BANCA D'ITALIA
EUROSISTEMA

Un viaggio nel futuro del sistema finanziario

Intervento di Chiara Scotti
Vice Direttrice Generale della Banca d'Italia

Congresso Annuale ASSIOM FOREX
Torino, 14-15 febbraio 2025

1. Introduzione

Buongiorno a tutte e a tutti. In primo luogo, desidero ringraziare gli organizzatori per avermi invitata a questa sessione dal titolo '*Intelligenza artificiale e transizione digitale del sistema finanziario*'.

La digitalizzazione – intesa in senso ampio per includere, tra l'altro, lo sviluppo di tecnologie a registro distribuito (DLT), criptoattività e intelligenza artificiale (IA) – sta trasformando il sistema finanziario 'tradizionale'[1]. Nuove opportunità emergono in ambito finanziario[2], dall'aumento dell'efficienza degli intermediari, al miglioramento dei servizi per la clientela, alla crescita dell'inclusione finanziaria. Tuttavia, non possiamo ignorare le sfide sempre maggiori che la digitalizzazione porta con sé. In particolare, le banche centrali e le autorità di vigilanza sono chiamate a individuare le potenziali minacce per la sana e prudente gestione degli intermediari, la stabilità complessiva del sistema finanziario, il regolare funzionamento del sistema dei pagamenti e la tutela dei consumatori.

Nel mio intervento rifletterò su questi cambiamenti e sulle loro possibili evoluzioni. Faremo insieme un viaggio nel sistema finanziario del futuro, attraverso tre itinerari che ci permetteranno di individuare le possibili sfide e le soluzioni potenzialmente più adeguate per conciliare stabilità finanziaria con innovazione ed efficienza. Richiamerò quindi le modalità con le quali l'Unione europea (UE) sta affrontando queste sfide attraverso la revisione del quadro regolamentare.

---

1 Petralia et al. (2019), *Banking Disrupted? Financial Intermediation in an Era of Transformational Technology*, Geneva Reports on the World Economy; Beck et al. (2022), *Will video kill the radio star? Digitalisation and the future of banking (europa.eu)*, Reports of the ESRB Advisory Scientific Committee N. 12; Fuster et al. (2019), *The Role of Technology in Mortgage Lending*, Review of Financial Studies, Vol. 32, Issue 5, pp. 1854-1899; Buchak et al. (2018), *Fintech, Regulatory Arbitrage, and the Rise of Shadow Banks*, Journal of Financial Economics, Vol. 130, pp. 453-483.

2 Cevik (2024), *Promise (Un)kept? Fintech and Financial Inclusion*, IMF Working Paper; Baba et al. (2020), *Fintech in Europe: Promises and Threats*, IMF Working Paper.

2. Possibili scenari derivanti dalla digitalizzazione del sistema finanziario

In un periodo di grandi cambiamenti politici, culturali e tecnologici, alcune tendenze di lungo periodo (i cosiddetti *mega-trends*) potrebbero rivoluzionare, ancor più di quanto stia già accadendo, le nostre vite, inclusi i modi in cui paghiamo, investiamo e gestiamo aziende. Vorrei metterne in evidenza tre in particolare: il crescente ruolo delle cosiddette *Big Tech* nella intermediazione finanziaria, la diffusione delle criptoattività e delle attività finanziarie digitali, le grandi promesse derivanti dallo sviluppo dell'intelligenza artificiale.

Questi *trend* non si sviluppano in isolamento, ma possono rinforzarsi a vicenda. Ad esempio, il potere di mercato che le *Big Tech* esercitano rispetto agli intermediari finanziari tradizionali può risultare amplificato dalle economie di scala proprie delle tecnologie digitali – pensiamo alla potenza di calcolo necessaria per gestire infrastrutture *cloud* ed elaborare l'enorme volume di dati su cui si basano i modelli di intelligenza artificiale.

Si tratta inoltre di *trend* che sono strettamente legati ad altri sviluppi. Il *quantum computing*, ad esempio, promette di accelerare la risoluzione di problemi complessi in campi come la biologia, la chimica e la finanza (si pensi all'ottimizzazione dei portafogli)[3]. In aggiunta, non dobbiamo dimenticare gli effetti delle scelte politiche di alcuni grandi paesi e le tensioni internazionali che ne derivano: accordi commerciali e finanziari, princìpi di cooperazione in tema di regolamentazione e collaborazioni tra pubblico e privato, o tra nazioni, possono essere messi in discussione improvvisamente.

Il contesto in cui noi – come persone, organizzazioni private e istituzioni pubbliche – agiamo e prendiamo decisioni è sempre più caratterizzato dalla complessità delle interconnessioni in gioco, dalle forti incertezze nelle previsioni, dai dubbi circa l'accuratezza delle informazioni e dall'estrema volatilità del contesto di riferimento. Si tratta di problematiche che, seppure non esclusivamente associate agli sviluppi tecnologici, sono acuite da questi ultimi.

