Intelligenza artificiale e resilienza operativa nel settore finanziario*

di Michele Siri

1. *L'identificazione dei rischi derivanti dall'intelligenza artificiale nel settore finanziario*

Lo sviluppo dell'intelligenza artificiale e l'atteso incremento di produttività anche nel settore finanziario si riflette, in parallelo, nei rischi generati dal suo impiego come pure in quelli già idiosincratici del mercato finanziario e che con essa potrebbero risultare accresciuti. La letteratura identifica quattro criteri inter-dipendenti per valutare gli algoritmi e gli strumenti di intelligenza artificiale nel settore finanziario[1]: la gestione dei dati, la valutazione della performance, la stabilità e la comprensibilità[2]. Il *data management* è fondamentale per ogni algoritmo, poiché sia le prestazioni che la conformità normativa sono condizionate dalla sua stessa gestione, cioè dai dati con cui esso viene "istruito" e dai dati sulla base dei quali esso lavora. L'intelligenza artificiale è, infatti, *data dependent* ed i risultati resi dipendono soprattutto dalle fonti, dalla loro selezione e acquisizione. È in queste fasi che dovranno essere prese in considerazione le questioni etiche, come l'equità dell'elaborazione e l'assenza di pregiudizi discriminatori[3].

---

* Il presente scritto è stato elaborato nel contesto di una ricerca Astrid su Intelligenza artificiale e diritto, ed è stato pubblicato in ASTRID, "Intelligenza artificiale e diritto: una rivoluzione? Amministrazione, responsabilità, giurisdizione", a cura di Filippo Donati, Alessandro Pajno, Antonio Perrucci, vol. III, Ed. il Mulino, Bologna, 2022

[1] D.A. Zetzsche, A.W. Douglas, R.P. Buckley e B. Tang, *Artificial Intelligence in Finance: Putting the Human in the Loop*, in CFTE Academic Paper Series: Centre for Finance, Technology and Entrepreneurship", n. 1., University of Hong Kong Faculty of Law Research Paper No. 2020/006, 2020, disponibile all'indirizzo web *www.ssrn.com*.

[2] Nell'analizzare i rischi collegati all'intelligenza artificiale e i metodi per una loro riduzione, si utilizza una classificazione in chiave di prospettive di incidenza: etica e politica, legale e sociale e, infine, sfide tecniche. Sul punto si veda C. Castelluccia, D. Le Mètayer, *Study on 'Understanding algorithmic decision making: Opportunities and challenges'*, Directorate-General for Parliamentary Research Services (DG EPRS) of the European Parliament, 2019, disponibile all'indirizzo web *www.europarl.europa.eu*.

[3] Si veda ancora C. Castelluccia, D. Le Mètayer, *Study on 'Understanding algorithmic decision making: Opportunities and challenges'*, cit, ove si rileva che i sistemi di intelligenza artificiale aggravano (amplificano) le questioni etiche e ne introducono di nuove a cui spesso è difficile dare una

La valutazione delle prestazioni di un algoritmo di *machine learning* può essere effettuata utilizzando una varietà di metriche per testarne l'accuratezza, secondo parametri che tengano conto sia dell'aspetto tecnico che di quello funzionale. In relazione alla stabilità, essa descrive quanto robusto e resiliente si riveli il comportamento di un algoritmo nel corso del suo ciclo di vita. Infine, la comprensibilità – che può essere considerata come una derivata della trasparenza algoritmica e dell'interpretabilità - deve essere contestualizzata per definire il suo scopo effettivo. La comprensibilità di un risultato specifico o del comportamento dell'algoritmo può rivelarsi necessaria in una duplice prospettiva: per gli utenti finali (siano essi clienti esterni o interni), al fine di una motivazione del risultato, o, in altri casi, servirà a coloro che sono incaricati della valutazione di conformità o della *governance* dell'algoritmo. La comprensibilità ha quindi lo scopo di informare il cliente, garantire la coerenza dei flussi di lavoro in cui gli esseri umani prendono decisioni, e facilitare la convalida e il monitoraggio dei modelli di *machine learning*. Perciò, la comprensibilità si declina nella duplice prospettiva di tutela del cliente finale sia di monitoraggio e controllo da parte del sistema di *governance* dell'intermediario.

