

---

# Modelli di regolazione (e supervisione) per l'AI finanziaria: neutralità tecnologica, etica e tutela dell'investitore\*

Daniel Foà

## Abstract

Nell'ambito del settore finanziario, l'intelligenza artificiale può essere impiegata per varie finalità, molte delle quali caratterizzate da grandi potenzialità; al contempo, l'utilizzo di tali strumenti pone rilevanti sfide. Il contributo intende, in primo luogo, indagare se la regolazione e supervisione finanziaria - nel fronteggiare le insidie poste dalle applicazioni dell'intelligenza artificiale - siano tenute a conformarsi al principio di neutralità tecnologica. In secondo luogo, alla luce del regolamento (UE) 2024/1689 (AI Act) e all'evoluzione dei servizi, viene valutato quale sia l'approccio ottimale per garantire una piena tutela dell'investitore nei confronti dei *roboadvisors*, anche nell'ambito di ambienti immersivi caratterizzati da interazioni *phygital*. È, infine, analizzato il caso d'uso dei *virtual worlds* per dimostrare l'esigenza di regolare e supervisionare le applicazioni dell'AI in ambito finanziario adottando un approccio *tech specific*.

Within the financial sector, artificial intelligence may be deployed for various purposes, many of which offer a great extent of capabilities yet posing significant challenges. Firstly, the contribution intends to investigate whether financial regulation (and supervision), when coping with the challenges posed by artificial intelligence applications, are bound to comply with the principle of technological neutrality. Secondly, in the light of the EU Regulation 2024/1689 (AI Act) and the developments in financial services, it is assessed which is the most appropriate approach to grant investor protection vis-à-vis roboadvisors, also in the context of immersive environments, characterised by phygital interactions. Thus, the use case of virtual worlds is analysed to show the urgency of regulating and supervising AI financial applications through a tech-specific approach.

## Sommario

1. Introduzione – 2. Una preliminare questione definitoria – 3. Neutralità tra tecnologia ed etica – 4. Regolazione neutrale – 5. (segue)...e modelli di supervisione – 6. *Roboadvi-*

\* L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

---

sors, etica e tutela dell'investitore – 7. *Virtual worlds*: “luogo” in cui l'esigenza di tutela diviene (ancora più) sentita – 8. Conclusioni

## Keywords

Intelligenza artificiale – *roboadvisor* – neutralità tecnologica – supervisione – regolazione

---

## 1. Introduzione.

1.1 L'intelligenza artificiale<sup>1</sup> ha numerose applicazioni e pone una serie di questioni per il regolatore: anzitutto occorre definirla, comprenderne le insidie, decidere se limitarne l'impiego e/o assoggettare a un penetrante scrutinio coloro che la utilizzino per prestare servizi.

Si tratta di sfide di cruciale rilevanza, rapidamente divenute prioritarie per i legislatori dei paesi più avanzati<sup>2</sup>. In primo luogo, perché l'applicazione di tali tecnologie (generaliste) è potenzialmente orizzontale, potendo essere integrate in qualsiasi settore economico o catena del valore.

Le modalità di regolazione dell'AI passano anzitutto dalla comprensione delle caratteristiche della tecnologia, della sua attitudine trasformativa dei processi, e dei limiti nell'applicazione delle regole già presenti nell'ordinamento. Quando, poi, le tecnologie di intelligenza artificiale siano impiegate nell'ambito del settore finanziario (da parte di istituzioni finanziarie o comunque nell'ambito della prestazione di servizi finanziari)<sup>3</sup>, si pongono ulteriori profili di complessità, in quanto occorre garantire la tutela degli investitori e la stabilità del sistema<sup>4</sup>. Difatti, l'uso scorretto – o anche solo incontrollato – di tali strumenti tecnologici potrebbe risultare pregiudizievole sia per gli interessi dei singoli (andando ad incidere anche su diritti costituzionalmente tutelati, quali ad es. quello alla piena e libera autodeterminazione) sia del sistema finanziario complessivamente inteso, potendo perfino porre a repentaglio la fiducia nei mercati finanziari

---

<sup>1</sup> Per una introduzione ai profili definitori (e giuridici) dell'intelligenza artificiale si veda G. Finocchiaro, *Intelligenza artificiale. Quali regole?*, Bologna, 2023. Più ampiamente sulle questioni definitorie, S. Samoili et al., *AI Watch. Defining Artificial Intelligence Towards an operational definition and taxonomy of artificial intelligence*, JRC Technical Reports, EUR 30117 EN, 2020.

<sup>2</sup> Si pensi, tra le altre, alle iniziative intraprese dall'Unione Europea, dagli Stati Uniti, dalla Cina. Pur adottando approcci molto differenti, sono tutte accomunate dalla percepita esigenza di definire regole (e limiti) per l'utilizzo di strumenti tecnologici dotati caratterizzati da rilevanti potenzialità. Cfr. Financial Times, *The global race to set the rules for AI*, di C. Criddle-J. Espinoza-Q. Liu, 13 settembre 2023.

<sup>3</sup> Cfr. F. Capriglione, *Diritto ed economia. La sfida dell'Intelligenza Artificiale*, in *Rivista Trimestrale Diritto dell'Economia*, 3, 2021, 24 ss.; G. Schneider, *La proposta di regolamento europeo sull'intelligenza artificiale alla prova dei mercati finanziari: limiti e prospettive (di vigilanza)*, in *Responsabilità Civile e Previdenza*, 3, 2023, 1014 ss.

<sup>4</sup> Per una panoramica delle principali applicazioni dell'intelligenza artificiale nel settore bancario e finanziario (e delle sfide che pongono) si veda J.C. Crisanto - C. Benson Leuterio - J. Prenio - J. Yong, *Regulating AI in the financial sector: recent developments and main challenges*, in FSI Insights on policy implementation No. 63, dicembre 2024, spec. 4 ss. In particolare, sul rischio sistemico A. Keller-C. Martins Pereira-M.L. Pires, *The European Union's Approach to Artificial Intelligence and the Challenge of Financial Systemic Risk*, in H. Sousa Antunes et al. (a cura di), *Multidisciplinary Perspectives on Artificial Intelligence and the Law*, vol, 58, Cham, 2024, 415 ss.

e negli intermediari che vi operano.

Pertanto, in questo settore, il legislatore e le autorità di vigilanza sono chiamati a fronteggiare i rischi, operativi e finanziari, che l'AI pone avvalendosi in primo luogo dello strumentario della regolazione finanziaria<sup>5</sup>. Ciò però non esaurisce i meccanismi d'intervento, anche in considerazione della natura non intrinsecamente prudenziale dei controlli sull'AI<sup>6</sup> e alla conseguente non riconducibilità alle autorità di vigilanza bancaria e finanziaria di ogni controllo sull'impiego di tali tecnologie da parte delle istituzioni finanziarie.

1.2 Il contributo intende quindi analizzare quale sia l'approccio regolatorio più adeguato a fronteggiare le sfide poste dalle applicazioni di intelligenza artificiale nel settore finanziario, valutando da un lato fino a che punto il principio di neutralità tecnologica limiti il legislatore (e le autorità di vigilanza) nelle proprie scelte e, dall'altro, come ciò impatti sui livelli di tutela degli investitori. A tale scopo, sono anzitutto esaminate le nozioni di intelligenza artificiale impiegate nel regolamento (UE) 2024/1689 (AI Act) e in altri testi ufficiali al fine di valutarne la neutralità (da un punto di vista tecnologico ed etico). Successivamente, ci si sofferma sulle origini e la portata concreta del principio di neutralità tecnologica, prendendo in considerazione i modelli di regolazione e supervisione adottati a livello europeo, con particolare riferimento al settore finanziario. In tale contesto, viene quindi dimostrato a quali condizioni sia possibile derogare a tale principio. Ci si interroga infine su quale sia l'approccio ottimale per garantire una piena tutela dell'investitore nei confronti dei *roboadvisors*, anche nell'ambito di ambienti immersivi caratterizzati da interazioni *phygital*. Proprio quest'ultimo caso d'uso dimostra l'esigenza di regolare e supervisionare le applicazioni di AI finanziaria adottando un approccio *tech specific*.