Fare previsioni precise su ciò che accadrà nei prossimi anni è impossibile. Negli anni '80 si pensava che nessuno avrebbe mai avuto bisogno di più di 640 KB di memoria sul proprio *personal computer*. Oggi, il mio telefono cellulare ha 256 GB di memoria ed è quasi insufficiente. Ma se non possiamo prevedere con precisione il futuro e dobbiamo comunque prendere decisioni, quale strategia dovremmo adottare?

Anzitutto, è necessario utilizzare un approccio sistemico. Come già accennato, i cambiamenti avvengono in diversi ambiti ed è necessario mantenere una visuale ampia, che abbracci le dimensioni economiche, politiche, tecnologiche, sociali e ambientali. È altrettanto importante avere una prospettiva di medio termine. In un contesto che evolve rapidamente, non è realistico – e forse nemmeno desiderabile – reagire a ogni singolo cambiamento; al tempo stesso, non possiamo aspettare che la tempesta si calmi, perché sarebbe troppo tardi. Dobbiamo quindi sfidare la logica di prendere decisioni basate sul presente o sul futuro probabile. L'obiettivo dovrebbe essere quello di sviluppare strategie robuste e flessibili che, basandosi su una vasta gamma di informazioni, siano

---

[3] Il *quantum computing* rappresenta una delle tecnologie più promettenti e rivoluzionarie degli ultimi anni. La sua potenza di calcolo potrebbe trasformare molti settori, incluso quello finanziario.

adatte ad affrontare non solo lo scenario più probabile, ma anche una serie di possibili scenari alternativi. Lo scopo ultimo è permettere di anticipare le azioni necessarie per gestire i rischi e ridurre l'impatto degli eventi avversi[4].

Per calare queste considerazioni nella discussione odierna, penso che sia utile delineare alcuni scenari futuri – del tutto ipotetici – che possano stimolare una riflessione sulle prospettive del sistema finanziario e sul ruolo che regolatori e supervisori dovrebbero svolgere per promuovere le opportunità legate all'innovazione, mitigando al contempo i rischi per la stabilità finanziaria.

Insieme ad alcuni colleghi, con esperienze professionali e formative diverse[5], abbiamo provato a ragionare sulle prospettive offerte dalla digitalizzazione, incluse le tecnologie DLT e il trasferimento di valori e diritti rappresentati digitalmente, che per semplicità indicherò nel seguito come criptoattività[6].

Vi propongo quindi tre scenari, tre alternative di viaggio nel futuro del sistema finanziario[7].

Itinerario a: Intermediari moderni e digitalizzati

In un primo scenario, gli intermediari finanziari tradizionali svilupperebbero internamente le tecnologie necessarie per reagire all'attuale *trend* di esternalizzazione (come nel caso del *cloud* e dell'IA), anche approfittando di un eventuale fallimento del modello di *business* che ha finora favorito lo sviluppo delle *Big Tech*. Gli intermediari tradizionali acquisirebbero il *know-how* necessario per stare al passo con l'evoluzione tecnologica e per guidare l'adozione dell'innovazione, adattandosi dinamicamente alle esigenze del mercato e dei consumatori. Inoltre, svilupperebbero piattaforme e soluzioni tecnologiche in grado di competere con quelle delle *Big Tech* nel fornire servizi e prodotti finanziari, limitando l'esternalizzazione unicamente a operatori specializzati all'interno del settore finanziario. Le relazioni con i clienti rimarrebbero sotto il loro controllo e i rischi operativi

---

4 L'idea prende spunto dalla *Strategic Foresight*, una tecnica di pianificazione che amplia le prospettive di analisi attraverso l'esplorazione sistematica di una pluralità di scenari futuri plausibili, elaborati con il contributo di varie categorie di *stakeholders*. Gli scenari plausibili sono quelli che pensiamo potrebbero verificarsi in base alle conoscenze attuali riguardo al mondo, a determinate dinamiche, processi, leggi della fisica o tecnologie, senza considerare quanto siano probabili. Un esempio di esplorazione di scenari in linea con la metodologia dello *Strategic Foresight* è rappresentato dall'analisi contenuta in D. Acemoglu (2025), *The real threat to American prosperity*, Financial Times.

5 Un particolare ringraziamento ad Andrea Pilati, Francesco Cannata, Luca Serafini, Marcello Bofondi, Giovanni Carletti, Alessio De Vincenzo, Emilia Bonaccorsi Di Patti, Sabina Marchetti, Gabriele Marcelli, Andrea Mele e Anna Maria Viscardi.

