DB non solo diritto bancario

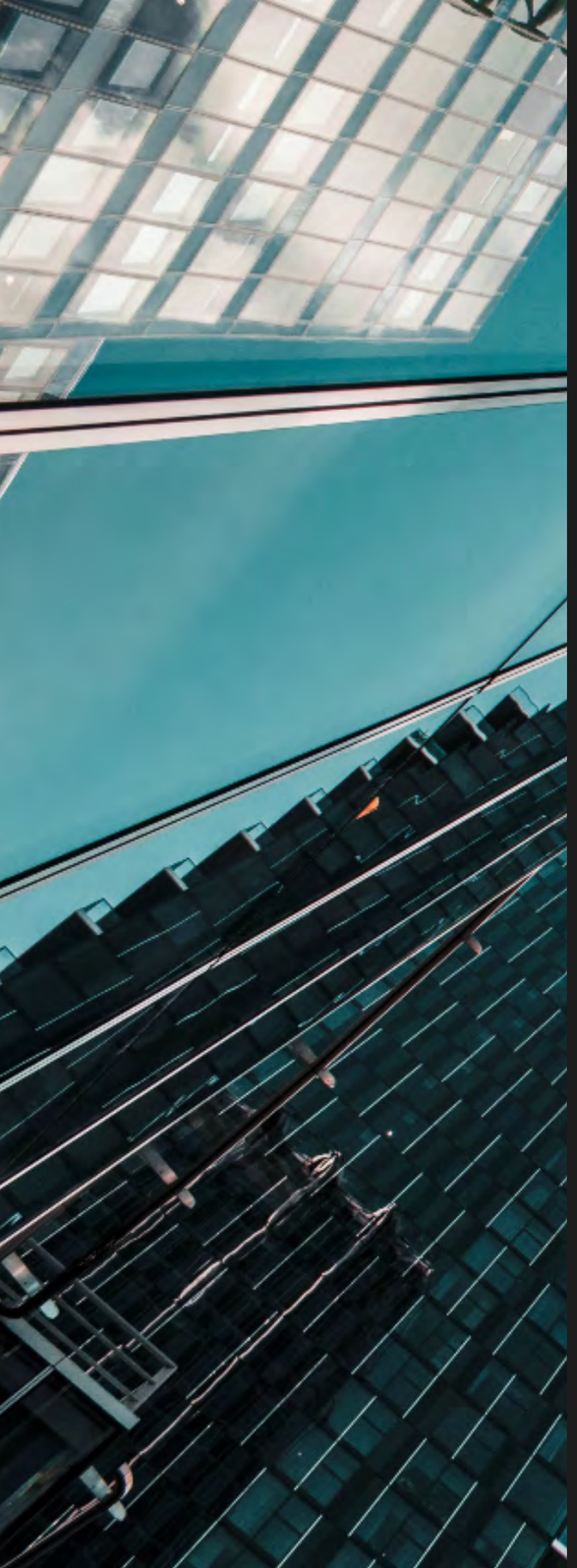
leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

Finanza Digitale e IA: nuove sfide e opportunità

Marzo 2025

Paolo Roberto Amendola, Annunziata & Conso
Thomaz Braga de Arruda, Annunziata & Conso



Paolo Roberto Amendola, Annunziata & Conso

Thomaz Braga de Arruda, Annunziata & Conso

1. Introduzione

Il galoppante e multiforme sviluppo tecnologico, oggi permeato dagli strumenti e i processi di *machine learning* e, più in generale, di IA ha prodotto consistenti impatti anche sul mercato finanziario e, in particolare, sulle modalità di prestazione dei servizi bancari e finanziari, aggiungendo nuovi spunti di innovazione alla - già estremamente diffusa - c.d. finanza digitale.

In tale contesto, i recenti progressi nel *deep learning (letteralmente, "apprendimento profondo"*, ossia un campo di ricerca del machine leargnin, "apprendimento automatico") hanno consolidato notevolmente il ruolo dell'IA nel settore dei servizi bancari e finanziari[1].

In effetti, volgendo l'attenzion al mercato, un'indagine sugli enti creditizi vigilati dalla Banca Centrale Europea (BCE) ha confermato che la maggior parte delle banche dell'UE utilizza già sistemi di IA in diversi ambiti[2]. Stesso fenomeno è stato osservato per il mercato dei capitali, come rilevato dall'Organizzazione internazionale delle commissioni sui valori mobiliari (IOSCO)[3] e dall'Autorità europea degli strumenti finanziari e dei mercati (ESMA)[4], con la precisazione che la diffusione dell'IA sul mercato dei capitali sta producendo uno slancio che ne favorisce la continua espansione. In considerazione della diffusione, sempre più capillare, dell'IA, la Commissione europea ha rilevato la necessità di emanare

1 In proposito, si noti che già nel marzo 2018 è stato nominato un gruppo di esperti per analizzare gli ostacoli normativi all'innovazione finanziaria (*Regulatory Obstacles to Financial Innovation Experts Group - ROFIEG*), ciò al fine di assistere la Direzione generale della Stabilità finanziaria, dei servizi finanziari e dell'Unione dei mercati dei capitali (FISMA) della Commissione europea, affiancandovi le competenze necessarie ad un'adeguata valutazione dell'impatto dell'IA sul settore FinTech: la relazione finale del ROFIEG - datata 13 dicembre 2019 - ha rilevato che l'IA sarebbe diventata sempre più rilevante sia per il settore FinTech, sia per il settore RegTech" (Cfr. ROFIEG, *30 Recommendations on Regulation, Innovation and Finance – Final Report to the European Commission* (2019)).