Su un piano più generale, il rischio tecnologico, che include anche gli aspetti legati alla sicurezza dei sistemi e di tutela dei dati, dovrebbe essere considerato come una forma separata di rischio, in aggiunta al rischio operativo come più tradizionalmente inteso. Infatti, per quanto attiene le istituzioni finanziarie occorre evidenziare come il "rischio intelligenza artificiale" potrebbe sorgere da una singola istituzione, così come dalle interconnessioni tra diverse realtà, con un impatto diretto sulla fiducia e sulla stabilità del settore finanziario. Il rischio tecnologico, nel settore finanziario, diventa fonte, così, di rischio sistemico[4], perché l'inter-settorialità, nonché l'ampia diffusione dei sistemi di intelligenza artificiale, potrebbero generare ricadute di portata esponenziale. La potenziale vulnerabilità che l'intelligenza artificiale imprime nel sistema finanziario è stata presa in considerazione anche dal Comitato Europeo per il

risposta chiara, certa e univoca. Rinvenire una linea di demarcazione netta tra ciò che è corretto e ciò che non lo è, segnare il confine di accettazione di una determinata pratica non è una questione di immediata soluzione. Una risposta, tuttavia, è necessaria e ineludibile soprattutto in una prospettiva di una sempre maggiore implementazione dei sistemi di intelligenza artificiale.

[4] R.P. Buckley, D.W. Arner, D.A. Zetzsche e E. Selga, *The Dark Side of Digital Financial Transformation: The New Risks of FinTech and the Rise of TechRisk*, in "UNSW Law Research Paper No. 19-89, European Banking Institute Working Paper 2019/54, University of Luxembourg Law Working Paper 2019-009", University of Hong Kong Faculty of Law Research Paper No. 2019/112, disponibile all'indirizzo web *www.ssrn.com*.

rischio sistemico [5] ed è richiamata nel considerando 3 della proposta di regolamento DORA.

2. *I rischi specifici indotti dall'intervento di terze parti*

Le istituzioni finanziarie si affidano a diversi tipi di fornitori per lo sviluppo, la gestione ed il monitoraggio necessari ai sistemi di intelligenza artificiale. Ai rischi connaturati all'impiego dell'intelligenza artificiale, si aggiungono pertanto quelli dovuti alla sua erogazione da parte di terzi[6], in particolare per l'*hosting* di servizi e applicazioni su un *cloud* pubblico[7]. I rischi generati dall'esternalizzazione delle competenze della progettazione e dell'implementazione del software sono particolarmente acuti nell'intelligenza artificiale. Si tratta di rischi difficili da mitigare in fase di operatività *se non sono stati sufficientemente previsti*. Quindi, una buona pratica prima di ogni decisione di *outsourcing* è quella di eseguire un'analisi dei rischi *ex-ante* ai fini di valutare l'oggetto dell'accordo, i rischi ad esso pertinenti e le conseguenze che questi potrebbero comportare. Come riportato dalle linee guida sull'*outsourcing* pubblicate dalle autorità di supervisione europee [8], la reversibilità delle soluzioni esternalizzate costituisce oggi una significativa fonte di vulnerabilità non specifica dell'intelligenza artificiale all'interno degli istituti finanziari.

La costante evoluzione dei sistemi tecnologici e la richiesta di competenze sempre più specifiche in relazione alle loro implementazione e gestione, nonché la complessità, potrebbe pregiudicare la risoluzione dell'accordo e la possibilità di uscita senza

[5] ESRB, *Report- Systemic cyber risk*, February 2020, disponibile all'indirizzo web *www.esrb.europa.eu.*

[6] Commissione Europea, *Request to Eba, Eiopa and Esma for technical advice on digital finance and related issues*, https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/210202-call-advice-esas-digital-finance_en.pdf. Si veda anche International Organization of Securities Commissions (IOSCO), *The use of artificial intelligence and machine learning by market intermediaries and asset managers (Final Report)*, 2021, 12, disponibile all'indirizzo web *www.iosco.org*.