6 Per completezza, si segnala che il legislatore europeo ha recentemente introdotto – con il Regolamento (UE) 2023/1114 (c.d. Regolamento MiCAR) – una definizione di "*cripto-attività*", che include ogni "*rappresentazione digitale di un valore o di un diritto che può essere trasferito e memorizzato elettronicamente, utilizzando la tecnologia a registro distribuito o una tecnologia analoga*". Si fa altresì presente che i diritti e gli obblighi introdotti dal medesimo Regolamento sono invece applicabili alle sole "*cripto-attività*" diverse da quelle classificabili come versioni digitali di prodotti o strumenti finanziari già regolati dal diritto europeo, come chiarito nell'ambito di applicazione dello stesso Regolamento MiCAR (*Markets in Crypto-Assets Regulation*).

7 Si tratta di un aggiornamento e dello sviluppo di alcuni scenari presentati dalla Basel Committee on Banking Supervision (2018), *Sound Practices: implications of fintech developments for banks and bank supervisors*.

(inclusi quelli informatici) verrebbero gestiti principalmente all'interno del settore finanziario. In sintesi, gli intermediari finanziari acquisirebbero un ampio controllo sulla componente tecnologica, seppur non necessariamente esclusivo[8].

Itinerario b: Intermediari di servizio (Banking-as-a-Service)

In un secondo scenario, la realizzazione e la gestione delle componenti tecnologiche verrebbero sviluppati dalle *Big Tech*, che fornirebbero soluzioni avanzate e canali digitali per distribuire prodotti finanziari. Esternalizzando buona parte della catena del valore dei servizi finanziari, le banche vedrebbero aumentare la propria dipendenza da fornitori di tecnologia e da prestatori di servizi per le criptoattività e ridurre il proprio vantaggio competitivo derivante dall'accesso ai dati e dal controllo dei processi. D'altra parte, l'interazione tra banche e *Big Tech*, ad esempio mediante *joint ventures*, potrebbe favorire lo sviluppo di soluzioni di pagamento innovative che utilizzano criptoattività, aumentando le interconnessioni tra mercati digitali e sistema finanziario tradizionale[9, 10].

Itinerario c: Sistema finanziario decentralizzato

Un terzo scenario vedrebbe l'ecosistema *crypto* divenire *mainstream* e la *Decentralised Finance* (DeFi) diventare il modo principale di utilizzare i servizi finanziari. Le criptoattività offerte al pubblico da soggetti privati (non finanziari) assumerebbero un ruolo centrale, permettendo trasferimenti di valore e pagamenti per mezzo di piattaforme DLT pubbliche/*permissionless* senza l'intervento delle banche tradizionali[11]. Si potrebbero immaginare

---

8 Questo primo scenario richiederebbe un livello di investimenti da parte delle banche difficilmente compatibile con la redditività registrata negli ultimi trent'anni, specie se confrontata con quella delle *Big Tech*, che già godono di un ruolo tecnologicamente dominante. Sul tema, Klein, P.O. e Weill, L. (2022), Bank profitability and economic growth, The Quarterly Review of Economics and Finance, Vol. 84, pp. 183-199; Di Vito et al. (2023), *Understanding the profitability gap between euro area and US global systemically important banks*, ECB Occasional Paper n. 327. D'altra parte, non si può escludere uno sviluppo alternativo a quanto finora osservato, considerando ad esempio l'ipotesi in cui le *Big Tech* – che hanno investito in maniera ingente sull'IA – non dovessero ottenere progressi significativi in termini di innovazione o crescita della produttività nel medio termine. In questo senso, si veda anche *Op.cit.* D. Acemoglu (2025).

9 Questo scenario pare essere il più verosimile, anche se è difficile quantificarne il "grado di intensità" a regime. La variabile IA, inoltre, aggiunge ulteriori margini di incertezza in quanto il grado di innovazione e l'intensità di utilizzo possono dar luogo a ulteriori varianti che non è facile oggi prevedere. Sul tema, Aldasoro, Gambacorta, Korinek, Shreeti, Stein (2024), *Intelligent financial system: how AI is transforming finance*, BIS Working Papers, n. 1194.

10 Si veda per esempio il caso di Silvergate Bank che, alla fine del 2022, risentì della crisi di questi mercati innescata dal crollo della piattaforma FTX negli Stati Uniti. Sul tema, Azar et al. (2024), *The Financial Stability Implications of Digital Assets*, Federal Reserve Bank of New York, Economic Policy Review, Vol. 30, n. 2.