## 2. Una preliminare questione definitoria

2.1 Intelligenza artificiale è una nozione commerciale, che non corrisponde in modo univoco a una specifica tecnologia<sup>7</sup>. Difatti, nell'accezione comunemente accolta vi rientrano diverse tecnologie (e relative applicazioni) basate sugli algoritmi di *supervised* e *unsupervised machine learning* (ML), di *natural language process* (NLP), *large language models* (LLM), *expert systems*, nonché i modelli di intelligenza artificiale generale (AGI)<sup>8</sup>. E tale

---

<sup>5</sup> Armour et al., *The Goals and Strategies of Financial Regulation*, in *Principles of Financial Regulation*, Oxford, 2016, 51 ss.; A. Sciarrone Alibrandi, *Innovazione tecnologica e regolazione dei mercati*, in R. Lener-G. Luchena-C. Robustella (a cura di), *Mercati regolati e nuove filiere di valore*, Torino, 2021, 5 ss.

<sup>6</sup> R. Lener, *Vigilanza prudenziale e intelligenza artificiale*, in *Rivista Trimestrale di Diritto dell'Economia*, 1, 2022, 214.

<sup>7</sup> Si ritiene che sia stata introdotta per la prima volta nello scritto, J. McCarthy-M. L. Minsky-N. Rochester-C.E. Shannon, *A proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, agosto 1955, in *AI Magazine*, 27(4) 2006, 12.

<sup>8</sup> Più ampiamente sulle nozioni di algoritmo e la loro riconducibilità al concetto di intelligenza artificiale G.F. Italiano, *Le sfide interdisciplinari dell'intelligenza artificiale*, in *Analisi giuridica dell'economia*, 2019, 9 ss.; N. Cristianini, *Machina sapiens*, Bologna, 2024. Con specifico riferimento all'applicazione di tali tecnologie nell'ambito finanziario, si veda The Alan Turing Institute, *The AI Revolution: Opportunities*

elencazione, che pur si pone ad un livello di dettaglio certamente superficiale, è tutt'altro che esaustiva.

Anche per questo motivo, la Commissione UE nel 2018 aveva proposto una definizione funzionale di intelligenza artificiale che ne evidenziava la caratteristica di «*sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi*»<sup>9</sup>. Nell'ambito della versione finale dell'AI Act<sup>10</sup>, che pur aderisce alla medesima impostazione, si è assistito ad una progressiva evoluzione della definizione, che tenta di delineare una nozione ampia e a basso tasso di tecnicismo, che ne permetta una lunga durata, limitando il rischio di rapida obsolescenza<sup>11</sup>: far riferimento all'intelligenza artificiale non significa quindi necessariamente far riferimento ad una (e una sola) tecnologia, ma ad una categoria di tecnologie che hanno alcuni elementi in comune<sup>12</sup>.

In altri termini, l'ampia definizione di intelligenza artificiale contenuta nell'AI Act – a cui consegue una marcata disomogeneità tra le tecnologie ricomprese nel suo ambito applicativo – potrebbe suggerire che non si tratti, a dispetto della rubrica, della regolamentazione di una tecnologia<sup>13</sup>. Difatti, il regolamento non disciplina un'attività – quantomeno non in modo diretto – bensì un modo di svolgere un'attività: non un'attività, non un prodotto, ma un processo. E le attività svolte avvalendosi di tali strumenti sono soggette, in base alla valutazione circa il livello di rischio che pongono<sup>14</sup>, a una disciplina dedicata (e ulteriore) rispetto alle medesime attività prestate con

---

*and Challenges for the Finance Sector*, 2023, 9 ss.; ESMA, *Artificial intelligence in EU securities markets*, 1 febbraio 2023, ESMA50-164-6247.

<sup>9</sup> Commissione UE, *L'intelligenza artificiale per l'Europa*, COM(2018) 237 final, 25 aprile 2018. A tale definizione aderisce anche il *White Paper sull'intelligenza artificiale, Un approccio europeo all'eccellenza e alla fiducia* COM(2020) 65 final, che dà anche conto della definizione – più tecnica – elaborata dal Gruppo di esperti di alto livello, *Orientamenti etici per un'IA affidabile*, 2019, 45.

<sup>10</sup> Regolamento (UE) 2024/1689 del Parlamento Europeo e Del Consiglio del 13 giugno 2024.

<sup>11</sup> Al riguardo, l'art. 3 (1) dell'AI Act definisce il sistema di intelligenza artificiale come «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali».

<sup>12</sup> Elementi caratterizzanti – non necessariamente omogenei tra le varie categorie di intelligenze artificiali – sono poi quelli relativi alla (mancanza) di esplicabilità del funzionamento, al livello di trasparenza e vulnerabilità. Quest'ultima, in particolare, può essere intesa in varie accezioni: sia in relazione al corretto funzionamento degli algoritmi e alla loro modificabilità sia al livello di sfruttamento delle debolezze degli utenti che sono rese possibili dalle applicazioni di intelligenza artificiale.

<sup>13</sup> Per il vero, gli artt. 5 e 6 dell'AI Act nonché gli allegati al regolamento (In particolare, l'Allegato III) elencano con un certo livello di dettaglio alcune tecnologie soggette alla disciplina del regolamento stesso, e quindi espressamente regolate. Va precisato, però, che le tecnologie individuate nell'Allegato sono indicate facendo riferimento al loro utilizzo e non invece alle caratteristiche tecniche, che consentirebbe un riferimento più univoco.

<sup>14</sup> In base a tale classificazione impone regole diverse e persino divieti, sul punto si veda G. Finocchiaro, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Il Diritto dell'informazione e dell'informatica*, 2, 2022, 303 ss. La specifica attenzione dedicata dai regolatori alle applicazioni di AI può ricondursi anzitutto alla mutevolezza e non staticità – caratteristica di quei sistemi basati su forme di autoapprendimento – che rendono complicato per un soggetto esterno valutare ed approvare definitivamente una determinata tecnologia, in quanto richiederebbe una valutazione circa la possibile evoluzione futura dello strumento. In secondo luogo, poiché casi d'uso diversi pongono sfide

diverse modalità.

Un approccio regolatorio di questo tipo risulterebbe però non tecnologicamente neutrale. Quel che occorre valutare è (i) se ciò sia legittimo e (ii) se sia giustificato.

### 3. Neutralità tra tecnologia ed etica

3.1 Parlando di neutralità tecnologica nel contesto del *rule-making*, ci si riferisce ad un principio emerso originariamente nel settore delle comunicazioni elettroniche<sup>15</sup>, espressione del generale dovere di non discriminazione. Tale principio – che impone di applicare le medesime regole ad attività sostanzialmente analoghe, anche quando siano svolte avvalendosi di tecnologie diverse – ha poi vissuto una *vis expansiva*, trovando applicazione anche in altri settori, ugualmente interessati dall’innovazione tecnologica e dalle conseguenti trasformazioni.

Ebbene, l’estensione dell’ambito applicativo del principio di neutralità tecnologica è probabilmente da ricondurre alla convinzione comune che la tecnologia sia un semplice strumento: se la tecnologia è un mero mezzo, che non attribuisce una connotazione specifica e diversa all’attività che viene così svolta, non vi è ragione per assoggettarla a regole diversificate. In realtà, le tecnologie (quantomeno, alcune di esse) concorrono a definire i connotati delle attività che vengono svolte avvalendosene. Costituiscono sovente un facilitatore di attività che altrimenti non potrebbero essere svolte o che risulterebbero più complesse. Se alcune tecnologie sono di per sé caratterizzate da elementi di positività o negatività perché il loro unico possibile uso è così connotato, per molte altre bisogna interrogarsi se siano neutre<sup>16</sup>. In questo senso, neutralità significherebbe indifferenza dello strumento rispetto ad un fine.

È assai raro però che una tecnologia sia effettivamente neutra, molto più spesso è “*double charged*”: in grado di produrre effetti sia positivi sia negativi<sup>17</sup>.

Quando osservate nella prospettiva statica anche le tecnologie “a doppia carica” potrebbero sembrare eticamente neutre, salvo poi disvelare le proprie caratteristiche nella prospettiva dinamica. Esattamente così avviene anche con riferimento all’intelligenza artificiale<sup>18</sup>.

