnerabilità e possibili utilizzi impropri.<sup>36</sup> L'attenzione, dunque, non è rivolta solo alle prestazioni, ma anche alla capacità del sistema di operare in modo stabile e sicuro nel tempo.

In ambito bancario, ciò si riflette, per esempio, nei sistemi antifrode, che devono distinguere accuratamente tra transazioni legittime e sospette, ma anche nei modelli di valutazione creditizia, per i quali è essenziale l'utilizzo di dati accurati e aggiornati. In questo contesto assume fondamentale importanza il ruolo delle infrastrutture di cybersecurity che proteggono dalla manipolazione dei modelli e prevengono accessi non autorizzati.

### 4. Principio di governance dei dati

L'OCSE pone, inoltre, l'attenzione sulla qualità e sulla gestione dei dati. I dati utilizzati per addestrare i sistemi devono essere rappresentativi e privi di bias al fine di prevenire risultati discriminatori.<sup>37</sup> Questo principio appare strettamente connesso agli obblighi previsti dal GDPR e oggi ripresi dall'AI Act. In un settore dove le decisioni si basano su grandi quantità di informazioni personali e finanziarie, come quello bancario, diventa fondamentale una corretta governance dei dati per evitare errori sistematici e garantire un trattamento equo dei clienti.

### 5. Principio di accountability

Infine l'OCSE afferma che i soggetti che progettano, sviluppano e utilizzano sistemi di AI devono poter essere ritenuti responsabili delle loro azioni e delle conseguenze generate dai sistemi stessi.<sup>38</sup> Questo implica la necessità di individuare chiaramente ruoli e responsabilità. L'accountability è un concetto chiave per tutte le normative successive, inclusa l'AI Act, e assume una dimensione particolare nel settore bancario, dove in caso di errore le conseguenze possono avere impatti significativi non solo sul piano economico, ma anche su quello reputazionale e giuridico.

---

<sup>35</sup> Ibidem, Principle 2

<sup>36</sup> Ibidem, Principle 3

<sup>37</sup> Ibidem, Principle 4

<sup>38</sup> Ibidem, Principle 5

Questi principi rappresentano uno dei primi tentativi di definire un quadro condiviso per lo sviluppo e l'uso responsabile dell'Intelligenza Artificiale a livello internazionale. Tuttavia, si tratta di linee guida non vincolanti, volte principalmente a orientare le politiche pubbliche e le pratiche degli operatori economici. Molti elementi dell'AI Act come, per esempio, l'approccio risk based, il concetto di trasparenza e la governance dei dati che riflettono l'orientamento antropocentrico dei principi OECD<sup>39</sup>.

Su questo aspetto è intervenuta anche l'UNESCO, per ampliare e approfondire tali principi, proponendo una visione globale del rapporto tra AI e diritti umani, assicurando uno sviluppo sostenibile.

La Recommendation on the Ethics of Artificial Intelligence<sup>40</sup>, primo strumento normativo globale dedicato alla regolazione etica dell'AI, pubblicato nel 2021, è stato adottato dai 193 Stati membri. Pur non essendo vincolante, si distingue dai precedenti strumenti normativi per il rilievo attribuito alle implicazioni etico sociali connesse all'uso dell'Intelligenza artificiale, offrendo un'analisi più articolata. L'UNESCO concepisce l'AI come uno strumento che deve contribuire a rafforzare la dignità umana senza comprometterla. Tale impostazione riflette una visione dell'intelligenza artificiale profondamente integrata nelle dinamiche sociali ed economiche. Il rispetto dei diritti fondamentali costituisce una condizione imprescindibile per la legittimazione dell'innovazione<sup>41</sup>. Risulta evidente una forte attenzione al contrasto delle discriminazioni, alla tutela dei gruppi vulnerabili e alla riduzione delle disuguaglianze.<sup>42</sup>

Sebbene il documento contenga oltre 50 pagine di indicazioni, è possibile individuare alcuni principi chiave che hanno influenzato direttamente il dibattito europeo e, in parte, lo stesso impianto normativo dell'AI Act.

#### 1. Principio di rispetto dei diritti umani e della dignità umana

La Recommendation dell'UNESCO pone la tutela della dignità umana al centro di ogni applicazione dell'AI, in altre parole l'Intelligenza Artificiale deve operare nel pieno rispetto dei diritti fondamentali sanciti dal diritto internazionale, dal diritto umanitario e dalle convenzioni sull'uguaglianza e la non discriminazione.<sup>43</sup> Nel settore bancario, questo principio ha applicazioni concrete, legate all'uso di algoritmi di profilazione o Credit Scoring, che possono incidere direttamente sul diritto di accesso ai servizi finanziari, creando potenziali disparità tra categorie di utenti.

---

<sup>39</sup> Passador M.L. AI Act and the ECB: Steering Financial Supervision in the EU Columbia Journal of European Law 2025 p.p. 10-15

<sup>40</sup> UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021) <https://en.unesco.org/themes/ethics-of-artificial-intelligence>

<sup>41</sup> Mirishli S. Regulating AI in Financial Services: Legal Frameworks and Compliance Challenges 2023 p.p. 29-39

<sup>42</sup> Ibidem, Introduction (pag. 4)

<sup>43</sup> Ibidem, Section I.A

## 2. Principio di giustizia equità e non discriminazione

Uno dei contributi più significativi della Recommendation è la forte enfasi che viene posta sulla necessità di prevenire e contrastare i Bias algoritmici. I dati utilizzati per addestrare i sistemi di AI, infatti, possono riflettere pregiudizi già radicati all'interno della società, per esempio basati sul genere, sull'etnia o sullo status socioeconomico, che rischiano di essere amplificati dalla tecnologia.<sup>44</sup> Per questo motivo l'UNESCO raccomanda ai governi non solo di migliorare la qualità dei dataset, ma anche di implementare misure attive per garantire equità nei sistemi automatizzati, promuovendo audit indipendenti sugli algoritmi ad alto impatto.

Nel contesto bancario questo si traduce nell'evitare che le pratiche di scoring o di valutazione della solvibilità producano discriminazioni sistemiche, come successo per esempio negli ormai noti casi in cui algoritmi finanziari hanno attribuito punteggi più bassi a determinate categorie demografiche, anche a parità di condizioni economiche reali.

## 3. Sostenibilità e sviluppo umano

Un elemento interessante della Recommendation è il collegamento esplicito tra AI e sviluppo sostenibile. L'idea di fondo è che queste tecnologie non debbano essere utilizzate solo in chiave economica, ma anche per ridurre le disuguaglianze e migliorare le condizioni di vita, favorendo l'educazione e la parità di genere e riducendo la povertà e le disuguaglianze<sup>45</sup>. In ambito finanziario ciò si traduce nell'uso dell'Intelligenza Artificiale per ampliare l'accesso al credito o sviluppare strumenti a supporto delle fasce più vulnerabili, per esempio, utilizzando modelli predittivi e sistemi di automazione anche per sostenere l'inclusione finanziaria e combattere la lotta al sovraindebitamento.

## 4. Protezione dei dati e della privacy

Un'intera sezione è dedicata proprio alla protezione dei dati personali. Qui viene evidenziato come l'uso massiccio di informazioni sensibili renda necessario implementare misure di sicurezza rigorose.<sup>46</sup> Il concetto di privacy by design viene introdotto dall'UNESCO per invitare gli Stati membri a promuovere e stabilire limiti chiari alle finalità del trattamento, oltre a effettuare controlli rigorosi sui trasferimenti transfrontalieri dei dati.

## 5. Trasparenza, responsabilità e spiegabilità

Un altro punto centrale riguarda la trasparenza dei sistemi di AI. Gli utenti devono essere in grado di comprendere, almeno nelle loro linee essenziali, il funzionamento dei sistemi decisionali automatizzati.<sup>47</sup>

---

<sup>44</sup> Ibidem, Section II.B

<sup>45</sup> Ibidem, Section III

<sup>46</sup> Ibidem, Section II.C

<sup>47</sup> Ibidem, Section II.D

Il principio di spiegabilità assume particolare importanza nel caso di: decisioni finanziarie, valutazioni creditizie, blocchi automatici di operazioni sospette, definizione di profili di rischio.

L'UNESCO amplia il concetto di trasparenza, includendo non soltanto gli utenti finali, ma anche le autorità pubbliche, chiamate a disporre degli strumenti necessari per analizzare e controllare il funzionamento degli algoritmi.

#### 6. Responsabilità e meccanismi di rimedio

Un capitolo importante della Recommendation riguarda l'accountability. Secondo l'UNESCO deve essere sempre chiaro chi è responsabile degli effetti prodotti dall'intelligenza artificiale e devono esistere meccanismi di ricorso efficaci e accessibili. Inoltre gli Stati devono prevedere politiche che permettano di contestare le decisioni automatizzate ingiuste.<sup>48</sup>

Nel settore bancario ciò si traduce nella possibilità per il cliente di richiedere una revisione umana delle decisioni, principio già tutelato dal GDPR (art. 22) e ulteriormente rafforzato dall'AI Act.

Sebbene questi documenti rimangano Soft Law, ovvero linee guida non vincolanti, la Recommendation UNESCO ha influenzato significativamente il dibattito europeo introducendo un quadro etico globale e condiviso, rafforzando l'idea di una AI antropocentrica e fornendo le basi concettuali per alcuni principi dell'AI Act come per esempio trasparenza, accountability e supervisione umana.

Rispetto all'impostazione dell'OCSE, l'UNESCO pone un accento più marcato sulla tutela dei diritti fondamentali, sulla riduzione delle disuguaglianze e sulla necessità di contrastare attivamente i bias algoritmici. Al tempo stesso rafforza concetti già presenti, inserendoli all'interno di una visione più ampia, che considera l'Intelligenza Artificiale non solo come strumento economico, ma anche come fattore di impatto sociale globale. I principi UNESCO possono essere letti come un'evoluzione e un consolidamento delle linee guida OCSE. Anch'essi hanno contribuito a creare le basi concettuali su cui si è sviluppato il successivo intervento normativo dell'Unione Europea, in particolare con l'adozione dell'AI Act. Si delinea così un percorso progressivo, che va da semplici principi etici non vincolanti a forme sempre più strutturate di regolazione giuridica.

L'Unione europea è stata tra le prime giurisdizioni a riconoscere il ruolo strategico dell'Intelligenza artificiale per la competitività economica. Al tempo stesso ne ha sempre riconosciuto i potenziali rischi legati al suo utilizzo, come la manipolazione dei dati, i problemi legati alla privacy e possibili

---

<sup>48</sup> Ibidem, Section II.E

forme di discriminazione algoritmica. Nel Libro Bianco sull'Intelligenza Artificiale del 2020<sup>49</sup> la Commissione Europea ha delineato un approccio costruito attorno a due direttrici principali: la promozione di un "ecosistema di eccellenza" e parallelamente la creazione di un "ecosistema di fiducia". L'ecosistema di eccellenza è volto a sostenere lo sviluppo tecnologico europeo in maniera da attrarre e trattenere talenti, potenziando le infrastrutture e investendo nel settore dell'AI, mentre l'ecosistema di fiducia, dovrebbe fondarsi su regole e garanzie che assicurino un utilizzo sicuro, etico e affidabile delle tecnologie.<sup>50</sup>

Il documento propone una lettura abbastanza chiara del ruolo dell'Intelligenza Artificiale come leva essenziale per la competitività industriale europea, ma allo stesso tempo evidenzia come la tecnologia possa creare rischi sistemici per individui e società. In tal senso il libro bianco anticipa e giustifica pienamente l'impianto risk based dell'AI Act riconoscendo che le Intelligenze Artificiali possono produrre benefici rilevanti, ma soltanto se sviluppate in un quadro normativo adeguato. Per quanto concerne il primo punto, ovvero la creazione di un "ecosistema di eccellenza", il White Paper riconosce apertamente che l'Europa si trova in una posizione intermedia nella competizione globale: possiede un forte patrimonio accademico e scientifico, ma risulta ancora carente per quanto riguarda investimenti privati, infrastrutture digitali e grandi imprese tech in grado di competere a livello planetario.<sup>51</sup> Per colmare questo divario la commissione individua una serie di linee d'azione attraverso:

#### 1. investimenti pubblici e privati mirati

La commissione proponeva già nel 2020 di mobilitare risorse pubbliche europee per almeno 20 miliardi di euro all'anno nel decennio successivo, promuovendo partenariati pubblico-privati e progetti strategici in aree come la sanità, i trasporti intelligenti, l'industria manifatturiera e i servizi finanziari.<sup>52</sup>

#### 2. Infrastrutture digitali e dati

La creazione di "spazi europei dei dati" viene considerata indispensabile per alimentare modelli di AI affidabili e competitivi. Questo tema anticipa il *Data Governance Act* del 2022) e il *Data Act* del 2023, che rappresentano la cornice complementare dell'AI Act.

#### 3. Supporto delle PMI

Le PMI rappresentano il tessuto economico dell'Unione Europea e il documento sottolinea la necessità di sostenerle attraverso la creazione di poli di innovazione digitale, l'accesso semplificato ai dati e l'utilizzo condiviso delle infrastrutture di calcolo avanzato.

---

<sup>49</sup> European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, 19 Febbraio 2020

<sup>50</sup> Ibidem, pag. 2

<sup>51</sup> Ibidem, pag. 7

<sup>52</sup> Ibidem, pag. 8

#### 4. Ricerca, formazione e sviluppo di competenze

Il libro bianco identifica con chiarezza la carenza di competenze digitali come una delle principali barriere allo sviluppo dell'AI europea.

Propone quindi programmi di formazione specialistica, lo sviluppo di Master europei sull'intelligenza artificiale oltre a incentivi per attrarre ricercatori internazionali.

Per quanto riguarda la creazione di un "ecosistema di fiducia" il cuore del libro bianco è costituito dall'idea che per sostenere l'adozione dell'AI sia indispensabile un quadro normativo unitario e vincolante.

È proprio in questo testo che viene introdotto il principio secondo cui non tutte le applicazioni dell'intelligenza artificiale richiedono la medesima intensità di regolazione. L'Unione Europea propone per la prima volta una classificazione basata sul rischio distinguendo tra:

- applicazione ad alto rischio, soggette a obblighi più severi
- applicazioni a rischio basso o minimo, soggette a regole più leggere<sup>53</sup>

La Commissione ritiene ad alto rischio quei sistemi in grado di incidere direttamente sulla vita dei cittadini, sulla loro integrità fisica o sui loro diritti fondamentali. Tra questi, il settore bancario viene menzionato come ambito potenzialmente critico in ragione dell'uso intensivo dei dati personali, delle decisioni automatizzate che possono determinare l'accesso o l'esclusione dai servizi finanziari.<sup>54</sup> Il White Paper identifica anche i requisiti per i sistemi ad alto rischio, che diventeranno poi obblighi giuridici nell'AI Act tra cui, ad esempio, la qualità dei dati utilizzati, la trasparenza sul funzionamento del sistema e la possibilità di ricostruire i processi decisionali. Per garantire tutto ciò è necessaria sia la supervisione umana, sia la robustezza della cyber security. Resta inteso che debbano esistere processi di valutazione della conformità ex ante, attraverso test e verifiche indipendenti.<sup>55</sup>

In questo contesto, il settore finanziario emerge come uno degli ambiti in cui l'adozione dell'AI produce i maggiori benefici in termini di efficienza operativa, ma al tempo stesso espone a rischi sistemici particolarmente elevati, soprattutto in relazione alla stabilità dei mercati e alla protezione dei consumatori, assumendo quindi una rilevanza centrale anche sotto il profilo macroprudenziale.<sup>56</sup> Questi elementi, elaborati inizialmente come linee guida politiche, sono stati successivamente trasformati in disposizioni normative vincolanti.

---

<sup>53</sup> Ibidem, pag. 10

<sup>54</sup> Ibidem, pag. 11

<sup>55</sup> Ibidem, Annex.

<sup>56</sup> Becerra-Vicario R. et al. The Impact of Artificial Intelligence in the Financial Sector: Opportunities and Challenges University of Málaga 2023 pp. 38-39

Il libro bianco può essere considerato la base concettuale della AI Act. Infatti, molte delle sue proposte sono entrate quasi integralmente nel regolamento del 2024.

Il percorso normativo che ha portato all'adozione dell'Artificial Intelligence Act è stato particolarmente lungo e complesso. Questo è dipeso da diversi fattori tra cui sicuramente la rilevanza strategica della materia, ma anche la necessità di trovare il giusto equilibrio tra innovazione tecnologica e tutela dei diritti fondamentali, in un contesto in rapida evoluzione. Questo equilibrio rappresenta una delle principali sfide regolatorie contemporanee, in quanto un eccesso di regolazione potrebbe rallentare l'innovazione, mentre una disciplina troppo permissiva rischierebbe di compromettere la fiducia degli utenti e la stabilità dei mercati finanziari.<sup>57</sup>

Per i motivi sopra citati, il processo legislativo è stato caratterizzato da continui aggiustamenti e momenti di confronto, al punto da configurarsi come un esempio significativo di quello che viene spesso definito "diritto dinamico".

L'origine politica dell'AI Act può essere individuata nel pacchetto di iniziative lanciate dalla Commissione Junker nel 2018 quando l'Unione Europea riconobbe l'intelligenza artificiale come una priorità trasversale per la propria competitività economica.<sup>58</sup> Un primo documento strategico fu rappresentato dalla Coordinated Plan on Artificial Intelligence, redatta in collaborazione con gli Stati membri e volta a identificare gli investimenti necessari nonché a promuovere la cooperazione pubblico-privata.<sup>59</sup>

Il passo decisivo, tuttavia, fu la pubblicazione del Libro Bianco del 2020, che chiarì l'intenzione della commissione di proporre uno strumento giuridico vincolante basato su un approccio fondato sul rischio, su obblighi di conformità più rigorosi per i sistemi ad alto rischio e su divieti per alcune pratiche considerate incompatibili con i diritti fondamentali. Fu proprio sulla base di questo documento programmatico che il 21 aprile 2021 la Commissione presentò ufficialmente la Proposta di Regolamento del Parlamento Europeo del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale, ossia il nucleo originario dell'AI Act.<sup>60</sup>

Dopo la pubblicazione della proposta, il processo legislativo è entrato nella sua fase più tecnica e delicata. In prima battuta il Parlamento ha promosso numerose audizioni con esperti, rappresentanti di imprese, associazioni dei consumatori, enti del terzo settore e istituzioni accademiche. Al centro del dibattito parlamentare vi erano questioni particolarmente controverse tra cui: il ruolo e i limiti della

---

<sup>57</sup> Maple C. et al. *The AI Revolution: Opportunities and Challenges for the Finance Sector* 2023 p. 6

<sup>58</sup> Commissione Europea, *Coordinated Plan on Artificial Intelligence*, 2018

<sup>59</sup> *Ibidem*

<sup>60</sup> Commissione Europea, *Proposal for a Regulation laying down harmonised rules on Artificial Intelligence*, 2021

biometria e del riconoscimento facciale, la definizione di sistema di AI, l'inclusione o l'esclusione dei sistemi di AI generativa e l'equilibrio tra tutela dei diritti e competitività.

Gli Stati membri hanno assunto posizioni diverse, spesso legate alle rispettive priorità politiche ed economiche. Francia e Germania per esempio hanno mostrato una certa cautela rispetto a regolamentazioni troppo onerose per l'industria. Non tutti gli Stati membri hanno però adottato la stessa impostazione. Paesi come Italia e Spagna hanno mostrato una maggiore attenzione alla tutela dei diritti fondamentali, insistendo sulla necessità di affiancare allo sviluppo tecnologico adeguate garanzie per gli individui. In altri contesti, invece, soprattutto in alcuni Stati dell'Europa orientale, il dibattito si è concentrato maggiormente sulle esigenze di sicurezza interna e sulle potenzialità dell'intelligenza artificiale nell'ambito dei servizi pubblici.<sup>61</sup>

Le divergenze hanno reso necessario un compromesso soprattutto sulle tecnologie biometriche e sui modelli di AI generativa.

Il confronto non ha coinvolto soltanto le istituzioni europee, ma anche attori esterni, come ONG e comunità accademiche, che hanno sollevato il rischio di una regolamentazione eccessivamente sbilanciata verso gli interessi industriali a discapito della protezione dei diritti fondamentali.

Il momento decisivo del processo legislativo è rappresentato dal trilogò, ovvero il negoziato informale tra Parlamento Europeo, Consiglio dell'Unione Europea e Commissione Europea. Dopo quasi tre anni di discussione, l'8 dicembre 2023, le istituzioni sono giunte a un accordo politico provvisorio dopo tre giorni consecutivi di trattative a porte chiuse.<sup>62</sup> L'accordo ha permesso di superare alcuni dei nodi più controversi, quali: la regolazione dei modelli di AI generativa, le limitazioni della sorveglianza biometrica, la definizione chiara di sistemi ad alto rischio, la governance multilivello. L'accordo politico del dicembre 2023 ha rappresentato la prima definizione concreta della futura architettura regolatoria europea.

Dopo il trilogò, il testo è stato approvato dal Parlamento Europeo il 13 marzo 2024, con una larga maggioranza (523 voti favorevoli, 46 contrari e 49 astensioni).<sup>63</sup>

Successivamente il 21 maggio dello stesso anno il Consiglio dell'Unione Europea ha espresso l'approvazione definitiva<sup>64</sup> e il regolamento è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea il 12 luglio 2024, ed è ufficialmente entrato in vigore il 1 agosto 2024.

L'AI Act è un regolamento, e come tale, è direttamente applicabile e immediatamente vincolante in tutti gli Stati membri senza necessità di recepimento.

---

<sup>61</sup> Consiglio dell'Unione Europea, General Approach, 2022

<sup>62</sup> Parlamento Europeo, Press Release - Artificial Intelligence Act: political agreement reached, 8 dicembre 2023.

<sup>63</sup> Parlamento Europeo, Roll-call vote on the Ai Act, 13 marzo 2024

<sup>64</sup> Consiglio dell'Unione Europea, Adoption of the AI Act, 21 maggio 2024.

Il regolamento ha previsto un'applicazione progressiva con una fase preliminare, di un anno e otto mesi, prima della completa applicazione prevista per il 2 agosto 2026, per consentire alle imprese di adeguarsi gradualmente ai nuovi obblighi. In questa fase sono stati rafforzati gli obblighi di trasparenza per garantire un funzionamento più sicuro e responsabile. Alle aziende è stato chiesto di informare chiaramente gli utenti quando interagiscono con sistemi di AI generativa. Sono, invece, entrati subito in vigore i divieti relativi alle pratiche ritenute a rischio inaccettabile.

Le disposizioni tecniche più complesse troveranno invece piena applicazione solo in una fase successiva.

L'AI Act non si limita a disciplinare aspetti tecnici, ma riflette un'impostazione più ampia rispetto ai ruoli delle Intelligenze Artificiali. L'idea di fondo è quella di accompagnare lo sviluppo senza ostacolarlo, ma cercando al contempo di garantire un adeguato livello di sicurezza per gli utenti. In sostanza mira alla creazione di un ecosistema affidabile, in cui le tecnologie possano svilupparsi in un ambiente regolamentato ma non eccessivamente restrittivo, creando un vantaggio competitivo per le aziende europee basato sulla fiducia e sulla trasparenza. L'obiettivo è dunque il mantenimento di elevati standard etici che consentano di proteggere i cittadini europei dai rischi dell'AI senza rinunciare alla promozione dell'innovazione e della competitività industriale europea nel settore tecnologico più strategico del 21° secolo.

Il quadro normativo si fonda su un approccio "risk-based", ovvero basato sul rischio, in parte già presente anche nel GDPR (General Data Protection Regulation, o Regolamento Generale sulla Protezione dei Dati). L'idea è piuttosto intuitiva: non tutte le applicazioni di intelligenza artificiale comportano lo stesso livello di pericolosità e, di conseguenza, non richiedono la stessa rigidità normativa. Concretamente, maggiore è il rischio connesso a un sistema, più stringenti saranno gli obblighi normativi cui saranno soggetti sia chi lo sviluppa sia chi lo utilizza. Alcune applicazioni vengono invece ritenute incompatibili con i valori dell'Unione, e per questo motivo vengono vietate. Ne sono un esempio il social scoring, alcune forme di manipolazione comportamentale, meccanismi di riconoscimento delle emozioni sul luogo di lavoro e negli istituti di istruzione.

I sistemi di Intelligenza Artificiale devono inoltre essere sottoposti a un processo di valutazione di conformità ex ante, prima cioè di essere immessi sul mercato. Questo passaggio è particolarmente importante perché tali sistemi spesso sono sviluppati attraverso una catena del valore complessa, che coinvolge più soggetti. Risulta dunque evidente che anche le responsabilità non debbano rimanere in capo a un solo attore, ma devono essere suddivise in base al ruolo effettivamente svolto. L'attribuzione delle responsabilità resta uno dei temi più caldi poiché non è sempre facile risalire alla catena del valore e ricondurre la responsabilità di un eventuale danno al reale colpevole.

L'art. 6 dell'AI Act individua i sistemi di AI ad alto rischio, cioè, quei sistemi che possono porre rischi significativi per la salute e la sicurezza, per i diritti fondamentali delle persone, la democrazia, lo Stato di diritto e le libertà individuali. Vi rientrano i sistemi di AI che coinvolgono uno o più settori critici quali l'istruzione, la sanità, la selezione del personale, la sicurezza, la giustizia e la pubblica amministrazione, se presentano un rischio significativo di danno per la salute umana, la sicurezza o i diritti fondamentali dei cittadini.

L'AI Act ha previsto che i sistemi ad alto rischio siano soggetti a una serie di requisiti e obblighi per accedere al mercato dell'UE. In particolare devono prevedere l'adozione di sistemi di gestione dei rischi; i set di dati che alimentano il sistema devono essere di qualità elevata e misurabile attraverso la predisposizione di una documentazione tecnica recante tutte le informazioni necessarie alle autorità per valutare la conformità dei sistemi di Artificial Intelligence ai requisiti richiesti; prevedere la conservazione delle registrazioni degli eventi ("log") e adeguati livelli di accuratezza, robustezza, cybersicurezza, e, infine, contemplare misure di sorveglianza umana.

L'art. 52 dell'AI Act sancisce il mero obbligo di trasparenza ai sistemi rilevati a rischio medio al fine di consentire all'utente di interagire con la tecnologia in modo consapevole e di assumere decisioni informate. L'utente dovrà dunque essere consapevole di stare interagendo con una IA, o che un determinato contenuto è stato generato dall'intelligenza artificiale.