2 Cfr. BCE, "*Banks' digital transformation: where do we stand*?", Supervision Newsletter (2023). Detta tendenza è stata confermata anche dall'Autorità Bancaria Europea (ABE), che nel suo rapporto di valutazione dei rischi del 2020 ha riferito che il 64% degli istituti di credito dell'UE utilizzava già strumenti basati sull'IA.

3 Organizzazione Internazionale delle Commissioni per i Titoli (IOSCO), "*The use of artificial intelligence and machine learning by market intermediaries and asset managers*" (settembre 2021).

4 Vedi ESMA, "*Artificial intelligence in EU securities markets*", ESMA TRV Risk Analysis (ESMA50-164-6247), 1° febbraio 2023. V. anche, più recentemente, ESMA, "*Public Statement on the Use of Artificial Intelligence (AI) in the Provision of Retail Investment Services*" (ESMA35-335435667-5924 del 30 maggio 2024; ESMA, "*Artificial intelligence in EU investment funds*" (ESMA50-43599798-9923) del 25 febbraio 2025.

vedi l'articolo online

standard normativi chiari con riferimento all'IA nel settore finanziario.

In tale contesto, le iniziative legislative introdotte dall'UE mirano a limitare i rischi derivanti dall'utilizzo dell'IA, sia da un punto di vista tecnologico - in particolare attraverso il c.d. *AI Act* (il Regolamento IA)[5] - sia dal punto di vista procedurale, attraverso la regolamentazione di cui al c.d. *Digital Operational Resilience Act* (il Regolamento DORA)[6].

L'approccio orientato ai rischi è ben motivato dalle analisi effettuate sul mercato come rilevato, *inter alia*, da un sondaggio condotto dall'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) nel 2024: nell'ambito di detto sondaggio sono stati identificati vari rischi associati all'implementazione dell'IA nel settore finanziario (cfr. Figura 1 sotto), ove però l'ingerenza dell'IA sulla prestazione del servizio finanziario pare essere ancora in una fase embrionale, concentrandosi per lo più sull'automazione dei processi e procedure propedeutiche e/o accessorie alla prestazione del servizio. In tale sondaggio è stata, altresì, rilevata la tendenza del mercato a monitorare attivamente i *trend* al fine di individuare (o, meglio, in qualche modo, prevedere) i rischi emergenti, i cui criteri di classificazione si sono evoluti e continuano ad evolversi: tale attenzione ai rischi deriva probabilmente dalla circostanza che la natura e le caratteristiche degli strumenti di IA può amplificare i rischi esistenti, innescare effetti di ricaduta in diverse aree di business, o addirittura generare rischi completamente nuovi e imprevedibili.

5 Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce norme armonizzate in materia di IA e che modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/85 8, (UE) 2018/1139 e (UE) 2019/2144 e Direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regolamento sull'IA) GU L, 2024/1689, 12.7. 2024. Cfr. Michael Veale e Frederik Zuiderveen Borgesius, "*Demystifying the Draft EU Artificial Intelligence Act*", 22 Comput. L. Rev. Int'l 97 (2021); Sciarrone Alibrandi A, Rabitti M e Schneider G, "*L'impatto del Regolamento europeo sull'IA sui mercati finanziari: dalla governance alla coregolamentazione*" (European Banking Institute Working Paper Series n. 138, 11 aprile 2023).

6 Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, sulla resilienza operativa digitale del settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1-79). 014 e (UE) 2016/1011 (GU L 333 del 27.12.2022, pag. 1-79).

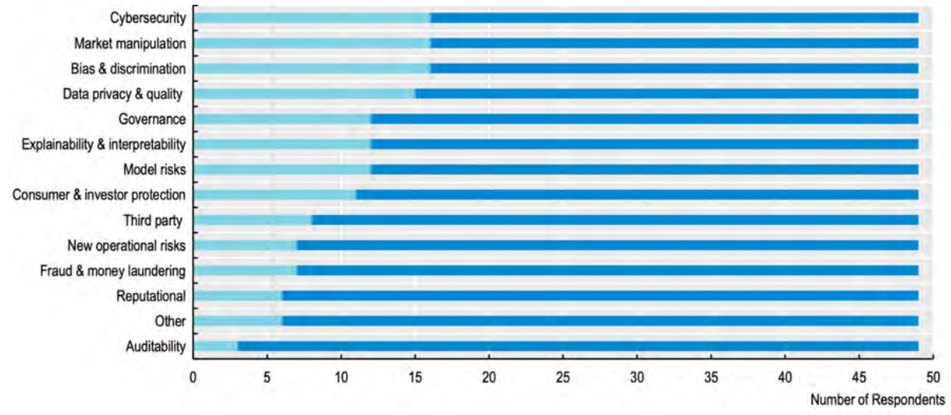


Figura 1: Rischi indicativi del settore finanziario legati all'uso dell'IA nel mercato dei servizi finanziari

Fonte: Indagine OCSE 2024 sugli approcci normativi all'IA nella finanza. Basato su un totale di 49 giurisdizioni rispondenti.

