UNIVERSITÀ DEGLI STUDI DI MILANO
DIPARTIMENTO DI STUDI INTERNAZIONALI
GIURIDICI E STORICO-POLITICI

# MERCATI FINANZIARI E TRANSIZIONE DIGITALE

## UNA TASSONOMIA

*a cura di*

L. AMMANNATI, A. CANEPA, G.L. GRECO, U. MINNECI

G. Giappichelli Editore

UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI STUDI INTERNAZIONALI
GIURIDICI E STORICO-POLITICI


COLLANA DI STUDI SCIENTIFICI

13

*La Collana di studi scientifici del Dipartimento di Studi Internazionali, Giuridici e Storico-Politici dell'Università degli Studi di Milano raccoglie monografie e altri risultati inediti di ricerche, individuali e collettive, di Professori, Ricercatori, titolari di assegni di ricerca afferenti al Dipartimento, dottorandi di ricerca che svolgano la loro attività sotto la guida di un docente del Dipartimento, nonché, eccezionalmente, di studiosi esterni che svolgano attività di studio e ricerca nel Dipartimento o che con esso abbiano stabilmente collaborato.*

*La qualità scientifica delle pubblicazioni è assicurata da una procedura di c.d.* double blind peer review *ad opera di revisori esterni.*

# MERCATI FINANZIARI E TRANSIZIONE DIGITALE

## UNA TASSONOMIA

*a cura di*

L. AMMANNATI, A. CANEPA, G.L. GRECO, U. MINNECI


G. Giappichelli Editore

VIA PO, 21 - TEL. 011-81.53.111
http://www.giappichelli.it

ISBN/EAN 979-12-211-1257-3
ISBN/EAN 979-12-211-6189-2 (ebook)

*Il presente volume è stato realizzato con il contributo dell'Università degli Studi di Milano finanziato dal Fondo per il Progetto di Rilevante Interesse Nazionale (PRIN) bando 2017 per il progetto Fintech: the influence of enabling technologies on the future of the financial markets. Codice CUP:G48D19001410006.*

*Stampa:* LegoDigit s.r.l. - Lavis (TN)

# Indice

*pag.*

*pag.*

*pag.*



## CRISI BANCARIE E INTELLIGENZA ARTIFICIALE TRA PREVENZIONE E NUOVE VULNERABILITÀ

Allegra Canepa



## DALLA GIUSTIZIA CIVILE ALLA GIUSTIZIA ALTERNATIVA NELL'ERA DIGITALE

Chiara Reali



## RILEVAZIONE E MITIGAZIONE DEI *BIAS* NEGLI ALGORITMI DI CLASSIFICAZIONE CON IL METODO BRIO: IL CASO DEL *CREDIT SCORING*

Alessandro Giuseppe Buda, Greta Coraglia, Francesco Genco, Chiara Manganini, Giuseppe Primiero

# Informazioni sugli Autori

Anderloni Luisa, *Professoressa di Finanza Aziendale, Università degli Studi di Milano*

Bonfanti Benedetta, *Ricercatrice t.d. Università degli Studi di Milano*

Bragante Daniela, *Chief Compliance Officer, Gruppo Cassa Centrale Banca*

Buda Giuseppe Alessandro, *IUSS Pavia & MIRAI SRL*

Canepa Allegra, *Professoressa di Diritto dell'Economia, Università degli Studi di Milano*

Coraglia Greta, *Assegnista di ricerca, Università degli Studi di Milano & MIRAI SRL*

Frega Giuseppe, *Responsabile Ufficio Vigilanza sui Fenomeni Abusivi, Divisione Ispettorato, già Divisione Tutela del Consumatore, Consob*

Genco Francesco, *Università degli Studi di Torino & MIRAI SRL*

Gobbi Lorenzo, *Divisione Fintech, Banca d'Italia Milano*

Greco Gian Luca, *Professore di Diritto dell'Economia, Università degli Studi di Milano*

Lorenzoni Mauro, *Responsabile Servizio Controllo Interno, già Responsabile Divisione Tutela del Consumatore, Consob*

Luchetti Federico, *Direttore Generale, Organismo Agenti e Mediatori*

Maggini Paolo, *Funzionario Consob*

Manganini Chiara, *Università degli Studi di Milano & MIRAI SRL*

Martini Paolo, *Amministratore Delegato di Azimut Holding SpA e CEO designato di TNB*

Minneci Ugo, *Professore di Diritto Commerciale, Università degli Studi di Milano*

Moro Ornella, *Professore di Economia degli Intermediari Finanziari, Università degli Studi di Sassari*

Pallavicino Francesco, *Market & Customer Insights Expert*

Pantaleo Andrea, *Avvocato DLA Piper*

Primiero Giuseppe, *Professore di Logica e Filosofia della Scienza, Università degli Studi di Milano*

Reali Chiara, *Responsabile Segreteria ABF, Banca d'Italia, Torino*

Ruggiero Francesco, *Ufficio Studi, Organismo Agenti e Mediatori*

Vandone Daniela, *Professoressa di Economia degli Intermediari Finanziari, Università degli Studi di Milano*

Vedana Fabrizio, *Head Legal & Compliance Office di Across Fiduciaria Spa e Presidente Asso Casp*

Ziccardi Giovanni, *Professore di Filosofia del Diritto, Università degli Studi di Milano*

# Introduzione

Questo volume si inserisce nel percorso di ricerca sviluppato grazie ad un finanziamento ricevuto nell'ambito del progetto sul tema "FinTech: the influence of enabling technologies on the future of the financial markets" presentato nel bando per Progetti di Rilevante Interesse Nazionale (PRIN) promosso dal Ministero dell'Università e della Ricerca Scientifica nel 2017.