Il settore bancario rientra tra i più complessi, poiché numerose applicazioni rientrano in categorie di rischio elevato o inaccettabile. Ciò comporta la necessità di adeguare i sistemi di Intelligenza Artificiale ai requisiti normativi, con conseguenze dirette sui contratti, sulla responsabilità civile e sulla tutela dei dati.

L'AI Act prevede un modello di governance multilivello: innanzitutto è stato eletto un Comitato Europeo per l'Intelligenza Artificiale incaricato di coordinare l'attuazione del regolamento e di armonizzare le prassi di enforcement. Parallelamente, le Autorità nazionali competenti hanno il dovere di supervisionare il rispetto delle norme e possono applicare sanzioni.

Tutte le aziende coinvolte hanno l'obbligo di cooperare e di fornire documentazione e accesso ai modelli in caso di ispezioni.

Le sanzioni previste sono significative e possono arrivare fino a 35 milioni di euro o al 7% del fatturato annuo globale per le violazioni più gravi.

Le autorità di vigilanza, infine, devono garantire un'applicazione effettiva dell'AI Act nel settore bancario. Le modalità tradizionali di supervisione sono chiamate a confrontarsi con tecnologie sempre più complesse e difficilmente interpretabili. La supervisione non può più limitarsi alla verifica del rispetto formale delle norme, ma deve estendersi alla comprensione dei modelli algoritmici utilizzati dagli intermediari, alla qualità dei dati impiegati e ai meccanismi di gestione del rischio adottati<sup>65</sup>.

La Banca Centrale Europea (BCE), svolge un ruolo centrale nella supervisione prudenziale degli istituti di credito, mentre autorità come l'European Banking Authority (EBA) e l'European Securities and Markets Authority (ESMA) contribuiscono alla definizione di linee guida e standard tecnici volti a garantire un'applicazione uniforme della normativa nei diversi Stati membri.

Si osserva una progressiva evoluzione della vigilanza bancaria, che mira a integrare le tradizionali competenze giuridiche ed economiche con conoscenze tecniche e informatiche. Le autorità di controllo devono valutare l'affidabilità dei sistemi di machine learning, la loro resistenza a potenziali manipolazioni e la capacità di produrre risultati equi e non discriminatori.

Questo richiede lo sviluppo di nuove metodologie di supervisione, come audit algoritmici, stress test sui modelli e verifiche sulla qualità dei dataset utilizzati.

Un ulteriore fattore di complessità riguarda il coordinamento tra l'AI Act e le normative bancarie e finanziarie già vigenti. Le autorità di vigilanza devono garantire che gli obblighi introdotti dal nuovo regolamento siano coerenti con quelli derivanti, per esempio, dal GDPR, dalla normativa antiriciclaggio e dai requisiti prudenziali di Basilea. In assenza di un coordinamento efficace, si rischia la duplicazione degli adempimenti e un aumento degli oneri di compliance per gli intermediari, senza un reale miglioramento della tutela.

## **2.2 Analisi dell'AI Act e impatti specifici nel settore bancario**

Nel settore bancario, l'introduzione di sistemi automatizzati, in particolare basati su algoritmi e intelligenza artificiale, solleva rilevanti questioni giuridiche. Tra queste, assumono particolare rilievo la definizione dei profili di responsabilità, gli obblighi di trasparenza e la tutela dei dati personali.<sup>66</sup> In ambito europeo, tali aspetti sono disciplinati dal GDPR, che all'art. 22 riconosce agli interessati il diritto di non essere sottoposti a decisioni interamente automatizzate che producano effetti giuridici significativi, come nel caso della concessione o del rifiuto di un credito.<sup>67</sup>

<sup>65</sup> Passador M.L. AI Act and the ECB: Steering Financial Supervision in the EU Columbia Journal of European Law 2025 pp. 12–15

<sup>66</sup> A. Mantelero, *Intelligenza artificiale e diritto. Una introduzione*, Torino, Giappichelli, 2022, pp. 131–148.

<sup>67</sup> L. Floridi, *The Ethics of Artificial Intelligence*, Oxford, Oxford University Press, 2019, pp. 87–92.

Un ulteriore nodo critico riguarda l'individuazione del soggetto responsabile in presenza di decisioni automatizzate errate o discriminatorie. Si pensi a un sistema di credit scoring che penalizzi automaticamente determinate categorie di clienti sulla base di dati storici distorti: in tali casi, pur essendo l'errore riconducibile all'algoritmo, la responsabilità tende a ricadere sull'istituto di credito, in quanto soggetto che ha adottato e utilizza il sistema. Questo orientamento trova conferma anche nelle linee guida delle autorità di vigilanza, che attribuiscono alle banche un ruolo centrale nel garantire la correttezza dei processi decisionali.

Le banche sono inoltre tenute a rispettare specifici obblighi di trasparenza, fornendo ai clienti informazioni chiare e comprensibili sul funzionamento dei sistemi automatizzati. In caso di rifiuto di un prestito, il cliente dovrebbe poter comprendere quali fattori (come reddito, storico creditizio o livello di indebitamento) abbiano inciso sulla decisione, in linea con quanto previsto dagli artt. 13 e 14 del GDPR in materia di informativa.<sup>68</sup>

Nonostante il quadro normativo europeo offra già strumenti importanti di tutela<sup>69</sup>, permane una certa difficoltà applicativa, soprattutto per quanto riguarda la reale comprensibilità degli algoritmi da parte degli utenti. In questo senso, sarebbe auspicabile un ulteriore sforzo normativo e tecnico volto a rendere le decisioni automatizzate non solo trasparenti formalmente, ma anche effettivamente intelligibili per i clienti.

Ciò comporta l'introduzione di nuove modalità di dialogo giuridico tra intermediari e utenti, con possibili ricadute sulla privacy e sulla protezione dei dati personali. L'uso di sofisticati modelli di machine learning nelle decisioni finanziarie accentua la tensione tra la necessità di adattare i servizi alle esigenze individuali e l'obbligo di attenersi ai principi europei che regolano l'uso dei dati. Resta tuttavia aperta la questione relativa alla reale efficacia del cosiddetto "diritto alla spiegazione", che, soprattutto nei sistemi più complessi, rischia di tradursi in una trasparenza formale e non sostanziale. Ciononostante, questo rappresenta un chiaro esempio di come le norme dell'AI Act si integrano, e si coordinano al GDPR, dando vita a un quadro normativo articolato, in cui le banche devono assicurare la legalità dell'uso dei dati per l'addestramento e il funzionamento dell'Intelligenza Artificiale<sup>70</sup>, specialmente nel trattamento di dati sensibili, come quelli relativi alla disabilità o alla salute.

Per quanto concerne le procedure di valutazione del rischio la normativa impone agli istituti bancari

---

<sup>68</sup> Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, *Regolamento generale sulla protezione dei dati (GDPR)*, Bruxelles, 2016, artt. 13–14.

<sup>69</sup> Moretti L. Rinaldi L. Sclosser P. Digital Finance in the EU: navigating new technological trends and the AI revolution 2024 p. 21

<sup>70</sup> Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, *Regolamento generale sulla protezione dei dati (GDPR)*, Bruxelles, 2016, artt. 5, 13–14, 22.

l'adozione di misure preventive e di gestione del rischio, potenzialmente comportando oneri amministrativi e tecnici significativi<sup>71</sup>.

Tale incremento degli oneri regolatori è spesso accompagnato dalla necessità di sviluppare nuove competenze interne e strutture organizzative dedicate alla gestione del rischio algoritmico, determinando un'evoluzione significativa dei modelli operativi tradizionali delle istituzioni finanziarie.<sup>72</sup> Accanto agli impatti a livello microeconomico, legati ai costi di adeguamento e agli obblighi di compliance, l'utilizzo diffuso dell'intelligenza artificiale nel settore bancario solleva interrogativi rilevanti anche sotto il profilo della stabilità complessiva del sistema finanziario. L'adozione crescente di modelli algoritmici nei processi decisionali, infatti, non incide soltanto sulle singole istituzioni, ma può generare effetti sistemici, soprattutto in presenza di comportamenti omogenei tra gli operatori.

Uno dei profili più dibattuti riguarda il rischio di pro-ciclicità. I sistemi di intelligenza artificiale, in particolare quelli basati su tecniche di machine learning, sono costruiti su dati storici e tendono a riprodurre le regolarità. Questo meccanismo, apparentemente neutro, può produrre effetti distorsivi lungo il ciclo economico. Nelle fasi espansive può favorire un aumento della propensione al rischio; nelle fasi recessive, al contrario, può tradursi in un irrigidimento diffuso delle politiche di credito, contribuendo ad accentuare la contrazione.<sup>73</sup>

Il problema assume maggiore rilievo se si considera la crescente omogeneità dei modelli utilizzati dagli intermediari. L'impiego di dataset simili e di tecniche di analisi convergenti tende a ridurre la varietà delle decisioni. Ne deriva un sistema meno diversificato, e quindi più esposto a shock improvvisi. Dinamiche di questo tipo sono già emerse in passato, come nel caso della crisi finanziaria del 2008, quando l'adozione di modelli di rischio analoghi ha contribuito a rafforzare comportamenti prociclici.

Un ulteriore fattore critico riguarda la rapidità dei processi automatizzati. La capacità di elaborare grandi volumi di dati in tempi estremamente brevi rappresenta un chiaro vantaggio operativo, ma al contempo può favorire reazioni simultanee. In presenza di segnali negativi, sistemi analoghi potrebbero attivare strategie difensive quasi contemporaneamente, amplificando gli effetti sul mercato e incrementando la volatilità complessiva.

Queste dinamiche diventano particolarmente rilevanti in una prospettiva macroprudenziale, che si concentra sulla stabilità dell'intero sistema finanziario. In tale contesto, anche le autorità di vigilanza,

---

<sup>71</sup> G. Finocchiaro, *Privacy e protezione dei dati personali*, Bologna, Il Mulino, 2021, pp. 201–215.

<sup>72</sup> Mirishli S. *Regulating AI in Financial Services: Legal Frameworks and Compliance Challenges 2023* p. 35

<sup>73</sup> Maple C. et al. *The AI Revolution: Opportunities and Challenges for the Finance Sector 2023* pp. 15–20

come la Banca Centrale Europea, hanno sottolineato l'importanza di monitorare l'impatto delle innovazioni tecnologiche non solo a livello micro, ma anche sistemico.

Il quadro normativo europeo si è progressivamente adattato a queste trasformazioni. L'AI Act introduce requisiti specifici per i sistemi classificati come ad alto rischio, includendo obblighi di trasparenza, tracciabilità e supervisione umana. Si tratta di un intervento rilevante soprattutto con riferimento alle implicazioni sistemiche dell'adozione diffusa dell'intelligenza artificiale nei mercati finanziari.<sup>74</sup>

Alla luce di tali considerazioni, l'impatto dell'AI nel settore bancario non appare riducibile a una questione di efficienza operativa o di mera conformità normativa. Le evidenze disponibili suggeriscono la necessità di un approccio regolatorio capace di intercettare anche i rischi che emergono a livello aggregato, in un contesto caratterizzato da elevata interconnessione e crescente omogeneità dei comportamenti.

Risulta evidente che sarà necessario formare personale specializzato in grado di valutare l'affidabilità e la spiegabilità degli algoritmi<sup>75</sup>.

In sintesi, l'AI Act non si limita alla mera introduzione di nuovi obblighi normativi, ma incide direttamente sulle modalità con cui le banche progettano e utilizzano i sistemi tecnologici. In questo modo gioca un ruolo attivo per quanto riguarda le strategie di innovazione. Letta in questo senso, la conformità normativa può trasformarsi in vantaggio competitivo, anche se resta intesa la necessità di investimenti concreti in audit, documentazione e formazione specialistica.

Tra le principali criticità connesse all'impiego dell'intelligenza artificiale nel settore bancario assume rilievo il tema del bias algoritmico, ossia il rischio che i sistemi automatizzati producano risultati distorti o discriminatori. Tali effetti non presuppongono necessariamente un intento discriminatorio, ma possono emergere in modo implicito a partire dai dati utilizzati per l'addestramento o dalle scelte progettuali alla base dei modelli.

I sistemi di machine learning, infatti, apprendono da dati storici che riflettono dinamiche economiche e sociali già esistenti. In questo quadro, l'algoritmo non introduce autonomamente il bias, ma tende a riprodurlo e, in alcuni casi, a rafforzarlo. Nel contesto bancario, il problema si manifesta in modo evidente nei processi di credit scoring e di valutazione del rischio, nei quali decisioni automatizzate incidono direttamente sull'accesso al credito e, più in generale, sui livelli di inclusione finanziaria.<sup>76</sup>

---

<sup>74</sup> Becerra-Vicario R. et al. *The Impact of Artificial Intelligence in the Financial Sector: Opportunities and Challenges* University of Málaga 2023 pp. 10–14

<sup>75</sup> Garante per la protezione dei dati personali, *Linee guida su intelligenza artificiale e protezione dei dati personali*, Roma, 2023, pp. 6–12.

<sup>76</sup> Becerra-Vicario R. et al. *The Impact of Artificial Intelligence in the Financial Sector: Opportunities and Challenges* University of Málaga 2023 pp. 10–15

Un caso noto riguarda il sistema di valutazione adottato per la Apple Card, sviluppata da Apple in collaborazione con Goldman Sachs. Alcuni utenti hanno segnalato differenze significative nei limiti di credito concessi tra uomini e donne, anche a parità di condizioni economiche. La vicenda ha dato origine a un ampio dibattito pubblico e all'intervento delle autorità statunitensi, mettendo in luce le difficoltà di ricostruire il processo decisionale e di accertare eventuali responsabilità in presenza di modelli opachi.

Spesso si tratta di una discriminazione indiretta. Diversamente da quella esplicita, essa si basa su correlazioni statistiche e su variabili apparentemente neutre, che tuttavia possono penalizzare sistematicamente alcune categorie. Individuarla con gli strumenti giuridici tradizionali è molto complicato.

Questo problema è strettamente legato alla trasparenza e alla spiegabilità dei modelli. Nei sistemi più complessi, come le reti neurali profonde, il funzionamento interno è spesso opaco, rendendo difficile per gli utenti comprendere le decisioni e limitando l'efficacia delle tutele previste dal diritto europeo, come il diritto alla spiegazione e alla revisione umana delle decisioni automatizzate.

Per far fronte a queste criticità, l'Unione Europea ha adottato misure complementari. Il Regolamento generale sulla protezione dei dati stabilisce principi come trasparenza, minimizzazione dei dati e divieto di decisioni completamente automatizzate. L'AI Act integra questo quadro, imponendo obblighi specifici per i sistemi ad alto rischio, tra cui la gestione dei dati e l'adozione di misure per ridurre i bias algoritmici.<sup>77</sup>

Nonostante queste normative, restano sfide pratiche. Dimostrare la presenza di bias è complesso, specialmente quando le decisioni derivano da algoritmi opachi e fortemente automatizzati.

Ciò limita l'efficacia delle norme antidiscriminatorie, rendendo necessari strumenti più sofisticati come audit indipendenti e monitoraggio continuo dei modelli.

La disciplina dell'intelligenza artificiale nel settore bancario si inserisce, inoltre, in un contesto regolatorio articolato. L'AI Act non sostituisce le normative settoriali esistenti, ma si integra<sup>78</sup> con esse, richiedendo agli intermediari un coordinamento tra diversi livelli di regolazione. Rimangono centrali, tra gli altri, la Direttiva PSD2 per l'open banking, la Direttiva MiFID II in materia di servizi di investimento e le direttive antiriciclaggio AMLD5 e AMLD6. A queste si aggiungono i requisiti prudenziali derivanti da Basilea III e Basilea IV.

---

<sup>77</sup> Mirishli S. *Regulating AI in Financial Services: Legal Frameworks and Compliance Challenges 2023* pp. 32–36

<sup>78</sup> Direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio, *AMLD5*, Bruxelles, 2018.

## Protezione dei dati personali e GDPR

La protezione dei dati personali rappresenta uno dei principali punti di contatto tra l'impiego dell'intelligenza artificiale e la disciplina bancaria. Il Regolamento generale sulla protezione dei dati definisce il quadro normativo di riferimento per il trattamento dei dati nell'Unione europea, imponendo obblighi specifici in capo ai soggetti che determinano le finalità e le modalità del trattamento.<sup>79</sup>

Nel settore bancario, l'utilizzo di sistemi di intelligenza artificiale implica il trattamento di quantità particolarmente elevate di informazioni, spesso riconducibili alla sfera personale degli individui. Si tratta non solo di dati finanziari, ma anche di informazioni comportamentali, dati di transazione e, in alcuni casi, elementi biometrici. Tali informazioni vengono impiegate per alimentare modelli di machine learning utilizzati, tra l'altro, nei processi di valutazione del merito creditizio, nella prevenzione delle frodi e nella personalizzazione dei servizi offerti alla clientela.

L'impiego di queste tecnologie deve tuttavia confrontarsi con i principi fondamentali del GDPR, che incidono in modo significativo sulla progettazione e sull'utilizzo dei sistemi algoritmici. In particolare, il principio di limitazione delle finalità impone che i dati siano raccolti per scopi determinati e legittimi, mentre il principio di minimizzazione richiede che vengano trattate solo le informazioni strettamente necessarie rispetto agli obiettivi perseguiti. A ciò si affianca l'esigenza di garantire un adeguato livello di trasparenza: gli interessati devono essere messi nelle condizioni di comprendere le modalità del trattamento e, almeno in termini generali, le logiche sottostanti alle decisioni automatizzate.

Particolare rilievo assume, inoltre, il tema delle decisioni basate esclusivamente su trattamenti automatizzati.<sup>80</sup> In tali ipotesi, la disciplina europea riconosce all'interessato il diritto di ottenere un intervento umano e di contestare la decisione adottata, limitando così il ricorso a processi interamente automatizzati in presenza di effetti giuridici rilevanti. Accanto a ciò, il GDPR prevede obblighi stringenti in materia di sicurezza, che si traducono nell'adozione di misure tecniche e organizzative adeguate, nonché nello svolgimento di valutazioni d'impatto sulla protezione dei dati nei casi in cui il trattamento presenti rischi elevati.

Le autorità di controllo hanno più volte richiamato l'attenzione sui rischi specifici derivanti dall'uso dell'intelligenza artificiale, in particolare con riferimento alla possibilità che dataset non adeguatamente bilanciati o modelli poco trasparenti producano effetti distorsivi. In questo senso, anche il Garante per la protezione dei dati personali ha sottolineato la necessità di integrare fin dalle fasi iniziali di sviluppo adeguati meccanismi di controllo.<sup>81</sup>

---

<sup>79</sup> European Banking Authority (EBA), *Guidelines on ML/TF Risk Factors*, Parigi, 2021, pp. 18–24.

<sup>80</sup> Direttiva (UE) 2014/65 del Parlamento europeo e del Consiglio, *MiFID II*, Bruxelles, 2014.

<sup>81</sup> European Securities and Markets Authority (ESMA), *Guidelines on automated advice and digital investment services*, Parigi, 2018, pp. 9–15.

Un ambito in progressiva espansione riguarda l'utilizzo dell'intelligenza artificiale nell'ambito dei criteri ESG, dove tali tecnologie consentono di elaborare grandi quantità di dati, anche non strutturati, al fine di valutare i profili ambientali, sociali e di governance delle attività finanziarie.<sup>82</sup> Questo sviluppo comporta, per gli intermediari, la necessità di rafforzare i sistemi di data governance e di introdurre strumenti di verifica in grado di garantire la coerenza delle decisioni automatizzate con i requisiti normativi.

Permangono tuttavia alcune criticità di fondo. L'applicazione dei principi del GDPR ai sistemi di machine learning solleva ancora diverse questioni, soprattutto per quanto necessità di limitare il trattamento dei dati e quella di assicurare un livello sufficiente di accuratezza dei modelli.

#### Normativa antiriciclaggio (AML) e Know Your Customer (KYC)

Il contrasto al riciclaggio di denaro e al finanziamento del terrorismo costituisce un ulteriore ambito nel quale l'impiego dell'intelligenza artificiale si intreccia con la regolazione bancaria. La disciplina europea, delineata in particolare dalle direttive AMLD5 e AMLD6, impone agli intermediari una serie di obblighi che includono l'identificazione della clientela, il monitoraggio delle operazioni e la segnalazione di attività sospette.<sup>83</sup>

In questo contesto, l'intelligenza artificiale viene sempre più frequentemente utilizzata per analizzare grandi volumi di dati e individuare schemi anomali che potrebbero indicare comportamenti illeciti. L'automazione consente di aumentare l'efficienza dei controlli, ma introduce anche nuove esigenze sotto il profilo della trasparenza e della tracciabilità delle decisioni. Gli intermediari devono infatti essere in grado di ricostruire il percorso logico che ha condotto a una determinata segnalazione o valutazione di rischio.

L'utilizzo di modelli algoritmici può infatti incidere, anche indirettamente, su specifiche categorie di clienti, soprattutto quando i dati utilizzati riflettono squilibri preesistenti. In tali casi, il tema del bias algoritmico assume un rilievo analogo a quello riscontrabile in altri ambiti dell'attività bancaria.

Le indicazioni fornite dalle autorità di vigilanza si muovono nella direzione di un approccio basato sul rischio. In particolare, l'Autorità bancaria europea ha evidenziato come l'adozione di strumenti avanzati debba essere accompagnata da adeguati presidi di controllo, proporzionati alla complessità dei modelli utilizzati e al livello di rischio delle operazioni considerate.<sup>84</sup>

---

<sup>82</sup> Xu J. AI in ESG for Financial Institutions: An Industrial Survey 2024 p. 6

<sup>83</sup> E. Avgouleas, *The Governance of Global Financial Markets*, Cambridge, Cambridge University Press, 2012, pp. 254–260.

<sup>84</sup> Comitato di Basilea per la vigilanza bancaria, *Basel III: Finalising post-crisis reforms*, Basilea, Bank for International Settlements, 2017, pp. 3–10.

## Mercati finanziari e consulenza: la Direttiva MiFID II

La Direttiva MiFID II (2014/65/UE) disciplina i servizi di investimento e la tutela degli investitori nell'Unione Europea. Questo strumento normativo potenzia la trasparenza dei costi, richiede una rigorosa profilatura del cliente (profilo di adeguatezza) e l'integrazione delle preferenze di sostenibilità (ESG).

Con l'introduzione di strumenti basati sulle intelligenze artificiali, come i sistemi di consulenza automatizzata (robo-advisory), e il trading algoritmico, si pone il problema di adattare gli obblighi previsti dalla normativa MIFID II. Gli algoritmi di trading devono rispettare il principio di ottenere il miglior risultato possibile per il cliente, riducendo rischi di manipolazione del mercato.

In particolare resta fondamentale garantire che le raccomandazioni fornite siano coerenti con il profilo di adeguatezza dell'investitore, così come l'obbligo di fornire informazioni chiare sulle modalità di funzionamento dell'algoritmo.

Un concetto di fondamentale importanza è che il legislatore ha deciso che nonostante l'auto azione dei processi, la responsabilità resta comunque in capo all'intermediario.

Le autorità di vigilanza, in particolare l'ESMA (European Securities and Markets Authority), hanno pubblicato linee guida specifiche sulla consulenza digitale e il trading algoritmico, sottolineando la necessità di audit periodici sui modelli utilizzati.

## Open Banking e PSD2

Uno dei principali fattori di trasformazione del settore dei servizi di pagamento, introdotto dal modello dell'open banking, è rappresentato dalla Direttiva PSD2. In base a tale impostazione, gli istituti bancari sono tenuti a consentire a soggetti terzi autorizzati l'accesso ai dati dei conti dei clienti, mediante interfacce sicure (API), previa acquisizione del consenso esplicito dell'utente.

L'apertura dei dati ha favorito lo sviluppo di nuovi servizi digitali basati sull'intelligenza artificiale. Tra questi rientrano strumenti di analisi predittiva delle spese, applicazioni di budgeting automatizzato e sistemi avanzati di valutazione del rischio creditizio. L'integrazione tra open banking e tecnologie di IA ha contribuito a rendere l'offerta finanziaria più personalizzata e, in alcuni casi, più efficiente.

Accanto ai benefici, emergono tuttavia profili di complessità rilevanti. La condivisione dei dati tra più soggetti aumenta infatti i rischi connessi alla sicurezza e alla protezione delle informazioni personali. In un ecosistema aperto, nel quale operano sia intermediari tradizionali sia nuovi attori tecnologici, diventa fondamentale garantire standard elevati di autenticazione e meccanismi affidabili di gestione degli accessi.

L'open banking ha inoltre favorito l'ingresso nel mercato di operatori FinTech e BigTech, contribuendo a ridefinire gli equilibri competitivi del settore. In questo contesto, l'esigenza di un quadro normativo uniforme sull'utilizzo dell'intelligenza artificiale assume un ruolo rilevante, anche al fine di evitare asimmetrie tra operatori e garantire condizioni di concorrenza equilibrate.

Un'altra criticità riguarda la distribuzione delle responsabilità tra i diversi soggetti coinvolti nel trattamento dei dati. La presenza di terze parti con accesso alle informazioni dei clienti rende più complesso stabilire chi è responsabile di cosa, in particolare per quanto riguarda la protezione dei dati personali e la sicurezza dei sistemi.

Si configura, in tal senso, una tensione strutturale tra apertura del mercato e tutela dei dati, che richiede un bilanciamento costante tra esigenze di innovazione e requisiti di sicurezza. In questo quadro, l'intervento del AI Act si inserisce in modo complementare rispetto alla PSD2, introducendo requisiti specifici per i sistemi di intelligenza artificiale che operano su dati sensibili o che incidono su decisioni rilevanti in ambito creditizio e nei servizi di pagamento.

#### Requisiti prudenziali e Basilea III/IV

Infine, l'adozione dell'intelligenza artificiale nel settore bancario deve risultare coerente con i requisiti prudenziali definiti dal comitato di Basilea la vigilanza bancaria<sup>85</sup>. Sebbene tali normative non disciplinino espressamente l'impiego delle Intelligenze Artificiali, esse incidono direttamente sulla loro applicazione, in particolare per quanto riguarda la gestione e il controllo dei modelli di rischio. Infatti il model risk management impone agli intermediari l'adozione di procedure strutturate di validazione, monitoraggio e revisione dei modelli, inclusi quelli basati su tecniche di machine learning. A ciò si affianca la necessità di integrare tali strumenti nei modelli nei processi di stress testing, al fine di valutarne la resilienza, anche in scenari avversi. Un ulteriore profilo riguarda la governance: gli organi di vertice devono essere in grado di comprendere, almeno nelle linee essenziali, il funzionamento dei modelli adottati, così da poter assumere decisioni consapevoli e coerenti con la strategia di rischio dell'istituto.