2. L'approccio normativo all'IA

L'interesse strategico dell'UE per l'IA risale al 2018, quando ben 25 Stati membri hanno sottoscritto una Dichiarazione di Cooperazione sull'IA[7], la quale ha rappresentato il primo pilastro verso l'emanazione di un quadro normativo europeo relativo all'IA[8]. In tale contesto, l'UE ha tenuto in considerazione, nell'approccio normativo molto prudenziale all'IA e alle tematiche connesse alla stessa, ciò nel timore che detto fenomeno si espandesse in maniera non regolamentata[9].

7 Cfr. Declaration of cooperation on Artificial Intelligence (AI) del 10 aprile 2018, disponibile su https://digital-strategy.ec.europa.eu/en/news/eu-member-states-sign-cooperate-artificial-intelligence.

8 Cfr. Commissione europea, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Coordinated Plan on Artificial Intelligence* (2018) 795 final.

9 V. Commissione Europea, *IA* (2022) https://digital-strategy.ec.europa.eu/en/policies/artificial-intelligence.

vedi l'articolo online

Sulla scorta di tali preoccupazioni e detto approccio, la Commissione europea ha introdotto, nell'aprile 2021, un nuovo pacchetto normativo relativo all'IA: detto pacchetto normativo includeva la Comunicazione sulla promozione di un approccio europeo all'IA[10], un piano coordinato con gli Stati membri[11] e il Regolamento IA, integrato da un *white paper* che propone un quadro normativo generale dell'UE per l'IA[12].

Nonostante l'ampio programma normativo e strategico delle istituzioni europee, tuttavia, il quadro legislativo europeo sull'IA disciplina le implicazioni sul mercato finanziario in maniera piuttosto superficiale. Il principale intervento normativo, ossia il Regolamento IA, nell'occuparsi dell'applicazione dell'IA nel settore finanziario, si concentra quasi esclusivamente sul *credit scoring* algoritmico, affrontando sulle questioni relative ai meccanismi di valutazione del merito creditizio, ignorando, tuttavia, gli altri potenziali rischi derivanti dall'uso dell'IA nel settore finanziario, ad esempio, nella prestazione dei servizi di investimento.

A ben vedere, trattasi di una lacuna che non pare essere accidentale, in quanto l'UE ha riconosciuto in diverse occasioni l'impatto dell'IA sui mercati finanziari ritenendo, evidentemente, che detto impatto non richieda ancora uno specifico intervento normativo. L'inerzia del legislatore europeo su questa tematica deriva probabilmente dalla ricerca di un bilanciamento tra innovazione e sicurezza, la cui chiave di lettura sono i principi normativi di neutralità tecnologica e proporzionalità.

Il principio di neutralità tecnologica[13] occupa un ruolo fondamentale per la strategia dell'UE in materia di IA e stabilisce che la regolamentazione non dovrebbe favorire né svantaggiare tecnologie specifiche, il che implica che le norme dedicate all'IA dovrebbero essere introdotte esclusivamente quando la legislazione esistente non riesce a mitigare adeguatamente i rischi legati all'IA. Di conseguenza, l'approccio dell'UE alla regolamentazione dell'IA è intrinsecamente basato sul rischio piuttosto che sulla tecnologia, il che significa che le nuove normative entreranno in vigore solo se l'IA introduce rischi nuovi e non ancora affrontati.

Seguendo questa logica, il Regolamento IA adotta una struttura normativa basata sul rischio, garantendo che l'intervento normativo rimanga limitato nella misura necessaria. L'obiettivo è quello di applicare una disciplina specifica solo laddove l'IA presenti un rischio giustificabile, evitando al contempo vincoli eccessivi in settori in cui i rischi sono minimi o già gestiti dalla disciplina esistente. Sia il *white paper*, sia Regolamento IA riconoscono che il panorama normativo finanziario dell'UE è già ampio e copre numerose applicazioni dell'IA. I regimi settoriali esistenti, come la MiFID II (Direttiva 2014/65/UE sui mercati degli strumenti finanziari), che impone requisiti alle imprese impegnate, ad esempio, nel *trading* algoritmico[14] e il Regolamento MAR (Regolamento 596/2014 relativo agli abusi di mercato), che affronta i rischi di manipolazione del mercato legati ai sistemi algoritmici[15], sono esempi di normative tecnologicamente neutre in grado di affrontare i rischi legati all'IA. L'approccio dell'UE in materia si basa dunque sull'assunto che l'IA non necessita di un livello separato di regolamentazione finanziaria, a meno che la stessa non crei rischi che la legislazione europea esistente non sia in grado di mitigare adeguatamente[16].