11 Questo scenario è forse meno probabile dei precedenti, anche perché presuppone soluzioni efficaci per affrontare i problemi di sicurezza associati alla DeFi, rivelatasi particolarmente vulnerabile a truffe e attacchi informatici. Sono un esempio di criticità di *cybersecurity* i casi di Poly Network (cfr. https://research.kudelskisecurity.com/2021/08/12/the-poly-network-hack-explained/) e Wormhole (cfr. https://www.chainalysis.com/blog/wormhole-hack-february-2022/), che mostrano come, sfruttando debolezze nel sistema degli *smart contract* o dei meccanismi di interoperabilità (e.g. *bridge*, oracoli), sia possibile condurre con successo attacchi informatici di cui spesso è difficile individuare i responsabili, a causa della natura decentralizzata di tali infrastrutture. Tuttavia, sviluppi nelle tecnologie criptografiche, come le *Zero Knowledge Proofs*, potrebbero seguire un andamento non lineare, determinando progressi in tempi più rapidi del previsto.

due versioni di questo scenario. Nella versione più estrema, non ci sarebbero intermediari e dunque le transazioni finanziarie avverrebbero tra utenti finali, tramite *smart contract* che garantirebbero il contatto diretto tra soggetti con esigenze diverse[12]. Nella versione meno radicale, la DeFi resterebbe la principale modalità di mediazione finanziaria, ma gli intermediari potrebbero continuare a esistere in una forma adattata, combinando tecnologie decentralizzate e centralizzate per garantire sicurezza e servizi personalizzati.

3. Quali sono gli *shock* e le vulnerabilità critici per un sistema finanziario in divenire e come farvi fronte?

Sono certa che ciascuno di voi avrà già cominciato a pensare a uno scenario alternativo a quelli da me descritti. Come detto, questi scenari non sono previsioni di ciò che accadrà, ma semplici narrazioni da utilizzare come metodo esplorativo per anticipare e prepararsi a sfide e opportunità future.

Per una banca centrale, in questi scenari è importante distinguere tra *shock* e vulnerabilità. Gli *shock* sono eventi improvvisi e per definizione difficili da prevedere. Le vulnerabilità sono invece quegli aspetti e caratteristiche del sistema finanziario e dei suoi operatori che potrebbero amplificare l'impatto di uno *shock* qualora si materializzasse. Le banche centrali possono contribuire a contenere le vulnerabilità attraverso la loro attività di supervisione e vigilanza[13]. Secondo le teorie correnti, le vulnerabilità del settore finanziario sono generalmente riconducibili ai rischi di sopravvalutazione delle attività (le cosiddette *valuation pressures*), a livelli elevati di indebitamento di famiglie e imprese, alla leva finanziaria, al rischio di *funding* degli intermediari e alla elevata interconnessione tra istituzioni. Chiaramente i tipi e le fonti di potenziali *shock* e vulnerabilità potrebbero evolvere nel tempo. Per questo le banche centrali si avvalgono di ricercatori di frontiera, ispettori esperti e analisti di vigilanza che studiano e individuano nuove fragilità e sviluppi del sistema finanziario.

Individuare scenari futuri aiuta a capire gli effetti che determinati *shock* potrebbero avere sul sistema finanziario e come essi potrebbero interagire con le vulnerabilità esistenti o emergenti. L'obiettivo è anticipare azioni di presidio e sviluppare strategie resilienti e flessibili, ma al tempo stesso semplici e stabili, affinché una banca centrale, nel ruolo di regolatore e supervisore, possa conciliare la solidità finanziaria con l'innovazione e l'efficienza.

Cosa emerge dagli scenari?

Quali sono quindi gli elementi più rilevanti che caratterizzano gli scenari proposti e che potrebbero introdurre nuove vulnerabilità nel settore finanziario o modificare in modo significativo quelle esistenti? Mi limiterò a discuterne due.

---

12 Ad esempio, i *liquidity pool* abbinano prestatori e mutuatari allineando liquidità, rischio di credito e appetito per il rischio. I fondi sono detenuti in *unhosted wallets*, e tutto è gestito su *blockchain* mantenute da sviluppatori *open-source*. Questo scenario è molto improbabile, al momento, per vari motivi tra cui l'esposizione costante degli utenti a truffe e *hack* nella DeFi. Sul tema, Schar (2022), *DeFi's Promise and Pitfalls*, IMF Finance and Development Magazine.

13 Adrian, Covitz, Liang (2015), *Financial stability monitoring*, Annual Review of Financial Economics, Vol. 7, pp. 357-395.

Un primo elemento riguarda il fatto che, con la ridefinizione dei mercati finanziari e dell'intermediazione bancaria, potrebbero emergere vulnerabilità (in parte nuove) legate a rischi operativi e cibernetici[14], all'uso improprio di informazioni, a strutture di *governance* decentralizzate[15]. Operatori non finanziari con modelli di *business* innovativi e complessi, criptoattività e tecnologie decentralizzate non necessariamente si conformano ai princìpi di informazione, tutela, correttezza dei mercati. Al contempo, potrebbero anche presentarsi vulnerabilità 'tradizionali' in nuovi contesti, come il rischio di *funding* o le valutazioni eccessive delle criptoattività.

Un secondo elemento, collegato al primo, è la crescente complessità del sistema finanziario tradizionale e le sue interconnessioni con fattori esterni, legati agli sviluppi dell'IA, delle criptoattività, e dei sistemi decentralizzati. Ad esempio, un drastico calo del prezzo di Bitcoin potrebbe spingere gli investitori con leva a vendere, amplificando la discesa iniziale del prezzo. Allo stesso modo, se un intermediario dovesse subire perdite in criptoattività, i suoi creditori potrebbero ritirare fondi su larga scala, costringendo l'intermediario a vendere anche altri *asset,* amplificando il calo iniziale del prezzo e generando potenziali *spillovers* verso altre attività[16].