Le ricerche sul tema del Fintech sviluppate dall'Unità di Milano hanno già portato alla pubblicazione di quattro volumi dei quali tre collettanee e una monografia. Il primo è stato dedicato al diritto di fronte alle nuove tecnologie ed è stato l'esito anche della discussione e delle considerazioni derivanti da un ciclo di webinar, il secondo è stato focalizzato sulle implicazioni generate dal crescente utilizzo di algoritmi, big data da parte delle piattaforme digitali. Gli ultimi due volumi pubblicati nel 2023 sono un libro ed una collettanea dedicati rispettivamente alla rilevanza degli algoritmi nel mercato finanziario ed all'applicazione del principio di proporzionalità nell'ordinamento bancario.

Anche alla luce di questo percorso ci è sembrato il momento di presentare una raccolta delle riflessioni finali, a conclusione del progetto, sull'impatto della tecnologia nel settore finanziario. Attraverso i contributi raccolti nel volume, che danno peraltro conto della natura multidisciplinare dell'unità di ricerca, si è inteso "ricostruire" il dialogo su queste tematiche a valle di numerosi incontri, webinar e convegni nei quali sono intervenuti anche operatori, esponenti delle autorità di regolazione e professionisti.

Nello specifico il libro è articolato in due sezioni, la prima delle quali è dedicata al ruolo delle piattaforme nei mercati finanziari ed alla differenziazione dei servizi erogati a partire dalla fisionomia degli utilizzatori e dalle loro competenze digitali; successivamente vi è spazio per riflessioni sullo sviluppo delle banche digitali, sul ruolo del crowdfunding nel mercato, con le connesse questioni di tutela, sulla "declinazione" digitale dell'obbligo di conservazione del creditore. Ai rischi di abusivismo e cybersecurity sono dedicati i contributi che chiudono la prima sezione, sul presupposto che una fotografia dell'offerta di servizi finanziari digitali non può limitarsi all'enunciazione dei vantaggi connessi all'applicazione delle nuove tecnologie.

Nella seconda sezione l'attenzione è focalizzata sul ruolo della Distributed Ledger Technology (DLT) e dell'Intelligenza Artificiale. Il contributo di apertura si occupa proprio delle prospettive della decentralizzazione della gestione titoli; ad esso fanno seguito, nei tre contributi successivi, alcuni approfondimenti

specifici sui temi delle criptovalute, degli abusi di mercato e dei token. Infine, l'ultima parte di questa sezione si concentra sul ruolo e sulle possibili applicazioni dell'Intelligenza Artificiale, a partire dai nuovi rischi e dalle contestuali potenzialità nella supervisione e nella gestione dei crediti deteriorati, per poi soffermarsi sul suo utilizzo nella risoluzione stragiudiziale delle controversie. Infine, gli ultimi due contributi del volume sono dedicati alla capacità di sfruttamento dell'Intelligenza Artificiale per ridurre (e non solo per produrre) *bias* cognitivi nel *credit scoring* e alle questioni di compliance. In particolare, il contributo dedicato alla mitigazione dei *bias* non ha un approccio esclusivamente teorico ma anche pratico perché illustra un progetto sviluppato da una start-up realizzata e "incubata" nel nostro ateneo, MIRAI, e nata dall'idea di un gruppo di ricercatori con competenze multidisciplinari.

Laura Ammannati, Allegra Canepa, Gian Luca Greco, Ugo Minneci

Sezione I

# *Piattaforme, mercati finanziari e profili di rischio*

# Alfabetizzazione finanziaria e digitale e fragilità finanziaria: quale relazione?

Luisa Anderloni, Ornella Moro, Daniela Vandone



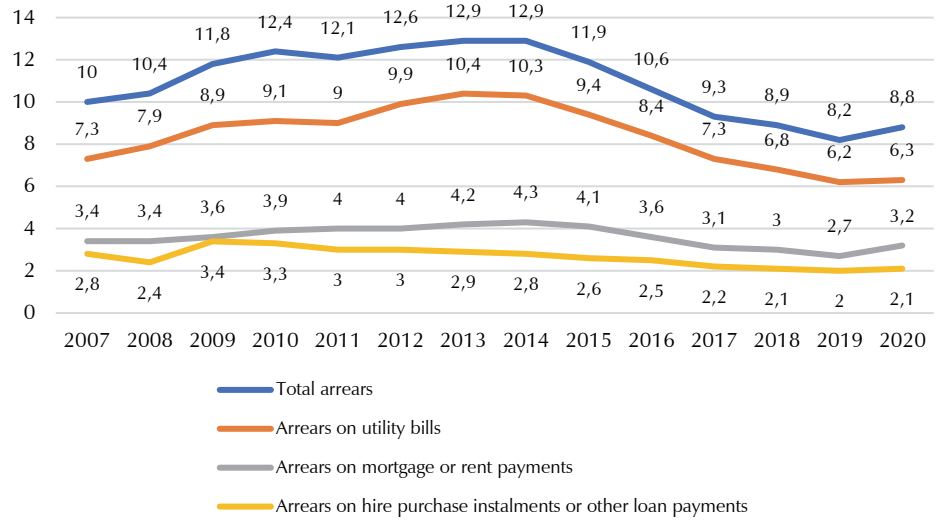
## 1. Introduzione

La fragilità finanziaria degli individui e delle famiglie è intesa come una condizione fattuale e percettiva di instabilità finanziaria, connessa a difficoltà ad "arrivare a fine mese" e/o a sostenere spese impreviste, a *over-commitment* dovuto a eccesso di indebitamento, nonché di percezione di instabilità economica e finanziaria avvertita dall'individuo (Anderloni L., Bacchiocchi E., Vandone D. 2011).