L'interpretazione dei modelli complessi, come le reti neurali, rappresenta una sfida significativa. La natura opaca di questi algoritmi mette in discussione l'efficacia degli strumenti tradizionali di validazione, rendendo necessario un ripensamento delle metodologie di controllo. In particolare, occorre adattare le procedure consolidate alle peculiarità dei sistemi di apprendimento automatico, che spesso operano come vere e proprie "black box".

---

<sup>85</sup> Comitato di Basilea per la vigilanza bancaria, *Basel III: Finalising post-crisis reforms*, Basilea, Bank for International Settlements, 2017, pp. 3–10.

Nel complesso, l'impiego dell'intelligenza artificiale nel settore bancario si inserisce in un quadro normativo articolato e multilivello. Gli intermediari devono confrontarsi con un insieme coordinato di disposizioni che includono l'AI Act, il Regolamento generale sulla protezione dei dati, la PSD2, la MiFID II, le direttive AMLD5 e AMLD6, oltre alla normativa prudenziale di riferimento.

In tale contesto, la sfida principale non consiste soltanto nel rispettare singoli obblighi, ma nell'integrare requisiti tecnologici e presidi organizzativi all'interno di un sistema di compliance coerente ed efficace.

Il confronto tra l'AI Act e la normativa settoriale evidenzia la presenza di alcune sovrapposizioni, che riflettono la stratificazione progressiva della regolazione europea in materia finanziaria e digitale. Nonostante tali ridondanze, l'AI Act introduce un elemento di discontinuità significativa, fondato su un approccio basato sul rischio che consente di graduare gli obblighi in funzione del livello di criticità dei sistemi di intelligenza artificiale. L'attenzione si concentra in particolare su profili quali la trasparenza, la tracciabilità dei processi decisionali e la gestione dei bias, che assumono un ruolo centrale soprattutto nei sistemi classificati come ad alto rischio.

Rispetto al GDPR introduce un ulteriore livello di regolamentazione: entrambe i testi condividono la centralità della protezione dei dati e della trasparenza, ma l'AI Act sposta l'attenzione sui requisiti tecnici e procedurali del modello di intelligenza artificiale non limitandosi quindi al solo profilo relativo alla privacy.

Il DORA regola la resilienza operativa delle infrastrutture ICT nel settore finanziario.<sup>86</sup> Seppur la prospettiva sia differente, è evidente come risulti interconnessa con la prospettiva dell'AI Act: la sicurezza informatica che deve garantire il sistema bancario che voglia sfruttare l'AI non può prescindere da un'adeguata resilienza ICT.

Questa complessità normativa rappresenta una sfida significativa, ma anche un'opportunità per sviluppare sistemi di governance avanzati che rafforzino la fiducia dei clienti e degli investitori.

Il quadro normativo, nel complesso, appare destinato a evolversi ulteriormente, anche alla luce del rapido sviluppo tecnologico, rendendo verosimile un progressivo adattamento alle regole esistenti piuttosto che una loro definitiva stabilizzazione.

### **2.3 Interpretazione della letteratura scientifica italiana dell'AI Act**

La letteratura giuridica recente ha dedicato crescente attenzione all'adozione dell'AI Act, analizzandone sia la struttura complessiva sia le implicazioni applicative nei diversi settori, incluso quello bancario e finanziario. In particolare, parte della dottrina ha evidenziato come l'impianto del

---

<sup>86</sup> Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, *Digital Operational Resilience Act (DORA)*, Bruxelles, 2022, artt. 5–11.

regolamento si fondi su un approccio risk-based, volto a graduare gli obblighi normativi in funzione del livello di rischio associato ai sistemi di intelligenza artificiale, con particolare riferimento alle applicazioni classificate come ad alto rischio.

In questo ambito, alcuni contributi hanno sottolineato come tale modello rappresenti un tentativo di bilanciare esigenze di innovazione tecnologica e tutela dei diritti fondamentali, pur evidenziando la presenza di profili di complessità legati all'effettiva implementazione delle misure previste. È stato osservato, infatti, che la gestione del rischio affidata agli operatori richiede lo sviluppo di sistemi interni di governance articolati, in grado di integrare valutazioni tecniche, giuridiche e organizzative.<sup>87</sup>

Un ulteriore filone della dottrina si è concentrato sui meccanismi di governance e di enforcement del regolamento, soffermandosi sul ruolo delle autorità europee e nazionali nella supervisione dei sistemi di intelligenza artificiale. In tale prospettiva, è stato evidenziato come l'efficacia dell'AI Act dipenda in larga misura dalla capacità di coordinamento tra i diversi livelli di governance, nonché dalla disponibilità di competenze tecniche adeguate a valutare sistemi complessi e spesso opachi.<sup>88</sup>

Particolare attenzione è stata inoltre dedicata al tema della trasparenza e della spiegabilità degli algoritmi, soprattutto in relazione ai sistemi basati su tecniche di machine learning. La dottrina ha rilevato come, in presenza di modelli caratterizzati da elevata complessità, la piena intelligibilità dei processi decisionali risulti difficilmente raggiungibile, ponendo interrogativi circa l'effettività degli obblighi informativi e dei diritti riconosciuti agli utenti.<sup>89</sup>

In questa prospettiva si inseriscono anche i contributi che analizzano il rapporto tra AI Act e altre discipline rilevanti, in particolare il Regolamento generale sulla protezione dei dati e la normativa settoriale bancaria e finanziaria.

La sovrapposizione di diversi livelli normativi ha indotto parte della dottrina a sottolineare la necessità di un coordinamento sistematico tra le fonti, per evitare duplicazioni di obblighi e incertezze interpretative. In letteratura giuridica sono numerosi i contributi che affrontano questa problematica; tra questi, Nicoletta Rangone e Luca Megale<sup>90</sup> hanno analizzato criticamente l'approccio adottato dall'AI Act rispetto alla tutela dei diritti e all'efficacia delle misure regolamentari, evidenziando come la disciplina dell'intelligenza artificiale richieda una chiara sintesi tra principi generali e applicazioni settoriali. OBJ

---

<sup>87</sup> E. Fameli, La nuova intelligenza artificiale e il problema della sua regolazione giuridica, in *Rivista italiana di informatica e diritto*, 2025.

<sup>88</sup> R. Novelli, A. Hacker, A. Morley, J. Trondal, L. Floridi, A Robust Governance for the AI Act, 2024 (working paper / preprint)

<sup>89</sup> A. Mantelero, The Fundamental Rights Impact Assessment in the AI Act, 2024 (working paper / preprint)

<sup>90</sup> Nicoletta Rangone e Luca Megale, *Risks Without Rights: The EU AI Act's Approach to AI in Law and Rulemaking*, Cambridge University Press, 2023,

Alcuni autori, in particolare, hanno posto l'accento sulla funzione del regolamento quale strumento di gestione del rischio sistemico, indicando come l'intelligenza artificiale non incida esclusivamente sul piano delle singole decisioni automatizzate, ma sollevi questioni rilevanti anche in relazione alla stabilità complessiva dei mercati e degli intermediari.

In tale contesto, l'attenzione si sposta dalla dimensione individuale della responsabilità alla necessità di garantire presidi organizzativi e meccanismi di controllo idonei a prevenire effetti aggregati indesiderati.

Nel complesso, la letteratura evidenzia un consenso diffuso circa la rilevanza dell'AI Act come primo tentativo organico di regolazione dell'intelligenza artificiale a livello europeo, pur persistendo un dibattito significativo in merito alla sua effettiva capacità di affrontare le sfide poste dall'evoluzione tecnologica e dalla crescente diffusione di sistemi algoritmici nei processi decisionali.<sup>91</sup>

## **2.4 Considerazioni sulla Legge italiana recepimento AI Act**

L'intervento del legislatore italiano in materia di intelligenza artificiale si colloca in una fase ancora iniziale del processo di adattamento dell'ordinamento interno al quadro europeo delineato dall'AI Act. La Legge 23 settembre 2025 n. 132, pur rappresentando un passaggio significativo, presenta una struttura in larga parte programmatica, caratterizzata da principi generali e da ampie deleghe al Governo per l'adozione di misure attuative.<sup>92</sup> Tale impostazione, se da un lato consente una certa flessibilità rispetto all'evoluzione tecnologica, dall'altro rinvia a una fase successiva la definizione di aspetti essenziali, con possibili riflessi sulla certezza del diritto.

Un primo profilo di rilievo riguarda il coordinamento tra la disciplina nazionale e quella europea. La natura direttamente applicabile dell'AI Act riduce gli spazi di intervento del legislatore interno, che è chiamato principalmente a disciplinare profili organizzativi e a individuare le autorità competenti. Tuttavia, la scelta di affiancare al regolamento europeo una normativa nazionale autonoma rischia, in alcuni casi, di generare sovrapposizioni non sempre agevoli da gestire sul piano operativo, soprattutto per gli operatori che già si confrontano con un sistema multilivello particolarmente articolato. Un ulteriore elemento di complessità concerne la distribuzione delle competenze tra le diverse autorità coinvolte. La legge individua una pluralità di soggetti istituzionali chiamati a svolgere funzioni di vigilanza e controllo, senza tuttavia delineare in modo del tutto puntuale i meccanismi di coordinamento tra gli stessi. In assenza di un assetto chiaramente definito, il rischio è quello di una frammentazione delle competenze, con possibili ricadute sull'efficacia complessiva dell'attività di

---

<sup>91</sup> G. Lemme, La proposta di regolamento europeo sull'intelligenza artificiale e la gestione dei rischi: una battaglia che può essere vinta?, in *Rivista Trimestrale di Diritto dell'Economia*, Supplemento 1/2024

<sup>92</sup> Legge 23 settembre 2025, n. 132, Disposizioni e deleghe al Governo in materia di intelligenza artificiale

supervisione.<sup>93</sup>

Sul piano sostanziale, la normativa italiana recepisce e rafforza alcuni principi già presenti nel quadro europeo, quali il controllo umano, la trasparenza e la non discriminazione algoritmica. Tuttavia, la loro concreta applicazione resta in larga misura affidata all'elaborazione di standard tecnici e linee guida operative, che risultano ancora in fase di definizione. Infatti l'attuazione delle tutele è soggetta all'interpretazione delle autorità di vigilanza e dalle prassi adottate dagli operatori.<sup>94</sup>

Un altro tema importante riguarda i costi di compliance. L'introduzione di ulteriori livelli regolatori, anche se finalizzata a rafforzare la tutela dei diritti e la sicurezza dei sistemi, può incidere sull'organizzazione interna degli intermediari, imponendo l'adozione di modelli di governance più complessi e l'integrazione di competenze tecniche e giuridiche. In settori già fortemente regolati, come quello bancario, il rischio è quello di una stratificazione normativa che renda più onerosa la gestione complessiva degli obblighi.<sup>95</sup>

Nel complesso, la disciplina nazionale appare orientata a costruire un quadro di riferimento coerente con i principi europei, ma ancora in evoluzione sotto il profilo applicativo. La sua efficacia dipenderà, in larga misura, dalla capacità di sviluppare strumenti attuativi chiari e coordinati, nonché dalla definizione di prassi condivise tra autorità e operatori. In assenza di tali elementi, permane il rischio che la regolazione si traduca in un sistema formalmente articolato, ma non sempre pienamente efficace nel governare le trasformazioni tecnologiche in corso.

## **2.5 Sfide giuridiche emergenti e lacune normative**

Nonostante il significativo progresso normativo degli ultimi anni, l'introduzione dell'AI nel settore bancario continua a sollevare una serie di questioni aperte, che incidono sulla certezza del diritto e sulla ripartizione delle responsabilità tra i diversi attori coinvolti.

Una prima criticità riguarda l'attribuzione della responsabilità per i danni derivanti da decisioni algoritmiche errate. In assenza di criteri uniformi, risulta complesso stabilire se la responsabilità debba ricadere sul fornitore del sistema, sullo sviluppatore o sull'istituto che lo utilizza. Tale incertezza è particolarmente rilevante nei sistemi di credit scoring e nei modelli predittivi, dove le decisioni possono avere impatti significativi sui diritti dei clienti.

L'attribuzione della responsabilità per i danni derivanti da decisioni automatizzate adottate mediante sistemi di intelligenza artificiale resta uno dei profili più complessi in ambito giuridico. La questione si

---

<sup>93</sup> R. Novelli, A. Hacker, A. Morley, J. Trondal, L. Floridi, A Robust Governance for the AI Act, 2024

<sup>94</sup> A. Mantelero, The Fundamental Rights Impact Assessment in the AI Act, 2024

<sup>95</sup> G. Lemme, La proposta di regolamento europeo sull'intelligenza artificiale e la gestione dei rischi: una battaglia che può essere vinta?, in Rivista Trimestrale di Diritto dell'Economia, Supplemento 1/2024

inserisce in un contesto caratterizzato da una filiera tecnologica sempre più frammentata, nella quale intervengono soggetti diversi: sviluppatori del modello, fornitori dell'infrastruttura tecnologica, coloro che raccolgono e preparano i dati, tipicamente data analyst o data engineer, sviluppatori e integratori dei sistemi e, infine, chi utilizza il sistema, in questo caso l'istituto bancario. Risulta evidente dunque la difficoltà nell'attribuzione delle responsabilità a un unico attore per le autorità di governance e regolazione, che agiscono in ultima istanza in questo lungo e frammentato processo.

Se, da un lato, appare coerente attribuire un ruolo centrale all'intermediario finanziario, in quanto soggetto che utilizza il sistema e interagisce direttamente con il cliente, dall'altro lato non può essere ignorato il contributo determinante dei fornitori tecnologici nella definizione delle logiche decisionali. Ne deriva una forma di responsabilità "distribuita", che purtroppo non sempre si traduce in una imputazione giuridica chiara.

Nei sistemi più complessi, come quelli basati su tecniche di machine learning, risulta spesso problematico ricostruire ex post il percorso che ha condotto a una determinata decisione. Ciò rende più complesso individuare il nesso causale tra il funzionamento dell'algoritmo e l'eventuale danno subito dall'utente.

A differenza dei modelli tradizionali, fondati su regole note e verificabili in modo diretto, gli algoritmi di apprendimento automatico elaborano le proprie logiche decisionali in maniera autonoma, a partire dai dati utilizzati nella fase di addestramento. Il processo decisionale, dunque, non è immediatamente intelligibile, né completamente ricostruibile attraverso una lettura ex ante delle regole, come avviene nei sistemi convenzionali.

Questa caratteristica incide in modo significativo sul piano giuridico, soprattutto quando è necessario accertare responsabilità o valutare eventuali profili di errore. In assenza di una chiara trasparenza del modello, la prova del collegamento tra comportamento del sistema e conseguenze prodotte può risultare particolarmente complessa, anche in presenza di strumenti. Questo comporta che il comportamento del sistema non sia interamente riconducibile a una sequenza di istruzioni esplicitamente programmate, ma piuttosto a un insieme di correlazioni statistiche che emergono dall'analisi dei dati. In altri termini, il processo decisionale non è sempre il risultato di scelte direttamente imputabili a un soggetto umano, ma di un'elaborazione autonoma del modello. La complessità aumenta ulteriormente nei sistemi che prevedono meccanismi di aggiornamento continuo o di apprendimento dinamico, nei quali il modello può modificare nel tempo i propri criteri decisionali in base ai nuovi dati raccolti. In tali ipotesi, la decisione finale risulta essere il prodotto di un processo evolutivo difficilmente cristallizzabile in un determinato momento. Da un punto di vista giuridico, ciò solleva interrogativi rilevanti in termini di imputabilità della condotta. È evidente che

quando il risultato deriva da un sistema che evolve nel tempo e che opera sulla base di logiche non interamente trasparenti, diventa complesso individuare quale sia il momento esatto in cui si è generato l'errore e, conseguentemente, quale soggetto possa esserne ritenuto responsabile. La complessità tecnica dei sistemi di machine learning dunque non rappresenta soltanto una questione ingegneristica, ma incide direttamente sulla struttura stessa delle categorie giuridiche tradizionali, mettendo in discussione modelli consolidati di imputazione della responsabilità. L'attuale quadro normativo, pur introducendo principi di accountability, non appare ancora del tutto adeguato a gestire tali criticità. Il rischio concreto è quello di una responsabilità diffusa ma difficilmente imputabile in modo puntuale, con conseguente incertezza applicativa e potenziali effetti distorsivi sul piano della tutela dei diritti. In questo scenario, parte della dottrina evidenzia come l'assenza di standard tecnici uniformi per la valutazione dei sistemi di intelligenza artificiale rischi di compromettere l'effettività della regolazione, generando applicazioni disomogenee e potenziali asimmetrie tra gli ordinamenti nazionali.<sup>96</sup>

Per quanto concerne la trasparenza dei modelli, l'impiego di tecniche di deep learning e di reti neurali rende difficile ricostruire il processo decisionale, creando tensioni con i principi di accountability e con le esigenze di audit richieste dalle autorità di vigilanza. In questo contesto, il rischio è che la trasparenza richiesta dalla normativa rimanga, almeno in parte, solo formale. Un nodo altrettanto importante è rappresentato dal tema della spiegabilità dei sistemi di intelligenza artificiale.

Il tema della discriminazione algoritmica rappresenta un'altra criticità rilevante. In questo ambito, assume rilievo il problema della qualità dei dati utilizzati per l'addestramento dei modelli, nonché della loro rappresentatività. I bias possono manifestarsi in diverse fasi del ciclo di vita del sistema: nella selezione dei dati, nella loro qualità e rappresentatività, nonché nelle scelte progettuali relative al modello. Un aspetto particolarmente problematico è rappresentato dal carattere spesso implicito di tali discriminazioni. A differenza delle forme tradizionali, infatti, il bias algoritmico non si fonda necessariamente su criteri espliciti, ma può emergere da correlazioni statistiche difficilmente individuabili, rendendo complessa sia la rilevazione del fenomeno sia la sua dimostrazione in sede giuridica. Possiamo dunque osservare come la tutela antidiscriminatoria tradizionale rischi di risultare in parte inadeguata, in quanto costruita su modelli di prova e categorie concettuali non sempre idonee a intercettare le dinamiche proprie dei sistemi automatizzati. Appare, quindi, sempre più necessario affiancare agli strumenti giuridici tradizionali nuove forme di controllo, come ad esempio

---

<sup>96</sup> Passador M.L. AI Act and the ECB: Steering Financial Supervision in the EU Columbia Journal of European Law 2025 pp. 17–20

audit algoritmici e meccanismi di monitoraggio continuo, al fine di garantire un'effettiva equità nei processi decisionali.

L'AI Act si inserisce in un contesto internazionale caratterizzato da quadri normativi frammentati<sup>97</sup>, che riflettono priorità economiche e politiche non sempre convergenti. L'Unione europea ha adottato un approccio improntato alla tutela preventiva dei diritti fondamentali, introducendo obblighi stringenti soprattutto per i sistemi classificati come ad alto rischio.<sup>98</sup> In altri ordinamenti, invece, prevalgono modelli più flessibili e maggiormente orientati alla promozione dell'innovazione tecnologica. Negli Stati Uniti, ad esempio, l'intervento normativo si è sviluppato in modo più frammentato e settoriale<sup>99</sup>, lasciando ampi margini di autonomia agli operatori; in Cina, al contrario, la regolazione dell'intelligenza artificiale si inserisce in una strategia più ampia di controllo e sviluppo tecnologico, con un forte ruolo dello Stato.<sup>100</sup>

Queste differenze si riflettono in modo diretto sull'operatività degli intermediari finanziari che operano su scala globale. Un istituto bancario europeo che utilizzi sistemi di intelligenza artificiale per il credit scoring, ad esempio, è tenuto a rispettare i requisiti dell'AI Act in materia di trasparenza, gestione del rischio e supervisione umana. Lo stesso sistema, se impiegato in altri contesti giurisdizionali, potrebbe essere soggetto a obblighi meno stringenti o strutturati in modo diverso, generando complessità nella gestione dei modelli e nei processi di compliance.

In questo scenario si inserisce anche il rischio di arbitraggio normativo.<sup>101</sup> Le imprese tecnologiche e finanziarie potrebbero essere incentivate a localizzare alcune attività – come lo sviluppo o l'addestramento degli algoritmi – in giurisdizioni caratterizzate da requisiti meno rigorosi, per poi offrire i propri servizi su mercati più regolati. Dinamiche di questo tipo sono già osservabili nel settore delle piattaforme digitali, come nel Digital Markets Act pubblicato dalla Commissione Europea, potrebbero estendersi anche all'ambito dell'intelligenza artificiale applicata ai servizi finanziari. Ne deriva una possibile tensione sul piano competitivo. Un quadro regolatorio particolarmente rigoroso, se non accompagnato da un adeguato coordinamento internazionale, rischia di incidere sui costi di conformità degli operatori europei, soprattutto nel confronto con grandi gruppi globali dotati di maggiori risorse e capacità di adattamento.

In prospettiva, si pone quindi il problema della capacità dell'Unione europea di promuovere standard regolatori<sup>102</sup> in grado di affermarsi anche oltre i propri confini, secondo una logica già emersa in altri

---

<sup>97</sup> European Commission, White Paper on Artificial Intelligence, 2020

<sup>98</sup> V. AI Act, considerando e artt. 6 ss.

<sup>99</sup> National Institute of Standards and Technology (NIST), AI Risk Management Framework, 2023.

<sup>100</sup> Cyberspace Administration of China, Regulations on Algorithmic Recommendation, 2022.

<sup>101</sup> V. Financial Stability Board, report su regolazione finanziaria internazionale.

<sup>102</sup> Anu Bradford, The Brussels Effect, 2020.

ambiti della regolazione digitale. Al tempo stesso, risulta necessario evitare che l'elevato livello di tutela perseguito si traduca in uno svantaggio competitivo per gli operatori interni, in un contesto caratterizzato da crescente interconnessione tra mercati e tecnologie.

La sfida consiste nel trovare un equilibrio tra esigenze di tutela e competitività, in un contesto tecnologico in continua evoluzione.

É inoltre doveroso considerare l'aumento significativo degli oneri di compliance, che l'introduzione dell'AI Act comporta per gli istituti bancari, incidendo non solo sul piano giuridico, ma anche su quello organizzativo ed economico. L'adeguamento ai nuovi requisiti implica infatti investimenti rilevanti in termini di risorse umane, infrastrutture tecnologiche e processi interni. Tali adempimenti richiedono competenze altamente specializzate, non sempre facilmente reperibili, soprattutto per gli operatori di dimensioni minori. Ne deriva una potenziale asimmetria tra grandi gruppi bancari, dotati di risorse adeguate, e istituti di dimensioni più contenute, per i quali i costi di adeguamento potrebbero risultare particolarmente gravosi. In tal senso, il rischio è che la regolamentazione, pur perseguendo finalità condivisibili, finisca per incidere sulla struttura concorrenziale del mercato. Si dovrebbero, quindi, monitorare attentamente gli effetti economici della normativa, al fine di evitare che l'eccessiva complessità degli obblighi possa tradursi in una barriera all'entrata o in un freno all'innovazione, soprattutto per gli operatori più piccoli.<sup>103</sup>

#### Lacune normative principali

Accanto alle sfide sopra evidenziate, permangono alcune lacune normative che incidono sull'effettiva applicazione della disciplina. In primo luogo, la definizione dei confini della responsabilità tra sviluppatori, fornitori e utilizzatori finali rimane ancora incerta. In particolare, nei casi in cui i modelli operino come black box, risulta difficile individuare il nesso tra decisione algoritmica e danno prodotto. Parte della dottrina ha evidenziato come ciò possa tradursi, in concreto, in un aggravamento della posizione degli intermediari, esposti a forme di responsabilità difficilmente delimitabili. Un secondo profilo riguarda la tutela del cliente nei processi decisionali automatizzati. Sebbene l'AI Act preveda obblighi di trasparenza, la concreta attuazione del principio di spiegabilità presenta limiti evidenti, soprattutto nei sistemi più complessi. Ciò rischia di creare un divario tra la tutela prevista a livello normativo e la sua effettiva applicazione. Ulteriori criticità emergono in relazione alla valutazione del rischio.

---

<sup>103</sup> G. Lemme, La proposta di regolamento europeo sull'intelligenza artificiale e la gestione dei rischi: una battaglia che può essere vinta?, in Rivista Trimestrale di Diritto dell'Economia, Supplemento 1/2024

L'assenza di criteri pienamente standardizzati può determinare approcci divergenti tra gli Stati membri, con la conseguenza che gli intermediari sono spesso chiamati a sviluppare modelli interni di controllo particolarmente complessi. In tale quadro, il rafforzamento delle pratiche di model risk management e dei sistemi di audit continuo assume un ruolo centrale, pur comportando costi organizzativi non trascurabili.

Particolarmente delicata risulta, inoltre, l'integrazione tra l'AI Act e le normative già esistenti, quali il Regolamento generale sulla protezione dei dati e la disciplina antiriciclaggio. La sovrapposizione di obblighi, non sempre perfettamente coordinati, è suscettibile di generare incertezze interpretative e duplicazioni nei processi di compliance, rendendo più complessa la gestione operativa da parte degli intermediari.

Ne consegue l'esigenza di un bilanciamento sempre più articolato tra obiettivi diversi, quali la trasparenza dei processi decisionali, la protezione dei dati personali e la prevenzione dei rischi finanziari. A ciò si aggiungono alcune criticità relative ai meccanismi di vigilanza. L'assenza di un sistema di supervisione pienamente integrato, capace di combinare audit algoritmico, controlli di sicurezza e verifiche sui bias, rischia infatti di limitarne l'efficacia sul piano preventivo. In questa prospettiva, permane il rischio che l'intervento regolatorio assuma una funzione prevalentemente reattiva, intervenendo a valle delle criticità piuttosto che anticiparle in modo efficace.

Nel complesso, l'AI Act rappresenta un passaggio significativo verso una regolamentazione più strutturata dell'intelligenza artificiale. Le lacune ancora presenti evidenziano tuttavia la necessità di ulteriori sviluppi, sia sul piano normativo sia su quello interpretativo. L'evoluzione tecnologica, per sua natura dinamica, sembra infatti richiedere un adattamento continuo delle regole, più che una loro definitiva stabilizzazione.

In questo scenario, la sfida principale sarà quella di garantire un equilibrio efficace tra innovazione, tutela dei diritti e sostenibilità degli oneri regolatori per gli operatori del settore.