---

diverse: le stesse tecnologie possono comportare diversi livelli di allarme sociale e rischi (micro e macro) a seconda del settore in cui vengono impiegate.

<sup>15</sup> U. Kamecke-T. Korber, *Technological Neutrality in the EC Regulatory Framework for Electronic Communications: A Good Principle Widely Misunderstood*, in *European Competition Law Review*, 2008, 330 ss.; W. Briglauer – V. Stocker – J. Whalley., *Public Policy Targets in EU Broadband Markets: The Role of Technological Neutrality*, 29th European Regional ITS Conference, Trento, 2018, 184936.

<sup>16</sup> S. Heyndels, *Technology and Neutrality*, in *Philosophy & Technology*, 2023, 36, 74 ss.

<sup>17</sup> L. Floridi, *On Good and Evil, the Mistaken Idea That Technology Is Ever Neutral, and the Importance of the Double-Charge Thesis*, in *Philosophy & Technology*, 36, 60, 2023, 2.

<sup>18</sup> Anche guardando specificamente al settore finanziario possono individuarsi esempi di “cariche” positive e meno positive (*rectius*, negative) dell’AI, nel senso di attitudine dello strumento tecnologico a migliorare o peggiorare gli esiti dell’attività umana. F. D’Acunto-N. Prabhala-A. Rossi, *The Promises and Pitfalls of Robo-advising*, 2018 CESifo Working Paper No 6907, 18. ss., studiando un ottimizzatore di portafoglio rivolto al mercato azionario indiano, rileva come il robo-advisor sia stato vantaggioso per gli investitori ex-ante poco diversificati, aumentando la diversificazione del loro portafoglio, riducendo

Come accennato, le applicazioni di intelligenza artificiale rappresentano sovente un efficace ausilio alle attività umane; in questo caso, si ritiene dunque che il “vettore buono” sia molto più forte di quello cattivo<sup>19</sup>. E pertanto, le possibili falle – tali da far emergere criticità e rischi che possono portare agli “*ethical disasters*” – sono da individuare non solo nelle fasi di progettazione e sviluppo, quanto piuttosto nell’impiego della specifica tecnologia<sup>20</sup>. Trattandosi di strumenti che, se correttamente progettati, rappresentano una *force for the good*, sui progettatori (e sui *deployers*) ricade una significativa responsabilità<sup>21</sup>. È quindi necessario fare in modo che non se ne faccia un cattivo uso. E anche questo è il compito della regolazione.

Pertanto, dalla constatazione della non-neutralità della tecnologia si può trarre un’argomentazione a favore della derogabilità del principio di neutralità tecnologica; a supporto di un approccio regolatorio *tech-specific*.

3.2. Nell’ambito del settore finanziario, il principio di neutralità tecnologica trova espressa previsione. Al riguardo, la comunicazione del Parlamento UE del 2017<sup>22</sup> in materia di FinTech affermava che la regolazione e supervisione, nell’ambito della *financial technology* si sarebbe dovuta basare sui seguenti principi «*a) same services and same risks; b) technology neutrality; c) a risk-based approach*». In tale contesto, il principio di neutralità tecnologica appariva essere una pietra angolare della disciplina europea del (allora ancora agli albori) *fintech*. Sembrava infatti che qualsiasi regolazione della tecnologia – anche quando strumento abilitante per prestare determinati servizi, caratterizzante la relativa fattispecie – fosse una discriminazione intollerabile perché avrebbe minato il *level playing field* tra gli operatori economici. Il presupposto, allora condiviso, è che la scelta dello strumento tecnologico sarebbe stata una mera opzione organizzativa, neutra dal punto di vista delle caratteristiche proprie del servizio prestato. A ciò sarebbe conseguito il vincolo per il legislatore di disciplinare in modo uniforme le attività, a prescindere dalle modalità operative concrete, salvo che queste dessero vita a rischi nuovi e disomogenei. Difatti, solo laddove sulla base dell’approccio basato sul rischio

---

il rischio e aumentando i loro rendimenti. Quanto, invece, agli investitori che già avevano un livello accettabile di diversificazione, il roboadvisor non ha migliorato le loro performances, anzi talvolta le ha peggiorate.

<sup>19</sup> Floridi, *On Good and Evil, the Mistaken Idea That Technology Is Ever Neutral*, cit., 3.

<sup>20</sup> L. Floridi, *The Ethics of Artificial Intelligence. Principles, Challenges, and Opportunities*, Oxford, 2023, passim.

<sup>21</sup> P.P. Verbeek, *Morality in Design: Design Ethics and the Morality of Technological Artifacts*, in P.E. Vermaas et al. (a cura di), *Philosophy and Design*, Cham, 2008, 91 ss. le qualità del *deployer* risultano decisive nel caratterizzare i rischi del sistema di AI, in quanto dalla sua condotta potrebbe dipendere la bontà dell’uso del sistema stesso, nonché la prontezza d’intervento a fronte di possibili criticità. P. Benanti, *IA e medicina più dello strumento conta il manico*, in Avvenire.it, 21 marzo 2024, occupandosi in particolare delle applicazioni dell’AI all’ambito sanitario e dei relativi rischi ha riconosciuto come rilevi ben più “il manico” rispetto allo strumento in sé. Similmente E. McCaul, *Technology is neither good nor bad, but humans make it so*, Discorso del membro del supervisory board ECB nell’ambito della conferenza “*The use of artificial intelligence to fight financial crime*”, organizzato da Intesa Sanpaolo, Torino 13 luglio 2022. Queste valutazioni paiono sottese anche alla disciplina di cui agli artt. 16 ss. dell’AI Act, i quali prevedono puntuali regole di condotta (e responsabilità) gravanti sul *deployer* del sistema.

<sup>22</sup> Parlamento europeo, *FinTech: the influence of technology on the future of the financial sector*, Risoluzione del 17 maggio 2017 (2016/2243(INI)), (2018/C 307/06).

emergessero esigenze di tutela ulteriori, ciò giustificerebbe una deroga legittima al principio della parità di trattamento: le regole diverse e più stringenti deriverebbero dall'esistenza di rischi diversi, e ciò sarebbe del tutto giustificato nel contesto di una procedura di valutazione dell'impatto della regolazione.

Al di fuori di queste ipotesi, che ne rappresentano il confine esterno, la funzione del principio di neutralità tecnologica sarebbe quindi quello di garantire la non discriminazione ma anche la certezza per gli operatori economici, che potrebbero così contare sull'applicazione di regole omogenee per le proprie attività, a prescindere dalle tecnologie impiegate.

Nonostante continuo ad esserci riferimenti al principio di neutralità tecnologica in tutte le principali iniziative europee di disciplina di fenomeni caratterizzati dalla penetrante presenza tecnologica<sup>23</sup>, tale principio pare ormai di fatto eroso. Basti pensare al GDPR (che richiama il principio al considerando 15) e al Regolamento MICA (considerando 9) che nonostante tali richiami nei considerando, contengono poi nell'articolo disposizioni che pongono regole dedicate per specifiche applicazioni tecnologiche. Anche nell'ambito della proposta della Commissione europea per l'introduzione di una disciplina dell'intelligenza artificiale si diceva espressamente che tale testo normativo «*aims to be as technology-neutral and future-proof as possible*»<sup>24</sup>. Ciononostante, tale proposito è stato disatteso nell'elaborazione concreta delle disposizioni normative (ad esempio, vietando alcune tipologie di sistemi di AI).

Sembra dunque evincersi - anche dallo svolgimento dell'*iter legis* dei provvedimenti citati - che il principio di neutralità tecnologica sia divenuto più un punto di partenza per il legislatore che un limite oltre il quale non sia lecito spingersi.

Occorre dunque domandarsi se e come un approccio non neutrale - sia regolatorio sia di vigilanza - possa meglio raggiungere gli obiettivi della regolazione finanziaria, consentendo di governare in modo più efficace e consapevole i rischi posti dalle variegate applicazioni dell'AI. In altri termini, si intende valutare quali caratteristiche debba avere la regolazione delle applicazioni finanziarie di AI (nonché i poteri d'intervento delle *supervisory authorities*) al fine di garantire una piena tutela degli obiettivi della regolazione finanziaria, nonché dei diritti fondamentali che potrebbero essere incisi.