Tale condizione è in linea di principio determinata dall'agire congiunto di una serie di concause, quali shock inattesi (perdita posto di lavoro, malattia, decesso, separazioni e divorzi), che fanno venire meno o riducono le fonti di reddito e/o determinano l'insorgenza di passività impreviste; basso livello di reddito e ricchezza, che rendono l'individuo particolarmente esposto a eventi negativi inattesi; livello di reddito e di ricchezza talmente bassi da collocare l'individuo in condizioni di povertà; scelte di indebitamento errate o non sostenibili, che portano l'individuo a indebitarsi più di quanto dovrebbe alla luce della propria capacità reddituale presente e futura; assenza di misure di prevenzione, copertura e gestione dei rischi, che, fornendo competenze e strumenti, mettano l'individuo nella condizione di gestire al meglio le conseguenze di eventuali shock esterni che possono modificarne la situazione finanziaria.

In molti casi, la fragilità finanziaria degrada poi in sovraindebitamento, un fenomeno che, dopo essere aumentato notevolmente in scala e intensità successivamente alla crisi finanziaria del 2008, aveva mostrato timidi segnali di miglioramento verso la fine della seconda decade del 2000 per poi peggiorare nuovamente (European Commission 2023, p. 41).

Figura 1 – Arrears on key commitments (mortgage or rent, utility bills or hire purchase) in the EU (2005-2011)




La pandemia di Covid-19 ha infatti messo a dura prova il reddito e la capacità delle famiglie di affrontare gli shock finanziari (Brickell et al. 2020) e la recente guerra in Russia, insieme all'aumento dei prezzi dell'energia e all'inflazione generale, ha creato ulteriori sfide per le famiglie [1]. In questo contesto, la fragilità finanziaria e il sovraindebitamento possono essere particolarmente gravi per le famiglie vulnerabili, arrivando anche all'esclusione sociale e a impatti negativi sulla salute fisica e mentale (Reeves et al. 2015; Patel et al. 2012; Sugawara, Zalduendo 2011; Beduk 2020).

Il contenimento della fragilità finanziaria degli individui è identificato dall'OECD come l'obiettivo ultimo di politiche sociale fra cui quelle di alfabetizzazione finanziaria e digitale (G20 2021, OCSE 2020), che mirano a rendere le persone più preparate a gestire il proprio denaro e le proprie finanze, a raggiungere i propri obiettivi finanziari ed evitare lo stress legato ai problemi finanziari e tutte le altre conseguenze negative.

L'OCSE definisce l'alfabetizzazione finanziaria come una combinazione di "*consapevolezza finanziaria, conoscenze, competenze, atteggiamenti e comportamenti necessari per prendere decisioni finanziarie oculate e, in ultima analisi, rag-*

[1] Secondo i dati del 2020 relativi ai paesi europei, il valore mediano del *debt service to income ratio* – calcolato come il rapporto tra il rimborso mensile del debito e il reddito mensile lordo delle famiglie – è intorno al 13%, con un minimo del 7,6% (Austria) e un massimo del 25,8% (Cipro). Nonostante la mediana relativamente bassa, una elevata proporzione di famiglie rimane vicina alla soglia critica del sovraindebitamento, pari convenzionalmente al 25% (BCE, 2021).

*giungere il benessere finanziario*" (OCSE, 2022). Questa competenza permette agli individui di prendere decisioni finanziarie informate e di avere un maggiore controllo sulle proprie questioni finanziarie [2]. L'alfabetizzazione finanziaria promuove anche il risparmio e l'investimento, così da consentite agli individui di gestire le fluttuazioni del reddito a breve termine e di raggiungere obiettivi finanziari a lungo termine [3].

Inoltre, l'alfabetizzazione finanziaria aiuta a evitare truffe finanziarie e a muoversi con sicurezza nei nuovi scenari del panorama finanziario e, invero, la rapida espansione dei servizi finanziari digitali durante la pandemia ha evidenziato la necessità di fornire alle persone le conoscenze e le competenze necessarie per utilizzare questi servizi in modo sicuro. Altri recenti cambiamenti nel panorama finanziario, come il crescente interesse per i cripto-asset, le nuove forme di consulenza finanziaria (ad esempio, i c.d. *finfluencers*) e l'aumento della complessità delle frodi e delle truffe finanziarie, sottolineano ulteriormente l'importanza di rafforzare le competenze di alfabetizzazione finanziaria tra gli adulti per permettere decisioni finanziarie consapevoli (Idris et al. 2019).

L'Unione Europea è consapevole della rilevanza del tema e nel corso degli anni ha affinato le misure di prevenzione e di gestione del sovraindebitamento e della fragilità finanziaria con interventi sia normativi sia di *policy*. Tra le misure di contrasto assume particolare rilevanza l'educazione finanziaria e i servizi di consulenza del debito, ai quali la nuova direttiva sul credito al consumo (EU 2023/2225) dedica un intero capitolo denominato "*Educazione finanziaria e aiuto ai consumatori in difficoltà finanziarie*" [4].

---

[2] Viceversa, gli studi empirici nel settore evidenziano che gli individui che ricorrono al mercato del credito al consumo mostrano livelli di alfabetizzazione finanziaria inferiori rispetto a coloro che non vi partecipano. In particolare, il livello di analfabetismo finanziario è più alto per gli individui con livelli più elevati di rapporto debito/reddito e gli stessi individui detengono anche quote maggiori di credito ad alto costo (Braunstein, Welch 2002; Disney, Gathergood 2013; Elliehausen et al. 2007; Robb 2011; Lusardi, Tufano 2015; Banca d'Italia 2023).