In uno scenario di limitate interconnessioni tra mercati digitali e tradizionali, il contributo delle criptoattività al rischio sistemico sarebbe contenuto. Questo è lo scenario in cui abbiamo vissuto fino ad ora, nel quale la fornitura diretta di servizi finanziari da parte del sistema *crypto* all'economia reale appare moderata. Tuttavia, con l'evolversi della digitalizzazione, le interconnessioni tra l'ecosistema *crypto* e il sistema finanziario tradizionale cresceranno, sia in uno scenario dominato dalle *Big Tech*, attraverso strumenti *in-platform*, sia nell'ipotesi di servizi finanziari completamente decentralizzati. Pertanto, all'aumentare delle interconnessioni, le fragilità dell'ecosistema *crypto* potrebbero divenire destabilizzanti, specialmente se dovessero acquisire una rilevanza sistemica

---

14 Ad esempio, i computer quantistici potrebbero compromettere gli attuali algoritmi di crittografia che proteggono i dati sensibili. Il G7 *Cyber Expert Group* ha di recente sottolineato l'urgenza di affrontare questa sfida, raccomandando azioni concrete per rendere il sistema finanziario resistente agli attacchi quantistici. È fondamentale che le istituzioni finanziarie, i regolatori e i fornitori di servizi tecnologici collaborino per sviluppare e implementare soluzioni di *cybersecurity post-quantum*. In particolare, è auspicabile l'adozione di protocolli cripto-agili (i.e. che consentono di modificare le primitive crittografiche, senza dover modificare completamente l'infrastruttura dei sistemi) in modo da poter, in prospettiva, adottare standard crittografici *post quantum* – quali quelli recentemente standardizzati dal NIST (cfr. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization).

15 I modelli di *governance* decentralizzata si applicano tipicamente alle DLT *permissionless*, in cui la gestione ordinaria del registro avviene attraverso automatismi codificati nel protocollo di consenso. I cambiamenti strutturali a tali regole vengono decisi attribuendo i diritti di voto secondo modalità che possono manifestare rischi legati ad asimmetrie informative e comportamenti opportunistici. La concentrazione dei diritti di voto e la difficoltà di applicare normative tradizionali in contesti decentralizzati possono compromettere l'efficienza del mercato e la tutela degli investitori. Inoltre, l'assenza di un'autorità centrale identificabile complica l'*enforcement* delle regole e la gestione dei conflitti, aumentando l'incertezza giuridica e operativa. Cfr. per approfondimenti Gola et al. (2023), *La governance delle blockchain e di sistemi basati sulla tecnologia dei registri distribuiti*, Banca d'Italia, Questioni di Economia e Finanza (Occasional Papers) n. 773.

16 Sul tema delle interconnessioni tra il sistema finanziario tradizionale e l'ecosistema *crypto*, si vedano per esempio i casi di Signature Bank e Silvergate Bank, illustrati nel dettaglio in *Op. cit*. Azar et al. (2024).

quei *crypto-assets* privi di valore intrinseco in quanto non ancorati ad alcuna attività dell'economia reale o finanziaria [17, 18].

Quali potrebbero essere le risposte per far fronte a tali vulnerabilità?

È evidente che le vulnerabilità descritte richiedano una maggior cooperazione tra autorità competenti in diversi settori (non solo quello finanziario) al fine di salvaguardare sia gli aspetti tipici della vigilanza prudenziale, sia quelli altrettanto importanti per il corretto funzionamento dei mercati e il rispetto dei diritti delle persone, quali l'integrità, la concorrenza e la tutela della *privacy* e della sicurezza dei dati.

Considerando la dimensione globale delle grandi aziende tecnologiche e dei modelli di *governance* decentrati, la cooperazione e il coordinamento dovrebbero includere la dimensione internazionale, un aspetto che purtroppo potrebbe essere messo in discussione visti alcuni orientamenti recenti.

Per affrontare i rischi emergenti potrebbe inoltre essere preferibile un metodo articolato e flessibile, che consideri sia le attività svolte sia le caratteristiche del soggetto che le svolge. In tale contesto, un approccio regolamentare di tipo "*activity-based*", che fa riferimento alla natura delle attività svolte a prescindere dal soggetto che le svolge, potrebbe essere più efficace. Un approccio "*entity-based*", invece, potrebbe presidiare meglio i rischi derivanti dalla combinazione di diverse attività e servizi in capo allo stesso soggetto (ad esempio, la trasformazione delle scadenze e il rischio di leva e di liquidità tipici delle banche che raccolgono depositi ed erogano finanziamenti)[19].