## **Conclusioni**

L'analisi condotta nel presente capitolo ha evidenziato come l'introduzione dell'AI Act rappresenti un passaggio cruciale nel processo di regolazione dell'intelligenza artificiale a livello europeo, incidendo in maniera significativa anche sul settore bancario e finanziario. L'approccio basato sul rischio adottato dal legislatore europeo consente, da un lato, di graduare gli obblighi in funzione delle potenziali criticità dei sistemi utilizzati, ma, dall'altro, pone rilevanti sfide applicative, soprattutto nei contesti caratterizzati da elevata complessità tecnologica. In particolare, è emerso come l'utilizzo dell'intelligenza artificiale nel settore bancario produca effetti che vanno ben oltre il piano dell'efficienza operativa, incidendo su profili centrali quali la tutela dei diritti fondamentali, l'equità nei processi decisionali e la stabilità complessiva del sistema finanziario. I rischi connessi al bias algoritmico, alla scarsa trasparenza dei modelli decisionali e alla possibile convergenza dei

comportamenti tra operatori rappresentano, infatti, elementi che richiedono un'attenta valutazione, sia da parte del legislatore, sia delle autorità di vigilanza. Allo stesso tempo, il capitolo ha messo in luce come la regolazione dell'intelligenza artificiale non possa essere affrontata esclusivamente attraverso strumenti normativi tradizionali.

La rapidità dell'innovazione tecnologica e la natura dinamica dei sistemi algoritmici richiedono un approccio regolatorio flessibile, capace di adattarsi nel tempo e di integrare competenze di diversa natura. Il ruolo delle autorità di vigilanza assume, dunque, un rilievo crescente, non soltanto sotto il profilo del controllo, ma anche in funzione di supporto agli operatori nell'adozione di pratiche conformi e responsabili.

Non mancano, tuttavia, elementi di criticità. L'assenza di standard tecnici pienamente condivisi, unitamente al rischio di divergenze interpretative tra gli Stati membri, può incidere sull'uniformità applicativa della disciplina e, di conseguenza, sulla sua efficacia complessiva. A ciò si aggiunge la difficoltà di rendere effettivamente trasparenti e spiegabili i sistemi più complessi, aspetto che solleva interrogativi circa la capacità delle norme vigenti di garantire una tutela sostanziale degli utenti. L'AI Act rappresenta, in questo quadro, un passaggio significativo verso una regolamentazione più organica dell'intelligenza artificiale, senza tuttavia esaurire le esigenze di intervento. La sfida, in prospettiva, consiste nel mantenere un equilibrio tra esigenze di innovazione e obiettivi di tutela, evitando sia il rischio di un'eccessiva rigidità normativa, sia quello di una regolazione inadeguata rispetto alla rapidità delle trasformazioni in atto.

Proprio alla luce di tali criticità e delle implicazioni operative della disciplina analizzata, appare particolarmente rilevante interrogarsi su come la normativa venga percepita e concretamente applicata all'interno delle istituzioni bancarie.

Nel prossimo capitolo analizzerò gli ambiti di applicazione dell'AI nel settore bancario, evidenziandone gli impatti economici e strategici. Infine, analizzerò l'impatto dell'intelligenza artificiale sul mercato del lavoro bancario, distinguendo tra automazione e trasformazione delle mansioni, rischio occupazionale e nascita di nuove professionalità, con particolare attenzione al ruolo della formazione e del reskilling.

### Capitolo 3 L'impatto dell'intelligenza artificiale sul settore bancario e sul lavoro

L'evoluzione dei sistemi di intelligenza artificiale e la loro crescente applicazione nel settore bancario rappresentano uno dei fenomeni più significativi della trasformazione digitale contemporanea. Questa innovazione non riguarda soltanto l'ottimizzazione dei processi interni o la gestione dei dati finanziari, ma investe profondamente le dinamiche di interazione tra istituzioni, clienti e dipendenti, con implicazioni economiche, giuridiche e sociali di ampia portata.

L'intento del capitolo è analizzare le principali questioni normative connesse all'adozione dell'AI nel settore bancario, inquadrando anche una riflessione più ampia sulla trasformazione digitale dei media e delle istituzioni. Numerosi autori hanno osservato come la digitalizzazione dei servizi implichi un profondo ripensamento dei rapporti di potere e delle modalità di partecipazione sociale. Marshall McLuhan, nella sua analisi dei media come estensioni delle facoltà umane, suggeriva che ogni innovazione tecnologica ridefinisce non solo i mezzi ma anche le esperienze sociali e cognitive degli individui.<sup>104</sup> Shoshana Zuboff ha documentato come la raccolta e l'elaborazione dei dati da parte di sistemi automatizzati trasformi radicalmente le relazioni tra cittadini e istituzioni, generando nuove forme di sorveglianza e dipendenza dai sistemi algoritmici.<sup>105</sup> Questi approcci teorici aiutano a comprendere il significato profondo della digitalizzazione bancaria, che va oltre la semplice automazione dei processi, ma incide sulla fiducia, l'equità e la percezione del rischio da parte dei clienti.

Dal punto di vista storico e sociologico, è interessante osservare come alcune dinamiche emergenti richiamino fenomeni già osservati durante la Rivoluzione Industriale. All'epoca, l'introduzione delle macchine in fabbrica determinò forme di resistenza operaia, note come "sabotaggio", finalizzate a proteggere la dignità del lavoro umano e a denunciare l'alienazione tecnologica. Il termine serviva da Sabot, che in francese significa Zoccolo: durante la rivoluzione industriale le donne infilavano le loro calzature all'interno degli ingranaggi per sabotarli, proprio per paura che le macchine sottraessero lavoro all'uomo. L'automazione dei servizi bancari, oggi guidata da algoritmi e intelligenze artificiali, genera preoccupazioni analoghe: se da un lato migliora l'efficienza e la rapidità delle operazioni, dall'altro rischia di ridurre i posti di lavoro, ma anche la capacità dei clienti di comprendere i processi decisionali, di interagire con operatori umani e di percepire la banca come istituzione affidabile e vicina.

---

<sup>104</sup> M. McLuhan, *Understanding Media: The Extensions of Man*, MIT Press, 1994

<sup>105</sup> S. Zuboff, *The Age of Surveillance Capitalism*, PublicAffairs, 2019

Scenari distopici e letterari offrono un'utile lente interpretativa per tali fenomeni. Nel romanzo *Player Piano* di Kurt Vonnegut, la gestione dell'economia è totalmente automatizzata e l'uomo perde progressivamente controllo e autonomia; in *The Circle* di Dave Eggers, le piattaforme digitali centralizzano ogni aspetto della vita dei cittadini, comprese le decisioni finanziarie, rendendo opache le logiche di valutazione. Anche il cinema ha esplorato queste tematiche: in *Minority Report* (Spielberg, 2002) e *I, Robot* (Proyas, 2004), scene di sportelli automatizzati senza operatori umani illustrano le potenziali conseguenze di una totale sostituzione dell'interazione personale con l'interazione macchina-cliente, anticipando questioni di fiducia, trasparenza e responsabilità che il legislatore oggi cerca di affrontare con l'AI Act.

Il capitolo si propone quindi di affrontare la regolazione dell'intelligenza artificiale nel settore bancario secondo una prospettiva multidisciplinare. Verranno inquadrati i principali profili giuridici, con particolare riferimento all'AI Act, al GDPR e alle normative nazionali di recente emanazione, ma anche i risvolti economici e organizzativi dell'adozione dell'AI, con attenzione alla relazione banca-cliente e alla percezione dei dipendenti.

In definitiva, l'obiettivo del capitolo è fornire un quadro articolato in grado di collegare l'evoluzione tecnologica alle sue implicazioni sociali, economiche e normative, offrendo così un contesto integrato per la successiva analisi empirica basata sui questionari somministrati a clienti e operatori bancari.

### **3.1 Ambiti di applicazione dell'intelligenza artificiale nel settore bancario**

L'intelligenza artificiale rappresenta oggi uno dei principali fattori di trasformazione del settore bancario, incidendo in modo significativo sia sull'organizzazione interna degli istituti sia sulle modalità di interazione con la clientela. In questa prospettiva, l'adozione di soluzioni basate su AI non si limita a introdurre strumenti innovativi, ma comporta una revisione più ampia dei modelli operativi e decisionali, orientata a una maggiore efficienza, rapidità e personalizzazione dei servizi.<sup>106</sup> L'obiettivo di questa sezione è quello di analizzare i principali ambiti in cui tali tecnologie trovano concreta applicazione, evidenziandone le implicazioni operative e strategiche.

Un primo ambito di utilizzo riguarda i processi interni delle banche, in particolare le attività di back-office, compliance e risk management. In questi contesti, l'intelligenza artificiale consente di automatizzare operazioni ripetitive e numerose, come la gestione documentale, la verifica delle transazioni e il controllo dei requisiti normativi, riducendo il margine di errore umano e migliorando l'efficienza complessiva.<sup>107</sup> Nell'ambito del risk management, inoltre, gli algoritmi sono in grado di

---

<sup>106</sup> McKinsey & Company, *Global Banking Annual Report*, 2023

<sup>107</sup> Deloitte, *AI in Banking: Applications and Implications*, 2022

analizzare grandi quantità di dati in tempo reale, supportando la valutazione del rischio di credito e l'individuazione di potenziali frodi con maggiore precisione rispetto ai metodi tradizionali.<sup>108</sup>

Un secondo ambito rilevante è rappresentato dai servizi rivolti alla clientela. Le banche stanno progressivamente integrando strumenti di intelligenza artificiale, come chatbot e assistenti virtuali, per fornire supporto continuo e immediato agli utenti, migliorando l'accessibilità e la qualità del servizio.<sup>109</sup> Parallelamente, si stanno diffondendo soluzioni di consulenza automatizzata (robo-advisory), che consentono di offrire suggerimenti personalizzati in materia di investimenti sulla base del profilo del cliente, delle sue esigenze e dei dati disponibili.<sup>110</sup> Queste innovazioni contribuiscono a rendere l'esperienza bancaria più fluida e personalizzata, pur sollevando interrogativi sul ruolo del fattore umano nella relazione fiduciaria tra banca e cliente.

Infine, l'intelligenza artificiale trova ampia applicazione nelle attività di marketing e nell'analisi dei dati. Le banche utilizzano modelli avanzati di data analytics per segmentare la clientela, prevedere comportamenti e preferenze e sviluppare offerte mirate.<sup>111</sup> In questo senso, i dati assumono un valore strategico centrale, in quanto permettono non solo di ottimizzare le strategie commerciali, ma anche di anticipare i bisogni dei clienti, migliorando la competitività degli istituti. L'integrazione dell'AI in questi ambiti evidenzia come il settore bancario stia evolvendo verso un modello sempre più data-driven, in cui la capacità di raccogliere, elaborare e interpretare le informazioni rappresenta un vantaggio competitivo determinante.<sup>112</sup>

### **3.2 Impatti economici e strategici dell'intelligenza artificiale nel settore bancario**

L'introduzione dell'intelligenza artificiale nel settore bancario sta producendo effetti rilevanti non solo sul piano operativo, ma anche in termini di performance economiche e scelte strategiche degli istituti. Le principali analisi condotte da società di consulenza e organismi internazionali evidenziano come l'adozione di tecnologie basate su AI possa determinare un incremento significativo della produttività, una crescita dei ricavi e un miglioramento della redditività complessiva.<sup>113</sup> Tali benefici derivano principalmente dalla capacità di automatizzare processi, ridurre i costi operativi e sviluppare modelli decisionali più efficaci. Tuttavia, una lettura critica di queste stime suggerisce come tali risultati non siano uniformemente distribuiti tra gli operatori del settore, ma tendano a favorire in misura maggiore

---

<sup>108</sup> European Central Bank, *Artificial Intelligence in Banking: Opportunities and Challenges*, 2021

<sup>109</sup> Accenture, *Banking Consumer Study: The Rise of AI-Powered Banking*, 2023

<sup>110</sup> OECD, *Artificial Intelligence in Finance*, 2021

<sup>111</sup> PwC, *Financial Services Technology 2020 and Beyond*, 2020

<sup>112</sup> World Economic Forum, *The Future of Financial Services*, 2022

<sup>113</sup> Accenture, *Banking on AI: Transforming Financial Services*, 2023

gli istituti di grandi dimensioni, dotati delle risorse necessarie per sostenere gli elevati investimenti richiesti.

In questo contesto, assume un ruolo centrale il tema dei dati, che rappresentano uno degli asset strategici più rilevanti nella cosiddetta data economy bancaria. Le informazioni relative ai comportamenti, alle preferenze e alle abitudini finanziarie dei clienti costituiscono infatti la base per l'addestramento degli algoritmi e per lo sviluppo di servizi sempre più personalizzati.<sup>114</sup>

Le banche non si limitano più a utilizzare i dati come supporto alle decisioni, ma li trasformano in una vera e propria fonte di valore, in grado di incidere direttamente sulla creazione di vantaggi competitivi. Ciò comporta una crescente attenzione alla capacità di raccolta, gestione e analisi dei dati, nonché alle tematiche connesse alla sicurezza e alla protezione delle informazioni.

Un ulteriore effetto dell'adozione dell'intelligenza artificiale riguarda il processo di concentrazione del settore bancario. La necessità di disporre di una maggiore "massa critica", in termini di capitale, clientela e dati, sta favorendo dinamiche di fusione e acquisizione, con l'obiettivo di rafforzare la posizione competitiva degli istituti.<sup>115</sup> Questo fenomeno risulta particolarmente rilevante nel contesto europeo, dove la frammentazione del sistema bancario rappresenta storicamente un elemento di debolezza. Tuttavia, tali dinamiche possono generare criticità per gli istituti di minori dimensioni, che rischiano di non riuscire a sostenere i costi dell'innovazione tecnologica e di essere progressivamente esclusi dal mercato o costretti a esternalizzare parte delle proprie attività.

Accanto agli effetti economici e strutturali, l'intelligenza artificiale incide in modo significativo anche sul mercato del lavoro bancario. In particolare, è possibile distinguere tra processi di automazione, che comportano la sostituzione di alcune mansioni, soprattutto quelle più ripetitive e standardizzate, e processi di trasformazione del lavoro, in cui le tecnologie digitali si affiancano all'attività umana, modificandone contenuti e modalità operative.<sup>116</sup> Se da un lato l'automazione può determinare un rischio occupazionale nel breve periodo, dall'altro l'evoluzione tecnologica favorisce la nascita di nuove figure professionali, caratterizzate da competenze avanzate in ambito digitale, analitico e gestionale.

In questo scenario, la formazione e il reskilling assumono un ruolo cruciale per garantire l'adattamento della forza lavoro ai cambiamenti in atto. La rapidità dell'innovazione tecnologica rende infatti necessario un aggiornamento continuo delle competenze, al fine di evitare fenomeni di

---

<sup>114</sup> OECD, Data-Driven Innovation in Finance, 2021

<sup>115</sup> European Central Bank, Financial Stability Review, 2022

<sup>116</sup> McKinsey Global Institute, The Future of Work in Banking, 2023

obsolescenza professionale e di favorire una integrazione efficace tra uomo e macchina.

Ne deriva l'esigenza di ripensare non solo le politiche aziendali, ma anche i sistemi di istruzione e formazione, in un'ottica di apprendimento permanente che consenta di affrontare in modo sostenibile le trasformazioni indotte dall'intelligenza artificiale.<sup>117</sup>

### **3.3 Uomo e intelligenza artificiale: modelli di collaborazione**

L'evoluzione dell'intelligenza artificiale nel settore bancario non si traduce esclusivamente in processi di sostituzione del lavoro umano, ma si configura sempre più come un fenomeno di integrazione tra competenze umane e capacità algoritmiche. In tale contesto, assume particolare rilevanza il paradigma della human-AI collaboration, che descrive un modello organizzativo in cui l'intelligenza artificiale affianca il lavoratore, potenziandone le capacità decisionali e operative. Questo approccio consente di superare una visione puramente sostitutiva della tecnologia, evidenziando come il valore aggiunto derivi dalla combinazione tra l'intuizione, l'esperienza e il giudizio umano e la capacità dell'AI di elaborare grandi quantità di dati in tempi rapidi.<sup>118</sup>

Le modalità di integrazione tra uomo e macchina si manifestano in diversi ambiti operativi. Ad esempio, nei processi di valutazione del merito creditizio, gli algoritmi possono analizzare una molteplicità di variabili (storico dei pagamenti, reddito, comportamento finanziario) e proporre un punteggio di rischio, lasciando tuttavia al gestore umano la decisione finale, soprattutto nei casi borderline o in presenza di elementi non pienamente codificabili. Analogamente, nei servizi di consulenza finanziaria, strumenti di robo-advisory elaborano portafogli di investimento sulla base del profilo dell'utente, mentre il consulente mantiene un ruolo di interpretazione, adattamento e relazione, soprattutto quando entrano in gioco obiettivi personali, propensione al rischio e dimensioni emotive del cliente.

Altri esempi riguardano l'assistenza clienti: i chatbot bancari sono in grado di gestire richieste semplici e ripetitive come per esempio informazioni su saldo, e assistenza tecnica, mentre i casi più complessi vengono trasferiti a operatori umani. In questo modo si realizza una forma di cooperazione sequenziale, in cui l'AI funge da primo filtro e il lavoratore interviene nelle fasi in cui è richiesta maggiore capacità di giudizio o empatia. Tuttavia, questa organizzazione può anche introdurre nuove forme di dipendenza tecnologica e ridefinire i tempi e le modalità del lavoro umano, che tende a concentrarsi su attività di supervisione e gestione delle eccezioni.

---

<sup>117</sup> World Economic Forum, The Future of Jobs Report, 2023

<sup>118</sup> Davenport, T. H., & Ronanki, R., Artificial Intelligence for the Real World, Harvard Business Review, 2018

Da un punto di vista più critico, l'integrazione tra uomo e intelligenza artificiale solleva anche questioni di natura epistemologica ed etica. In particolare, il cosiddetto problema della "scatola nera" (black box) evidenzia come molti sistemi di AI producano risultati senza che sia pienamente comprensibile il processo decisionale sottostante. Questo pone interrogativi sulla trasparenza e sull'affidabilità degli algoritmi, soprattutto in ambiti sensibili come quello finanziario, dove le decisioni hanno un impatto diretto sulla vita economica delle persone.<sup>119</sup> Inoltre, emerge il rischio che l'automazione progressiva conduca a una forma di "de-responsabilizzazione", in cui la responsabilità delle decisioni viene distribuita tra uomo e macchina in modo non sempre chiaramente definito.

Il rapporto tra uomo e macchina richiama alcune riflessioni filosofiche sul significato del lavoro e sul ruolo della tecnologia nella società. Il lavoro non rappresenta soltanto una fonte di reddito, ma anche uno spazio di realizzazione personale e di costruzione dell'identità. L'introduzione dell'intelligenza artificiale può essere letta come opportunità di liberare l'uomo dalle attività più ripetitive e alienanti, ma potrebbe portare alla riduzione del contributo umano a funzioni residuali o puramente di supervisione. Il punto di equilibrio tra queste due dimensioni dipende in larga misura dalle scelte organizzative, dalle politiche aziendali e dal contesto istituzionale in cui tali tecnologie vengono implementate.<sup>120</sup> Ciò porta alla ridefinizione del concetto stesso di competenza. Non si tratta più soltanto di possedere conoscenze tecniche specifiche, ma anche di sviluppare la capacità di interagire con sistemi intelligenti, interpretarne i risultati e comprenderne i limiti. Se letta in questa chiave, il lavoratore non è sostituito dalla tecnologia, ma si trasforma in un soggetto che opera in un ambiente aumentato (augmented working), in cui il valore delle decisioni nasce dall'interazione tra capacità umane e supporto algoritmico. Questo cambiamento richiede un approccio culturale nuovo, in cui tecnologia e umanità non sono in contrapposizione, ma componenti complementari di uno stesso sistema produttivo.<sup>121</sup>

### **3.4 Scenari futuri del settore bancario**

Si stanno delineando nuovi scenari per il settore bancario, in cui modelli organizzativi, processi operativi e modalità di interazione con la clientela risultano profondamente ridefiniti. È possibile individuare alcune traiettorie di sviluppo che rappresentano direzioni verso cui il sistema bancario potrebbe evolvere nei prossimi anni.

Un primo scenario è rappresentato dall'evoluzione verso il modello di banca come piattaforma (platform banking), in cui l'istituto non si limita più a erogare direttamente prodotti e servizi finanziari,

---

<sup>119</sup> European Commission, Ethics Guidelines for Trustworthy AI, 2019

<sup>120</sup> Floridi, L., The Ethics of Artificial Intelligence, Oxford University Press, 2021

<sup>121</sup> World Economic Forum, Shaping the Future of Work in the Age of AI, 2022

ma opera come intermediario in un ecosistema aperto, mettendo a disposizione infrastrutture digitali su cui operano anche soggetti terzi. In questa logica, la banca assume un ruolo simile a quello di un marketplace finanziario, in cui diversi attori offrono servizi integrati all'interno di un unico ambiente digitale. Tale modello consente di ampliare l'offerta, migliorare la personalizzazione dei servizi e sfruttare le sinergie derivanti dalla collaborazione tra operatori diversi.<sup>122</sup> Tuttavia, esso implica anche una maggiore complessità nella gestione dei dati e nella regolamentazione. Lo scenario può cambiare in base al possibile grado di digitalizzazione del settore. Da un lato, i servizi bancari potrebbero essere progressivamente erogati in modalità completamente digitale, attraverso canali online, applicazioni mobili e assistenti virtuali, riducendo al minimo la necessità di interazione fisica. Dall'altro lato, potrebbe invece permanere l'esigenza di mantenere una componente umana, soprattutto nelle attività che richiedono consulenza personalizzata, gestione di situazioni complesse o costruzione di relazioni di fiducia con la clientela. In questo senso, il futuro del settore bancario potrebbe configurarsi non come una sostituzione totale dell'interazione umana, ma come una sua riconfigurazione all'interno di un modello ibrido, in cui digitale e presenza fisica coesistono in modo complementare.<sup>123</sup>

Sul piano del lavoro, tali trasformazioni comportano una ridefinizione significativa dei ruoli e delle competenze richieste. Le attività più routinarie e standardizzate tendono a essere progressivamente automatizzate, mentre emergono nuove figure professionali legate alla gestione dei dati, alla supervisione dei sistemi di intelligenza artificiale, alla cybersecurity e all'analisi avanzata delle informazioni. Il lavoratore bancario del futuro sarà quindi sempre meno coinvolto in operazioni esecutive e sempre più impegnato in attività di controllo, interpretazione e gestione dei processi supportati dalla tecnologia. Questo cambiamento implica anche un'evoluzione organizzativa, con strutture aziendali più flessibili e orientate a competenze interdisciplinari.<sup>124</sup>

In questa prospettiva, la formazione continua e il **reskilling** assumono un ruolo centrale per accompagnare la transizione. La rapidità dell'innovazione tecnologica rende necessario un aggiornamento costante delle competenze, non solo tecniche ma anche trasversali, come la capacità di adattamento, il pensiero critico e le competenze relazionali. Inoltre, la gestione di questi cambiamenti richiede un approccio sistemico che coinvolga non solo le imprese, ma anche le istituzioni, i sistemi educativi e le parti sociali, al fine di garantire una transizione equilibrata e sostenibile.

---

<sup>122</sup> Gomber, P., Koch, J. A., & Siering, M., Digital Finance and FinTech: Current Research and Future Research Directions, *Journal of Business Economics*, 2017

<sup>123</sup> McKinsey & Company, *The Future of Banking: Customer Experience in a Digital World*, 2023

<sup>124</sup> World Economic Forum, *The Future of Jobs Report*, 2023

Infine, uno degli elementi più rilevanti nei futuri scenari del settore bancario riguarda il ruolo della fiducia. Anche in un contesto altamente digitalizzato, la relazione tra banca e cliente continua a basarsi su un rapporto fiduciario, che difficilmente può essere completamente sostituito da interazioni automatizzate. In termini filosofici, ciò richiama il tema del “limite” della tecnologia: se da un lato l’intelligenza artificiale è in grado di ottimizzare processi e migliorare l’efficienza, dall’altro non può sostituire completamente dimensioni qualitative come la fiducia, la responsabilità e il giudizio umano. Il futuro della banca, pertanto, non sembra orientato verso una totale disumanizzazione del servizio, quanto piuttosto verso una ridefinizione dell’equilibrio tra tecnologia e relazione umana, in cui entrambe contribuiscono, in modo diverso ma complementare, alla creazione di valore.<sup>125</sup>

L’adozione su larga scala di tecnologie basate sull’intelligenza artificiale si inserisce in un contesto di progressiva trasformazione del settore bancario, nel quale si osserva una tendenza sempre più marcata verso processi di concentrazione. Sebbene tali dinamiche non possano essere ricondotte esclusivamente all’impatto dell’AI Act o, più in generale, all’innovazione tecnologica, risulta evidente come la crescente centralità dei dati e degli strumenti di analisi avanzata stia contribuendo a ridefinire gli equilibri competitivi tra intermediari.<sup>126</sup>

L’implementazione di sistemi di intelligenza artificiale richiede investimenti significativi in infrastrutture digitali, capacità di gestione dei dati e sviluppo di competenze specialistiche. In questo contesto, gli operatori di maggiori dimensioni risultano avvantaggiati, potendo beneficiare di economie di scala e di una maggiore disponibilità di risorse. Ne deriva una pressione, seppur indiretta, verso forme di aggregazione o rafforzamento dimensionale, finalizzate a sostenere i costi dell’innovazione e a mantenere un adeguato livello di competitività.<sup>127</sup>

Le strategie adottate da alcuni grandi gruppi bancari europei confermano tale tendenza.

In particolare, istituti come UniCredit e ING hanno avviato negli ultimi anni rilevanti programmi di trasformazione digitale, con un crescente ricorso a tecnologie di intelligenza artificiale per l’analisi dei dati, la gestione del rischio e la personalizzazione dei servizi. Questi processi evidenziano come la competizione nel settore bancario si stia progressivamente spostando sul terreno tecnologico, rendendo sempre più centrale la capacità di sviluppare e integrare soluzioni avanzate.<sup>128</sup>

In tale quadro si collocano anche le recenti dinamiche di consolidamento del mercato bancario europeo, come nel caso delle interlocuzioni che hanno coinvolto Banco BPM e possibili operazioni con UniCredit o Crédit Agricole. Pur non essendo direttamente riconducibili all’adozione

---

<sup>125</sup> Floridi, L., *The Ethics of Artificial Intelligence*, Oxford University Press, 2021

<sup>126</sup> Commissione europea, *Artificial Intelligence in Financial Services*, 2021

<sup>127</sup> European Central Bank, *Financial Stability Review*, 2023

<sup>128</sup> European Banking Authority, *Report on the Use of Big Data and Advanced Analytics*, 2020

dell'intelligenza artificiale, tali operazioni si inseriscono in un contesto in cui la dimensione tecnologica rappresenta un fattore competitivo sempre più rilevante, contribuendo a rafforzare le logiche di concentrazione.<sup>129</sup>

La posizione di Banco BPM ha attirato una significativa attenzione da parte del mercato e degli operatori, in particolare con riferimento alle possibili prospettive di integrazione con UniCredit e Crédit Agricole.