Anche alla luce delle premesse sin qui esposte si intende dimostrare come sia sempre più indispensabile adottare un modello di regolazione e supervisione tecnologicamente orientata, che consenta di fronteggiare gli specifici rischi che un'applicazione tecnologica può porre, confrontandosi efficacemente con le evoluzioni della stessa, difficilmente governabili con strumenti neutrali.

---

<sup>23</sup> M.A. Scopellitti, *È ancora possibile la neutralità tecnologica della normativa?*, in V. Falce (a cura di), *Strategia dei dati e intelligenza artificiale*, Torino, 2023, 213 ss.

<sup>24</sup> Proposta di Bruxelles, Regolamento del parlamento europeo e del consiglio che stabilisce regole armonizzate sull'intelligenza artificiale e modifica alcuni atti legislativi dell'unione, 21.4.2021, COM(2021) 206 final, 2021/0106 (COD), p. 12.

---

## 4. Regolazione neutrale

4.1 La regolazione tecnologicamente neutrale è quindi quella che ponga regole uniformi, guardando alle attività e ai loro rischi tipici, senza distinguere (e discriminare) in ragione degli strumenti impiegati per lo svolgimento delle stesse. Non preoccupandosi di quanto tali tecnologie possano mutare le modalità operative e abilitare interazioni nuove. La regolazione neutrale può impiegare tecniche normative per principi o *rules based*, così come può fare ampio rinvio a disposizioni attuative. In altri termini, anche rimanendo nel perimetro di una regolazione primaria formalmente neutrale, è possibile tenere in considerazione alcune delle specificità di determinate modalità operative. Ciò a cui sempre più spesso si assiste è quindi un approccio combinato: accanto a regole (tendenzialmente) tecnologicamente neutrali, vengono emanati regolamenti complementari su specifici ambiti di applicazione e soluzioni tecnologiche<sup>25</sup>. Un chiaro esempio in questo senso è la disciplina contenuta nella direttiva sui mercati degli strumenti finanziari (MIFID II) - nonostante contenga essa stessa disposizioni che non sono affatto in linea con la neutralità tecnologica (ad esempio l'art. 17 della MIFID II che regola il trading algoritmico) – che è poi integrata da puntuali regole “*tech-specific*”. Si tratta comunque di un approccio non privo di punti deboli: come rilevato dal Presidente della CONSOB in un suo recente intervento, a fronte dell'emersione di tecnologie che caratterizzano i servizi prestati, se si vuole imporre al legislatore di mantenere un approccio tecnologicamente neutrale, deve poi riconoscersi un ruolo più invasivo alle autorità indipendenti, chiamate ad adottare regolamenti per fronteggiare i rischi non adeguatamente presidiati dalle fonti primarie<sup>26</sup>. È evidente, però, che siffatto modello non risulterebbe autenticamente rispettoso del principio di neutralità tecnologica.

4.2 Se il principio di neutralità tecnologica può ancora essere un obiettivo da perseguire in termini generali, questo è invece recessivo con riferimento ad applicazioni che danno luogo a rischi particolari. Tali considerazioni portano ad escludere che sia ancora possibile adottare un approccio pienamente neutrale nella regolazione delle applicazioni dell'AI<sup>27</sup>.

Il principio di neutralità tecnologica, pur avendo solide basi negli atti europei – ed essendo un principio animato da finalità meritevoli – sembra ormai rappresentare un approccio idealistico, in grado di orientare il procedimento di formazione delle norme, ma con limitata portata cogente. La dirompente evoluzione tecnologica trasformativa ne ha fortemente ridimensionato la portata applicativa: la sua applicazione letterale rischierebbe di causare danno all'ordinamento, non garantendo sufficiente protezione dinnanzi a rischi derivanti dall'utilizzo di specifiche tecnologie.

---

<sup>25</sup> W. Buczynski et al., *Hard Law and Soft Law Regulations of Artificial Intelligence in Investment Management*, in *Cambridge Yearbook of European Legal Studies*, 24, 2022, 262 ss.

<sup>26</sup> P. Savona, Intervento del Presidente della Consob in occasione dell'assemblea annuale 2023 Assosim Competitività dei mercati italiani, Milano 29 maggio 2023.

<sup>27</sup> In senso contrario, P. Grady, *The AI Act Should Be Technology-Neutral*, Center for data innovation, febbraio 2023.



È tale conclusione appare ancora più evidente quando si calino tali strumenti nel settore finanziario. Difatti, si pone una questione di governabilità delle tecnologie in campo finanziario, non solo di imposizione di requisiti su uno strumento: il mercato finanziario tecnologizzato genera dinamiche diverse rispetto a quello tradizionale analogo, che devono essere previste, monitorate e gestite<sup>28</sup>.

Laddove, dunque, sussistano queste esigenze risulta legittima una regolazione che preveda regole dedicate alla tecnologia e che distingua le regole sull'attività anche in base ai procedimenti impiegati per esercitare tali attività. Ciò purché tale non neutralità sia limitata al minimo indispensabile.

Gli approcci non neutrali, peraltro, non sono necessariamente pregiudizievoli per lo sviluppo delle nuove tecnologie e per chi le impieghi: non necessariamente sono introdotti limiti più stringenti alla prestazione delle attività, ma talvolta disposizioni specifiche e più favorevoli, a vantaggio dello sviluppo e del più ampio utilizzo di tecnologie di cui si voglia incentivare l'utilizzo e che siano ritenute in grado di mitigare i rischi di specifiche attività. Ad esempio, nell'ambito del DLT Pilot Regime (regolamento (UE) 2022/858) è previsto che all'utilizzo di infrastrutture di mercato decentralizzate consegua l'applicazione di un regime normativo semplificato rispetto a quello ordinariamente applicabile alle infrastrutture non decentralizzate<sup>29</sup>. Ebbene, la potenziale bidirezionalità della non-neutralità tecnologica della disciplina normativa concorre a riportare una siffatta scelta – quando oggettivamente giustificata – nell'alveo della discrezionalità del legislatore, senza violare principi inderogabili.

## 5. (segue) ...e modelli di supervisione

5.1 Delineate le caratteristiche per una efficace regolazione dell'AI finanziaria, occorre ora soffermarsi sulla supervisione, complementare rispetto alla prima e parimenti fondamentale per un corretto funzionamento del mercato.

Nel contesto della supervisione bancaria e finanziaria, il principio di neutralità tecnologica assume confini più sfumati, operando solamente “di rimbalzo”; non limiterebbe le modalità d'azione, ma piuttosto rappresenterebbe un obbligo di risultato, corollario del principio *same risks, same rules, same supervision*.

Accogliendo una nozione ampia di neutralità tecnologica, questa può assumere almeno due significati in relazione alla supervisione.

In primo luogo, una supervisione neutrale è quella che effettui il medesimo scrutinio (e.g., in relazione agli atti esaminati, ai rischi posti dall'attività, all'organizzazione) nei confronti degli intermediari che prestino analoghi servizi senza operare differenziazioni sulla base di quali siano le tecnologie impiegate per fornirli, nonché ad eventuali specificità che tali servizi possano assumere proprio in ragione del supporto tecnologico-

<sup>28</sup> Al riguardo, assume anche rilievo la disciplina di cui al regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 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, (UE) n. 909/2014 e (UE) 2016/1011.

<sup>29</sup> T.N. Poli, *MiCA, Pilot Regime e Decreto Fintech: la regolazione del fenomeno crypto e le difficoltà di inquadramento nel sistema finanziario*, in Dialoghi di diritto dell'economia, dicembre 2023.

co. La debolezza di un siffatto modello è che si rischia di non identificare correttamente le insidie derivanti dall'impiego di tecnologie *disruptive*, sottostimandone gli effetti e limitando gli spazi di intervento delle autorità di controllo. Una seconda accezione, invece, è quella che pone l'attenzione sull'autorità di vigilanza: dunque, è neutrale quel modello di supervisione che utilizzi uno strumentario omogeneo in relazione a tutti i soggetti e attività vigilate, senza impiegare *tech-specific tools*<sup>30</sup> che consentirebbero invece di monitorare in modo più efficace le caratteristiche dell'oggetto della vigilanza, così da intervenire quando ritenuto opportuno.