[3] La ricerca empirica riconosce come l'alfabetizzazione finanziaria e l'educazione siano fondamentali per il benessere finanziario e socio-economico delle famiglie (Lusardi et al. 2010; Lusardi et al. 2017; Stolper, Walter 2017; OECD 2020), sia per prevenire e limitare i comportamenti che portano al sovraindebitamento sia per migliorare le competenze decisionali in ambito finanziario (Zehra, Singh 2023).

[4] In particolare, l'art. 24 recita: "*1. Gli Stati membri promuovono misure atte a favorire l'educazione dei consumatori in merito a un indebitamento e a una gestione del debito responsabili, in particolare per quanto riguarda i contratti di credito. Per orientare i consumatori, in particolare quelli che sottoscrivono un credito al consumo per la prima volta, specialmente per mezzo di strumenti digitali, sono fornite informazioni chiare e generali sulla procedura per la concessione del credito. Nell'elaborare e promuovere tali misure, gli Stati membri consultano i pertinenti portatori di interessi, comprese le organizzazioni di consumatori. 2. Gli Stati membri provvedono inoltre affinché siano divulgate informazioni sulla guida che le organizzazioni di consumatori e le autorità nazionali possono fornire ai consumatori. 3. La Commissione effettua una valutazione degli strumenti di educazione finanziaria a disposizione dei consumatori negli Stati membri e pubblica una relazione al riguardo, individuando gli esempi di migliori pratiche che potrebbero essere ulteriormente sviluppate al fine di accrescere la consapevolezza in materia finanziaria dei consumatori*".

La ricerca empirica riconosce l'importanza dell'educazione finanziaria come strumento di contrasto alla fragilità finanziaria, sia perché previene e limita i comportamenti che portano al sovraindebitamento sia perché migliora le competenze decisionali in ambito finanziario (Lusardi et al. 2010; Lusardi et al. 2017; Stolper, Walter 2017; OECD 2020; Zehra, Singh 2023). Tuttavia, l'efficacia dell'alfabetizzazione finanziaria sulla riduzione della fragilità finanziaria degli individui dipende anche da altri fattori, tra cui ad esempio i tratti comportamentali. In uno studio sulla relazione tra alfabetizzazione finanziaria, impulsività e sovraindebitamento, Gathergood (2013) evidenzia che sia una bassa alfabetizzazione finanziaria che l'impulsività vanificano i benefici dell'educazione finanziaria nelle scelte di "*buy now and pay later*", che a loro volta sono positivamente associate al sovraindebitamento. Risultati analoghi anche in Meier, Spreng (2013) e Ottaviani, Vandone (2011, 2018). La definizione di programmi efficaci di educazione finanziaria non è, dunque, un tema di semplice realizzazione e l'analisi di una pluralità di informazioni a più livelli può contribuire a fare chiarezza sui diversi elementi che caratterizzano il legame tra educazione finanziaria e digitale e fragilità finanziaria.

Alla luce delle considerazioni sopra sviluppate, in questo lavoro abbiamo deciso di utilizzare i dati della terza indagine sull'Alfabetizzazione e le Competenze Finanziarie degli Italiani (questionario IACOFI) condotta nel 2023 da Banca d'Italia su di un campione di 4.862 individui rappresentativi della popolazione italiana, con l'obiettivo di indagare lo stato dell'alfabetizzazione finanziaria e digitale degli italiani e la relazione con le situazioni di fragilità finanziaria presentate in questo capitolo.

Nel paragrafo 2 descriviamo gli indicatori di alfabetizzazione finanziaria, alfabetizzazione finanziaria digitale e fragilità finanziaria; nel paragrafo 3 presentiamo alcune statistiche descrittive; nel paragrafo 4 indaghiamo la relazione tra gli indicatori di alfabetizzazione e la fragilità finanziaria. Il paragrafo 5 conclude.

## 2. Gli indicatori

Al fine di analizzare la relazione sussistente tra alfabetizzazione finanziaria, conoscenza digitale e fragilità finanziaria abbiamo dapprima provveduto ad estrapolare del questionario IACOFI alcune domande volte a misurare i tre aspetti e poi abbiamo costruito degli indicatori di sintesi.

### 2.1. L'indicatore di alfabetizzazione finanziaria

L'indicatore volto a cogliere il livello di alfabetizzazione finanziaria dei rispondenti è costruito sulla base delle risposte fornite a quesiti che misurano sia

il profilo della conoscenza finanziaria, su temi quali interessi, costo del denaro, rapporto rischio-rendimento, sia quello degli atteggiamenti finanziari più o meno "esperti" e dimostrati attraverso azioni come il rapporto con il denaro, la fissazione di obiettivi finanziari a lungo termine e la pianificazione attenta della propria attività.

L'indicatore di conoscenza finanziaria – *FinLitKnow* – è la somma delle risposte corrette alle domande presentate nel riquadro 1; esso assume un valore tra 0 (nessuna risposta corretta) e 7 (tutte le risposte sono corrette). Maggiore è il valore dell'indicatore e maggiore è il livello di conoscenza finanziaria.