[7] Per fronteggiare questa tendenza, una prima serie di linee guida sull'*outsourcing* è stata pubblicata dalle autorità di controllo europee in ambito bancario (EBA, 2019) e assicurativo (EIOPA, 2020). Tali linee guida riguardano pressoché lo stesso ambito in entrambi i settori ed in particolare: la valutazione della criticità dei processi aziendali (e analisi dell'impatto); i requisiti di documentazione; l'obbligo di informare l'autorità di vigilanza; i diritti di accesso e la revisione da parte dell'istituto finanziario ma anche dell'autorità di vigilanza; la sicurezza informatica; i rischi associati alla gestione dei dati; la sub-fornitura; i piani di emergenza (compresi i piani di continuità operativa); la strategia di uscita dall'accordo di *outsourcing.*

[8] EBA, *Orientamenti in materia di esternalizzazione*, EBA/GL/2019/02, 25 febbraio 2019; EIOPA, *Orientamenti in materia di esternalizzazione a fornitori di servizi cloud*, EIOPA-BoS-20-002, 2020.

conseguenze gravemente pregiudizievoli. Soprattutto, l'esternalizzazione dello sviluppo di intelligenza artificiale induce un cambiamento strutturale nel modello d'impresa e nel sistema di controllo interno (in particolare per il rischio di sviluppo intelligenza artificiale in *outsourcing*), fra i quali, ad esempio, la perdita della capacità di creare e conservare adeguate risorse interne (umane e tecnologiche), per validare il codice elaborato all'esterno dell'organizzazione ed assicurarsi che il *software* soddisfi i criteri delle procedure di controllo interno. In termini di gestione aziendale, ciò non solo influisce in modo rilevante nella selezione del personale e sugli investimenti nel settore tecnologico, ma introduce anche rilevanti rischi di concentrazione sui relativi fornitori[9].

3. *L'approccio funzionale alla resilienza digitale*

La proposta di Regolamento[10] sulla resilienza operativa digitale[11] ("DORA") mira a garantire che tutti i partecipanti all'ecosistema finanziario dispongano delle necessarie salvaguardie per prevenire gli attacchi informatici e mitigare altri rischi informatici, affrontando quindi l'ultimo degli obiettivi della strategia per la finanza digitale[12], nonché le due aree di intervento individuate dal parere congiunto delle autorità di supervisione europee[13]. Per quanto riguarda il suo campo di applicazione, in un'ottica di armonizzazione orizzontale, DORA copre un'ampia gamma di entità finanziarie regolamentate a livello dell'Unione, quali gli enti creditizi e di pagamento, gli istituti di moneta elettronica, le imprese di investimento, i fornitori di servizi di cripto-valute, le infrastrutture dei mercati finanziari, i repertori di dati sulle negoziazioni, i gestori di

[9] D. Gozman, T. Machaiah, L. Willcocks, *Cloud sourcing and mitigating concentration risk in financial services*, in *Information systems outsourcing the era of digital transformation*, a cura di R. Hirschheim, A. Heinzl, J. Dibbern, Springer, 2020, 336.

[10] Commissione Europea, Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014 COM(2020) 595 final, 2020/0266 (COD).

[11] Come indicato dall'art. 3 della Proposta, per "resilienza operativa digitale" si intende "la capacità dell'entità finanziaria di creare, assicurare e riesaminare la propria integrità operativa da un punto di vista tecnologico, garantendo, direttamente o indirettamente, tramite il ricorso ai servizi offerti da fornitori terzi di TIC, l'intera gamma delle capacità connesse alle TIC necessarie per garantire la sicurezza delle reti e dei sistemi informativi impiegati dall'entità finanziaria, su cui si fondano la costante offerta dei servizi finanziari e la loro qualità".

[12] Commissione Europea, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni relativa a una strategia in materia di finanza digitale per l'UE*, Bruxelles, 24.9.2020, COM(2020) 591 final.

[13] ESAs, *Joint Advice on Information and Communication Technology risk management and cybersecurity*, https://esas-joint-committee.europa.eu/Pages/News/ESAs-publish-Joint-Advice-on-Information-and-Communication-Technology-risk-management-and-cybersecurity.aspx.

fondi di investimento alternativi e le società di gestione, i fornitori di servizi di comunicazione dei dati, le imprese di assicurazione e riassicurazione, gli intermediari assicurativi, gli intermediari riassicurativi e gli intermediari assicurativi ausiliari, gli enti pensionistici aziendali o professionali, le agenzie di *rating* del credito, i revisori legali e le società di revisione, gli amministratori di parametri critici e i fornitori di servizi di *crowdfunding*. Coerentemente con la struttura generale della *Digital Finance Strategy*, DORA, insieme alla proposta MICAR, rappresenta il primo atto legislativo per includere i fornitori di servizi di *cripto-asset* tra le istituzioni finanziarie regolamentate [14].