Le prime ipotesi di aggregazione con UniCredit sono emerse già nel corso del 2022, in un contesto caratterizzato da una crescente pressione competitiva e dalla necessità di rafforzare la redditività degli intermediari bancari. In più occasioni, nel corso del 2023 e del 2024, tali scenari sono stati ripresi dalla stampa specializzata e dagli analisti finanziari, che hanno evidenziato la potenziale complementarità tra i due gruppi, soprattutto in termini di presenza territoriale e base clienti.<sup>130</sup>

Parallelamente, Crédit Agricole ha progressivamente consolidato la propria presenza nel capitale di Banco BPM, rafforzando il proprio posizionamento nel mercato italiano e alimentando ulteriori ipotesi circa una possibile operazione di acquisizione o integrazione. Tali sviluppi sono stati oggetto di attenzione mediatica nel corso del 2023–2025, anche alla luce delle strategie espansive del gruppo francese nel settore retail europeo.<sup>131</sup>

Nonostante la ricorrenza di tali ipotesi, nessuna operazione di acquisizione si è, finora, concretizzata. Le ragioni di tale esito devono essere ricondotte a una pluralità di fattori. In primo luogo, assumono rilievo le valutazioni economico-finanziarie e le condizioni di mercato, che incidono sulla determinazione del prezzo e sulla convenienza complessiva dell'operazione. Le divergenze tra le aspettative degli azionisti e le valutazioni degli acquirenti rappresentano, in questo senso, un elemento frequentemente ostativo alla conclusione delle trattative.

Sotto il profilo giuridico, assumono particolare rilevanza i vincoli derivanti dalla disciplina di vigilanza prudenziale e dal diritto della concorrenza. Operazioni di tale portata richiedono, infatti, l'autorizzazione della Banca Centrale Europea, nonché la verifica della loro compatibilità con le regole in materia di concentrazioni, con possibili interventi da parte delle autorità antitrust nazionali ed europee. Tali procedure comportano tempi e condizioni che possono incidere significativamente sulla fattibilità dell'operazione.<sup>132</sup>

Ulteriori elementi di complessità riguardano i profili organizzativi e tecnologici. L'integrazione tra gruppi bancari di grandi dimensioni implica, infatti, la necessità di armonizzare sistemi informatici,

---

<sup>129</sup> Comunicazioni societarie e notizie di mercato relative a Banco BPM, UniCredit e Crédit Agricole (2023–2025)

<sup>130</sup> Cfr. articoli di stampa economico-finanziaria (es. Il Sole 24 Ore, 2022–2024) sulle ipotesi di aggregazione tra UniCredit e Banco BPM

<sup>131</sup> Cfr. notizie e analisi di mercato su Crédit Agricole e la sua partecipazione in Banco BPM (Reuters, Financial Times, 2023–2025)

<sup>132</sup> Banca Centrale Europea, Guide on the assessment of mergers and acquisitions in the banking sector, 2021

modelli di gestione del rischio e infrastrutture digitali. La crescente diffusione di sistemi basati sull'intelligenza artificiale introduce ulteriori criticità, legate alla compatibilità tra modelli algoritmici, alla governance dei dati e al rispetto dei requisiti normativi in materia di trasparenza e controllo.<sup>133</sup>

Nel panorama recente del sistema bancario italiano, un ruolo di particolare rilievo è stato assunto dall'operazione che ha coinvolto Banca Monte dei Paschi di Siena (MPS) e Mediobanca, considerata una delle più significative operazioni di consolidamento degli ultimi anni. L'operazione è stata avviata formalmente nel gennaio 2025 attraverso un'offerta pubblica di scambio. Il contesto in cui si colloca è caratterizzato da una rinnovata attenzione verso la creazione di poli bancari di dimensioni maggiori, in grado di competere a livello europeo.<sup>134</sup> L'iniziativa ha progressivamente acquisito rilievo nel mercato, fino a registrare nel settembre 2025 una soglia di adesione superiore al 60% del capitale di Mediobanca, consentendo a Banca Monte dei Paschi di Siena di acquisire il controllo dell'istituto milanese.<sup>135</sup> Successivamente, i consigli di amministrazione delle due banche hanno approvato un progetto di fusione per incorporazione, la cui efficacia risulta subordinata sia al completamento dell'iter autorizzativo, sia all'approvazione da parte delle assemblee societarie, con una possibile attuazione entro la fine del 2026.<sup>136</sup>

L'operazione presenta elementi di particolare complessità anche in ambito giuridico in quanto si colloca nella disciplina delle concentrazioni bancarie, soggette all'autorizzazione della Banca Centrale Europea. La BCE ha, infatti, richiesto la predisposizione di un piano di integrazione dettagliato, comprensivo degli impatti su capitale, liquidità e sistemi informativi.<sup>137</sup> Tali requisiti evidenziano come le operazioni di fusione nel settore bancario non possano essere valutate esclusivamente sotto il profilo economico, ma richiedano una verifica approfondita.

L'operazione è stata attenzionata dalle autorità e della magistratura, con riferimento a possibili ipotesi di coordinamento tra azionisti rilevanti e a presunte irregolarità informative. Tali sviluppi hanno contribuito ad accrescere l'incertezza del mercato e a evidenziare la rilevanza dei requisiti di correttezza e trasparenza nelle operazioni di maggiore dimensione.

Non meno rilevanti risultano, infine, le tensioni emerse sul piano strategico e societario.

L'integrazione tra Banca Monte dei Paschi di Siena e Mediobanca ha infatti sollevato interrogativi circa la compatibilità tra modelli di business differenti, nonché circa il futuro assetto di partecipazioni strategiche, tra cui quella detenuta in Generali. La partecipazione di quest'ultima contribuisce a

---

<sup>133</sup> European Banking Authority, Report on Big Data and Advanced Analytics, 2020

<sup>134</sup> Banca Monte dei Paschi di Siena, comunicato stampa sull'offerta pubblica di scambio su Mediobanca, gennaio 2025

<sup>135</sup> Dati sull'adesione all'OPS e acquisizione del controllo (settembre 2025)

<sup>136</sup> Approvazione del progetto di fusione e concambio azionario (marzo 2026)

<sup>137</sup> Banca Centrale Europea, valutazione e requisiti per operazioni di M&A bancarie; cfr. anche obblighi di piano di integrazione

rendere l'operazione particolarmente delicata anche sotto il profilo degli assetti di governance. Assume particolare rilievo anche la dimensione tecnologica dell'operazione. La creazione di un gruppo bancario integrato implica la necessità di armonizzare infrastrutture digitali, sistemi di gestione dei dati e modelli di analisi avanzata. In particolare, l'adozione di strumenti basati sull'intelligenza artificiale richiede la convergenza di dataset eterogenei e di architetture algoritmiche differenti, con possibili implicazioni in termini di rischio operativo, trasparenza e controllo.<sup>138</sup>

L'esperienza dell'integrazione evidenzia come il successo dell'operazione sia strettamente legato alla capacità di unificare dati, canali e sistemi decisionali in tempi relativamente brevi, al fine di generare sinergie e sostenere l'innovazione. In assenza di tale integrazione, il rischio è quello di una frammentazione tecnologica che potrebbe compromettere i benefici attesi dall'operazione.

I casi analizzati evidenziano come le recenti dinamiche di consolidamento nel settore bancario non possano essere lette attraverso una chiave interpretativa univoca. Le operazioni che hanno coinvolto gli istituti sopracitati, mostrano come i processi di concentrazione siano il risultato di un equilibrio complesso tra fattori economici, vincoli regolatori e scelte strategiche. L'adozione di soluzioni basate sull'intelligenza artificiale, così come la centralità dei dati nei modelli di business bancari contribuiscono a ridefinire le condizioni della competizione. Tali elementi incidono indirettamente sulle strategie di crescita degli intermediari e sulle scelte relative a operazioni di aggregazione. Al tempo stesso, l'evoluzione tecnologica tende a rendere più complessi i processi di integrazione, soprattutto quando coinvolgono strutture organizzative articolate e sistemi informativi tra loro eterogenei, con conseguenti riflessi sulla gestione dei rischi. Le esperienze considerate mettono inoltre in luce il ruolo sempre più incisivo delle autorità di vigilanza, chiamate a valutare non soltanto la solidità finanziaria delle operazioni, ma anche la sostenibilità dei modelli organizzativi e tecnologici. L'attività di controllo si estende progressivamente anche ai profili legati alla governance dei dati e all'utilizzo di sistemi automatizzati, in linea con l'evoluzione del quadro normativo europeo.

Ne deriva che la concentrazione bancaria non può essere interpretata esclusivamente come risposta a esigenze di efficienza o di rafforzamento patrimoniale. Le trasformazioni tecnologiche in atto costituiscono infatti un elemento di sfondo sempre più rilevante, capace di incidere sulle condizioni di sostenibilità delle strategie di lungo periodo. L'intelligenza artificiale, pur non rappresentando il fattore determinante delle operazioni di integrazione,, contribuisce comunque a ridefinire il contesto competitivo entro cui esse si sviluppano, rendendo necessario un esame più ampio delle relative implicazioni, anche sotto il profilo giuridico e sistemico. Accanto a queste dinamiche, assume rilievo anche l'ingresso nel settore finanziario di operatori tecnologici globali quali Amazon e Google. Pur

---

<sup>138</sup> European Banking Authority, Report on Big Data and Advanced Analytics, 2020

non operando come intermediari bancari tradizionali in senso tradizionale, offrono servizi di pagamento, soluzioni di credito e strumenti avanzati di gestione dei dati finanziari. In questo modo contribuiscono a ridefinire i confini di mercato e ad accrescere la pressione competitiva sugli operatori tradizionali.

A partire dalla seconda metà degli anni 2010, Amazon ha progressivamente ampliato la propria offerta nel settore finanziario, introducendo servizi di credito rivolti ai venditori operanti sulla propria piattaforma (Amazon Lending) e soluzioni di pagamento integrate nei propri ecosistemi digitali. Tali servizi si basano in larga misura sull'analisi dei dati generati dagli utenti, consentendo alla società di sviluppare modelli di valutazione del rischio creditizio alternativi rispetto a quelli tradizionali, fondati su informazioni comportamentali e transazionali.<sup>139</sup>

Analogamente, Google ha sviluppato servizi di pagamento digitale (Google Pay) e ha avviato, seppur con esiti non sempre lineari, progetti volti a offrire conti correnti in collaborazione con istituti bancari (progetto "Plex"). Pur non configurandosi come intermediari bancari in senso stretto, tali operatori svolgono funzioni che si avvicinano a quelle tipiche del settore creditizio, ponendosi come interfaccia tra cliente e sistema finanziario.<sup>140</sup>

Sotto il profilo giuridico, l'ingresso delle BigTech solleva questioni rilevanti in termini di regolazione e vigilanza. A differenza degli intermediari bancari tradizionali, soggetti a requisiti stringenti in materia prudenziale e di supervisione, operatori come Amazon e Google operano spesso all'interno di quadri normativi differenti, beneficiando di una maggiore flessibilità regolatoria. Tale asimmetria può determinare distorsioni concorrenziali e pone interrogativi circa l'adeguatezza degli strumenti normativi esistenti.<sup>141</sup>

Un ulteriore elemento di criticità riguarda la centralità dei dati. Le BigTech dispongono di quantità estremamente elevate di informazioni sugli utenti, raccolte nell'ambito di ecosistemi digitali complessi, che possono essere utilizzate per finalità finanziarie. L'integrazione tra dati commerciali, comportamentali e finanziari consente lo sviluppo di modelli di intelligenza artificiale particolarmente sofisticati, ma solleva al contempo rilevanti questioni in materia di protezione dei dati personali, trasparenza e rischio di discriminazione algoritmica.<sup>142</sup>

Sotto il profilo della struttura del mercato, la presenza di tali operatori contribuisce a ridefinire le dinamiche competitive, spostando il focus dalla tradizionale intermediazione bancaria verso modelli

---

<sup>139</sup> Bank for International Settlements, *Big Tech in Finance: Opportunities and Risks*, 2019

<sup>140</sup> Cfr. sviluppo di Google Pay e progetto "Plex" (fonti: Financial Times, Reuters, 2020–2023)

<sup>141</sup> European Central Bank, *Financial Stability Review*, 2023

<sup>142</sup> European Data Protection Board, *linee guida su trattamento dei dati e profilazione*

basati su piattaforme digitali. In questo scenario, le banche sono chiamate a confrontarsi non solo tra loro, ma con soggetti che operano su scala globale e che dispongono di significativi vantaggi tecnologici. Ciò determina una pressione crescente verso l'innovazione e, in alcuni casi, incentiva strategie di collaborazione o integrazione tra intermediari tradizionali e operatori tecnologici.<sup>143</sup>

Nel complesso, i casi di Amazon e Google evidenziano come l'intelligenza artificiale e la disponibilità di dati rappresentino fattori chiave nella ridefinizione del perimetro dei servizi finanziari. L'ingresso delle BigTech non si traduce necessariamente in una sostituzione del sistema bancario tradizionale, ma pone nuove sfide sul piano regolatorio, concorrenziale e della tutela degli utenti.

Come già evidenziato l'ingresso di questi operatori aumenta la pressione competitiva, per via della loro capacità di sfruttare grandi quantità di dati e della loro maggior predisposizione verso l'utilizzo di modelli di business fortemente orientati all'innovazione tecnologica. Le banche sono dunque spinte ad accelerare i processi di digitalizzazione e ad adottare soluzioni di intelligenza artificiale per mantenere la propria posizione nel mercato.<sup>144</sup>

Queste trasformazioni sollevano questioni rilevanti in materia di concorrenza, vigilanza e gestione dei rischi tecnologici, infatti i processi di concentrazione possono incidere sulla struttura del mercato.

L'integrazione di sistemi algoritmici complessi pone invece problemi in termini di trasparenza, responsabilità e conformità ai requisiti normativi europei. La crescente centralità dei dati e delle tecnologie digitali richiede un rafforzamento dei presidi di governance e dei meccanismi di controllo, anche alla luce degli obblighi previsti dal quadro regolatorio europeo.

L'intelligenza artificiale non costituisce una causa diretta dei processi di fusione e acquisizione, tuttavia contribuisce a intensificare le dinamiche competitive e a rafforzare le tendenze alla concentrazione del settore bancario. La competizione si configura sempre più come un confronto tra ecosistemi tecnologici, nei quali la capacità di gestire e valorizzare i dati assume un ruolo determinante.

L'avvento di piattaforme digitali come Revolut e Satispay rappresenta un altro elemento chiave nella trasformazione dei servizi bancari e finanziari, ponendo in primo piano l'impatto dell'intelligenza artificiale sulla relazione tra istituto e cliente. Revolut, neobank di respiro internazionale, integra l'AI in tutti i processi critici: dai sistemi di valutazione del rischio creditizio, che analizzano dati transazionali e comportamentali per offrire limiti di credito personalizzati<sup>145</sup>, alla prevenzione delle frodi mediante rilevazione in tempo reale di schemi anomali, fino alla personalizzazione dei servizi e all'assistenza

---

<sup>143</sup> European Banking Authority, Report on Big Data and Advanced Analytics, 2020

<sup>144</sup> Bank for International Settlements, Big tech in finance: opportunities and risks, 2019

<sup>145</sup> Revolut, Annual Report 2023, Relazione sulla gestione e analisi dei dati transazionali (Revolut Ltd., 2024)

clienti tramite chatbot intelligenti<sup>146</sup>. Questo impiego diffuso di algoritmi avanzati consente una maggiore efficienza operativa e un'esperienza utente più mirata, ma solleva questioni giuridiche legate alla trasparenza dei modelli decisionali e alla protezione dei dati personali.<sup>147</sup>

Satispay, pur operando con un modello più focalizzato sul mercato nazionale e sui pagamenti digitali, ha iniziato a sperimentare applicazioni di AI principalmente nella prevenzione delle frodi e nell'ottimizzazione dei flussi di pagamento.<sup>148</sup> Con l'introduzione imminente della possibilità di creare IBAN, l'azienda potrà ampliare l'impiego di algoritmi per il monitoraggio del rischio e, potenzialmente, per l'analisi comportamentale dei clienti.

L'uso dell'AI in Satispay è più limitato e si concentra principalmente sulla sicurezza e sull'efficienza dei processi. Ciò invita a riflettere su come anche gli operatori più piccoli possano avvalersi dell'innovazione tecnologica per ampliare la gamma dei servizi offerti. Dal punto di vista della relazione banca-cliente, le differenze tra le due piattaforme mettono in luce effetti distinti sulla percezione dei servizi. Nei sistemi ad alto grado di automazione come Revolut, l'efficienza e la personalizzazione possono accrescere la soddisfazione del cliente, ma la complessità dei modelli e la scarsa trasparenza dei processi decisionali rischiano di generare sfiducia, soprattutto in presenza di errori o decisioni inattese. Nei servizi più limitati e lineari come quelli di Satispay, l'AI contribuisce principalmente alla sicurezza e alla continuità del servizio, rafforzando invece la fiducia nella piattaforma. Questa comparazione è utile per comprendere come l'introduzione dell'intelligenza influenzi direttamente la qualità dell'interazione con il cliente e la percezione della banca o dell'istituto finanziario.<sup>149</sup>

L'evoluzione dell'intelligenza artificiale nel settore bancario e fintech apre a scenari futuri caratterizzati da impatti economici, strategici e giuridici che meritano un'analisi critica.

Un primo scenario è quello della digitalizzazione spinta, in cui l'adozione diffusa di sistemi di AI limitata al credit scoring, alla prevenzione delle frodi e alla gestione del rischio rappresenta un'opportunità di efficienza operativa e riduzione dei costi. Tale evoluzione comporta rischi concreti come l'affidamento eccessivo a decisioni automatizzate, che potrebbe compromettere la responsabilità giuridica degli intermediari. Inoltre la scarsa trasparenza di alcuni modelli potrebbe limitare la capacità dei clienti di comprendere le decisioni che li riguardano.

---

<sup>146</sup> Jagtiani, J. & Lemieux, C., "The Roles of Alternative Data and Machine Learning in FinTech Lending: Evidence from Revolut", *Journal of Financial Intermediation*, vol. 52, 2022, pp. 1-15

<sup>147</sup> European Banking Authority, *Report on the Use of Big Data and Advanced Analytics*, EBA, 2020; European Data Protection Board, *Guidelines on AI and Data Protection*, 2021

<sup>148</sup> Satispay, *Comunicazione ufficiale sul lancio del servizio IBAN*, comunicato stampa, 2026

<sup>149</sup> Bank for International Settlements, *Big Tech in Finance: Opportunities and Risks*, BIS Papers, n. 107, 201

Un secondo scenario riguarda la penetrazione delle Big Tech nei servizi finanziari. Queste dinamiche sollevano questioni di concorrenza e governance dei dati: le banche tradizionali devono gestire il rischio di perdita di clienti verso operatori caratterizzati da economie di scala tecnologiche. Da questa ipotesi emergono sfide normative relative alla responsabilità sui dati e alla protezione dei diritti fondamentali.<sup>150</sup> La letteratura critica suggerisce che la regolazione europea con l'AI Act e il GDPR, potrebbe non essere sufficiente a prevenire fenomeni di concentrazione e arbitraggio normativo, richiedendo un monitoraggio costante e adattamenti legislativi mirati.

Lo scenario di concentrazione del mercato attraverso fusioni e acquisizioni, come nel caso di Banco BPM/UniCredit o MPS/Mediobanca, evidenzia invece la centralità delle capacità di gestione del rischio e dell'adozione di AI nel definire il valore strategico delle operazioni. Tuttavia, la convergenza dei modelli algoritmici tra operatori, può incrementare la vulnerabilità del sistema a shock simultanei, sollevando questioni di stabilità finanziaria e di responsabilità in caso di errori sistemici.<sup>151</sup>

Un ulteriore scenario riguarda la democratizzazione dei servizi finanziari tramite neobank e fintech come Revolut e Satispay, che impiegano AI per personalizzare servizi e valutazioni del rischio. L'intelligenza artificiale consente di analizzare grandi quantità di dati, migliorando l'accesso al credito per clienti che altrimenti sarebbero esclusi dal sistema bancario, soprattutto nel caso di microimprese o di soggetti con scarsa storia creditizia.<sup>152</sup> Questo approccio aumenta l'inclusione finanziaria e migliora l'esperienza dell'utente, ma pone criticità in termini di governance dei dati, mitigazione dei bias algoritmici e trasparenza decisionale. La letteratura evidenzia che l'efficacia di questi strumenti dipende fortemente dalla capacità degli operatori di integrare principi etici e normativi fin dalla progettazione dei modelli.

Infine, non può essere trascurato lo scenario di crisi normativa o tecnologica, in cui la complessità dei sistemi AI e l'assenza di standard tecnici uniformi generano incertezze applicative e possibili contenziosi legali. La difficoltà di rendere spiegabili sistemi altamente complessi, unita a divergenze interpretative tra Stati membri, potrebbe compromettere la tutela effettiva degli utenti e la stabilità complessiva del sistema bancario europeo.

In sintesi, gli scenari delineati sottolineano che l'AI costituisce un driver strategico imprescindibile, ma la sua integrazione deve essere accompagnata da una valutazione critica dei rischi e delle implicazioni giuridiche.

---

<sup>150</sup> GDPR, Regolamento UE 2016/679, artt. 13-22

<sup>151</sup> IMF, Financial Stability Report, aprile 2022, par. 3.4

<sup>152</sup> Cfr. Banca d'Italia, Rapporto sulla stabilità finanziaria e inclusione creditizia, 2021

Tali considerazioni costituiscono la premessa concettuale per l'analisi empirica condotta nel capitolo successivo, che si propone di valutare, attraverso i questionari somministrati, il grado di consapevolezza di clienti e dipendenti degli istituti di credito, la fiducia nei sistemi automatizzati e la percezione delle interazioni con strumenti di AI nei servizi bancari digitali.

### 3.5 L'ipotesi di una funzione di controllo basata su AI

La suggestione di una funzione di controllo interamente affidata a sistemi di intelligenza artificiale solleva una questione radicale: è concepibile che l'AI controlli se stessa? In altre parole, è ipotizzabile, in una banca soggetta a vigilanza, l'istituzione di una funzione di controllo interno integralmente basata su sistemi algoritmici, incaricata di monitorare tutti i progetti e i processi AI dell'intermediario?<sup>153</sup>

Sul piano tecnico, tale ipotesi non appare del tutto irrealistica. Esistono già strumenti di machine learning impiegati per il monitoraggio continuo delle performance dei modelli e per la rilevazione automatica di fenomeni quali il model drift e il data drift. Per chiarire: il model drift indica la degradazione della performance di un modello predittivo nel tempo, dovuta alla variazione delle condizioni o dei comportamenti sui quali il modello è stato addestrato; il data drift si verifica quando la distribuzione dei dati in input si discosta rispetto a quella originaria, compromettendo l'accuratezza delle previsioni.<sup>154</sup> A questi strumenti si affiancano tecniche di fairness testing, volte a rilevare eventuali bias discriminatori nei modelli, strumenti di explainability che permettono di interpretare le decisioni algoritmiche e sistemi di detection per anomalie nei dataset, capaci di segnalare comportamenti atipici o errori di input.<sup>155</sup> In letteratura, l'insieme di tali pratiche rientra nel concetto di AI for AI governance, ossia l'impiego di sistemi algoritmici per sorvegliare altri sistemi algoritmici.<sup>156</sup> Negli Stati Uniti, la riflessione sull'algorithmic accountability ha sottolineato come l'automazione dei processi decisionali richieda strumenti di audit e supervisione, talvolta anch'essi automatizzati, per garantire trasparenza e tracciabilità.

Analogamente, nel dibattito europeo sulla governance delle automated decision-making systems, si è sostenuto come la complessità tecnica dei modelli contemporanei renda inevitabile l'uso di strumenti computazionali per il loro monitoraggio.<sup>157</sup> Tuttavia, la questione non può essere ridotta a un

---

<sup>153</sup> Vincenzo Giovanni Dragone, *Le tre fratture dell'intelligenza artificiale in banca*, [dirittobancario.it](http://dirittobancario.it), 2026

<sup>154</sup> Gama, J., Žliobaitė, I., Bifet, A., Pechenizkiy, M., & Bouchachia, A., *A Survey on Concept Drift Adaptation*, *ACM Computing Surveys*, 2014

<sup>155</sup> Barocas, S., Hardt, M., & Narayanan, A., *Fairness and Machine Learning*, 2019; Molnar, C., *Interpretable Machine Learning*, 2020

<sup>156</sup> Cath, C., *Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges*, *Philosophical Transactions of the Royal Society A*, 2018

<sup>157</sup> European Banking Authority, *Guidelines on Automated Decision-Making and AI Governance in Financial Institutions*, 2021

problema di efficienza tecnica. In un intermediario vigilato, il controllo interno rappresenta un presidio fondamentale di responsabilità organizzativa, non un mero meccanismo di verifica funzionale.

L'istituzione di una "AI-only control function" presenta, infatti, almeno tre ordini di criticità.

Primo, un problema di imputazione. Nel modello delle tre linee di difesa, il sistema dei controlli interni presuppone responsabilità umane identificabili e indipendenti. Se un algoritmo di controllo omette di segnalare un'anomalia o produce una falsa rassicurazione, chi ne risponde? L'organo amministrativo, cui la normativa attribuisce il dovere di predisporre assetti adeguati, non può invocare l'autonomia del sistema come esonero dalla responsabilità umana.<sup>158</sup>

Secondo, un problema di regressione. Se un algoritmo controlla un altro algoritmo, chi controlla il controllore? L'automazione del controllo rischia di generare una catena autoreferenziale, amplificando l'opacità complessiva. La dottrina anglosassone parla di meta-black box: quando sistemi algoritmici supervisionano altri sistemi algoritmici, il livello di supervisione può diventare esso stesso incomprensibile, generando un rischio di regressione potenzialmente infinita.<sup>159</sup> Un esempio concreto si osserva in alcune piattaforme di trading algoritmico, dove sistemi di monitoraggio automatici hanno generato falsi segnali durante picchi di volatilità, richiedendo l'intervento umano per prevenire perdite sistemiche.