Tabella 1 – La conoscenza finanziaria

| *Domande* | *Punteggio* |
|---|---|
| Cinque fratelli ricevono oggi in regalo 1.000 euro. Immagini che debbano attendere un anno per poter disporre della loro quota e che il tasso di inflazione annuo sia pari all'8%. Tra un anno, ciascuno con la propria somma, quanto potrà comprare? | 1 se la risposta è "Meno di quanto potrebbe comprare oggi" oppure "Dipende da che cosa vogliono acquistare" |
| Supponga di prestare 25 euro a un Suo amico una sera. Il giorno dopo il Suo amico le restituisce 25 euro. Quale tasso di interesse ha fatto pagare al Suo amico per il prestito? | 1 se la risposta è zero |
| Supponga di depositare €100 in un conto di deposito che rende un tasso di interesse del 2% annuo. Su questo conto non sono effettuate altre operazioni, né di deposito né di prelievo. Quanto ci sarà sul conto alla fine del primo anno, dopo il pagamento degli interessi e senza considerare le spese? | 1 se la risposta è 102 |
| E dopo 5 anni, quanto immagina sarà la cifra disponibile se su questo conto non sono effettuate altre operazioni, né di deposito né di prelievo, non ci sono spese e continua a essere remunerato a un tasso di interesse garantito del 2% annuo? | 1 se la risposta è "più di 110" |
| Un investimento con un rendimento elevato è probabilmente molto rischioso | 1 se la risposta è "vero" |
| Inflazione elevata significa che il costo della vita cresce rapidamente | 1 se la risposta è "vero" |
| Solitamente è possibile ridurre il rischio di investimenti nel mercato finanziario acquistando titoli e azioni diversi (di diversi emittenti). | 1 se la risposta è "vero" |

L'indicatore di atteggiamento finanziario – *FinLitAtt* – è la somma dei punteggi corrispondenti al grado di accordo o disaccordo rispetto ai quesiti presen-

tati nella tabella 2[5], (diviso per il numero dei quesiti). Il valore minimo è pari a 1, mentre il massimo è pari a 5. Anche in questo caso, maggiore è l'indicatore e maggiore è il livello di atteggiamento finanziario "consapevole".

Tabella 2 – L'atteggiamento finanziario

| *Domande* | *Punteggio* |
|---|---|
| Trovo più soddisfacente spendere piuttosto che risparmiare per il futuro | Risposta su una scala da 1 a 5, dove "1 = sono completamente d'accordo" e "5 = sono completamente in disaccordo" |
| Preferisco vivere alla giornata | Risposta su una scala da 1 a 5, dove "1 = sono completamente d'accordo" e "5 = sono completamente in disaccordo" |
| Se il denaro c'è meglio spenderlo | Risposta su una scala da 1 a 5, dove "1 = sono completamente d'accordo" e "5 = sono completamente in disaccordo" |

La somma degli indicatori di conoscenza finanziarie e attitudine finanziaria costituisce l'indicatore complessivo di alfabetizzazione finanziaria – *FinLitTotale* – che varia da 1 a 12, dove 1 è il livello minimo di alfabetizzazione finanziaria e 12 il livello massimo.

## 2.2. L'indicatore di alfabetizzazione finanziaria digitale

L'indicatore volto a cogliere il livello di alfabetizzazione finanziaria digitale dei rispondenti è costruito, analogamente al precedente, sulla base delle risposte fornite a quesiti che misurano sia il profilo della conoscenza digitale, come la stipula di contratti finanziari con strumenti digitali, l'uso dei dati personali e le caratteristiche dei cripto-assets, sia quello di atteggiamenti più o meno "esperti" in ambito digitale con particolare riferimento al tema della sicurezza.

L'indicatore di conoscenza finanziaria digitale – *FinDigKnow* – è la somma delle risposte corrette ai quesiti indicati nella tabella 3, e assume valore tra 0 (nessuna risposta corretta) e 3 (tutte le risposte sono corrette). Maggiore è il valore dell'indicatore e maggiore è il livello di conoscenza finanziaria digitale.

[5] Poiché ciascuna risposta consente di ottenere un punteggio massimo pari a cinque, il risultato complessivo è diviso per tre così da mantenere una proporzione dimensionale tra il punteggio relativo alle conoscenze finanziarie e quello relativo alle attitudini finanziarie.

Tabella 3 – La conoscenza finanziaria digitale

| *Domande* | *Punteggio* |
|---|---|
| Concludere un contratto finanziario con strumenti digitali ha valore solo se lo stesso contratto è disponibile anche in forma cartacea con la firma delle parti contraenti | 1 se "falso" |
| I dati personali che condivido pubblicamente online possono servire a delineare le mie preferenze, e a farmi ricevere offerte commerciali personalizzate | 1 se "vero" |
| Le crypto-attività hanno lo stesso corso legale delle banconote e delle monete | 1 se "falso" |

L'indicatore di atteggiamento finanziario digitale – *FinDigAttit* – è la somma delle risposte corrette e assume valore tra 0 (nessuna risposta corretta) e 3 (tutte le risposte sono corrette). Maggiore è il valore dell'indicatore e maggiore è il livello di attitudine finanziaria digitale "consapevole".

Tabella 4 – L'atteggiamento finanziario digitale

| *Domande* | *Punteggio* |
|---|---|
| Penso che effettuare acquisti online usando reti Wi-Fi pubbliche sia un'attività sicura (per es. in bar, aeroporti, centri commerciali) | 1 se risposta è "non sono d'accordo" |
| È importante fare attenzione alla sicurezza di un sito web prima di effettuare una transazione online (per es. controllo di siti https, sicurezza del logo, certificazioni) | 1 se risposta è "sono d'accordo" |
| Penso che non sia importante leggere i termini e le condizioni quando si effettuano acquisti online | 1 se risposta è "non sono d'accordo" |

La somma dei due indicatori di conoscenza e atteggiamento finanziario digitale è l'indicatore complessivo di alfabetizzazione finanziaria digitale – *FinDigTotale* – che varia da 0 a 6, dove 0 è il livello minimo di alfabetizzazione finanziaria digitale e 6 il livello massimo.