Non è tuttavia sufficiente includere nuovi soggetti (approccio *entity-based*) o nuove attività (approccio *activity-based*) nell'orbita del solo supervisore finanziario. Quest'ultimo potrebbe non avere i poteri, le competenze e gli strumenti adeguati ed efficaci per vigilare su tutti i rischi che emergono da modelli di *business* innovativi. Non pare infatti né realistico né auspicabile affrontare le sfide poste dalla digitalizzazione solo ampliando continuamente il perimetro della regolamentazione e applicando tecniche regolamentari e di supervisione tipiche della vigilanza sugli intermediari finanziari.

Per questo è necessaria una stretta collaborazione tra il settore pubblico e quello privato, per definire standard condivisi, promuovere tecnologie finanziarie sicure e affidabili, e favorire l'innovazione. Questa sinergia è fondamentale per proteggere

---

17 Si fa in particolare riferimento alle c.d. *unbacked crypto-assets*, quali ad esempio Bitcoin, criptoattività prive di un meccanismo di stabilizzazione che ne ancori il valore a un'attività di riferimento, oppure le cc.dd. "*stablecoins* algoritmiche", il cui meccanismo di stabilizzazione è basato su un algoritmo che ne condiziona la domanda e l'offerta sul mercato, o le *meme coins*.

18 *Op. cit.* Azar et al. (2024).

19 Carstens et al. (2021), *Regulating big techs in finance*, BIS Bulletin n. 45; Borio et al. (2022); *Entity-based vs activity-based regulation: a framework and applications to traditional financial firms and big techs*, BIS Occasional Paper n. 19.

i consumatori, assicurare la stabilità del sistema finanziario e garantire che il cambiamento avvenga in modo sicuro, etico e sostenibile. Per la Banca d'Italia, un esempio di questo approccio è l'offerta integrata di facilitatori di innovazione volta a favorire il dialogo con il mercato e a sostenere lo sviluppo di progetti fintech (tra gli altri, Canale Fintech e Milano Hub)[20].

4. La risposta delle Autorità Europee: dove siamo arrivati?

La scelta del legislatore europeo di lanciare la c.d. *Digital Finance Strategy* nel 2020 mira ad aumentare la competitività dell'UE nel settore della finanza digitale, senza trascurare la tutela dei consumatori e la stabilità finanziaria. L'assenza di un intervento coordinato a livello europeo aveva inizialmente portato a soluzioni nazionali frammentate (con sovrapposizioni, incongruenze e costi elevati), che trovavano un limite importante nella natura transfrontaliera dei rischi, lasciandoli in parte non rilevati o generando possibili interferenze tra diverse autorità nazionali.

Una prima misura chiave della *Digital Finance Strategy* è il *Digital Operational Resilience Act* (DORA)[21], che stabilisce requisiti uniformi per la sicurezza delle reti e dei sistemi informativi degli operatori del settore finanziario, nonché per i soggetti terzi che forniscono loro servizi informatici (tra cui le *Big Tech*). In base a DORA, i fornitori di tali servizi devono accrescere la loro resilienza a fronte di tutti i rischi informatici, mentre gli intermediari finanziari devono rispettare standard rigorosi per prevenire e limitare l'impatto di eventuali incidenti. DORA stabilisce anche un quadro di vigilanza specifico per i fornitori di servizi di *cloud computing* agli intermediari finanziari.

---

20 In considerazione della complessità delle sfide, la Banca d'Italia sta inoltre continuando a investire sul suo ruolo di interlocutore con il mercato, dialogando con gli intermediari tradizionali e i nuovi operatori riguardo alle opportunità e ai rischi derivanti dalle attività innovative, e segnalando loro gli aspetti sui quali rafforzare i presidi volti alla mitigazione dei predetti rischi in vista dell'applicazione delle nuove normative. Ad esempio, in vista dell'entrata in vigore del Regolamento DORA (*Digital Operational Resilience Act*), la Banca d'Italia ha pubblicato due Comunicazioni rivolte al mercato, con l'obiettivo di: (***i***) sollecitare gli intermediari a condurre un'autovalutazione dei propri sistemi di gestione dei rischi informatici, con particolare attenzione alla prevenzione delle violazioni della riservatezza dei dati causate sia da attacchi malevoli sia da accessi non autorizzati da parte del personale (Comunicazione del 23 dicembre 2024); (***ii***) richiamare l'attenzione degli intermediari sui principali aspetti applicativi del Regolamento. In particolare, con riguardo: alla collocazione, nel rispetto dei princìpi di proporzionalità e di neutralità organizzativa, della funzione deputata al controllo dei rischi informatici; alle modalità di segnalazione dei gravi incidenti informatici e delle minacce significative; allo svolgimento di test avanzati di *cybersicurezza* basati sulla metodologia TIBER-IT, che per alcuni intermediari divengono obbligatori e i cui risultati saranno incorporati nei processi di supervisione (Comunicazione del 30 dicembre 2024). Inoltre, con riferimento a MiCAR, la Banca d'Italia è più volte intervenuta (cfr. nota 29 *infra*) per segnalare agli intermediari vigilati e a chi opera a vario titolo negli ecosistemi decentralizzati, anche come utente, i rischi connessi all'uso di tali tecnologie nella finanza e, in particolare, alle attività e ai servizi relativi alle criptoattività (e.g. custodia, scambio, servizi di pagamento).