Quanto al principio di proporzionalità, occorre che lo stesso è già incorporato nell'ambito della documentazione dell'UE sull'IA ed è, in effetti, esplicitamente menzionato nel *Considerando 14* del Regolamento IA e nell'art. 4 del Regolamento DORA, i quali stabiliscono proprio l'applicazione proporzionata ed efficace di ciascun regime normativo. Nel contesto del Regolamento IA, detto principio si traduce in un trattamento normativo differenziato in base ai livelli di rischio, garantendo che le applicazioni di IA ad alto rischio siano strettamente regolamentate, mentre i sistemi di IA a basso rischio rimangono in gran parte non regolamentati o regolamentati in maniera meno invasiva. Una caratteristica signifi-

10 Commissione europea, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions fostering a European approach to Artificial Intelligence* COM (2021) 205 final.

11 Commissione europea, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Fostering a European approach to Artificial Intelligence COM (2021) 205 definitivo.

12 Commissione europea, *White Paper on Artificial Intelligence: a European approach to excellence and trust* COM (2020) 65 final.

13 Greenberg BA, "*Rethinking Technology Neutrality*" (2016) 207 *Minnesota Law Review* 1495-1562.

14 Cfr. artt. 17 e 48 della MiFID II.

15 Per quanto riguarda il trattamento giuridico multiforme dell'IA nell'ambito del regime MAR, si veda Annunziata F, *Artificial Intelligence and Market Abuse Legislation: A European Perspective* (Edward Elgar Publishing 2023).

16 Commissione europea, *White Paper on Artificial Intelligence: a European approach to excellence and trust*, cit.

vedi l'articolo online

cativa di questo approccio è l'adozione volontaria di misure di autoregolamentazione, come i codici di condotta proposti ai sensi dell'art. 69 del Regolamento IA, che incoraggiano i fornitori di IA che operano al di fuori della categoria ad alto rischio a aderire volontariamente alle *best practice* di settore. Per il Regolamento DORA, la proporzionalità implica che l'attuazione delle norme dovrebbe tenere conto delle dimensioni e del profilo di rischio delle entità, nonché della natura, della portata e della complessità dei loro servizi, attività e operazioni.

3. L'applicazione del Regolamento sull'IA nel settore finanziario

Al fine di determinare in che misura il Regolamento IA possa effettivamente prevenire o mitigare i rischi creati dai sistemi di IA, si rende necessario analizzare proprio la definizione di "alto rischio" contenuta nel Regolamento IA stesso. Ai sensi degli artt. 6 e 7 del Regolamento IA, infatti, la classificazione di un particolare sistema di IA come "ad alto rischio" dipende principalmente dal suo uso previsto e dal suo potenziale di rischio per la salute e la sicurezza, nonché dal suo potenziale impatto negativo sui diritti fondamentali delle persone,

In effetti, l'attenzione alla protezione delle persone è chiaramente indicata nel Considerando 7 del Regolamento IA[17] e permea la maggior parte delle sue disposizioni.

Oltre ai sistemi di IA ad alto rischio che rientrano nelle condizioni di cui sopra, l'art. 6, par. 2, stabilisce che i sistemi di cui all'Allegato III sono considerati ad alto rischio. Al momento, gli unici sistemi elencati in tale allegato relativi ai servizi finanziari sono quelli (i) destinati a essere utilizzati per valutare il merito creditizio delle persone fisiche o stabilire il loro punteggio di credito, ad eccezione dei sistemi di IA utilizzati allo scopo di rilevare frodi finanziarie; e (ii) destinati a essere utilizzati per la valutazione del rischio e la determinazione del prezzo in relazione alle persone fisiche nel caso di assicurazioni sulla vita e sulla salute. I sistemi di IA ad alto rischio, che includono quelli utilizzati nel *credit scoring* e nei processi occupazionali[18], sono soggetti a obblighi estesi, tra cui valutazioni del rischio, requisiti di trasparenza e supervisione umana.

Tuttavia, l'art. 7, par. 2, lett. d) del Regolamento sull'IA suggerisce che le valutazioni del rischio che consentono di aggiornare l'elenco dei sistemi "ad alto rischio" già identificati dalla Commissione europea nell'Allegato III dovrebbero tenere conto della potenziale entità del danno o dell'impatto negativo per gli individui in termini di intensità e capacità di colpire più persone. La misura in cui ciò potrebbe cogliere altri rischi finanziari in futuro è discutibile.