## 2.3. L'indicatore di fragilità finanziaria

L'indicatore di vulnerabilità finanziaria è costruito utilizzando i tre quesiti riportati nella tabella 5, che misurano la disponibilità di un reddito adeguato alle spese, anche impreviste.

Esso può assumere un valore che spazia da 0, valore minimo di fragilità finanziaria, a 3, valore massimo di fragilità finanziaria.

Tabella 5 – La fragilità finanziaria

| *Domande* | *Punteggio* |
|---|---|
| Nel caso in cui dovesse sostenere una spesa imprevista pari al suo reddito mensile, sarebbe in grado di farvi fronte senza dover chiedere somme in prestito a banche, altri intermediari finanziari o a parenti/amici? | 1 se risposta è "no" |
| Negli ultimi 12 mesi Le è capitato che il reddito non fosse sufficiente a coprire le spese? | 1 se risposta è "si" |
| Se lei dovesse perdere la sua principale fonte di reddito, per quanto tempo riuscirebbe a coprire le spese senza ricorrere a prestiti? | 1 se risposta è "per meno di tre mesi" |

## 3. Le statistiche descrittive degli indicatori

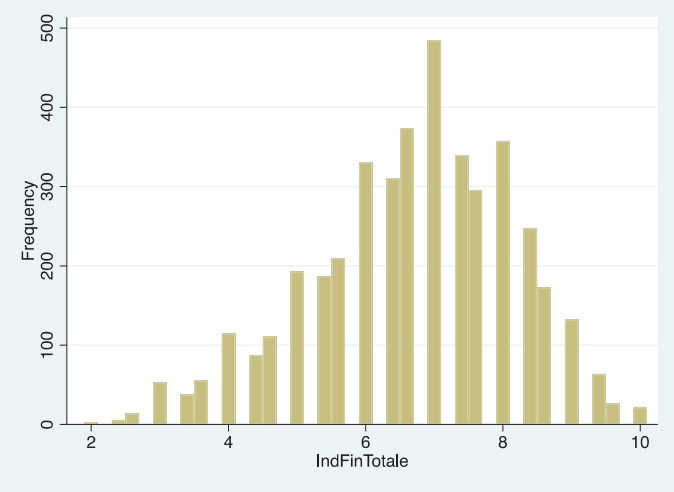
Nelle tabelle che seguono si riportano le statistiche descrittive degli indicatori di alfabetizzazione e fragilità finanziaria.

Tabella 6 – Le statistiche descrittive degli indicatori

| *Indicatore* | *Media* | *Mediana* | *Min* | *Max* | *Range potenziale* |
|---|---|---|---|---|---|
| Alfabetizzazione finanziaria | 6,70 | 7 | 2 | 10 | 0-12 |
| *Conoscenza finanziaria* | *3,18* | *3* | *0* | *5* | *0-7* |
| *Attitudine finanziaria* | *3,35* | *3,33* | *1* | *5* | *0-5* |
| Alfabetizzazione finanziaria digitale | 1,90 | 2 | 0 | 5 | 0-6 |
| *Conoscenza finanziaria digitale* | *1,0* | *1* | *0* | *3* | *0-3* |
| *Attitudine finanziaria digitale* | *0,9* | *1* | *0* | *2* | *0-3* |
| Fragilità finanziaria | 1,33 | 1 | 0 | 3 | 0-3 |

## 3.1. L'alfabetizzazione finanziaria

Il valore medio dell'indicatore di alfabetizzazione finanziaria (*InFinTotale*) relativo al campione oggetto di analisi è pari a 6,7, con un minimo pari a 2 e uno massimo pari a 10 (su un totale potenziale di 12). Un terzo del campione ha un punteggio pari o inferiore a 6, mentre solo una frazione contenuta, pari al 5,8% degli intervistati, ha un punteggio pari o superiore a 9.

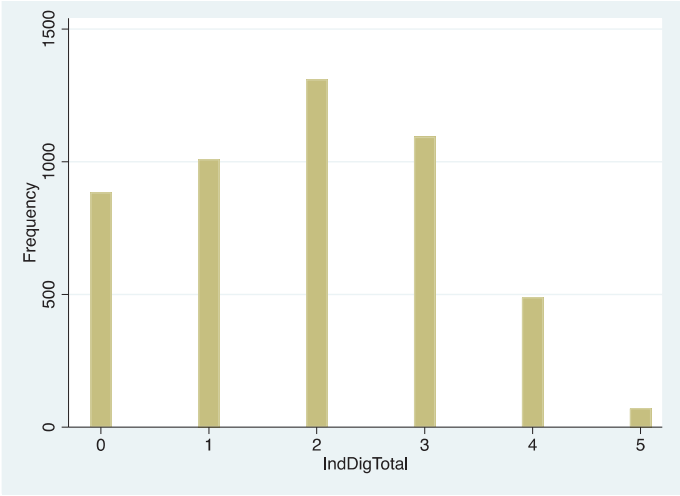



Con riferimento all'indicatore di conoscenza finanziaria, nel campione oggetto di analisi il valore massimo è pari a 5 su un totale potenziale di 7, cioè nessun intervistato ha risposto correttamente a tutte le domande, mentre ben 308 individui (pari al 6,3% del totale) non hanno risposto correttamente nemmeno a una domanda. L'80% degli intervistati è in grado di rispondere almeno a 4 domande su 7; il dato medio dell'indicatore è pari a 3,2, mentre il dato mediano è pari o inferiore a 3.

Con riferimento all'indicatore di attitudine finanziaria, il 4,4% degli intervistati presenta un livello di atteggiamento finanziario molto "consapevole", avendo acquisito un punteggio complessivo pari a 5 su 5, mentre solo meno del 3% degli individui ha un livello di atteggiamento finanziario poco o nulla "consapevole". Il dato medio è in linea con quello mediano e pari a 3,3.