La proposta mira, inoltre, ad affrontare alcune carenze specifiche del settore finanziario identificate dalla valutazione d'impatto della Commissione, nonché dai processi di consultazione pubblica. In particolare, delinea un processo di armonizzazione, volto a eliminare le differenze attualmente esistenti tra i requisiti di sicurezza ICT nei diversi settori della legislazione finanziaria dell'UE. Infatti, alcuni attori del settore finanziario sono soggetti a requisiti specifici per quanto riguarda il rischio ICT (come nel caso di PSD2, CSDR, EMIR), mentre per altri partecipanti al mercato finanziario sono indicati solo alcuni requisiti generali (CRD, CRR, Solvibilità II, UCITS e AIFMD). Inoltre, estende la supervisione sulle attività dei fornitori terzi di ICT ("TPP") ai partecipanti al mercato finanziario europeo.

L'introduzione di un efficiente quadro di supervisione assume un ruolo fondamentale all'interno della proposta, in quanto i TPP, che possono incorrere in problemi operativi o limitazioni contrattuali, entrambi in grado di compromettere temporaneamente l'efficacia delle istituzioni finanziarie che beneficiano dei loro servizi, sono attualmente soggetti a un monitoraggio variabile, incoerente a livello UE, con un rischio materiale per una mancata identificazione tempestiva di tali fallimenti. Inoltre, gli istituti finanziari hanno avuto difficoltà a raccogliere informazioni sui TPP a cui esternalizzano i servizi ICT, che, per quanto riguarda alcuni servizi ICT, sono limitati nel loro numero, con possibili rischi più gravi legati alla concentrazione del mercato e conseguenti rischi di contagio, in grado di minare il sistema finanziario dell'UE.

4. Le implicazioni sul governo societario dell'intermediario

[14] D.A. Zetzsche, F. Annunziata, D.W. Arner, R.P. Buckley, *The Markets in Crypto-Assets regulation (MiCA) and the EU digital finance strategy*, in *Capital Markets Law Journal*, 2021, 2, 203.

L'utilizzo dell'intelligenza artificiale nei processi aziendali ha inevitabilmente un impatto sulla *governance* degli intermediari finanziari[15], anche alla luce di quanto appena espresso e dettato dalla previsione normativa della proposta di Regolamento che porta a inserire il rischio ICT quale oggetto della gestione rischi all'interno della *governance* dell'impresa. Per quanto riguarda i requisiti di *governance*, la proposta richiede che gli enti finanziari si dotino di strutture di *governance* e controllo in grado di assicurare una gestione efficace e prudente dei rischi ICT. Sebbene con una formulazione in termini di principio generale, DORA attribuisce la supervisione dei rischi ICT all'organo di gestione dell'impresa, il quale, nonostante la delega interna a ruoli e funzioni ICT, rimane responsabile per eventuali errori o malfunzionamenti, alla luce degli obblighi di approvazione e supervisione di tali dispositivi di *governance*.

La scelta affida la *cybersecurity* e la resilienza alle strategie aziendali, piuttosto che considerarle come un mero obbligo di *compliance*. Pertanto, a partire dalla fase di progettazione dell'algoritmo, è necessario comprendere i rischi derivanti dall'integrazione nei processi di gestione aziendali.

La gestione dell'IA quale elemento della *governance* solleva anche quesiti circa il rapporto uomo – algoritmo nel risultato delle decisioni e nella validazione delle stesse in termini di responsabilità. Le interazioni uomo/algoritmo possono richiedere un particolare tipo di comprensibilità, destinata sia agli operatori interni che devono confermare o rifiutare l'*output* di un algoritmo, sia ai clienti che hanno il diritto di capire le decisioni che li riguardano o le offerte commerciali fatte loro. Inoltre, i processi che coinvolgono l'intelligenza artificiale – come peraltro richiesto dall'art. 14 della Proposta di Regolamento - lasciano spesso spazio all'intervento umano, che è benefico o addirittura necessario ai fini della mitigazione dei rischi, ma comporta comunque l'insorgerne di nuovi ad esempio correlati ad insufficienti competenze degli operatori.