Nel quadro del Regolamento IA, i sistemi di IA classificati come ad alto rischio devono soddisfare specifici requisiti legali per assicurare la loro conformità. Questi requisiti includono, *inter alia*: (i) l'implementazione di misure adeguate alla gestione e la mitigazione dei rischi associati all'uso dei sistemi di IA, con particolare attenzione alle conseguenze per la sicurezza e i diritti fondamentali degli individui; (ii) l'adozione di politiche rigorose per la gestione dei dati che garantiscano l'integrità, la protezione e la legalità del loro utilizzo, conformemente alle normative sulla protezione dei dati; (iii) il mantenimento di documentazione completa che dettagli i processi operativi del sistema di IA, le metodologie impiegate e le misure di sicurezza adottate, accessibile per *audit* e ispezioni; (iv) documentazione accurata di tutte le operazioni del sistema di IA, inclusi i dati di *input* e di *output* e le decisioni prese, per garantire tracciabilità e responsabilità; (v) la garanzia di trasparenza nelle operazioni dei sistemi di IA, fornendo informazioni chiare su come funzionano i sistemi e come vengono prese le decisioni; (vi) l'assicurazione di un adeguato controllo umano sui sistemi, permettendo interventi umani nei processi decisionali dell'IA per prevenire o correggere azioni potenzialmente dannose; e (vii) l'assicurazione che i sistemi di IA operino con elevati livelli di accuratezza e robustezza, e implementazione di robuste misure di *cybersecurity* per proteggere i sistemi da attacchi informatici e violazioni dei dati.

17 Il considerando dispone che al fine di garantire un livello coerente ed elevato di protezione degli interessi pubblici in materia di salute, sicurezza e diritti fondamentali, è opportuno stabilire norme comuni per i sistemi di IA ad alto rischio. Tali norme dovrebbero essere coerenti con la Carta, non discriminatorie e in linea con gli impegni commerciali internazionali dell'Unione. Dovrebbero inoltre tenere conto della Dichiarazione europea sui diritti digitali e dei Principi per il decennio digitale e degli orientamenti etici per un'IA affidabile del Gruppo di esperti ad alto livello sull'IA (AI HLEG).

18 Si veda il considerando 57 del Regolamento sull'IA: "*Anche i sistemi di IA utilizzati nel settore dell'occupazione, nella gestione dei lavoratori e nell'accesso al lavoro autonomo, in particolare per l'assunzione e la selezione delle persone, per l'adozione di decisioni riguardanti le condizioni del rapporto di lavoro la promozione e la cessazione dei rapporti contrattuali di lavoro, per l'assegnazione dei compiti sulla base dei comportamenti individuali, dei tratti o delle caratteristiche personali e per il monitoraggio o la valutazione delle persone nei rapporti contrattuali legati al lavoro, dovrebbero essere classificati come sistemi ad alto rischio, in quanto tali sistemi possono avere un impatto significativo sul futuro di tali persone in termini di prospettive di carriera e sostentamento e di diritti dei lavoratori (…)*".

3.1 L'IA e il credit scoring

Il *credit scoring*, utilizzato da banche e degli intermediari finanziari per valutare l'affidabilità creditizia di individui o imprese, si avvale sempre più dell'IA per elaborare grandi quantità di dati in modo rapido e preciso. Questi sistemi di IA integrano una varietà di informazioni, dalla storia creditizia e reddito alle informazioni professionali e, in alcuni casi, ai dati provenienti dai *social media*, per decidere su prestiti, tassi di interesse e limiti di credito.

L'adozione dell'IA nel *credit scoring*, tuttavia, solleva problematiche significative[19]. I modelli di IA possono, anche involontariamente, perpetuare o amplificare pregiudizi esistenti legati a fattori come razza, genere o condizione socioeconomica, riflettendo *bias* storici o disuguaglianze presenti nei dati di partenza. Questo può tradursi in esiti di prestito ingiusti per determinati gruppi, minando il principio di equità nel credito.

Inoltre, la natura spesso opaca di questi sistemi di IA crea difficoltà di comprensione per i consumatori sul come vengono prese le decisioni che li riguardano. La mancanza di trasparenza, descritta frequentemente attraverso la metafora della "scatola nera", solleva questioni di *accountability* e giustizia, essendo complicato per gli utenti contestare o comprendere le decisioni creditizie basate su algoritmi che non sono spiegati chiaramente[20].

19 V., *ex multis*, Nydia Remolina, "*The Role of Financial Regulators in the Governance of Algorithmic Credit Scoring*", SMU Centre for AI and Data Governance Working Paper 2/2022; Emilia Bonaccorsi di Patti, Filippo Calabresi, Biagio De Varti, et al., "*IA nel credit scoring. Analisi di alcune esperienze nel sistema finanziario italiano*", Banca d'Italia, Questioni di Economia e Finanza (Occasional Papers), no. 721, Ottobre 2022; Katja Langenbucher, "*Consumer Credit in the Age of AI - Beyond Anti-discrimination Law*", LawFin Working Paper No. 42, Goethe University Frankfurt, February 2023.