Ultimo, non per importanza, un problema di legittimazione. Il controllo interno non si esaurisce in una funzione puramente tecnica, ma rappresenta un elemento di garanzia nei confronti degli organi sociali, delle autorità di vigilanza e del mercato. La sua credibilità dipende non solo dalla capacità di individuare eventuali anomalie, ma anche dal rispetto di principi di trasparenza, indipendenza e correttezza professionale.<sup>160</sup>

Anche ipotizzando che un sistema AI sia programmato per seguire regole deontologiche, rimane evidente che tale intelligenza sarebbe sprovvista di coscienza morale, della capacità di giudizio etico o di responsabilità giuridica.<sup>161</sup> In altre parole, la conformità alle regole non equivale a moralità: un sistema di AI può applicare principi etici programmati, ma non può sostituire la riflessione e la responsabilità umana.

Questo scenario suggerisce una riflessione critica più ampia: l'automazione dei controlli, pur offrendo vantaggi come riduzione di comportamenti opportunistici, auditabilità e formalizzazione delle regole, non può prescindere da un presidio umano. La tecnologia può aumentare l'efficienza, ma la responsabilità ultima, il giudizio etico e la legittimazione del sistema restano prerogative dell'uomo.

---

<sup>158</sup> Basel Committee on Banking Supervision, Corporate Governance Principles for Banks, 2015

<sup>159</sup> Pasquale, F., The Black Box Society: The Secret Algorithms That Control Money and Information, 2015

<sup>160</sup> Ibidem

<sup>161</sup> Floridi, L., The Ethics of Artificial Intelligence, Oxford University Press, 2021

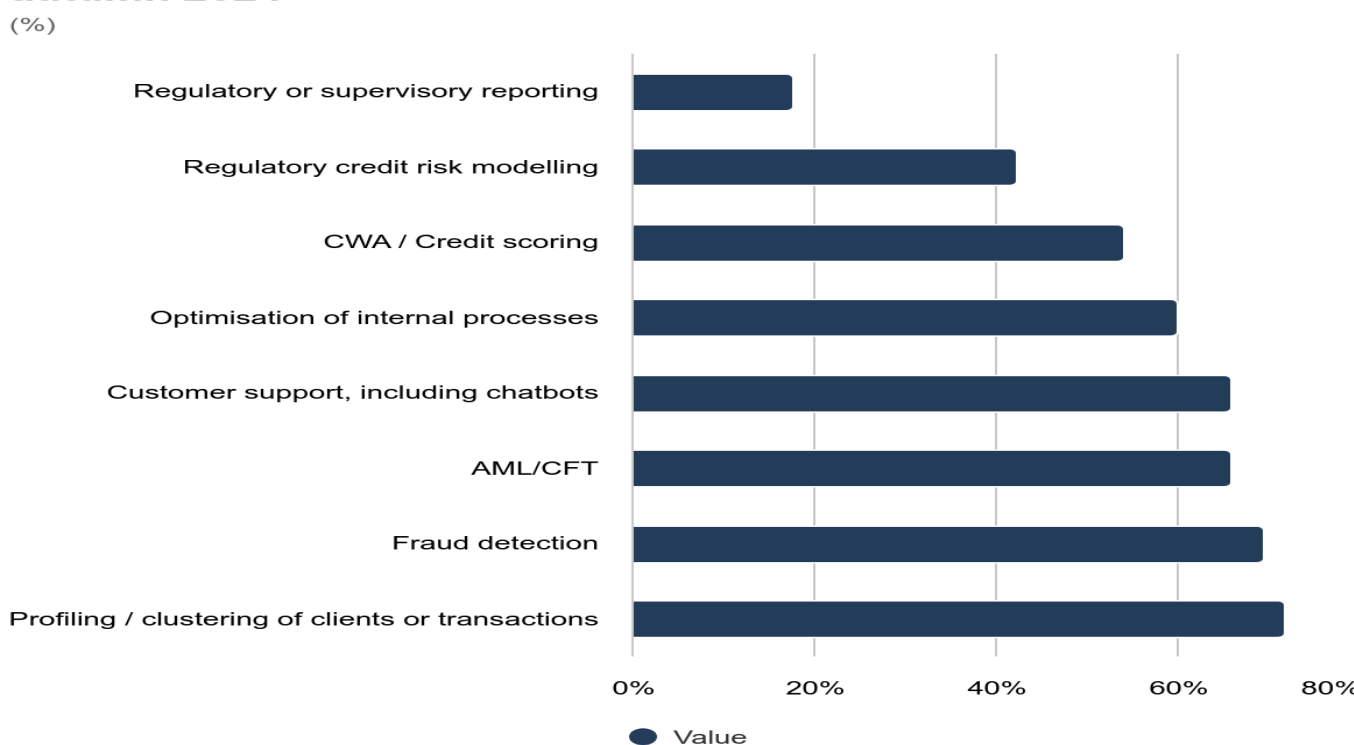
## Capitolo 4 Percezioni di clienti e dipendenti sull'utilizzo dell'Intelligenza Artificiale nel settore bancario

### 4.1 Le principali indagini condotte a livello europeo

Le principali indagini condotte a livello europeo e internazionale evidenziano come l'adozione dell'intelligenza artificiale nel settore bancario sia accompagnata da benefici significativi in termini di efficienza operativa, ma anche da criticità persistenti sul piano della governance e della fiducia. I contributi della European Banking Authority, di PwC e di Deloitte offrono prospettive complementari, che consentono di cogliere la complessità del fenomeno sia dal punto di vista degli operatori sia da quello della clientela.

In particolare, i report della European Banking Authority evidenziano come l'impiego di sistemi di intelligenza artificiale sia ormai diffuso in una pluralità di ambiti operativi, tra cui il credit scoring, la prevenzione delle frodi e i processi di antiriciclaggio.<sup>162</sup>

**Figure 73b: Uses of AI by EU banks per use case in 2024, autumn 2024**



Tuttavia, l'EBA sottolinea come tali applicazioni comportino l'emersione di nuove categorie di rischio, riconducibili in larga misura alla qualità dei dati utilizzati, alla difficoltà di interpretazione dei modelli più complessi e alla necessità di assicurare un adeguato livello di controllo umano.

Assume particolare rilievo l'adozione di adeguati sistemi di model risk management, ossia di

<sup>162</sup> European Banking Authority, Report on Big Data and Advanced Anal

quell'insieme di strumenti organizzativi e procedurali finalizzati a prevenire e gestire i rischi derivanti dall'utilizzo dell'AI nei processi decisionali. Tali sistemi si fondano, in primo luogo, sulla definizione di adeguati presidi di controllo lungo l'intero ciclo di vita del modello, dalla fase di sviluppo fino al suo utilizzo operativo. A ciò si affiancano attività di monitoraggio continuo delle performance, necessarie per verificare nel tempo l'affidabilità dei risultati prodotti, nonché processi di validazione indipendente, volti a garantire una verifica imparziale della correttezza metodologica e della coerenza del modello rispetto alle finalità per cui è stato progettato. L'insieme di tali strumenti contribuisce a ridurre il rischio di errori o distorsioni, rafforzando l'affidabilità delle decisioni automatizzate.<sup>163</sup>

Le analisi condotte da PwC si collocano su un piano parzialmente diverso, concentrandosi prevalentemente sulla percezione della clientela. I dati raccolti mostrano come i consumatori tendano a riconoscere i vantaggi dell'intelligenza artificiale in termini di rapidità, accessibilità e personalizzazione dei servizi.<sup>164</sup> Al contempo, emerge una diffusa cautela nei confronti dell'utilizzo di tali tecnologie nei processi decisionali più rilevanti, in particolare quando incidono sull'accesso al credito o sulla gestione delle risorse finanziarie. In tali ambiti, la mancanza di trasparenza e la difficoltà di comprendere le logiche sottostanti alle decisioni automatizzate rappresentano fattori che limitano il livello di fiducia degli utenti.<sup>165</sup>

Un quadro in parte analogo emerge dalle indagini di Deloitte, che analizzano la trasformazione digitale del settore bancario in una prospettiva più ampia. Da un lato, Deloitte evidenzia come l'adozione di tecnologie avanzate, inclusa l'intelligenza artificiale, contribuisca a migliorare l'efficienza dei processi e la qualità dei servizi offerti.<sup>166</sup> Dall'altro lato, viene sottolineato come la relazione banca–cliente continui a fondarsi su elementi di fiducia che difficilmente possono essere sostituiti integralmente da sistemi automatizzati. In particolare, nei momenti decisionali più complessi, la presenza di un operatore umano rimane un elemento percepito come essenziale, suggerendo la necessità di modelli ibridi in cui l'automazione sia affiancata da forme di supervisione umana.<sup>167</sup> Dal confronto tra le diverse fonti emerge un quadro sostanzialmente coerente, pur nella diversità degli approcci adottati. Mentre l'European Banking Authority pone l'accento sui profili di rischio e sulle esigenze di governance interna, PwC e Deloitte evidenziano le criticità legate alla percezione degli utenti e alla qualità dell'interazione con la clientela. In particolare, tutte le analisi convergono nel rilevare una tensione tra l'aumento dell'efficienza operativa e la necessità di preservare un adeguato livello di trasparenza e fiducia.

---

<sup>163</sup> European Banking Authority, Discussion Paper on Machine Learning for IRB Models, 2021

<sup>164</sup> PwC, Global Artificial Intelligence Study: Exploiting the AI Revolution, 2017 (aggiornamenti Consumer Intelligence Series)

<sup>165</sup> PwC, Trust in Artificial Intelligence, 2021

<sup>166</sup> Deloitte, AI in Banking: Ready, Steady, Go?, 2020

<sup>167</sup> Deloitte, Digital Banking Maturity Report, 2022

Tale convergenza risulta particolarmente rilevante in quanto consente di collocare i risultati dei questionari all'interno di un quadro interpretativo già consolidato. Le percezioni espresse sia dalla clientela sia dagli operatori possono essere lette non come fenomeni isolati, ma come espressione di dinamiche più ampie che caratterizzano l'evoluzione del settore bancario in relazione all'intelligenza artificiale.

Il presente capitolo si propone di affiancare all'analisi teorica e normativa sviluppata nei capitoli precedenti una prospettiva empirica, volta a indagare la percezione dell'intelligenza artificiale nel settore bancario. In particolare, l'obiettivo della ricerca è quello di comprendere come tali tecnologie vengano percepite dalla clientela e dagli operatori del settore, con specifico riferimento ai profili di fiducia, trasparenza e accettazione dei processi decisionali automatizzati.

A tal fine, è stata condotta un'indagine empirica mediante la somministrazione di due distinti questionari: il primo rivolto alla clientela bancaria, con l'obiettivo di analizzare il livello di conoscenza e consapevolezza dell'intelligenza artificiale, nonché le principali percezioni in termini di benefici e criticità; il secondo indirizzato agli operatori del settore, al fine di approfondire le implicazioni operative e organizzative connesse all'adozione di tali tecnologie.

I questionari sono stati strutturati prevalentemente attraverso domande a risposta chiusa, al fine di consentire una più agevole elaborazione dei dati e un confronto sistematico tra le diverse variabili considerate. Accanto a quesiti di natura socio-demografica, sono state incluse domande volte a rilevare il grado di familiarità con i servizi bancari digitali, la percezione della diffusione dell'intelligenza artificiale, il livello di fiducia nei confronti dei sistemi automatizzati e le principali preoccupazioni connesse al loro utilizzo, con particolare riferimento alla trasparenza dei processi decisionali e alla protezione dei dati personali.

L'indagine presenta natura esplorativa, in considerazione della dimensione contenuta del campione e delle modalità di raccolta dei dati, che non consentono di attribuire ai risultati una piena rappresentatività statistica dell'intera popolazione di riferimento. Tuttavia, i dati raccolti risultano comunque significativi ai fini dell'individuazione di tendenze e percezioni prevalenti, offrendo spunti utili per una riflessione più ampia sul rapporto tra innovazione tecnologica e fiducia nel settore bancario.

L'analisi dei risultati viene pertanto condotta in una prospettiva integrata, ponendo in relazione le evidenze empiriche con i principali contributi della letteratura scientifica e con il quadro normativo di riferimento, con particolare attenzione ai principi introdotti dall'AI Act. In tal modo, si intende fornire una lettura complessiva del fenomeno che tenga conto non solo delle implicazioni tecniche e

regolatorie, ma anche delle dinamiche percettive che influenzano l'accettazione dell'intelligenza artificiale da parte degli utenti.

In questa prospettiva, il capitolo mira a verificare se e in quale misura le criticità individuate sul piano teorico — quali la scarsa trasparenza dei modelli decisionali, il rischio di bias algoritmico e la riduzione del controllo umano — trovino riscontro nella percezione della clientela e degli operatori, contribuendo così a delineare un quadro più completo delle implicazioni dell'intelligenza artificiale nel settore bancario.

## **4.2 Analisi empirica delle percezioni della clientela**

L'indagine condotta su un campione di 62 rispondenti consente di delineare un quadro articolato della percezione dell'intelligenza artificiale nel settore bancario, evidenziando dinamiche che riflettono, in parte, le tendenze già emerse nella letteratura di riferimento.

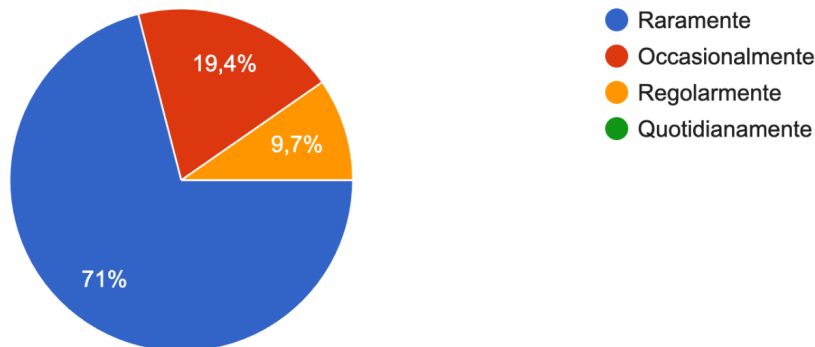
Sotto il profilo socio-demografico, il campione si caratterizza per un livello di istruzione mediamente elevato: il 54% degli intervistati possiede una laurea magistrale o un titolo superiore, il 25% una laurea triennale e il restante 21% un diploma. Anche la distribuzione per età risulta significativa, con una prevalenza di soggetti oltre i 55 anni (54%), seguiti dalla fascia 25–34 anni (22%), mentre risultano più contenute le quote relative alle altre classi anagrafiche.

Dal punto di vista occupazionale, il campione è composto prevalentemente da impiegati (35%) e liberi professionisti (30%), mentre una quota più limitata utilizza i servizi bancari anche per finalità lavorative (30%).

Particolarmente rilevante è il dato relativo alle abitudini di utilizzo dei servizi bancari: il 71% degli intervistati dichiara di recarsi raramente in filiale, a fronte di un 10% che vi si reca con regolarità.

### Frequenza utilizzo dei servizi bancari in filiale

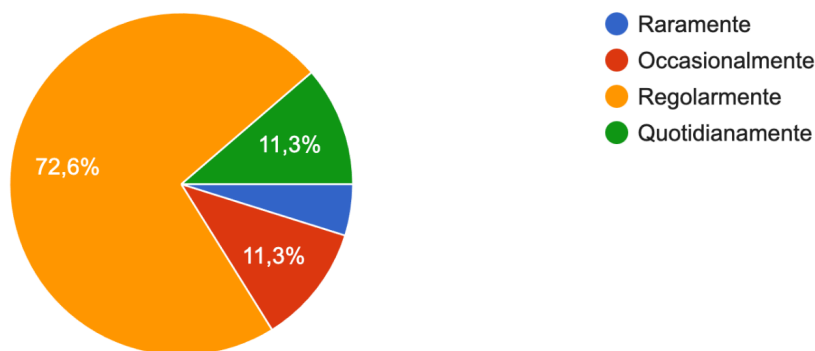
62 risposte



Parallelamente, emerge un elevato grado di digitalizzazione, con il 72,6% che utilizza regolarmente l'home banking e ulteriori quote che vi fanno ricorso quotidianamente (11,3%) o occasionalmente (11,3%).

### Frequenza utilizzo dell'home banking

62 risposte



Tali dati evidenziano come la clientela, pur mantenendo una composizione anagrafica relativamente matura, presenti un livello significativo di familiarità con gli strumenti digitali, elemento che costituisce una premessa rilevante per l'analisi della percezione dell'intelligenza artificiale.

#### Conoscenza e percezione della diffusione dell'AI

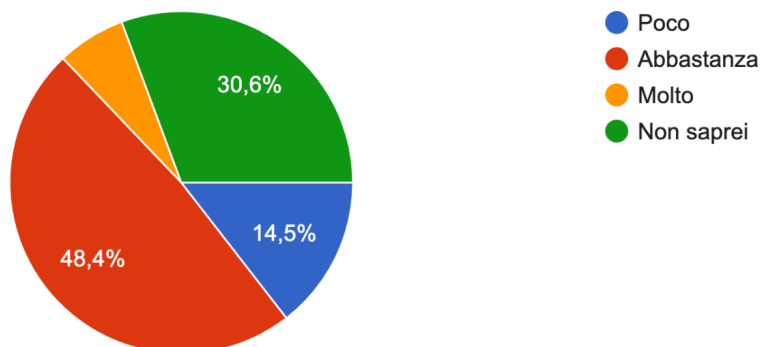
Con riferimento al livello di conoscenza, il 63% degli intervistati dichiara di aver sentito parlare dell'intelligenza artificiale applicata ai servizi bancari, pur riconoscendo una conoscenza limitata dell'argomento.

Per quanto riguarda la percezione della diffusione, il 48,4% ritiene che l'utilizzo dell'intelligenza

artificiale nelle banche sia “abbastanza diffuso”, mentre il 14,5% lo considera poco diffuso e solo una quota marginale (6%) lo percepisce come molto diffuso.

Secondo te, quanto è diffuso l'uso dell'AI nelle banche?

62 risposte



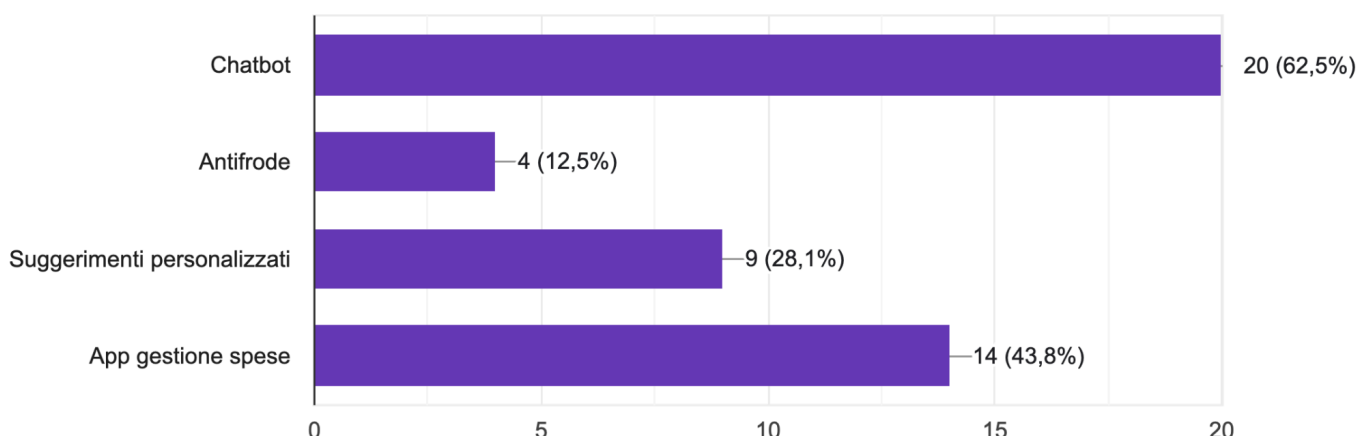
Interessante è inoltre il dato relativo all'esperienza diretta: il 50% dei rispondenti ritiene di non aver mai utilizzato servizi bancari basati sull'intelligenza artificiale, mentre il 30% afferma di averne fatto uso e il 20% non è in grado di stabilirlo con certezza.

Tale risultato appare particolarmente significativo, in quanto suggerisce una disconnessione tra utilizzo effettivo e consapevolezza dell'utente, verosimilmente riconducibile alla natura “invisibile” di molte applicazioni di intelligenza artificiale.

Tipologie di utilizzo

Quali servizi hai utilizzato?

32 risposte



Tra i soggetti consapevoli di aver utilizzato servizi basati sull'intelligenza artificiale, emergono applicazioni prevalentemente legate all'interazione e alla gestione operativa: il 62% ha utilizzato chatbot, il 44% applicazioni per la gestione delle spese, il 28% sistemi di suggerimenti personalizzati e il 12,5% strumenti antifrode.

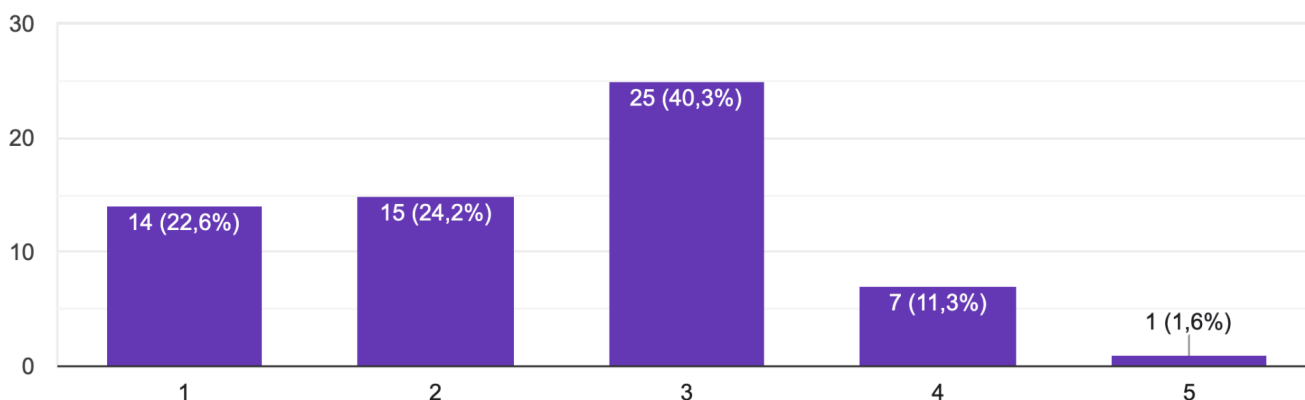
Tali evidenze confermano come l'intelligenza artificiale sia percepita principalmente nei servizi più visibili e a diretto contatto con l'utente, mentre rimangono meno evidenti le applicazioni più sofisticate, quali quelle legate alla valutazione del rischio o ai processi decisionali interni.

#### Fiducia e accettazione delle decisioni automatizzate

Sotto il profilo della fiducia, i dati evidenziano una certa cautela: solo il 40,3% degli intervistati dichiara di fidarsi delle decisioni automatizzate delle banche. Tale diffidenza emerge con maggiore evidenza in relazione a decisioni particolarmente rilevanti, come la concessione di un finanziamento: solo il 16,1% si dichiara a proprio agio con una decisione interamente algoritmica, mentre il 46,8% esprime una posizione contraria.

#### Quanto ti fidi delle decisioni automatizzate delle banche?

62 risposte



In linea con tali risultati, il 58,1% degli intervistati considera fondamentale l'intervento umano nei processi decisionali automatizzati, e il 66,1% individua nella mancanza di controllo umano il principale rischio associato all'utilizzo dell'intelligenza artificiale.

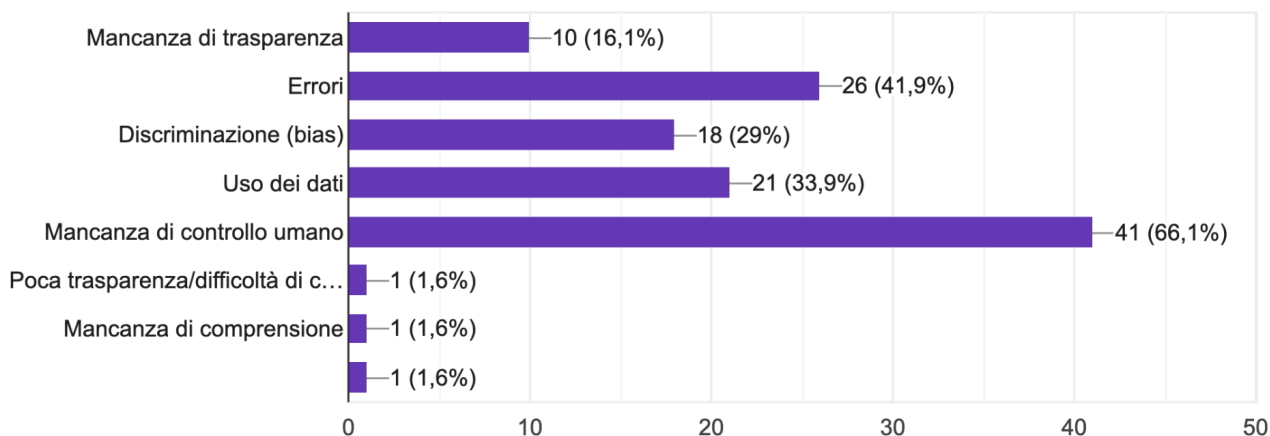
Questi dati evidenziano come la dimensione fiduciaria rappresenti un elemento centrale nella relazione tra cliente e banca, difficilmente sostituibile da sistemi interamente automatizzati.

## Percezione dei rischi

L'analisi delle criticità percepite conferma ulteriormente tale tendenza. Il 35,5% degli intervistati ritiene che l'intelligenza artificiale possa generare effetti discriminatori, mentre una quota analoga (33,9%) esclude tale rischio, evidenziando una significativa eterogeneità nelle percezioni

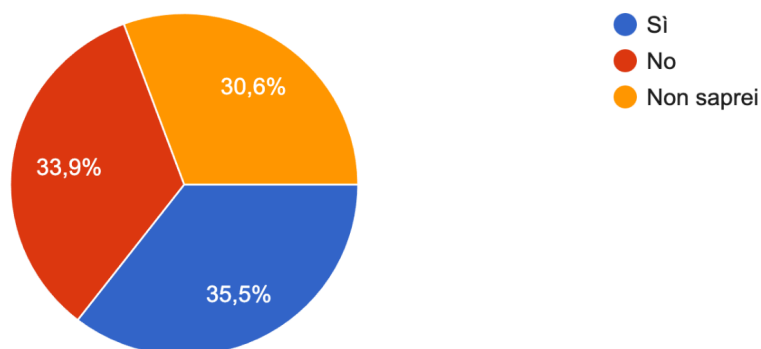
### Quali rischi ti preoccupano maggiormente?