5.2 La supervisione sulle applicazioni di AI nel settore finanziario<sup>31</sup> può quindi far uso - purché l'autorità di vigilanza sia dotata di idonee competenze tecniche e sufficienti risorse - di uno strumentario tecnologico, sovente *tech-specific*, e può modulare le proprie modalità d'intervento tenendo conto delle specificità dell'oggetto della vigilanza<sup>32</sup>. Tra gli strumenti di SupTech, l'applicazione del modello della *supervision as code*<sup>33</sup> ha rilevanti potenzialità:

la risposta di vigilanza, espressa in termini di codice ed inclusa nella tecnologia impiegata dal prestatore di servizi fa sì che questa possa essere resa eseguibile dalla macchina<sup>34</sup>, monitorando eventuali evoluzioni dello strumento, degli output che restituisce e consentendo un intervento tempestivo.

In questo contesto, la non neutralità può consistere nelle indicazioni delle autorità di vigilanza circa il tipo di codice da utilizzare, le caratteristiche degli strumenti tecnologici impiegati e le modalità di interazione tecnologica che possono avvenire tra vigilante e vigilato, risultando potenzialmente particolarmente invasiva della libertà organizzativa del prestatore di servizi.

Si consente così alle autorità di effettuare una vigilanza assai più effettiva ed efficace rispetto ai meri controlli ispettivi e documentali, che rimangono comunque indispensabili in quanto complementari.

Non neutrali potrebbero risultare anche le cd. valutazioni di conformità "*in action*" dei sistemi di AI impiegati dall'intermediario, le quali potrebbero essere condotte anche alimentando i sistemi in sperimentazione con dati selezionati e predisposti dalle au-

---

<sup>30</sup> A ciò si aggiungano anche le ipotesi di utilizzo da parte delle autorità di vigilanza di strumenti di intelligenza artificiale al fine di svolgere in modo più efficace ed efficiente i propri compiti. Su tali applicazioni di suptech, si veda ad esempio A. Azzutti-P. Magalhães Batista-W.G. Ringe, *Navigating the Legal Landscape of AI-Enhanced Banking Supervision: Protecting EU Fundamental Rights and Ensuring Good Administration*, EBI Working Paper Series 2023 – no. 140, aprile 2023.

<sup>31</sup> G. Siani, *AI-driven bank: Opportunità e sfide strategiche per il sistema finanziario e la vigilanza*, intervento del Capo del Dipartimento Vigilanza bancaria e finanziaria della Banca d'Italia, Banking Insight 2023, Boston Consulting Group Milano, 3 Ottobre 2023.

<sup>32</sup> M. Rabitti-A. Sciarrone Alibrandi, *RegTech e SupTech*, in A. Pajno-F. Donati-A. Perrucci (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Quaderni Astrid, Bologna, 2022, 439 ss.

<sup>33</sup> Il modello di riferimento è quello delle «*rules as code*». Al riguardo cfr., J. Mohun-A. Roberts, *Cracking the Code: Rulemaking for Humans and Machines*, OECD Working Papers on Public Governance No. 42, 2020, 39 ss. In senso critico, J. Oster, *Code is code and law is law—the law of digitalization and the digitalization of law*, in *International Journal of Law and Information Technology*, Volume 29, Issue 2, 2021, 101 ss.

<sup>34</sup> A. Celotto, *Verso l'algoretica. Quali regole per le forme di intelligenza artificiale?*, in V. Falce (a cura di), *Strategia dei dati e intelligenza artificiale*, Torino, 2023, in particolare 28 ss.

torità, consentendo di far emergere possibili debolezze ed effetti discriminatori. Nel caso in cui l'autorità, a conclusione della verifica, riscontrasse errori nelle performance degli algoritmi, dovrebbe avere il potere di imporre la sospensione e l'eventuale correzione del suo funzionamento, anche attraverso l'introduzione di correttivi e filtri da applicare agli output.<sup>35</sup>

Rendendo le regole e gli strumenti di reazione *embedded* nell'algoritmo utilizzato per la prestazione di servizi si rende la supervisione più efficace, meglio in grado di tutelare gli investitori, vigilare sull'osservanza delle disposizioni in materia finanziaria previste dall'ordinamento, al contempo salvaguardando il buon funzionamento del sistema finanziario e la fiducia degli investitori<sup>36</sup>.

Anche in questo caso non mancano le controindicazioni. Anzitutto, non ogni regola o aspettativa di vigilanza può essere resa codice, ma solo quelle disposizioni che siano prescrittive ed univoche; d'altra parte, una siffatta modalità operativa delle autorità di vigilanza può risultare molto onerosa poiché richiede specifiche competenze tecniche ed è fortemente legata alle singole tipologie di servizi offerti. Prioritaria, dunque, potrebbe esserne l'applicazione con riferimento a quelle applicazioni di AI che determinano rischi ritenuti più pressanti.

## 6. *Roboadvisors*, etica e tutela dell'investitore

6.1 Tra le applicazioni di AI al settore finanziario, i servizi di *roboadvice*<sup>37</sup> costituiscono un rilevante terreno di prova. Sia in ragione della loro diffusione - e quindi alla capacità di determinare effetti per ampie fasce di utenti - sia per la loro insidiosità. Grazie alla loro accessibilità e ai costi ridotti rispetto alle alternative tradizionali costituiscono, infatti, anche un rilevante canale di accesso ai servizi finanziari (e, ancor prima, alle informazioni finanziarie) e pertanto usi impropri o fuorvianti possono cagionare pregiudizio agli utenti/investitori.

Come accennato, nell'ambito della ampia categoria di consulenza finanziaria che si avvale di sistemi di intelligenza artificiale si possono annoverare servizi caratterizzati da modelli operativi molto differenti. Tradizionalmente viene operata una distinzione tra *roboadvisors* puri e ibridi<sup>38</sup>, utile a fini descrittivi ma anche idonea a rappresentare

<sup>35</sup> La vigilanza che operasse in questo modo applicherebbe di fatto regole di "secondo ordine". cioè filtri inseriti dal programmatore per correggere eventuali malfunzionamenti (ovvero risultati che rischiano di produrre un pregiudizio per l'individuo o di violare una disposizione di legge) del processo di elaborazione dei dati. Sul tema F. Schauer, *Second-Order Vagueness in the Law*, in G. Keil-R. Poscher (a cura di), *Vagueness and Law: Philosophical and Legal Perspectives*, Oxford, 2016, 177 ss.

<sup>36</sup> Art. 5, c. 1, TUF.

<sup>37</sup> Consob, *La digitalizzazione della consulenza in materia di investimenti finanziari*, in N. Linciano-P. Soccorso-R. Lener (a cura di), Quaderni Fintech n. 3, gennaio 2019; F. Sartori, *La consulenza finanziaria automatizzata: problematiche e prospettive*, in *Rivista Trimestrale Diritto dell'Economia*, 1, 2018, 258 ss.; D. Rossano, *Il Robo advice alla luce della normativa vigente*, in F. Capriglione (a cura di), *Liber Amicorum Guido Alpa*, Padova, 2019, 365 ss.

<sup>38</sup> Una puntuale distinzione è delineata da Consob, *La digitalizzazione della consulenza in materia di investimenti finanziari*, cit., 10 ss. A ciò si aggiunga l'ulteriore - e assai diversa - fattispecie del robo4advisor, servizio BtoB, offerto dal prestatore di servizi (consulente professionale) ad altro consulente finanziario.

l'impatto, assai differente, che questi possono avere sugli utenti. I primi costituiscono forme di consulenza completamente automatizzata, basate sull'intelligenza artificiale e veicolate all'investitore attraverso interfacce che non prevedono l'interazione con operatori umani, né attività di filtro operate da questi ultimi; nell'ambito dei servizi di *roboadvisor* ibrido – decisamente più diffusi – per quanto l'apporto della valutazione operata mediante consulenti robotizzati possa essere comunque decisiva, vi è un intervento umano. Il ruolo dell'AI è quindi mediato: alle fasi dell'attività automatizzate se ne alternano altre in cui è prevista l'interazione con persone fisiche<sup>39</sup>, che non solo sono chiamate a correggere eventuali “errori” dell'AI, ma anche a seguire il cliente in tutte le fasi della consulenza. Il consulente finanziario umano opera come filtro ed è vincolato da obblighi di professionalità e buona fede<sup>40</sup>.