20 Si veda, il provvedimento del 27 febbraio 2025, causa C-203/22, la Corte di Giustizia UE si è pronunciata sulla valutazione automatizzata del merito creditizio (credit scoring), con particolare riferimento al diritto dell'interessato ad una spiegazione sulla logica sottesa alla decisione circa la concessione o meno del credito, che gli consenta di comprendere e contestare la decisione automatizzata. Secondo la Corte, in sintesi, il titolare del trattamento deve descrivere la procedura e i principi concretamente applicati nella valutazione circa il merito creditizio del cliente, in modo tale che l'interessato possa comprendere quali dei suoi dati personali sono stati utilizzati, e in che modo, nel processo decisionale automatizzato (come quello di credit scoring): ad esempio, informando l'interessato se, e come, una variazione dei dati personali presi in considerazione avrebbe condotto a un risultato diverso; la semplice comunicazione di un algoritmo non sarebbe, invece, una spiegazione sufficientemente concisa e comprensibile.

Un'altra sfida importante è la protezione dei dati personali. L'uso intensivo di dati personali negli algoritmi di *credit scoring* guidati dall'IA incrementa il rischio di violazioni della *privacy*. È importante, dunque, che tali dati siano protetti in modo efficace per prevenire accessi non autorizzati o abusi, in conformità con le normative vigenti sulla protezione dei dati.

dal punto di vista normativo, il *credit scoring* è regolamentato in modo specifico attraverso l'art. 8 della Direttiva 2008/48/CE del Parlamento europeo e del Consiglio del 23 aprile 2008 relativa ai contratti di credito ai consumatori e che abroga la direttiva 87/102/CEE (CCD I) e l'art. 18 della Direttiva (UE) 2023/2225 del Parlamento europeo e del Consiglio, del 18 ottobre 2023, relativa ai contratti di credito ai consumatori e che abroga la direttiva 2008/48/CE (CCD II). Dette disposizioni obbligano i creditori a valutare adeguatamente la solvibilità dei consumatori. Inoltre, una sentenza della Corte di Giustizia dell'UE (CGUE) nel caso C-755/22 del 2024 stabilisce che le sanzioni per la mancata valutazione della solvibilità possono essere applicate anche ai crediti interamente rimborsati, e che tali sanzioni devono essere proporzionate, potendo anche annullare gli accordi di credito.

Il Regolamento IA proibisce i sistemi di *social scoring* che comportano trattamenti dannosi in contesti non correlati alla raccolta dei dati o sproporzionati rispetto al comportamento sociale. Come accennato, i sistemi di *credit scoring* che non rientrano in queste proibizioni sono considerati ad alto rischio e quindi soggetti a rigidi requisiti di conformità, gestione del rischio, e trasparenza.

Significativamente, la sentenza della CGUE sul caso C-634/21 del 2023, la c.d. causa "Schufa", ha chiarito che la creazione di un valore di probabilità creditizia attraverso l'IA costituisce una "*decisione automatizzata individuale*" ai sensi dell'art. 22, par. 1, del GDPR[21] e rientra nella definizione di "profilazione" secondo l'art. 4, par. 4, del GDPR. Questo implica che tali processi di decisione automatizzata devono essere gestiti con particolare attenzione per garantire che non violino i diritti dei titolari dei dati.

21 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GU L 119 del 4.5.2016, pag. 1).

vedi l'articolo online

3.2 La Valutazione d'Impatto sui Diritti Fondamentali (FRIA)

Nell'ambito del Regolamento IA, i soggetti che implementano sistemi di IA ad alto rischio come specificato nei punti 5 (b) e (c) dell'Allegato III devono ottemperare agli obblighi delle Valutazioni di Impatto sui Diritti Fondamentali (*Fondamental Rights Imppact Assessment - FRIA*). In questo senso, le banche, nell'ambito della valutazione del merito creditizio, e le compagnie assicurative, sono tenute a soddisfare tali requisiti. L'esecuzione di FRIA approfondite richiede tempo e risorse significative, rappresentando un onere notevole per società di minori dimensioni o per le startup. Inoltre, la necessità di competenze specifiche in materia di diritti umani e protezione dei dati potrebbe richiedere il ricorso a consulenti esterni, incrementando così i costi.

Inoltre, le società potrebbero incontrare difficoltà nel determinare cosa costituisca un impatto c.d. "significativo" sui diritti fondamentali, complicando il processo di valutazione. A ciò si aggiunge la problematica delle discrepanze interpretative tra gli stati membri dell'UE riguardo i diritti fondamentali, che possono portare a un'applicazione disomogenea delle FRIA, rendendo complessa la conformità per le società multinazionali. Queste sfide sottolineano la complessità dell'integrazione delle normative sulla protezione dei dati e dei diritti umani nel contesto delle tecnologie di IA, richiedendo un approccio attentamente calibrato per garantire sia l'innovazione che la tutela dei diritti fondamentali.