62 risposte



### Ritieni che l'AI possa essere discriminatoria?

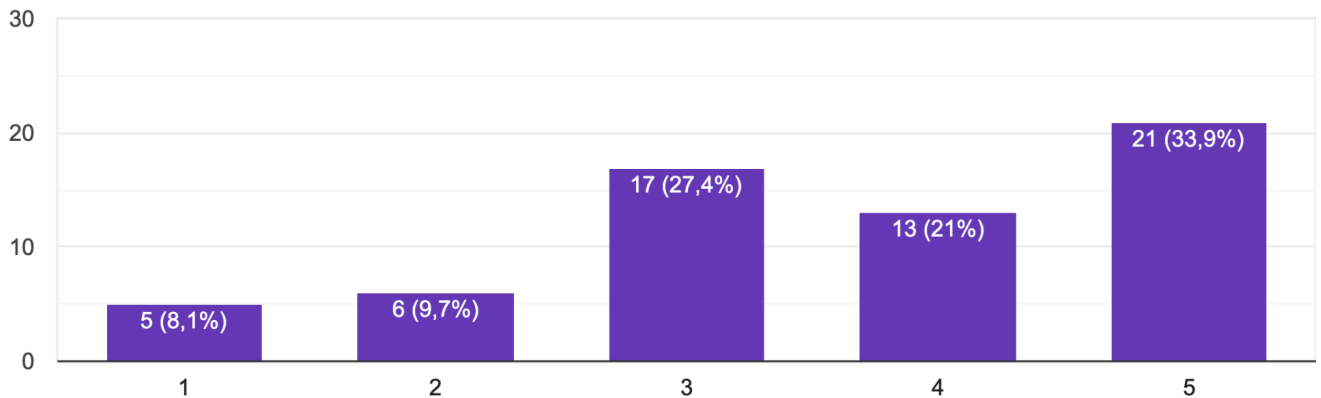
62 risposte



Particolarmente rilevante è il tema della protezione dei dati personali: il 33,9% si dichiara preoccupato per l'utilizzo dei propri dati, mentre il 61,3% afferma di non sentirsi adeguatamente informato sulle modalità con cui le banche trattano tali informazioni.

## Quanto ti preoccupa l'uso dei tuoi dati personali?

62 risposte



In

questo contesto, la medesima percentuale (61,3%) ritiene necessario un intervento regolatorio volto a disciplinare l'utilizzo dell'intelligenza artificiale nel settore bancario, evidenziando una chiara domanda di maggiore tutela e trasparenza.

### Considerazioni di sintesi

Nel complesso, l'analisi evidenzia una percezione ambivalente dell'intelligenza artificiale da parte della clientela bancaria. Da un lato, emerge un elevato livello di utilizzo dei servizi digitali e una generale apertura verso l'innovazione tecnologica; dall'altro, persistono significative criticità in termini di fiducia, trasparenza e controllo dei processi decisionali.

In particolare, i dati mettono in luce una tensione tra l'efficienza garantita dall'automazione e la necessità, avvertita dagli utenti, di mantenere un adeguato presidio umano nelle decisioni più rilevanti. Tale dinamica risulta coerente con le evidenze emerse nella letteratura di settore e conferma la centralità del tema della fiducia nell'ambito della trasformazione digitale del sistema bancario.

I risultati dell'indagine suggeriscono come l'accettazione dell'intelligenza artificiale non dipenda esclusivamente dalle sue performance tecniche, ma anche dalla capacità degli intermediari di garantire trasparenza, comprensibilità e adeguate forme di supervisione umana.

### 4.3 Percezione dell'intelligenza artificiale tra gli operatori del settore bancario

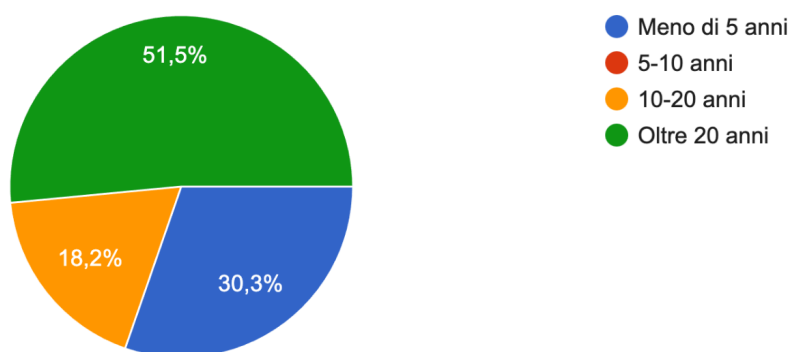
L'indagine condotta presso gli operatori del settore bancario consente di approfondire il punto di vista degli intermediari, offrendo una prospettiva complementare rispetto a quella della clientela.

I dati raccolti evidenziano come l'intelligenza artificiale sia percepita, da un lato, come un fattore di innovazione e opportunità, ma, dall'altro, come una fonte di criticità operative e regolamentari che richiedono un adeguato presidio.

Il questionario è stato sottoposto a un campione non rappresentativo di 33 rispondenti di diversi istituti di credito. Il campione analizzato presenta una significativa eterogeneità sotto il profilo funzionale, con una prevalenza di operatori nell'area commerciale (51,5%), seguiti da ambiti quali il credito (21,2%) e l'IT (12,1%), mentre risultano meno rappresentate le funzioni di controllo e supporto (HR, audit, compliance e legale). Dal punto di vista dell'esperienza professionale, emerge una presenza rilevante di soggetti con elevata anzianità nel settore: oltre il 50% dei vanta più di vent'anni di esperienza, mentre il 18,2% si colloca tra i dieci e i vent'anni. Più contenuta risulta invece la quota di operatori con esperienza inferiore ai cinque anni (30,3%).

## 2. Anni di esperienza nel settore bancario:

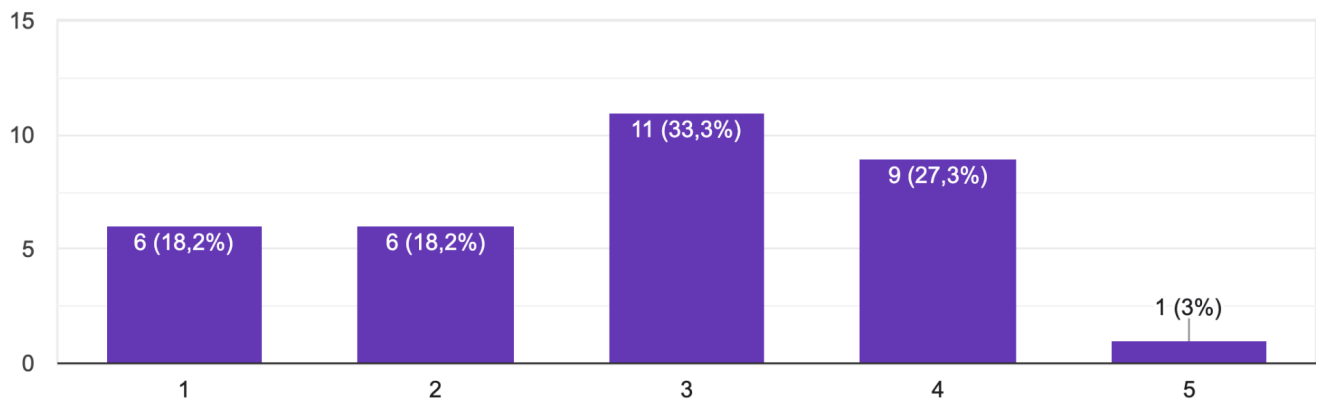
33 risposte



Con riferimento all'inquadramento, il campione è composto prevalentemente da quadri (51,5%) e personale operativo (45,5%), con una presenza marginale di dirigenti (3%). La limitata presenza di dirigenti nel campione può essere ricondotta sia alla minore numerosità di tale categoria all'interno delle strutture bancarie, sia alla maggiore difficoltà di coinvolgimento di figure apicali in indagini di natura volontaria, spesso per ragioni legate al tempo disponibile e alla riservatezza delle informazioni trattate. Tali caratteristiche contribuiscono a delineare un campione composto in larga parte da soggetti direttamente coinvolti nei processi operativi e decisionali.

4. Ritieni di avere una conoscenza generale dell'intelligenza artificiale applicata al settore bancario?  
Scegli un valore che va da 1 (per nulla) a 5 (molto)

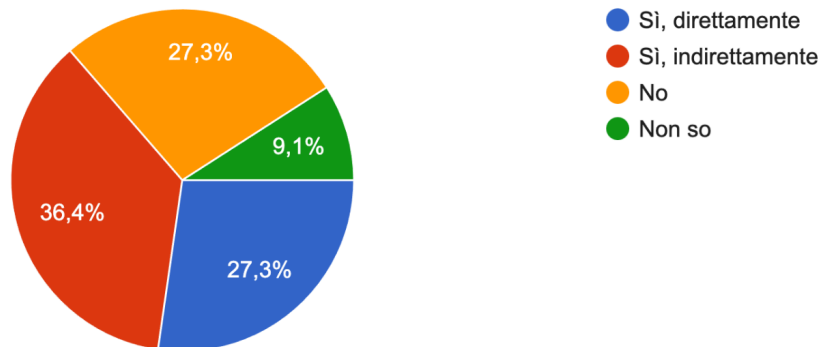
33 risposte



Per quanto riguarda il livello di conoscenza, solo il 30,3% degli intervistati dichiara di possedere una conoscenza generale dell'intelligenza artificiale, mentre il 33,3% esprime una posizione neutra e una quota leggermente maggioritaria (36,4%) manifesta una conoscenza limitata o assente.

5. Nella tua attività lavorativa utilizzi (direttamente o indirettamente) sistemi basati su IA?

33 risposte

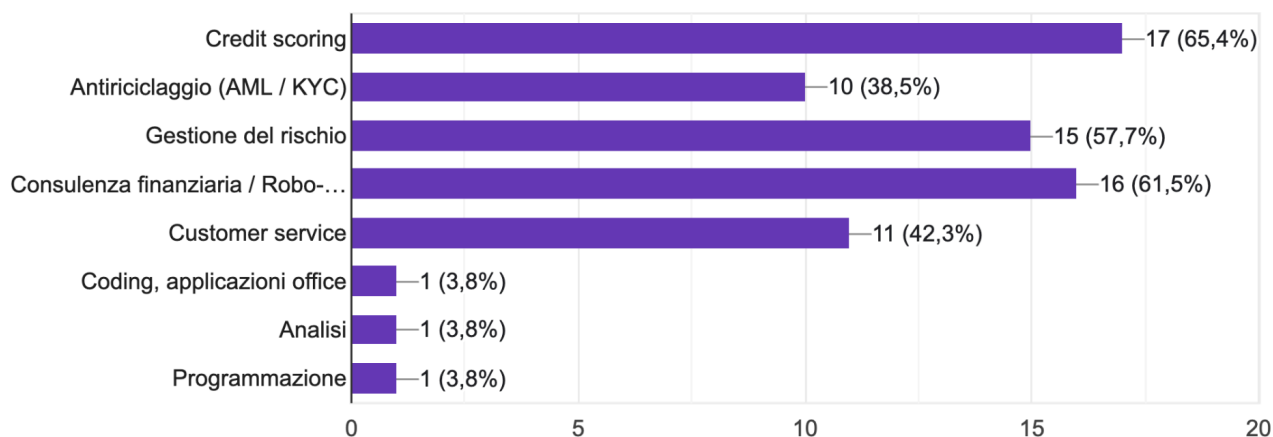


Tuttavia, come evidenziato in figura, l'utilizzo di sistemi basati sull'intelligenza artificiale risulta più diffuso di quanto la percezione suggerisca: il 27,3% degli operatori dichiara di utilizzarli direttamente e il 36,4% indirettamente, mentre il 27,3% afferma di non farne uso e il 9,1% non è in grado di stabilirlo con certezza. Tale dato evidenzia una possibile asimmetria tra utilizzo effettivo e

consapevolezza, analoga a quella riscontrata nella clientela, ma con implicazioni più rilevanti sul piano operativo.

## 6. In quali ambiti ritieni che l'IA sia maggiormente utilizzata in banca?

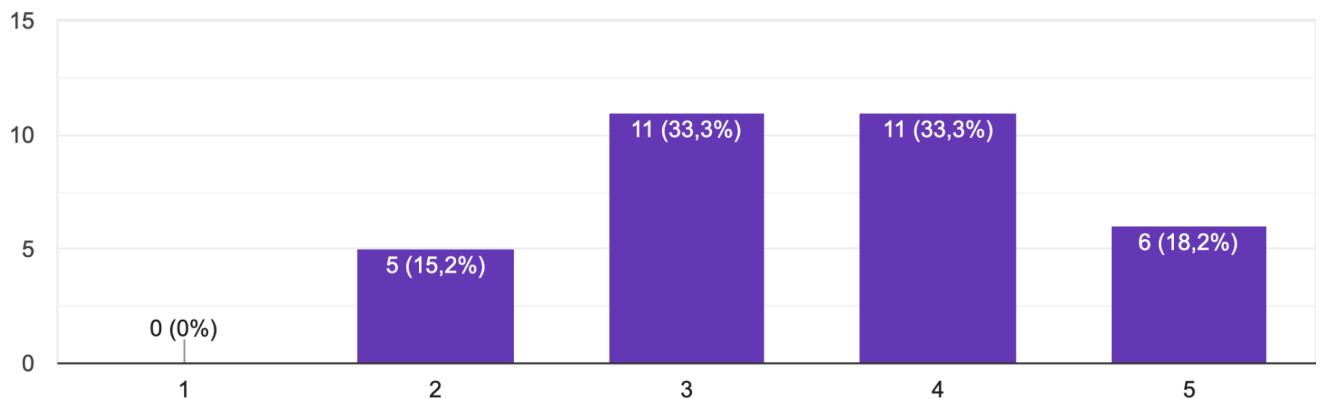
26 risposte



Gli ambiti nei quali l'intelligenza artificiale è ritenuta maggiormente utilizzata riflettono le principali funzioni core del sistema bancario: il 65,4% indica il credit scoring, il 57,7% la gestione del rischio, il 61,5% le attività finanziarie e il 38,5% i processi di antiriciclaggio. Più limitata appare invece la percezione del suo utilizzo in ambiti quali il customer service o lo sviluppo applicativo.

7. Ritieni che l'uso dell'IA nel settore bancario possa migliorare l'efficienza dei processi decisionali? Scegli un valore che va da 1 (per nulla) a 5 (molto)

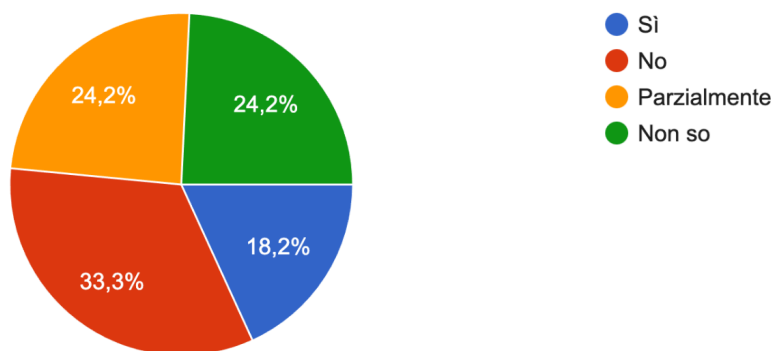
33 risposte



Con riferimento ai benefici, il 51,5% dei rispondenti ritiene che l'intelligenza artificiale possa migliorare l'efficienza dei processi decisionali, mentre il 33,3% mantiene una posizione neutra e il 15,2% esprime un giudizio negativo. Nel complesso, emerge una valutazione moderatamente positiva, accompagnata tuttavia da una certa cautela, che riflette probabilmente la complessità dei contesti applicativi.

8. Secondo te, i sistemi di IA utilizzati dalle banche sono sufficientemente trasparenti e comprensibili per i clienti?

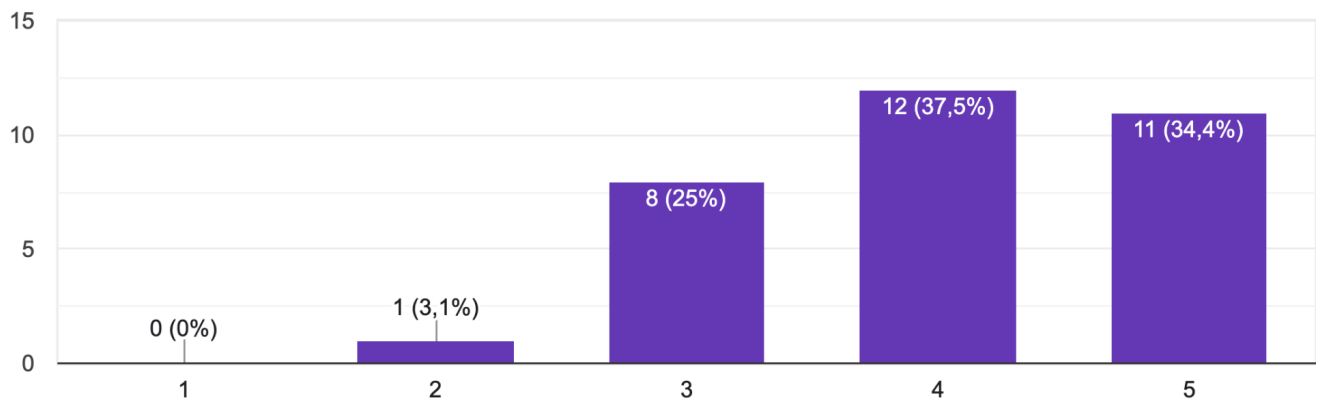
33 risposte



Uno degli aspetti più critici riguarda la trasparenza dei sistemi utilizzati. Solo una quota marginale degli intervistati ritiene che i sistemi di intelligenza artificiale siano sufficientemente comprensibili per i clienti, mentre una parte significativa esprime valutazioni negative o incerte.

16. Ritieni necessario un maggiore intervento umano nelle decisioni automatizzate basate su IA? Scegli un valore che va da 1 (per nulla) a 5 (molto)

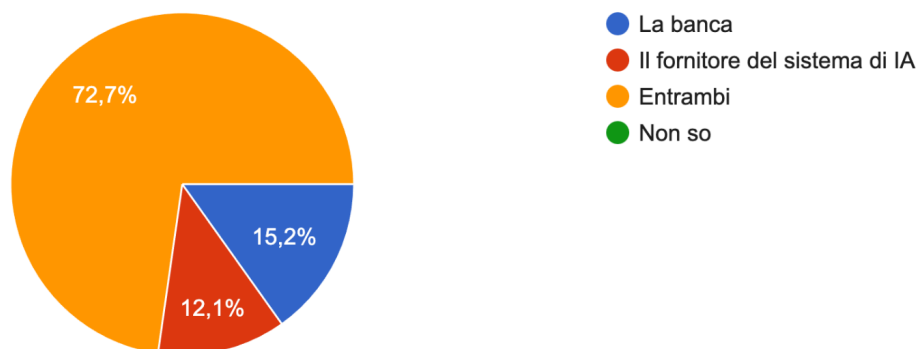
32 risposte



Tale dato si accompagna a una forte richiesta di intervento umano: il 71,9% dei rispondenti considera necessario un elevato livello di supervisione umana nelle decisioni automatizzate, mentre solo una quota residuale ritiene tale esigenza poco rilevante.

15. Chi dovrebbe essere principalmente responsabile in caso di errore o danno causato da un sistema di IA?

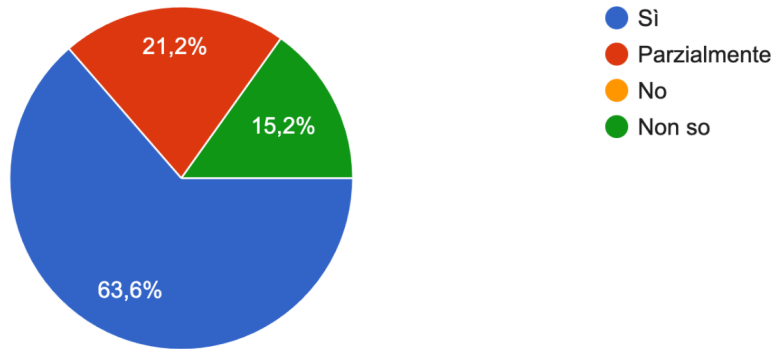
33 risposte



In relazione al tema della responsabilità, il 72,7% degli intervistati ritiene che, in caso di errore o danno, la responsabilità debba essere condivisa tra banca e fornitore del sistema, mentre quote più contenute attribuiscono tale responsabilità esclusivamente a uno dei due soggetti. Questo dato evidenzia la complessità del quadro giuridico connesso all'utilizzo di sistemi algoritmici, soprattutto in presenza di modelli sviluppati da terze parti.

### 13. Ritieni che l'AI Act avrà un impatto significativo sull'attività delle banche?

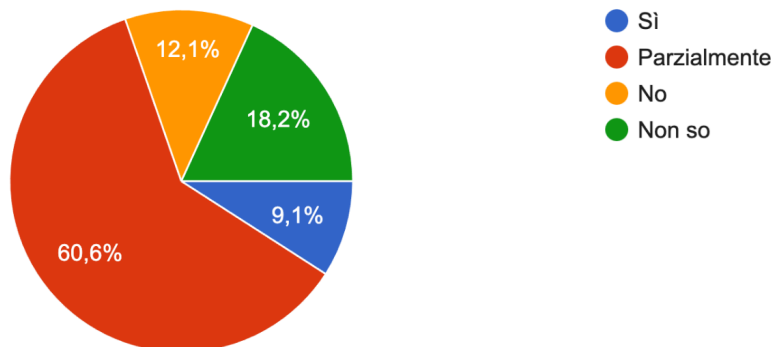
33 risposte



Sotto il profilo regolamentare, il 63,6% degli intervistati ritiene che l'AI Act avrà un impatto significativo sull'attività bancaria, a fronte di una minoranza che ne ridimensiona la portata o non esprime una valutazione definitiva.

### 14. Secondo te, le banche sono attualmente preparate a rispettare i requisiti normativi sull'IA (AI Act, GDPR, ecc.)?

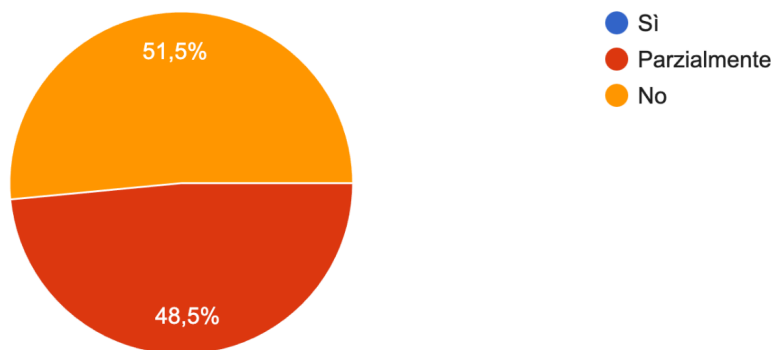
33 risposte



Tuttavia, emerge una percezione diffusa di preparazione ancora incompleta: solo il 9,1% ritiene che le banche siano pienamente pronte a rispettare i requisiti normativi, mentre il 60,6% valuta tale preparazione come solo parziale e una quota ulteriore esprime un giudizio negativo o incerto. Tale risultato evidenzia come l'adeguamento al nuovo quadro normativo rappresenti una sfida ancora in corso per gli intermediari.

### 17. Ritieni adeguata la formazione attuale del personale bancario sull'uso dell'IA?

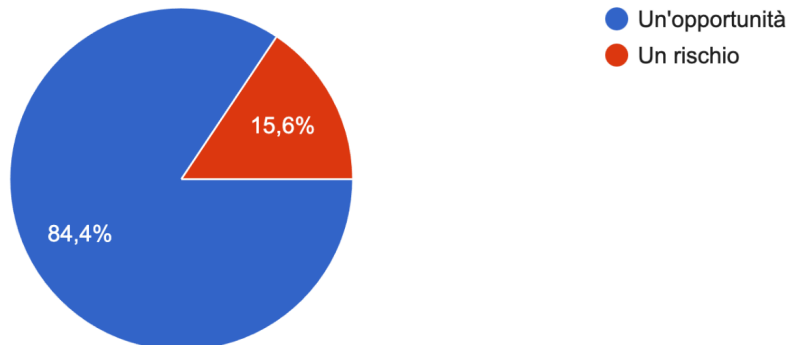
33 risposte



Un elemento particolarmente rilevante riguarda il tema della formazione: il 51,5% degli intervistati ritiene che la preparazione del personale sull'intelligenza artificiale sia inadeguata, mentre la restante parte la considera solo parzialmente sufficiente.

### 18. In futuro, l'IA rappresenterà per il settore bancario principalmente:

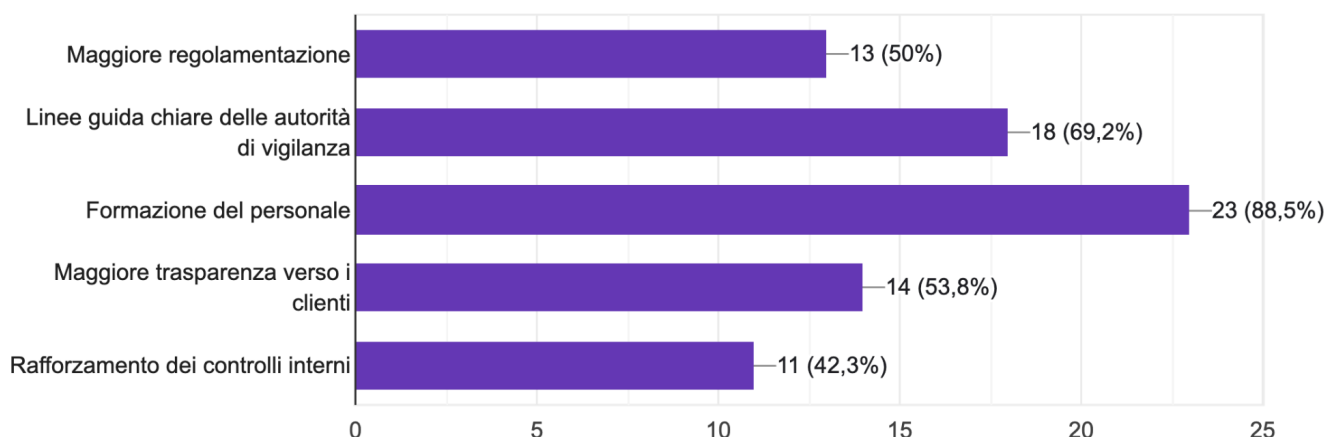
32 risposte



Nonostante tali criticità, la percezione complessiva delle prospettive future appare positiva: l'84,4% degli operatori considera l'intelligenza artificiale un'opportunità per il settore bancario, mentre solo una minoranza la percepisce prevalentemente come un rischio.