21 Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario.

Altro passo egualmente importante è stato l'approvazione del *Markets in Crypto-Assets Regulation* (MiCAR)[22], che ha lo scopo di assicurare un livello adeguato di tutela per i consumatori, garantire l'integrità del mercato e salvaguardare la stabilità finanziaria. MiCAR pone quindi le premesse affinché le iniziative nel settore *crypto* siano in grado di combinare innovazione tecnologica, sicurezza, guadagni in efficienza e benefici per i clienti.

Con riferimento all'IA, il suo impiego nel settore finanziario è oggi parzialmente disciplinato da linee guida e princìpi di *governance*[23]. Tra questi vi sono le disposizioni dell'*AI Act*[24], che vedranno le autorità di vigilanza concentrarsi sui sistemi di IA utilizzati da banche e assicurazioni per assumere decisioni suscettibili di influenzare taluni profili di tutela della clientela[25].

La *Digital Finance Strategy* rappresenta un primo tentativo di adattare il quadro normativo e di supervisione europeo al nuovo ecosistema finanziario, applicando il principio di neutralità tecnologica e confermando un approccio *risk-based*. In questa prospettiva, il legislatore europeo espande l'ambito della regolamentazione finanziaria oltre i confini tradizionali, includendo nel perimetro regolamentare anche soggetti diversi dagli intermediari finanziari, come i *third-party service providers* in DORA e gli emittenti di *stablecoins* e i fornitori di servizi per le criptoattività (c.d. CASP) in MiCAR.

Nel fare ciò, tuttavia, si sono seguiti approcci diversi, coerentemente con la necessità, precedentemente indicata, di adattare gli strumenti alle situazioni concrete: mentre DORA si basa su un approccio essenzialmente "*activity-based*", concentrandosi sulla gestione del rischio ICT nel settore finanziario europeo, MiCAR si fonda su princìpi di natura "*entity-based*", applicando i presidi a nuove categorie di intermediari. Entrambi gli interventi normativi considerano con attenzione l'aspetto multinazionale degli operatori coinvolti, introducendo forme di cooperazione rafforzata tra le autorità di vigilanza a livello europeo[26].

---

22 Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio del 31 maggio 2023 relativo ai mercati in criptoattività. Il MiCAR disciplina tre categorie di criptoattività: (***i***) *asset-referenced tokens* (ART); (***ii***) *e-money tokens* (EMT), entrambi riconducibili alla nozione di c.d. "*stablecoins*" sebbene differenti in termini di sottostante e diritti attribuiti al possessore; (***iii***) criptoattività diverse dalle precedenti (c.d. *crypto-assets "other than"*); queste ultime rappresentano una categoria "residuale" individuata per differenza rispetto ad ART ed EMT, in modo da rendere la disciplina "*future proof*", in grado cioè di applicarsi anche a possibili sviluppi di nuove criptoattività.

23 Si vedano ad esempio le linee guida dell'EBA e dell'EIOPA per i settori bancario e assicurativo, rispettivamente.

24 Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 relativo alle regole armonizzate sull'intelligenza artificiale.

25 Con riferimento ad alcuni rischi emergenti che potrebbero scaturire dall'utilizzo di IA, cfr. C. Biancotti, C. Camassa, A. Coletta, O. Giudice, A. Glielmo, *Chat Bankman-Fried? An Exploration of LLM Alignment in Finance*, in corso di pubblicazione, Banca d'Italia, Collana Mercati, Infrastrutture e Sistemi di Pagamento.

26 Nel caso di MiCAR, ad esempio, sono stati introdotti appositi collegi di supervisori – con funzione consultiva – per la vigilanza degli "*stablecoins*" (e.g. ART e EMT) considerati significativi in base a specifici criteri dimensionali. Tali collegi sono istituiti e presieduti dall'EBA, a cui sono attribuiti i compiti di supervisione sugli emittenti di *stablecoins* significativi, e sono composti da EBA, ESMA, autorità nazionale *home* dell'emittente, autorità dei CASP che prestano servizi rilevanti in relazione a detto *stablecoin*, BCE o altra banca centrale nel caso in cui lo *stablecoin* faccia riferimento a valute UE diverse dall'euro, nonché da altre autorità di vigilanza di Stati terzi.