Gli intermediari finanziari, a partire dagli organi di amministrazione e controllo, restano pienamente responsabili del rispetto di tutti i loro obblighi normativi, compresa la capacità di vigilare sull'esternalizzazione di funzioni essenziali o importanti e sull'utilizzo dell'intelligenza artificiale nella gestione dell'attività d'impresa[16]. È

[15] V. D.A. Zetzsche, D.W. Arner, R.P. Buckley e T. Brian, *Artificial Intelligence in Finance: Putting the Human in the Loop*, in "CFTE Academic Paper Series: Centre for Finance, Technology and Entrepreneurship", n. 1., University of Hong Kong Faculty of Law Research Paper No. 2020/006, 2020, disponibile all'indirizzo web *www.ssrn.com*.

[16] European Banking Authority, *Orientamenti in materia di esternalizzazione*, cit., par. 35. Si veda anche Parlamento europeo, *Risoluzione sulla tecnologia finanziaria: l'influenza della tecnologia sul futuro del settore finanziario*, 2016/2243(INI), 17 maggio 2017, punto 14, disponibile all'indirizzo web *www.europarl.europa.eu*. In letteratura si veda L. Enriques, W.G. Ringe, *Bank-Fintech partnerships, outsourcing arrangements and the case for a mentorship regime*, ECGI Law Working Paper No. 572/2020, 9, disponibile all'indirizzo web *www.ssrn.com*.; J.A. McCahery, A. De Roode,

plausibile ritenere che anche i requisiti richiesti agli amministratori debbano riflettere un adeguamento nelle competenze e professionalità, come già accade per le fintech bancarie[17], per comprendere e supervisionare le scelte strategiche che implicano processi di intelligenza artificiale [18] anche avvalendosi di comitati manageriali specializzati sui rischi tecnologici [19]. È una sfida nella sfida anche per i migliori sistemi di governo societario delle istituzioni finanziarie chiamate a ripensare i processi decisionali di fronte al "TechRisk" [20].

Governance of financial services outsourcing: managing misconduct and third-party risk, ECGI Law Working Paper No. 417/2018, 23, disponibile all'indirizzo web *www.ssrn.com*; A. Sacco Ginevri, *Esternalizzazione (*outsourcing*)*, in *Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, diretto da G. Finocchiaro, V. Falce, Zanichelli, 2019, 205; A. Chirico, *Outsourcing in the financial services industry*, in *European Business Law Review*, 2020, pp. 89 ss.

[17] European Central Bank (ECB), *Guida alla valutazione delle domande di autorizzazione all'esercizio dell'attività bancaria degli enti creditizi* fintech, 2018, par. 2, disponibile all'indirizzo web *www.bankingsupervision.europa.eu*., sui si veda A. Brozzetti, *La nuova tipologia di banca* FinTech *nelle "guide" della BCE in tema di rilascio dell'autorizzazione*, in *FINTECH. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, a cura di M.T. Paracampo, vol. 2, Giappichelli, 2019, p. 85.

[18] European Banking Authority, *Report on Big Data and Advanced Analytics*, 2020, 45, disponibile all'indirizzo web *www.eba.europa.eu,* ove si legge: "accountability for outsourced [technological] systems remains with the institution and cannot be delegated […]. Therefore, it can be a success factor if institutions that rely on technology providers and other third parties when using [Big Data and Advanced Analytics (BD&AA) include these risks in their risk management strategy. For example, lack of explainability can be a risk in the case of models developed by external third parties and then sold as opaque black box packages".

[19] M.L. Montagnani, M.L. Passador, *Artificial intelligence for post-Covid companies: an empirical analysis of Tech Committees in the EU and US*, Stanford-Vienna Transatlantic Technology Law Forum Working Papers No. 70/2020. Si veda anche B.A. Aubert, S. Rivard, *The outsourcing of IT governance*, in *Information systems outsourcing the era of digital transformation*, a cura di R. Hirschheim, A. Heinzl, J. Dibbern, Springer, 2020, p. 44.

[20] R.P. Buckley, D.W. Arner, D.A. Zetzsche, E. Selga, *The dark side of digital financial transformation: the new risks of FinTech and the rise of TechRisk*, EBI Working Paper No. 54/2019, 30.