## 19. Quali interventi ritieni prioritari per una gestione responsabile dell'IA in banca?

26 risposte



Tra gli interventi ritenuti prioritari per una gestione responsabile dell'intelligenza artificiale emergono, in particolare, il rafforzamento della formazione del personale (88,5%), il maggiore coinvolgimento delle autorità di vigilanza (69,2%), nonché l'introduzione di più elevati standard di trasparenza (53,8%) e di controllo interno (42,3%).

Le risposte alla domanda aperta (A tuo avviso, qual è la principale criticità giuridica o operativa legata all'uso dell'intelligenza artificiale nel settore bancario?) posta alla fine del questionario consentono di cogliere ulteriori elementi qualitativi di particolare interesse. In particolare, le criticità maggiormente segnalate dai rispondenti si concentrano su tre ambiti principali: la definizione dei profili di responsabilità in caso di errore o danno derivante da sistemi automatizzati, la tutela dei dati personali e la necessità di garantire un adeguato livello di supervisione umana. Tali evidenze risultano coerenti con le principali questioni emerse nel dibattito dottrinale e regolamentare, confermando come le preoccupazioni degli operatori si collochino in linea con le criticità strutturali connesse all'utilizzo dell'intelligenza artificiale nel settore bancario.

Nel complesso, l'analisi evidenzia come gli operatori del settore bancario sviluppino una percezione articolata dell'intelligenza artificiale, caratterizzata da una consapevolezza più elevata rispetto alla clientela, ma anche da una maggiore attenzione alle criticità operative e regolamentari. In particolare, emerge una tensione tra il riconoscimento del potenziale innovativo dell'intelligenza artificiale e la necessità di rafforzare i presidi organizzativi, la formazione del personale e i meccanismi di controllo. Tali evidenze risultano coerenti con il quadro normativo delineato a livello europeo, che pone al centro temi quali la trasparenza, la responsabilità e la supervisione umana, confermando come

l'effettiva integrazione dell'intelligenza artificiale nel settore bancario richieda un approccio equilibrato tra innovazione tecnologica e gestione dei rischi.

#### **4.4 Confronto tra percezione della clientela e degli operatori bancari**

L'analisi congiunta dei risultati emersi dai questionari somministrati alla clientela e agli operatori del settore bancario consente di mettere in luce alcune significative convergenze, ma anche rilevanti divergenze nella percezione dell'intelligenza artificiale, offrendo una lettura più completa delle dinamiche in atto.

**Convergenze: consapevolezza dei benefici e centralità del fattore umano**

Un primo elemento di convergenza riguarda il riconoscimento dei benefici associati all'utilizzo dell'intelligenza artificiale. Sia la clientela sia gli operatori tendono a individuare nell'automazione un fattore di miglioramento dell'efficienza e della rapidità dei servizi bancari. Tale dato risulta particolarmente evidente tra gli operatori, il 50% dei quali ritiene che l'AI possa migliorare i processi decisionali, ma trova riscontro anche nella percezione della clientela, che associa l'innovazione tecnologica a una maggiore accessibilità e semplificazione dei servizi.

Accanto a ciò, entrambe le categorie evidenziano la persistente centralità dell'intervento umano. La clientela manifesta una chiara preferenza per il coinvolgimento di un operatore nelle decisioni più rilevanti, come nel caso della concessione del credito, mentre gli operatori stessi sottolineano la necessità di mantenere un elevato livello di supervisione umana nei processi automatizzati. In particolare, il 71% dei rispondenti appartenenti al settore bancario ritiene necessario un significativo intervento umano, dato che si pone in linea con le preoccupazioni espresse dalla clientela in merito alla perdita di controllo sui processi decisionali.

Tali evidenze suggeriscono come, nonostante il crescente grado di automazione, la relazione fiduciaria continui a rappresentare un elemento strutturale del rapporto banca-cliente, difficilmente sostituibile da sistemi interamente algoritmici.

**Divergenze: consapevolezza, utilizzo e percezione del rischio**

Accanto agli elementi di convergenza, l'analisi mette in evidenza anche alcune differenze significative tra le due categorie di rispondenti, che appaiono riconducibili soprattutto al diverso grado di familiarità con gli strumenti tecnologici.

In primo luogo, emerge una diversa consapevolezza circa l'effettivo utilizzo dell'intelligenza artificiale. Gli operatori del settore, pur con livelli di conoscenza non sempre elevati, mostrano una maggiore

esposizione concreta a tali strumenti, spesso integrati nei processi lavorativi quotidiani. La clientela, al contrario, tende a manifestare una conoscenza più frammentaria e incerta. Questo aspetto trova conferma nel fatto che una quota rilevante di utenti non è in grado di stabilire se abbia effettivamente utilizzato servizi basati sull'intelligenza artificiale, segno di una percezione ancora poco definita e, in parte, mediata dall'esperienza d'uso piuttosto che dalla comprensione dei meccanismi sottostanti. A tal proposito è possibile osservare coerenza tra la percezione della clientela secondo lo studio di PWC e quella emersa nell'analisi empirica da me svolta. In entrambi i casi, infatti, i clienti si mostrano propensi all'uso dell'intelligenza artificiale nel settore bancario per la velocizzazione dei processi, ma mostrano qualche cautela in circostanze quali l'analisi del credito o la gestione delle risorse finanziarie. Gli operatori, invece, pur non trascurando tali profili, appaiono maggiormente sensibili alle implicazioni di natura organizzativa e regolamentare, come la gestione del rischio, la definizione delle responsabilità in caso di errore e l'adeguamento ai vincoli normativi.

Ne deriva una differenza di prospettiva piuttosto netta: mentre la clientela sviluppa una forma di diffidenza legata soprattutto all'esperienza diretta e al livello di fiducia nei confronti dell'intermediario, gli operatori tendono a inquadrare il fenomeno in termini più tecnici, ponendo l'accento sui meccanismi di funzionamento e sui presidi di controllo.

Un elemento di particolare interesse è rappresentato dal tema della trasparenza, rispetto al quale si registra una convergenza tra le due prospettive. Da un lato, la clientela lamenta una difficoltà nel comprendere le logiche alla base delle decisioni automatizzate e una percezione di scarsa informazione sull'utilizzo dei propri dati; dall'altro, gli stessi operatori riconoscono che i sistemi adottati non sempre risultano pienamente intelligibili per l'utente finale.

Questa convergenza assume un rilievo significativo, in quanto evidenzia una criticità che non riguarda esclusivamente la percezione esterna, ma investe più in generale il funzionamento del sistema. La limitata trasparenza, infatti, non incide soltanto sulla fiducia della clientela, ma pone anche questioni rilevanti sotto il profilo della responsabilità e della capacità degli intermediari di garantire un adeguato livello di controllo sui processi decisionali automatizzati.

Un ulteriore profilo di interesse riguarda la percezione del quadro regolamentare. Gli operatori mostrano una chiara consapevolezza dell'impatto che la disciplina europea, e in particolare l'AI Act, potrà avere sull'attività bancaria, pur evidenziando un livello di preparazione ancora parziale da parte degli intermediari.

La clientela, dal canto suo, manifesta un'esigenza piuttosto chiara di rafforzamento del quadro regolatorio, in particolare con riferimento alla tutela dei dati personali e alla maggiore trasparenza dei processi decisionali automatizzati. Tale richiesta appare strettamente connessa a una percezione

ancora incerta delle modalità attraverso cui le tecnologie vengono impiegate, nonché al timore che decisioni rilevanti possano essere assunte sulla base di logiche difficilmente comprensibili.

Se si considera nel complesso il quadro emerso, si può osservare una sostanziale convergenza tra clientela e operatori nell'attribuire alla regolazione un ruolo centrale nel garantire un utilizzo responsabile dell'intelligenza artificiale. Tuttavia, le ragioni sottostanti a tale convergenza non risultano del tutto sovrapponibili: gli operatori tendono a valorizzare maggiormente i profili legati alla gestione dei processi e alla conformità normativa, mentre la clientela appare più sensibile alle esigenze di tutela e al mantenimento di un adeguato livello di fiducia nei confronti dell'intermediario. Sotto questo profilo, il confronto tra le due prospettive restituisce un'immagine articolata del fenomeno. L'intelligenza artificiale nel settore bancario non viene infatti percepita in modo uniforme, ma attraverso punti di osservazione differenti, che riflettono il ruolo ricoperto dai soggetti coinvolti. Se, da un lato, gli operatori mostrano una maggiore consapevolezza delle implicazioni tecniche e regolamentari, dall'altro lato la clientela tende a porre l'accento su aspetti quali la comprensibilità delle decisioni e la tutela dei propri interessi.

Le differenze emerse non sembrano tuttavia configurare una contrapposizione, quanto piuttosto evidenziare la complessità del processo di integrazione delle nuove tecnologie nei servizi bancari. In questa prospettiva, appare sempre più necessario un approccio che sappia tenere insieme le esigenze operative degli intermediari e le aspettative della clientela, evitando soluzioni eccessivamente sbilanciate in una sola direzione.

L'introduzione dell'intelligenza artificiale non può quindi essere letta esclusivamente in termini di innovazione tecnologica, ma richiede la costruzione di un contesto di fiducia condiviso, nel quale assumono rilievo la trasparenza dei processi, la chiara individuazione delle responsabilità e la presenza di adeguati meccanismi di supervisione umana.

Proprio in questa direzione si colloca l'intervento del legislatore europeo: i risultati dell'indagine empirica sembrano infatti confermare, almeno in parte, la rilevanza degli obiettivi perseguiti dall'AI Act, che mira a conciliare le esigenze di sviluppo tecnologico con la necessità di garantire un livello adeguato di tutela degli utenti.

#### **4.5 Considerazioni conclusive dell'analisi empirica**

L'analisi empirica condotta attraverso i questionari rivolti alla clientela e agli operatori del settore bancario consente di formulare alcune considerazioni di sintesi che contribuiscono a completare il quadro delineato nei capitoli precedenti. I risultati raccolti evidenziano, infatti, come l'introduzione

dell'intelligenza artificiale nel sistema bancario non produca effetti esclusivamente sul piano tecnico-operativo, ma incida in modo significativo anche sulla percezione degli utenti e sulle dinamiche organizzative interne agli intermediari.

Un primo elemento che emerge con chiarezza è rappresentato dalla diffusione, ormai significativa, dei servizi digitali e dall'utilizzo, spesso implicito, di sistemi basati sull'intelligenza artificiale. Tuttavia, tale diffusione non appare accompagnata da un adeguato livello di consapevolezza, soprattutto da parte della clientela, che in molti casi non è in grado di riconoscere quando tali tecnologie vengano effettivamente impiegate. Questa asimmetria informativa costituisce uno degli aspetti più rilevanti emersi dall'indagine, in quanto incide direttamente sulla percezione della fiducia e sulla capacità degli utenti di valutare i servizi offerti.

Un ulteriore profilo emerso dall'analisi riguarda il modo in cui vengono percepiti benefici e rischi connessi all'utilizzo dell'intelligenza artificiale. Sia la clientela sia gli operatori tendono a riconoscere i vantaggi legati all'automazione, soprattutto in termini di maggiore efficienza, rapidità dei processi e capacità di migliorare l'organizzazione delle attività. Allo stesso tempo, però, tali elementi positivi si accompagnano a una serie di perplessità che riguardano, in particolare, la trasparenza dei sistemi, la comprensibilità delle decisioni e la gestione dei dati personali.

Tra questi aspetti, assume un rilievo specifico la difficoltà, spesso segnalata dagli utenti, di comprendere le logiche che guidano le decisioni automatizzate. Quando tali decisioni incidono su profili rilevanti come, per esempio, l'accesso al credito, questa opacità tende a tradursi in una riduzione del livello di fiducia nei confronti dell'intermediario.

In questo quadro, il tema del controllo umano emerge in modo piuttosto netto. Le risposte raccolte mostrano come, pur in presenza di un crescente ricorso all'automazione, sia ancora avvertita l'esigenza di mantenere un intervento umano nei processi decisionali, soprattutto nei casi più complessi. La supervisione da parte di un operatore continua infatti a essere percepita come una forma di garanzia, capace di compensare i limiti dei sistemi automatizzati e di offrire un margine di valutazione discrezionale.

Un ulteriore elemento di riflessione riguarda il livello di preparazione del sistema bancario. Dal punto di vista degli operatori, emerge l'impressione che le competenze necessarie per gestire in modo efficace l'intelligenza artificiale non siano ancora pienamente diffuse, così come non appare del tutto consolidata la capacità di far fronte ai nuovi obblighi normativi. In questo senso, il tema della formazione del personale assume un ruolo particolarmente rilevante, insieme alla necessità di rafforzare i presidi di controllo interno.

Se si considerano congiuntamente le due prospettive analizzate, emerge quindi una duplice esigenza. Da un lato, quella di intervenire sul piano organizzativo e tecnico, attraverso investimenti in

competenze, modelli di governance e strumenti di controllo; dall'altro, quella di migliorare la relazione con la clientela, rendendo più trasparenti le modalità di utilizzo delle tecnologie e più comprensibili i processi decisionali.

Alla luce di tali elementi, il ruolo della regolazione appare destinato ad assumere un'importanza crescente. I risultati dell'indagine suggeriscono infatti come, accanto alle esigenze di innovazione, si sviluppi una domanda di maggiore tutela, condivisa, seppur con accenti diversi, sia dagli operatori sia dagli utenti. In questa prospettiva, il quadro normativo europeo, e in particolare l'AI Act, si inserisce come uno strumento volto a orientare l'evoluzione del settore, promuovendo un utilizzo dell'intelligenza artificiale che sia non solo efficiente, ma anche trasparente e responsabile.

Nel complesso, l'analisi empirica conferma come l'integrazione dell'intelligenza artificiale nel settore bancario rappresenti un processo ancora in evoluzione, caratterizzato da opportunità rilevanti ma anche da criticità non trascurabili. La sfida principale appare quella di costruire un equilibrio sostenibile tra innovazione tecnologica ed esigenze di tutela, in modo da favorire un'adozione consapevole e responsabile delle nuove tecnologie.

I risultati del presente capitolo non si limitano a offrire una fotografia dello stato attuale, ma forniscono anche indicazioni utili per orientare le future scelte degli intermediari e del legislatore, evidenziando la necessità di un approccio integrato che tenga conto, in modo coordinato, delle dimensioni tecnologiche, organizzative e giuridiche del fenomeno.

## Conclusioni

L'analisi svolta nel corso della presente tesi consente di evidenziare come l'intelligenza artificiale rappresenti oggi un fattore strutturale di trasformazione del settore bancario, incidendo in maniera significativa tanto sui modelli organizzativi quanto sui processi decisionali. L'evoluzione tecnologica, lungi dall'essere un fenomeno circoscritto alla dimensione tecnica, assume infatti una rilevanza sistemica, coinvolgendo profili economici, giuridici ed etici che richiedono un approccio integrato e multidisciplinare.

Dallo studio emerge come l'introduzione di sistemi basati sull'intelligenza artificiale comporti indubbi benefici in termini di efficienza, rapidità e capacità predittiva, contribuendo a migliorare la qualità dei servizi offerti e a rafforzare i processi di gestione del rischio. Tuttavia, tali vantaggi si accompagnano a una serie di criticità, riconducibili principalmente alla trasparenza dei modelli, alla tutela dei dati personali, alla definizione delle responsabilità e alla necessità di garantire un adeguato livello di supervisione umana.

Le evidenze empiriche raccolte attraverso i questionari somministrati a operatori del settore e alla clientela confermano, seppur da prospettive differenti, la presenza di una duplice dinamica. Da un lato, gli operatori mostrano una maggiore consapevolezza delle implicazioni tecniche e regolamentari connesse all'utilizzo dell'intelligenza artificiale; dall'altro, la clientela manifesta esigenze più marcate in termini di comprensibilità, fiducia e protezione, evidenziando una percezione talvolta incerta o parziale delle modalità di utilizzo di tali tecnologie.

In questo contesto, il parallelismo con il fenomeno del sabotaggio, sviluppatosi durante la rivoluzione industriale, appare particolarmente significativo. All'epoca, l'introduzione delle macchine generò timori diffusi circa la sostituzione del lavoro umano e la perdita di controllo sui processi produttivi, alimentando forme di resistenza che, pur radicate in un contesto storico profondamente diverso, riflettevano una più generale diffidenza nei confronti dell'innovazione tecnologica. Analogamente, l'intelligenza artificiale tende oggi a suscitare un insieme di incertezze e preoccupazioni, in particolare nei settori, come quello bancario, caratterizzati da un elevato grado di responsabilità e da una forte dipendenza dalla fiducia degli utenti.

Tuttavia, così come la rivoluzione industriale ha progressivamente dimostrato la capacità delle tecnologie di affermarsi come strumenti di progresso economico e sociale, anche l'intelligenza artificiale può essere interpretata in una prospettiva evolutiva, quale risorsa in grado di supportare — e non sostituire — l'attività umana. In ambito bancario, ciò implica la possibilità di utilizzare sistemi

intelligenti come strumenti di ausilio ai processi decisionali, capaci di aumentare la rapidità e l'accuratezza delle valutazioni, senza tuttavia prescindere dal ruolo insostituibile dell'intervento umano, soprattutto nei casi più complessi.

Un esempio emblematico di tale logica è rappresentato dall'ambito medico, ove l'intelligenza artificiale viene già impiegata per supportare il monitoraggio e la gestione di condizioni cliniche attraverso sistemi integrati che affiancano il paziente e il personale sanitario, contribuendo a ridurre il margine di errore e a migliorare l'efficacia delle decisioni. Tale modello evidenzia come l'integrazione tra competenze umane e capacità computazionali possa generare benefici significativi, purché sia inserita all'interno di un quadro regolamentare adeguato e di meccanismi di controllo efficaci.

Alla luce di quanto emerso, il ruolo della regolazione assume una funzione centrale nel guidare lo sviluppo dell'intelligenza artificiale verso un utilizzo responsabile. In questa prospettiva, il legislatore europeo, attraverso l'AI Act, si propone di delineare un assetto normativo volto a garantire un equilibrio tra innovazione, tutela dei diritti fondamentali e stabilità del sistema finanziario, introducendo obblighi in materia di trasparenza, gestione del rischio e supervisione umana.

In conclusione, l'intelligenza artificiale non rappresenta di per sé una fonte di rischio o di opportunità assoluta, ma uno strumento il cui impatto dipende dalle modalità con cui viene progettata, implementata e governata. La sfida principale per il settore bancario consiste dunque nel saper integrare tali tecnologie all'interno di modelli organizzativi solidi, capaci di valorizzarne le potenzialità senza rinunciare ai principi di responsabilità, trasparenza e fiducia che costituiscono il fondamento dell'intermediazione finanziaria.

## Bibliografia

- Avgouleas, Emiliios, *The Governance of Global Financial Markets*, Cambridge, Cambridge University Press, 2012, pp. 254–260.
- Barto, Andrew G. – Sutton, Richard S. – Anderson, Charles W., *Neuronlike adaptive elements that can solve difficult learning control problems*, *IEEE Transactions on Systems, Man and Cybernetics*, vol. SMC 13, 1983, pp. 834–846.
- Becerra-Vicario, Ramón – altri autori, *The Impact of Artificial Intelligence in the Financial Sector: Opportunities and Challenges*, University of Málaga, 2023, pp. 10–39.
- Bolaffi, Guido, “Nel mondo cambia la distribuzione della ricchezza”, *Fondazione Med-Or*, settembre 2023.
- Cath, Corinne, *Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges*, *Philosophical Transactions of the Royal Society A*, 2018.
- Davenport, Thomas H. – Ronanki, Rajeev, *Artificial Intelligence for the Real World*, *Harvard Business Review*, 2018.
- Dragone, Vincenzo Giovanni, “Le tre fratture dell’intelligenza artificiale in banca”, *dirittobancario.it*, 2026.
- Elliott, Anthony, *The Culture of AI*, Cambridge, Polity Press, 2019.
- Fuster, Andreas – et al., *Predictably Unequal? The Effects of Machine Learning on Credit Markets*, *NBER Working Paper Series*, 2022, p. 5.
- Finocchiaro, Giovanni, *Privacy e protezione dei dati personali*, Bologna, Il Mulino, 2021, pp. 201–215.
- Floridi, Luciano, *The Ethics of Artificial Intelligence*, Oxford, Oxford University Press, 2021.
- Gama, João – Žliobaitė, Indrė – Bifet, Albert – Pechenizkiy, Mykola – Bouchachia, Abderrahmane, *A Survey on Concept Drift Adaptation*, *ACM Computing Surveys*, 2014.
- Gomber, Peter – Koch, Jens A. – Siering, Michael, *Digital Finance and FinTech: Current Research and Future Research Directions*, *Journal of Business Economics*, 2017.

- Hopfield, John J., *Neural networks and physical systems with emergent collective computational abilities*, *Proceedings of the National Academy of Sciences USA*, vol. 79, 1982, pp. 2554–2558.
- Jagtiani, Julapa – Lemieux, Catharine, *The Roles of Alternative Data and Machine Learning in FinTech Lending: Evidence from Revolut*, *Journal of Financial Intermediation*, vol. 52, 2022, pp. 1–15.
- Kissinger, Henry A. – Schmidt, Eric – Huttenlocher, Daniel, *L'era dell'Intelligenza artificiale. Il futuro dell'identità umana*, Milano, Mondadori, 2023, pp. 48–55.
- Kohonen, Teuvo, *Self-organized formation of topologically correct feature maps*, *Biological Cybernetics*, vol. 43, 1982, pp. 59–69.
- Lemme, Giuliano, “La proposta di regolamento europeo sull'intelligenza artificiale e la gestione dei rischi: una battaglia che può essere vinta?”, *Rivista Trimestrale di Diritto dell'Economia*, Supplemento 1/2024.
- Mantelero, Alessandro, *Intelligenza artificiale e diritto. Una introduzione*, Torino, Giappichelli, 2022, pp. 131–148.
- Id., *The Fundamental Rights Impact Assessment in the AI Act*, working paper / preprint, 2024.
- Maple, Carsten – et al., *The AI Revolution: Opportunities and Challenges for the Finance Sector*, 2023, pp. 6–20.
- Marr, David, *Vision: A Computational Investigation into the Human Representation and Processing of Visual Information*, San Francisco, W.H. Freeman, 1982.
- McLuhan, Marshall, *Understanding Media: The Extensions of Man*, Cambridge (MA), MIT Press, 1994.
- Meta, Federica, articolo in *CorCom*, 10 ottobre 2018.
- Minsky, Marvin – Papert, Seymour, *Perceptrons: An Introduction to Computational Geometry*, Cambridge (MA), MIT Press, 1969.
- Mirishli, Samira, *Regulating AI in Financial Services: Legal Frameworks and Compliance Challenges*, 2023, pp. 29–39.
- Molnar, Christoph, *Interpretable Machine Learning*, 2020.

Mühlhoff, Rainer, *Intelligenza artificiale assistita dall'uomo: ovvero come eseguire calcoli complessi nel cervello umano?*, *New Media & Society*, 2020.

Pasquale, Frank, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge (MA), Harvard University Press, 2015.

Passador, Maria L., *AI Act and the ECB: Steering Financial Supervision in the EU*, *Columbia Journal of European Law*, 2025, pp. 10–20.

Rangone, Nicoletta – Megale, Luca, *Risks Without Rights: The EU AI Act's Approach to AI in Law and Rulemaking*, Cambridge, Cambridge University Press, 2023.

Rinaldi, Patrizio, "Strategie di data security nell'era dell'AI Generativa", *Rapporto Clusit 2024*, pp. 298–299.

Rosenblatt, Frank, *The Perceptron: A probabilistic model for information storage and organization in the brain*, *Psychological Review*, 1958.

Turing, Alan, *Computing Machinery and Intelligence*, *Mind*, 1950, pp. 433–460.

Turkle, Sherry, *Insieme ma soli*, Milano, Cortina Raffaello, 2019, p. 350.

Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, PublicAffairs, 2019.

## **Fonti normative e istituzionali**

- Banca Centrale Europea, *Guide on the Assessment of Mergers and Acquisitions in the Banking Sector*, 2021.
- Commissione Europea, *Proposal for a Regulation Laying Down Harmonized Rules on Artificial Intelligence (AI Act)*, Bruxelles, 2021.
- Commissione Europea, *White Paper on Artificial Intelligence: A European Approach to Excellence and Trust*, Bruxelles, 2020.
- Commissione Europea, *Coordinated Plan on Artificial Intelligence*, Bruxelles, 2018.
- Comitato di Basilea per la Vigilanza Bancaria, *Basel III: Finalising Post-Crisis Reforms*, Basilea, Bank for International Settlements, 2017.
- European Banking Authority, *Report on Big Data and Advanced Analytics*, Parigi, 2020.

- European Securities and Markets Authority, *Guidelines on Automated Advice and Digital Investment Services*, Parigi, 2018.
- OCSE, *OECD Principles on Artificial Intelligence*, 2019.
- UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, Parigi, UNESCO, 2021.
- Regolamento (UE) 2016/679, *Regolamento generale sulla protezione dei dati (GDPR)*, Bruxelles, 2016.
- Regolamento (UE) 2022/2554, *Digital Operational Resilience Act (DORA)*, Bruxelles, 2022.
- Legge 23 settembre 2025, n. 132, *Disposizioni e deleghe al Governo in materia di intelligenza artificiale*.

### **Siti web**

- [www.statista.com](http://www.statista.com)
- [www.microbiologiaitalia.it](http://www.microbiologiaitalia.it)
- [www.agendadigitale.eu](http://www.agendadigitale.eu)
- [www.wikipedia.org](http://www.wikipedia.org) (voce: “Società dell’informazione”)
- [www.dirittobancario.it](http://www.dirittobancario.it)
- Fondazione Med-Or – [www.med-or.org](http://www.med-or.org)