Da un punto di vista operativo, le banche sono tenute a garantire che l'applicazione della FRIA segua un processo ben definito per rispettare i requisiti stabiliti dalle leggi applicabili. Il primo passo consiste nell'identificare tutte le parti interessate, inclusi i consumatori e le comunità che potrebbero essere influenzate dall'uso dei sistemi di IA nel *credit scoring*. Ciò permette di comprendere chiaramente i destinatari dell'impatto delle decisioni automatizzate e facilita una valutazione più mirata degli effetti dell'IA. Successivamente, si analizza in che modo l'IA potrebbe infrangere diritti fondamentali come la privacy, l'uguaglianza e il trattamento equo. Questo include l'esame delle modalità con cui i sistemi di IA potrebbero portare a discriminazioni o trattamenti ingiusti verso gruppi specifici. Si procede con la valutazione dei *set* di dati utilizzati negli algoritmi di *credit scoring* per assicurare che siano equi e accurati. Questo passaggio è cruciale per identificare e correggere eventuali pregiudizi incorporati nei dati o nelle modalità di elaborazione degli stessi. Vengono poi sviluppate misure proattive per affrontare i rischi identificati. Ciò può includere l'implementazione di *audit* regolari degli algoritmi per identificare e eliminare i *bias*, assicurando che le decisioni di *credit scoring* siano giuste e non discriminatorie.

È fondamentale coinvolgere attivamente gli *stakeholder* nel processo di valutazione, affrontando le loro preoccupazioni e raccogliendo prospettive diverse. Questo passaggio migliora la trasparenza e la fiducia nel processo di *credit scoring*, rendendo le decisioni più accettabili e giustificate agli occhi di tutti gli interessati. Infine, è essenziale mantenere una documentazione dettagliata di tutto il processo di FRIA, compresi i risultati e le azioni intraprese per mitigare i rischi. Questo non solo garantisce la conformità normativa ma anche facilita la revisione e l'*audit* del processo da parte delle autorità regolatorie o di altri revisori esterni.

Questi passaggi garantiscono che il *credit scoring* basato su IA sia condotto in modo responsabile, con un'attenzione costante alla protezione dei diritti fondamentali e alla prevenzione di eventuali abusi o discriminazioni, ai sensi del Regolamento IA

3.3 L'IA e il Regolamento DORA

Il Regolamento DORA rappresenta un passo significativo negli sforzi dell'UE per rafforzare il settore finanziario contro i rischi delle tecnologie dell'informazione e della comunicazione (ICT o TIC) e le minacce informatiche. Detto regolamento introduce un quadro normativo armonizzato che mira a migliorare la resilienza operativa digitale tra gli istituti finanziari e i loro fornitori di servizi ICT. La normativa nasce in risposta alla crescente dipendenza delle entità finanziarie dalle infrastrutture digitali, una tendenza che ha intensificato le vulnerabilità sistemiche e aumentato i rischi per la sicurezza informatica[22].

Il Regolamento DORA stabilisce un approccio intersettoriale, applicando *standard* uniformi di gestione del rischio ICT a tutte le entità finanziarie, comprese banche, compagnie di assicurazione, fornitori di servizi di cripto-asset e fornitori di servizi ICT di terze parti (ICT TPP), che includono, sebbene non esplicitamente menzionati, fornitori di servizi di *cloud computing*, *software*, servizi di analisi dei dati, *data center*, nonché fornitori di servizi di IA. Il regime impone agli intermediari finanziari di adottare

22 Cfr. CP Buttigieg e BB Zimmermann, "*The Digital Operational Resilience Act: Challenges and Some Reflections on the Adequacy of Europe's Architecture for Financial Supervision*" (2024) *ERA Forum* (di prossima pubblicazione). V. anche J Woxholth e DA Zetzsche, "DORA on DeFi" (2024).

quadri di sicurezza avanzati, condurre regolari *test* di resilienza e implementare meccanismi di segnalazione degli incidenti per mitigare efficacemente i rischi. Inoltre, introduce un quadro di supervisione centralizzato, che consente alle autorità europee di vigilanza (AEV) di monitorare la conformità a livello dell'Unione.

In termini di oggetto, il nucleo del regime è costituito dai cosiddetti servizi ICT che, ai sensi dell'art. 3, par. 21, i quali comprendono i "*servizi digitali e di dati forniti attraverso sistemi di TIC a uno o più utenti interni o esterni su base continuativa, inclusi l'hardware come servizio e i servizi hardware, comprendenti la fornitura di assistenza tecnica mediante aggiornamenti di software e firmware da parte del fornitore dell'hardware, esclusi i servizi telefonici analogici tradizionali*". Sebbene non si faccia esplicito riferimento ai sistemi di IA, il Regolamento DORA copre indirettamente gli aspetti dell'IA nel quadro più ampio della gestione dei rischi ICT nel settore finanziario. A questo proposito, ai sensi dell'art. 3, paragrafo 5, un "rischio informatico" corrisponde a qualunque circostanza ragionevolmente identificabile in relazione all'uso dei sistemi informatici e di rete che, qualora si concretizzi, può compromettere la sicurezza dei sistemi informatici e di rete, di eventuali strumenti o processi dipendenti dalle tecnologie, di operazioni e processi, oppure della fornitura dei servizi causando effetti avversi nell'ambiente digitale o fisico. Altri rischi coperti dal regolamento includono quelli relativi a incidenti ICT[23], minacce informatiche[24], attacchi informatici[25], vulnerabilità[26], rischi ICT di terze parti[27] e rischi di concentrazione ICT[28], tutti direttamente correlati ai rischi legati all'A che possono potenzialmente innescare eventi sistemici.