Spesso i servizi di *roboadvice* puro si rivolgono, quale cliente target, alla clientela *retail*, e ciò ne acuisce i profili di rischio. Anzitutto, in relazione alla consapevolezza del cliente circa la tipologia di contratto che sta concludendo, a maggior ragione quando ciò avvenga nell'ambito di piattaforme generaliste.

Ad ogni modo, anche quando sia prestata mediante tali modalità, la consulenza personalizzata ed individualizzata soggiace alle regole di condotta previste dalla disciplina europea e del Regolamento emittenti CONSOB<sup>41</sup>. Quanto all'effettività di tale regime normativo<sup>42</sup>, va evidenziato come la mancanza di interazione con un consulente umano – sia pure online – potrebbe impattare negativamente sulla veridicità dei dati raccolti, inducendo il cliente ad una rapida scelta di cui potrebbe non percepire la rilevanza. Nella prospettiva delle regole di comportamento non solo è dunque fondamentale che siano rispettati i medesimi requisiti di correttezza dei consulenti umani, che l'interazione sia svolta in maniera etica e non volta a trarre in inganno la controparte, ma anche che i procedimenti di raccolta di informazioni sul cliente, nell'ambito delle *know your customer rules*, siano effettivi. Se con riferimento ai consulenti finanziari persone fisiche, autorizzati dall'autorità di vigilanza, sono previste penetranti regole volte garantire che questi agiscano nel rispetto dei canoni deontologici, la verifica circa il rispetto delle stesse può risultare più complessa in relazione ai servizi di *roboadvice* basati su algoritmi a cui non è agevole avere accesso. Le autorità di vigilanza si trovano dunque di fronte alla sfida di valutare le caratteristiche tecnologiche del *roboadvisor* al momento della loro autorizzazione, ma anche a monitorarne efficacemente gli sviluppi successivi.

Anche considerando tali elementi, è elevato il rischio che al cliente sia veicolata una informazione fuorviante – quantomeno nelle modalità comunicative – al fine di indurlo a concludere contratti: il *roboadvisor*, pur di raggiungere il proprio obiettivo, potrebbe discostarsi dai modelli “etici” che gli siano stati sottoposti come input in fase di *trai-*

<sup>39</sup> R. Lener, *Intelligenza Artificiale e interazione umana nel robo-advice*, in Rivista Trimestrale Diritto dell'Economia, 3s, 2021, 101 ss.

<sup>40</sup> U. Gasser-C. Schmitt, *The Role of Professional Norms in the Governance of artificial intelligence*, in M.D. Dubber- F. Pasquale-S. Das (a cura di), *The Oxford Handbook of Ethics of AI*, Oxford, 2020, 141 ss.

<sup>41</sup> Regolamento CONSOB n. 20307/2018, artt. 40 ss. che si pone in linea con quanto previsto dal regolamento delegato UE/2017/565 artt. 54 e 55.

<sup>42</sup> Sul punto, P. Maume, *Robo-advisors How do they fit in the existing EU regulatory framework, in particular with regard to investor protection?*, study Requested by the ECON committee, giugno 2021.

ning<sup>43</sup>. Ciò non solo sarebbe pregiudizievole per il cliente, ma violerebbe espressamente l'obbligo gravante sull'intermediario di agire nel *best interest* del cliente<sup>44</sup>.

6.2 In relazione al caso d'uso del *roboadvice* è possibile, dunque, dimostrare le argomentazioni finora sostenute.

Il *roboadvice* puro, quello che – sebbene sia raramente offerto nella pratica – maggiormente costituisce una minaccia per gli investitori in quanto “scavalca” l'interazione con soggetti professionali, tenuti a doveri di diligenza, è foriero di pericoli. Questi, solo in parte, sono neutralizzati dall'applicazione delle regole ordinariamente previste per la consulenza finanziaria<sup>45</sup>, le quali sono costruite individuando un soggetto responsabile – l'intermediario – destinatario di obblighi. L'utilizzo di tecnologie avanzate può attenuare le forme di possibile controllo da parte di quest'ultimo (nonostante l'intermediario-*deployer* ne rimanga pienamente responsabile sia ai sensi della disciplina finanziaria, sia in base al modello delineato dagli artt. 16 ss. dell'AI Act), aprendo la strada a rischi nuovi.

È dunque più che mai necessario realizzare una *trustworthy AI*, obiettivo espressamente al centro delle strategie UE<sup>46</sup> ed è essenziale che le istituzioni finanziarie, che impieghino tali tecnologie, siano in grado di offrire una tutela piena ed effettiva dei diritti fondamentali dei propri clienti<sup>47</sup>.

Ciò passa non solo dalla corretta progettazione della tecnologia, dell'individuazione dei servizi tecnologizzati più adatti per le preferenze della clientela, ma anche dal continuo monitoraggio umano degli stessi<sup>48</sup>.

Tali difese consentono anche di fronteggiare il problema delle “allucinazioni”<sup>49</sup> nell'AI generativa, ipotesi in cui il modello genera informazioni che siano falsamente basate su dati reali, particolarmente problematica quando l'AI venga utilizzata in contesti in cui l'accuratezza delle informazioni è fondamentale. Si pensi, ad esempio, quando il servizio di consulenza finanziaria robotizzata produca tali allucinazioni, con effetti fuorvianti per il cliente al quale potrebbero così essere offerti prodotti inadeguati.

---

<sup>43</sup> Similmente a quanto avviene nel caso di comportamenti collusivi autonomamente sviluppati da parte di sistemi di intelligenza artificiale indipendenti, in quanto ciascuno volto a massimizzare il proprio profitto. A. Ezrachi-M.E. Stucke, *Artificial Intelligence & Collusion: When Computers Inhibit Competition*, in *University of Illinois Law Review*, 2017, 1776 ss.

<sup>44</sup> ESMA, *Public Statement On the use of Artificial Intelligence (AI) in the provision of retail investment services*, 30 maggio 2024, ESMA35-335435667-5924, spec. 4.

<sup>45</sup> F. Annunziata, *Servizi e attività di investimento. Definizioni e accesso al mercato*, in *La disciplina del mercato dei capitali*, Torino, 2023, 175 ss.

<sup>46</sup> Ad esempio nell'ambito dei seguenti documenti: Commissione Europea, *Communication on Artificial Intelligence for Europe*, (COM(2018) 237 final) e Gruppo di esperti di alto livello, *Orientamenti etici per un'IA affidabile*, 2019. In tema, I. Carnat, *Ethics Lost In Translation: Trustworthy Ai From Governance To Regulation*, in *Opinio Juris in Comparatione*, 1(1), 2023, 90 ss.; G. Comandé, *Unfolding the legal component of trustworthy AI: a must to avoid ethics washing*, in *Annuario di diritto comparato*, Napoli, 2020, 39 ss.

<sup>47</sup> O. Pollicino, *AI ACT: «Banche e assicurazioni preparate alla Valutazione di impatto sui diritti fondamentali»*, Conversazione su Democrazia digitale alla ricerca di check and balance, su *Altalex.com*, 29 luglio 2024.

<sup>48</sup> D. Rossano, *L'Intelligenza Artificiale: ruolo e responsabilità dell'uomo nei processi applicativi (alcune recenti proposte normative)*, in *Rivista Trimestrale di Diritto dell'Economia*, 3, 2021, 212.

<sup>49</sup> ESMA, *Public Statement On the use of Artificial Intelligence*, cit., 3.