## 3.2. L'alfabetizzazione finanziaria digitale

Per quanto riguarda il livello di alfabetizzazione finanziari digitale (*IndDigTotal*), l'indicatore complessivo mostra un dato medio pari a 1,90 e uno mediano leggermente più elevato e pari a 2. Il massimo è pari a 5 rispetto a un dato teorico complessivo di 6 che non è mai osservato nel campione oggetto di analisi.

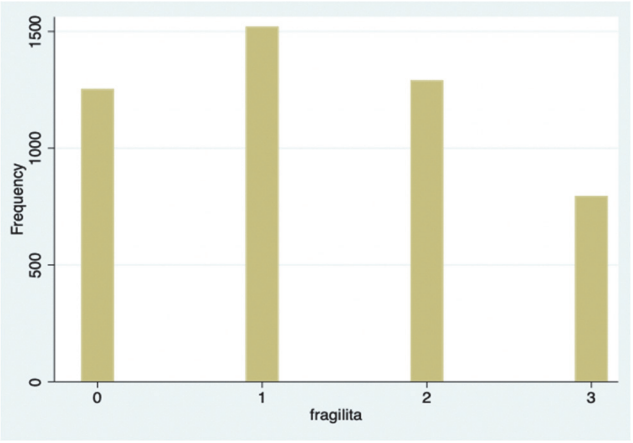



Il valore medio dell'indicatore di alfabetizzazione finanziaria digitale è pari a 1, ma ben un terzo degli intervistati ottiene un punteggio pari a 0 dunque non è in grado di rispondere a nemmeno una delle tre domande che indagano questo aspetto, mentre solo meno dell'8% del campione risponde correttamente a tutte e tre i quesiti.

Con riferimento, invece, all'attitudine verso le questioni di sicurezza digitale, il 23% degli intervistati mostra un indicatore di atteggiamento di consapevolezza abbastanza elevata, pari a 2 su un punteggio massimo pari a 3; tuttavia, quasi il 37% degli intervistati ottiene un punteggio pari a 0.

## 3.3. La fragilità finanziaria

L'indicatore di fragilità finanziaria presenta una distribuzione sbilanciata verso la sinistra del grafico, ad indicare che è maggiore il numero di individui con bassi o nulli livelli di fragilità finanziaria rispetto a quelli problematici; il dato mediano è infatti pari a 1 e più del 25% ha registra un punteggio pari a 0 (assenza di vulnerabilità finanziaria). Tuttavia, il dato medio è più elevato di quello mediano, pari a 1,33, perché esiste una quota significativa di individui pari al 16,4% che è caratterizzata invece da un livello massimo di fragilità finanziaria.




| Fragilità | Percentuale |
|---|---|
| 0 | 25,8 |
| 1 | 31,2 |
| 2 | 26,6 |
| 3 | 16,4 |

In particolare, come si evince dalle tabelle di seguito riportate, più del 22% degli intervistati non è in grado di sostenere una spesa mensile imprevista (e pari al proprio reddito mensile) senza dover chiedere somme in prestito a banche, altri intermediari finanziari o a parenti/amici; più del 12% degli intervistati negli ultimi 12 mesi si è ritrovato nella condizione di non essere in grado di coprire le spese con il proprio reddito, mentre quasi il 22% degli intervistati riuscirebbe a coprire le spese senza ricorrere a prestiti nel caso in cui dovesse perdere la sua principale fonte di reddito.

Tabella 7. – Le risposte ai quesiti di fragilità finanziaria (composizione in %)

| *Domande* | *Percentuale* |
|---|---|
| Nel caso in cui dovesse sostenere una spesa imprevista pari al suo reddito mensile, sarebbe in grado di farvi fronte senza dover chiedere somme in prestito a banche, altri intermediari finanziari o a parenti/amici? | |
| *No* | *22,2* |
| *Sì, con soldi immediatamente disponibili* | *69,8* |
| *Sì vendendo titoli o beni* | *8,0* |
| Negli ultimi 12 mesi Le è capitato che il reddito non fosse sufficiente a coprire le spese? | |
| *No* | *87,5* |
| *Sì* | *12,5* |

*Segue*

| | |
|---|---|
| Se lei dovesse perdere la sua principale fonte di reddito, per quanto tempo riuscirebbe a coprire le spese senza ricorrere a prestiti? | |
| *Meno di una settimana* | *7,9* |
| *Più di una settimana, ma meno di un mese* | *13,6* |
| *Almeno un mese, ma meno di tre mesi* | *31,3* |
| *Almeno tre mesi, ma meno di sei mesi* | *27,6* |
| *Più di sei mesi* | *19,6* |

## 4. Le determinanti della fragilità finanziaria

Al fine di individuare i fattori che maggiormente contribuiscono a incrementare o a ridurre la fragilità finanziaria degli individui è stata eseguita una regressione lineare, robusta all'eteroschedasticità, che utilizza come variabile dipendente l'indice di fragilità finanziaria, e come regressori gli indicatori di alfabetizzazione finanziaria e digitale.

Il modello di regressione lineare è il seguente:

$$FF_i = \beta_0 + \beta_1 AF_i + \beta_2 AFD_i + + \varepsilon_i$$

La struttura dei regressori può essere descritta nel seguente modo: $AF_i$ indica le variabili volte a descrivere gli effetti dell'alfabetizzazione finanziaria sulla vulnerabilità dell'i-esima persona; equivalentemente, $AFD_i$ le variabili volte a descrivere gli effetti dell'alfabetizzazione finanziaria digitale sulla vulnerabilità dell'i-esima persona. I $\beta$ sono i relativi coefficienti, mentre $\varepsilon_i$ è il termine residuo. Tutte le stime sono eseguite da OLS con errori standard robusti alla eteroschedasticità.