3.4 La navigazione attraverso le diverse applicazioni dell'IA nel settore finanziario

Oltre a quanto sopra, altre applicazioni dell'IA nel settore finanziario sono soggette a un livello inferiore di controllo normativo o non sono affatto regolamentate da norme specifiche per questa tecnologia. Un esempio sono le *chatbot* per il servizio clienti basati sull'IA, classificati come sistemi di IA a rischio limitato, che devono rispettare obblighi notevolmente meno stringenti. Gli intermediari finanziari che utilizzano le funzioni delle chatbot devono rispettare gli standard di trasparenza e garantire che gli utenti siano consapevoli di interagire con un sistema di IA, consentendo loro di prendere decisioni informate in merito alla possibilità di continuare a interagire con il sistema di IA o di ritirarsi.

Altri usi dell'IA nel settore finanziario includono l'IA nelle piattaforme di trading per l'ottimizzazione del capitale, la semplificazione dei processi KYC/CDD, l'IA per scopi antiriciclaggio (e.g., per il monitoraggio e segnalazione di transazioni sospette), robo-advisor per fornire servizi di investimento e IA per la gestione di portafogli/fondi. In questo senso, diverse discipline verticali (relative a settori specifici) e orizzontali (intersettoriali) si applicano separatamente o congiuntamente, a seconda dei casi: la CRD/CRR, il nuovo regime AML/CFT, la MiFID, le discipline relative agli organismi di investimento collettivo del risparmio, il Regolamento MAR, la direttiva sul credito al consumo, il Regolamento IA, il Regolamento DORA e persino il regolamento MiCA, nonché i rispettivi testi legislativi e regolamentari a livello nazionale, dovrebbero essere attentamente presi in considerazione dagli intermediari che adottano sistemi di IA.

Per affrontare efficacemente l'evoluzione del panorama normativo, gli intermediari finanziari devono adottare un approccio strutturato e metodico. In primo luogo, è essenziale condurre valutazioni del rischio approfondite per identificare e mitigare i potenziali rischi associati all'uso dei sistemi di IA, soprattutto in ambiti ad alto rischio come il *credit scoring* e la gestione delle risorse umane. Questo processo aiuterà a prevenire problematiche legate ai diritti fondamentali e alla sicurezza finanziaria. In secondo luogo, gli intermediari finanziari dovrebbero sviluppare robusti *framework* interni di governance dell'IA. È fondamentale stabilire linee guida chiare e politiche dettagliate per lo sviluppo, l'implementazione e il monitoraggio dei sistemi di IA, al fine di garantire una piena conformità al Regolamento sull'IA. La creazione di un *framework* solido e ben definito è cruciale per la gestione efficace delle tecnologie avanzate e per il rispetto dei rigorosi standard normativi.

In terzo luogo, investire nella formazione dei dipendenti è vitale. I lavoratori devono essere pienamente consapevoli delle implicazioni legali ed etiche delle tecnologie di IA. Promuovere un'educazione continua e approfondita sui requisiti del Regolamento IA può aumentare la consapevolezza e la preparazione del personale, elementi chiave per navigare con successo nell'ecosistema digitale in continua

23 Regolamento DORA, art. 3, para. 8 e 10
24 Regolamento DORA, art. 3, para. 12 e 13
25 Regolamento DORA, art. 3, par. 14.
26 Regolamento DORA art. 3, par. 16.
27 Regolamento DORA, art. 3, par. 18.
28 Regolamento DORA, art. 3, par. 29.

vedi l'articolo online

evoluzione. Quarto, è imperativo promuovere la trasparenza e l'*accountability*. Assicurarsi che i sistemi di IA siano trasparenti e spiegabili, specialmente quando utilizzati in applicazioni ad alto rischio, è fondamentale per mantenere la fiducia del pubblico e garantire la correttezza dei processi decisionali automatizzati.

Infine, la collaborazione con i regolatori è essenziale. Lavorare a stretto contatto con le autorità di regolamentazione può aiutare a risolvere le incertezze e assicurare un'applicazione coerente del Regolamento IA in tutti gli Stati membri dell'UE. Questo tipo di collaborazione può facilitare una migliore comprensione delle aspettative normative e contribuire a sviluppare pratiche di IA che siano sia innovative che conformi.

Adottando queste strategie, gli intermediari finanziari saranno in grado di bilanciare la necessità di conformità normativa con l'imperativo di innovare e rimanere competitivi nel dinamico panorama della finanza digitale.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it