Questi risultati erodono la fiducia del pubblico nei sistemi di AI, ma anche nelle istituzioni finanziarie che utilizzano questa tecnologia: l'“ambiente” in cui operano i sistemi di intelligenza artificiale finanziaria impone una maggiore cautela essendo la fiducia negli intermediari finanziari e nel mercato bancario un prerequisito per il loro funzionamento.

Pertanto, per mitigare le allucinazioni dell'AI è necessaria un'attenta progettazione dei modelli, basata su training con dati di alta qualità e aggiornamenti frequenti con informazioni accurate, accanto ad un'indispensabile supervisione umana<sup>50</sup>.

Sempre con riferimento alla tutela dell'investitore, gli intermediari che facciano utilizzo dell'AI per offrire servizi automatizzati - in tutto o in parte - dovrebbero svolgere un *assessment* puntuale dell'impatto che tali strumenti possono avere sui diritti fondamentali dei propri clienti<sup>51</sup> (similmente a quanto previsto dall'art. 27 AI Act), adottando contromisure più consistenti o addirittura giungendo a desistere dall'utilizzo qualora si ritenga che sia messa a repentaglio la libertà di scelta del soggetto o la *gamification* dell'esperienza possa alterare la capacità decisionale dell'individuo (ipotesi già vietata ai sensi dell'AI Act).

In particolare, quanto alle contromisure da adottare, è auspicabile che siano incluse anche contromisure tecnologiche: risulta infatti opportuno includere nello stesso algoritmo meccanismi che consentano al *deployer* e alle autorità di vigilanza un effettivo monitoraggio del funzionamento della tecnologia – sincerandosi che questa non devii da quanto originariamente previsto – potendo così bloccare eventuali evoluzioni indesiderate dello strumento. In questo senso, si tratterebbe certamente di un approccio non tecnologicamente neutrale, ma che appare legittimo perché volto a garantire che la tecnologia operi nell'alveo di quanto autorizzato e non determini rischi (ulteriori rispetto a quelli che deriverebbero dalla prestazione della medesima attività con altre modalità) pregiudizievoli per l'intermediario, per i consumatori e per il mercato.

## **7. Virtual worlds: luogo in cui l'esigenza di tutela diviene (ancora più) sentita**

7.1 Una delle più recenti frontiere dell'interazione online è rappresentata dai *virtual worlds*, mondi virtuali caratterizzati da una forte immersività<sup>52</sup>.

Calare i servizi di *roboadvice* nell'ambito dei *virtual worlds* fa emergere ancora più chiaramente gli scenari (e le criticità) messi sinora in evidenza e rende manifesta l'esigenza di una decisa reazione dell'ordinamento, adottando un approccio *tech-specific*.

In questo contesto, caratterizzato dall'immersività della esperienza dell'utente, la vul-

<sup>50</sup> Artt. 14, 26 AI Act con riferimento ai sistemi ad alto rischio.

<sup>51</sup> O. Pollicino, *AI ACT: «Banche e assicurazioni preparate alla Valutazione di impatto sui diritti fondamentali»*, cit. Si tratta di una valutazione da condurre non solo in relazione ai servizi di roboadvice o all'utilizzo di sistemi di credit scoring che potrebbero avere l'effetto di escludere un soggetto dall'accesso al credito, ma anche con riferimento ad altri utilizzi dell'AI nell'ambito dell'organizzazione della banca, che potrebbero incidere sui diritti dei clienti.

<sup>52</sup> Sul tema sia consentito rinviare a F. Di Porto-D. Foà-S. Ennis, *Emerging Virtual Worlds: Implications for Policy and Regulation*, CERRE – Centre on Regulation in Europe, febbraio 2024.

nerabilità digitale<sup>53</sup> risulta fortemente accentuata. Ciò in ragione della possibilità di acquisire dati biometrici e cognitivi, anche attraverso l'*eye tracking*, e la presenza di *avatars* (che molto spesso sono la proiezione, anche nei connotati fisici, dell'essere umano che agisce), in uno con la forte personalizzazione dei servizi, possono ridurre la percezione dei rischi.

Ciò può essere determinato anche dall'inconsapevole sottoposizione a tecniche di profilazione e alla soggezione a pratiche commerciali scorrette che incidono in modo sempre più rilevante sulla consapevolezza dell'investitore circa le conseguenze delle proprie scelte e azioni.

All'utente, dunque, dovrà essere garantito un sufficiente livello di comprensione e consapevolezza del tipo di attività che si sta svolgendo: se un servizio appare "come un videogioco", l'investitore potrebbe non essere sufficientemente consapevole del tipo di attività che si sta svolgendo, dei relativi rischi anche in termini di possibile impatto sul proprio patrimonio. Difatti, le specifiche modalità di interazione possono diminuire la comprensione dei fenomeni e dei rischi connessi, incidendo sul processo decisionale dell'utente. In primo luogo, per evitare che ciò accada, è necessario che gli intermediari agiscano sempre in piena applicazione dei principi di correttezza, buona fede e diligenza, cercando così - con ogni mezzo possibile - di sterilizzare i possibili rischi derivanti da tali specifiche vulnerabilità ulteriori<sup>54</sup>.

La personalizzazione dei servizi – che risponde anzitutto all'esigenza di fornire prodotti maggiormente in linea con le preferenze degli utenti – consente altresì di trarre vantaggio dei limiti cognitivi dei consumatori, sfruttando le vulnerabilità individuali con un approccio commerciale granulare<sup>55</sup>.

Le insidie per l'investitore potrebbero poi aumentare considerevolmente a causa della completa personalizzazione dell'esperienza (si pensi alla possibilità di fornire a ciascun individuo un consulente che sia compatibile con il proprio *background* culturale), in grado di innescare fenomeni di *familiarity bias*. Inoltre, la sensorialità dell'esperienza del metaverso (abilitata dalle interfacce aptiche) può creare situazioni inedite in cui i sensi dei clienti possono essere stimolati in modo tale da spingerli verso una determinata scelta. Si tratta di caratteristiche – peculiari dell'offerta di servizi finanziari in ambienti immersivi *phygital* – che dovranno essere prese in considerazione nei processi di *product oversight and governance* dei produttori e distributori.<sup>56</sup>

Per far fronte ai citati bisogni di tutela emergenti, i confini tra le aree presidiate dalle normative sulle pratiche commerciali scorrette, le regole di condotta, i doveri di informazione e le regole di negoziazione a distanza appaiono sempre più labili<sup>57</sup>; proprio

---

<sup>53</sup> N. Helberger et al., *Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability*, in *Journal of Consumer Policy*, 45, 2022, 175 ss.

<sup>54</sup> Sul concetto di vulnerabilità del consumatore digitale si veda F. Lupiáñez-Villanueva et al., *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation*, Final Report European Commission, aprile 2022.

<sup>55</sup> A. Davola, *Fostering Consumer Protection in the Granular Market: the Role of Rules on Consent, Misrepresentation and Fraud in Regulating Personalized Practices*, in *Technology and Regulation*, 2021, 76–86.

<sup>56</sup> EBA, *Guidelines on product oversight and governance arrangements for retail banking products*, EBA/GL/2015/18, 15 giugno 2015.

<sup>57</sup> F. Annunziata, *Towards an EU charter for the protection of end users in financial markets*, EBI Working

queste ultime sono oggetto di proposte di riforma volte ad introdurre rimedi per mitigare la vulnerabilità dell'utente in ambienti digitali sofisticati<sup>58</sup>.

Va evidenziato però come né il rafforzamento delle regole di *disclosure*, né la previsione di rimedi puramente ex post (come il diritto di recesso), paiano idonei a garantire sufficienti livelli di protezione per il cliente e a neutralizzare i rischi insiti in tali modelli di contrattazione. Questi, infatti, potrebbe comunque sperimentare un'esperienza d'uso negativa e lesiva che minerebbe la sua fiducia nel sistema.