In linea con questa diversità di approccio, la regolamentazione europea considera l'IA come uno strumento, anziché un prodotto, e distingue le sue applicazioni in base ai rischi. Ad esempio, sono ritenuti "ad alto rischio" i sistemi con una piena autonomia decisionale quando svolgono attività che possono compromettere diritti fondamentali[27]. In altre parole, l'utilizzo dell'IA deve seguire linee guida e princìpi generali per assecondare le evoluzioni tecnologiche e sfruttarne la versatilità, senza una definizione rigida e statica della tecnologia stessa in qualità di prodotto finale.

Tuttavia, alcune delle sfide poste dalla digitalizzazione rimangono aperte e su queste sarà necessario continuare a lavorare.

DORA, per esempio, attribuisce alle autorità competenti poteri di supervisione applicabili solo ai fornitori "critici" e pertanto – in alcune giurisdizioni – gli operatori medi e piccoli potrebbero rimanere fuori dal perimetro regolamentare[28]. Non viene inoltre affrontato il problema della concentrazione eccessiva dei fornitori (ad esempio le *Big Tech*).

Per quanto riguarda MiCAR, per i *cryptoassets* c.d. "*other than*" è previsto soltanto un regime "*light*" di mera notifica, condotta e trasparenza a favore degli investitori. A ciò si aggiungono le criticità derivanti dall'impossibilità di applicare i presidi c.d. "*entity-based*" a modelli puramente decentralizzati, a fronte dei quali l'autorità di vigilanza non riesce ad individuare un destinatario degli obblighi.

L'*AI Act*, infine, non copre rischi di carattere finanziario. La futura declinazione di eventuali requisiti normativi e prudenziali nel settore, quindi, necessiterà di un elevato grado di flessibilità, per consentire un adattamento dinamico alle rapide evoluzioni sia della tecnologia sia dell'industria che la sviluppa.

Conclusioni

L'intreccio sempre più stretto tra finanza, tecnologia e digitalizzazione delle attività è ormai una realtà. Gli sviluppi non ci devono cogliere impreparati. In questo contesto, due fattori sono cruciali per gestire possibili *shock* e vulnerabilità: la capacità delle autorità di intercettare i cambiamenti, anche attraverso un dialogo cooperativo con gli intermediari e gli altri attori coinvolti, e la rapidità nel rispondere alle nuove sfide ed opportunità. Gli interventi già adottati nell'ambito della *Digital Finance Strategy* europea e le iniziative in via di attuazione rappresentano passi significativi in questa direzione. In un contesto che cambia molto velocemente, definire ruoli e responsabilità, come fatto con gli interventi recenti a livello sia europeo sia nazionale, è un risultato importante.

Dobbiamo tuttavia fare attenzione a non creare un quadro regolamentare troppo complesso e difficilmente interpretabile. Una maggior semplicità non può mettere a rischio la stabilità finanziaria, il corretto funzionamento dei mercati e il rispetto dei diritti delle

---

27 Cfr. Art. 6(3) del Regolamento (UE) 2024/1689.

28 In Italia si può continuare a far affidamento, come negli ultimi anni, su un quadro normativo che già attribuisce all'autorità competente alcuni poteri anche sui fornitori più piccoli.

persone. È necessario proteggere i consumatori da frodi e abusi, rendendoli innanzitutto consapevoli che taluni servizi o attività sono particolarmente rischiosi[29] e assicurare che il sistema finanziario rimanga resiliente in un contesto in continua evoluzione. Un compito che potrebbe complicarsi alla luce dei recenti orientamenti americani, particolarmente in materia di criptoattività, data la dimensione multinazionale del fenomeno.

Definire standard condivisi, promuovere la ricerca, sviluppare competenze specializzate e favorire la stretta collaborazione tra settore pubblico e privato sono elementi essenziali per garantire che le nuove tecnologie siano sviluppate secondo logiche sostenibili, supportando attività e modelli di *business* economicamente validi e aderendo a princìpi etici di responsabilità sociale.

[29] Ad esempio, con riferimento alle criptoattività, occorre considerare che alcune sono completamente prive di valore intrinseco (c.d. *unbacked crypto-assets*), non sono assistite da alcun diritto di rimborso e, in via generale, non possono essere considerate idonee a svolgere una funzione di pagamento in virtù della loro natura altamente rischiosa. Sul tema la Banca d'Italia è più volte intervenuta per segnalare agli intermediari vigilati e a chi opera a vario titolo negli ecosistemi decentralizzati, anche come utente, i rischi connessi all'uso di tali tecnologie nella finanza e, in particolare, alle attività e ai servizi relativi alle criptoattività (e.g. custodia, scambio, servizi di pagamento). Si vedano, *inter alia*, la Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e criptoattività del 15 giugno 2022 e, più recentemente, la Comunicazione della Banca d'Italia in tema di Regolamento (UE) 2023/1114 relativo ai mercati delle criptoattività del 22 luglio 2024 e le successive Indicazioni operative del 13 settembre 2024.

Grafica a cura della Divisione Editoria e stampa della Banca d'Italia