In questo contesto, il legislatore e le autorità di vigilanza saranno quindi chiamati a valutare se i rischi posti dalla prestazione di servizi finanziari in ambiente *phygital* e basati su AI siano da considerare intollerabili e richiedano una specifica disciplina: se sia necessario delimitare le tecnologie utilizzabili, le caratteristiche degli ambienti immersivi (in relazione, ad esempio, a colori che possano sollecitare specifiche reazioni) e ai livelli di personalizzazione (e.g., vietando che gli *avatars* antropomorfi riproducano soggetti aventi la medesima etnia del cliente) in modo da evitare che le vulnerabilità del cliente possano essere sfruttate a suo sfavore. Similmente a quanto già previsto nella proposta di modifica della direttiva sui servizi finanziari conclusi a distanza, appare auspicabile limitare la possibilità per la banca di impiegare strumenti – nell'ambito della propria interfaccia online – che potrebbero distorcere o compromettere la capacità dei consumatori di prendere una decisione o una scelta libera, autonoma e informata<sup>59</sup>.

Appare ad ogni modo essenziale garantire la trasparenza sul livello di personalizzazione dell'esperienza utente e dei servizi offerti, in modo da consentire all'utente di comprendere le ragioni per cui determinati servizi gli vengono offerti nonché le peculiarità che li differenziano da quelli offerti ad altri utenti.

Quest'ultima costituirebbe un utile elemento complementare, ma certamente insufficiente come unico presidio di tutela. In altri termini, di fronte a tecnologie così avanzate, in grado di distorcere la percezione umana spingendo il consumatore ad assumere decisioni d'investimento, la mera realizzazione del principio del *caveat emptor*, con la consegna di una ricca informativa al cliente lasciando poi a quest'ultimo la scelta se concludere il contratto risulta del tutto inadeguata. Al contrario, un livello adeguato di tutela potrebbe essere ottenuto mediante una regolazione *tech-specific*, che ponga precisi limiti "tecnologici" per la conclusione di contratti finanziari in ambiente immersivo.

---

Papers Series, no. 128/2022.

<sup>58</sup> È già stata formulata una proposta sulla modifica della disciplina sulla commercializzazione a distanza dei servizi finanziari, cfr. Commissione europea, Proposta di direttiva del Parlamento europeo e del Consiglio che modifica la direttiva 2011/83/UE concernente i contratti di servizi finanziari conclusi a distanza e che abroga la direttiva 2002/65/CE, COM(2022) 204 definitivo 2022/0147 (COD), 11.5.2022.

<sup>59</sup> Potrebbe, al riguardo, risultare utile l'introduzione di strumenti per la valutazione dell'effettiva comprensione da parte del cliente delle implicazioni dell'utilizzo di determinate tecnologie (anche prevedendo effetti bloccanti, similmente a quanto avviene con il test di adeguatezza di cui alla MIFID). Tale ipotesi è stata prospettata da F. Annunziata, *Retail Investment Strategy How to boost retail investors' participation in financial markets*, Study requested by ECON Committee, giugno 2023, 7.



---

## 8. Conclusioni

8.1 L'applicazione delle tecnologie di intelligenza artificiale nell'ambito del settore finanziario ha numerose potenzialità, in grado di rendere la prestazione di servizi più efficace ed efficiente; rilevanti sono anche gli effetti positivi in termini di inclusione sociale, rendendo i servizi finanziari accessibili anche alle fasce della popolazione *underbanked*. A ciò si aggiungono rilevanti applicazioni aventi "rilevanza interna" ai fini di una efficiente organizzazione delle istituzioni finanziarie<sup>60</sup>.

Al contempo, molti e rilevanti sono i rischi derivanti dalle medesime tecnologie. E, come evidenziato, le insidie sono ben maggiori (e certamente presentano profili di specificità) nel settore finanziario rispetto all'ordinamento generalmente considerato. Tali considerazioni suggeriscono perciò che la regolazione finanziaria assuma idonee contromisure.

In primo luogo, occorre che sia garantita la governabilità dell'innovazione, anche incidendo sulla *governance* del mercato finanziario "tecnologizzato". E per fare ciò, non appare più sufficiente la regolazione basata su attività, che non tenga in debita considerazione anche le specificità dei processi. Questi ultimi sono spesso specifici in relazione alle singole tecnologie.

In tale contesto, è quindi ormai indispensabile che il legislatore disciplini specifiche applicazioni tecnologiche, perché non è indifferente il modo in cui viene svolta una certa attività: pertanto, non sarà sufficiente prevedere una disciplina "generale" per l'AI finanziaria, ma occorrerà valorizzare le specificità poste dalle sue varie applicazioni.

L'adesione fideistica al principio di neutralità tecnologica potrebbe invece pregiudicare i livelli di tutela, consentendo la proliferazione di rischi, aprendo rilevanti *vulnera* per gli utenti e per gli altri operatori del mercato.

Anche nella prospettiva della vigilanza finanziaria, un approccio tecnologicamente neutrale non appare più idoneo a ottenere i risultati che gli sono richiesti: non appare percorribile garantire la sana e prudente gestione dell'intermediario e la tutela degli investitori senza poter operare controlli intrusivi e *tech-specific*.

Come ben evidenziato dal caso d'uso "di frontiera" dei *virtual worlds*, alla vigilanza bancaria e finanziaria deve essere consentito un approccio tecnologicamente orientato che quindi calibra differenzialmente le regole e strumenti d'intervento in base alle tecnologie impiegate per fornire un servizio, riconoscendo come questi strumenti tecnologici siano in grado di caratterizzare il servizio stesso, mutandone i rischi caratteristici. Pertanto, deve essere incoraggiato l'uso degli strumenti tecnologici nel contesto della vigilanza sulle applicazioni, per operare un efficace monitoraggio sull'utilizzo, limitare gli abusi ed avere la possibilità di intervenire tempestivamente. Inoltre, potrà essere adottato l'approccio del *supervision as code*, spingendosi fino a introdurre *by design* nell'algoritmo "controlimiti". Per poter essere concretamente operative ed efficaci, regole autoeseguibili di questo tipo dovranno avere contenuto prescrittivo e non prevedere spazi di discrezionalità. Dunque, è chiaro che non ogni regola di condotta potrà essere così codificata, ma tale strategia rappresenterà comunque un utile meccanismo com-

---

<sup>60</sup> M. Pellegrini, *L'intelligenza artificiale nell'organizzazione bancaria: quali sfide per il regolatore?*, in *Rivista Trimestrale di Diritto dell'Economia*, 3, 2021, 422 ss.

plementare alle tradizionali modalità operative della vigilanza bancaria e finanziaria. Per poter ottenere tali risultati sarà in ogni caso preziosa la cooperazione tra industria e autorità di vigilanza nello sviluppo delle soluzioni più appropriate (anche utilizzando strumenti simili alle *sandboxes* regolamentari<sup>61</sup>).

8.2 Tornando all'esempio del *roboadvisor*, impiegando un siffatto strumentario *tech specific*, l'autorità di vigilanza – pur sempre cooperando con l'intermediario che faccia uso della tecnologia – potrà sincerarsi che il *roboadvisor* operi entro i confini di quanto autorizzato. Ciò consentirebbe agli utenti di godere di una tutela paragonabile – e probabilmente superiore – a quella attualmente realizzata nel contesto dei rapporti con consulenti finanziari fisici: la libertà di autodeterminazione, nonché la dignità del cliente potranno essere tutelati in modo più efficace.

La disciplina della prestazione di servizi finanziari mediante intelligenza artificiale nell'ambito di ambienti digitali immersivi potrà essere il luogo di sperimentazione per introdurre una disciplina tecnologicamente specifica, finalizzata a limitare possibili abusi da parte dell'intermediario e a scongiurare gli effetti pregiudizievoli delle sue vulnerabilità.

L'esigenza di introdurre regole di questo tipo nel settore bancario e finanziario è più pressante che in altri settori, proprio per l'esistenza della necessità di salvaguardare – oltre alla libera formazione della volontà del consumatore – altri interessi di rilievo pubblicistico, in quanto il venire meno della fiducia dell'utente non sarebbe limitata ad uno specifico intermediario (o al solo “metaverso bancario”), ma avrebbe con ogni probabilità ricadute sulla fiducia nel sistema bancario e finanziario nel suo complesso.

---

<sup>61</sup> S. Ranchordas - V. Vinci, *Regulatory Sandboxes and Innovation-friendly Regulation: Between Collaboration and Capture*, in *Italian Journal of Public Law*, 16(1), 2024, 107 ss.