Tabella 8 – I risultati della regressione

| *Variabili* | *(i)* *fragilità* | *(ii)* *fragilità* | *(iii)* *fragilità* |
|---|---|---|---|
| Indicatore alfabet. finanz. | – 0.1260*** | | – 0.1085*** |
| | (0.0101) | | (0.0102) |

*Segue*

| | | | |
|---|---|---|---|
| Indicatore alfabet. finanz. digit. | | – 0.1670*** | – 0.0994*** |
| | | (0.0111) | (0.0119) |
| Genere | | | |
| Area geografica | | | |
| Constant. | 2.0774*** | 1.6522*** | 2.1652*** |
| | (0.0698) | (0.0264) | (0.0698) |
| Observations | 4,235 | 4,235 | 4,235 |
| R-squared | 0.0351 | 0.0441 | 0.0500 |

*Robust standard errors in parentheses.*

*** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$

L'analisi multivariata ha messo in luce una relazione significativa tra la fragilità finanziaria e i livelli di alfabetizzazione finanziaria e di alfabetizzazione finanziaria digitale. La relazione è negativa e suggerisce che un aumento delle conoscenze finanziarie, sia tradizionali che digitali, contribuisce a ridurre la probabilità di incorrere in situazioni di vulnerabilità economica. L'alfabetizzazione finanziaria si riferisce infatti alla capacità di comprendere e gestire concetti finanziari, come il calcolo degli interessi o la valutazione del costo del denaro, che sono fondamentali per una pianificazione finanziaria efficace. Quando un individuo possiede una buona conoscenza finanziaria, è in grado di prendere decisioni più informate riguardo agli investimenti, al risparmio e all'indebitamento e questo riduce il rischio di assumere debiti insostenibili o di fare scelte che potrebbero compromettere la stabilità economica nel lungo termine. Anche l'alfabetizzazione finanziaria digitale gioca un ruolo sempre più rilevante poiché, in un contesto dove le transazioni economiche avvengono sempre più online, la capacità di utilizzare strumenti digitali per la gestione delle finanze, di proteggere i propri dati sensibili di gestire le proprie finanze in modo più sicuro diventa cruciale. Le competenze digitali, in particolare quelle relative alla sicurezza online e alla capacità di riconoscere e evitare phishing, malware, sono infatti importanti per prevenire problemi finanziari derivanti da frodi o errori nella gestione delle transazioni e ridurre il rischio di perdite economiche dovute a furti d'identità o ad altre forme di frode digitale.

## 5. Conclusioni

La fragilità finanziaria rappresenta una condizione di instabilità economica, sia percepita che reale, che può derivare da molteplici fattori tra cui eventi inaspettati, bassi livelli di reddito e ricchezza, decisioni di indebitamento insostenibili, e la mancanza di strumenti e competenze per gestire rischi finanziari. Questo fenomeno è ulteriormente aggravato in periodi di crisi economica globale, come evidenziato dalla crisi finanziaria del 2008, la pandemia di Covid-19, e recenti eventi geopolitici che hanno messo a dura prova la resilienza finanziaria delle famiglie, con gravi conseguenze per le famiglie più vulnerabili.

Le politiche di alfabetizzazione finanziaria e digitale sono importanti per contrastare la fragilità finanziaria, come riconosciuto dall'OECD e dall'Unione Europea. L'analisi dei dati dell'indagine IACOFI 2023 della Banca d'Italia rivela che il livello di alfabetizzazione finanziaria e digitale in Italia è variegato, con un terzo del campione che presenta punteggi di alfabetizzazione finanziaria bassi e una parte significativa che dimostra scarse competenze finanziarie digitali.

La nostra analisi multivariata evidenzia una relazione significativa e negativa tra fragilità finanziaria e alfabetizzazione finanziaria, sia tradizionale che digitale. Questo significa che un aumento delle conoscenze finanziarie riduce la probabilità di trovarsi in condizioni di vulnerabilità economica. Parallelamente, l'alfabetizzazione finanziaria digitale è sempre più importante in un contesto di transazioni online, poiché aiuta a utilizzare strumenti digitali in sicurezza e a prevenire frodi, proteggendo i dati personali e riducendo i rischi di perdite economiche.

Tuttavia, sebbene l'alfabetizzazione finanziaria e digitale possa contribuire a ridurre la fragilità finanziaria, è comunque necessario un approccio più integrato per affrontare le vulnerabilità strutturali che caratterizzano la popolazione italiana, che includa politiche di supporto economico e misure di prevenzione più mirate, La fragilità finanziaria è infatti presente in una quota significativa della popolazione, con il 22% del campione che non riuscirebbe a sostenere una spesa imprevista pari al proprio reddito mensile senza ricorrere a prestiti, e il 16,4% che presenta livelli massimi di fragilità finanziaria. Una attenzione particolare dovrebbe essere rivolta ai gruppi più vulnerabili, per i quali la fragilità finanziaria può avere conseguenze particolarmente gravi, inclusa l'esclusione sociale e impatti negativi sulla salute fisica e mentale.

## Bibliografia

ANDERLONI L., BACCHIOCCHI E., VANDONE D. (2012), *Household financial vulnerability: an empirical analysis*, in *Research in Economics*, 66, pp. 284-96.

ANDERLONI L., TANDA A., VANDONE D. (2018), *The European consumer credit industry: determinants of performance*, in *Journal of Accounting and Finance*, 8(2), pp. 181-193.

BANCA D'ITALIA (2023), *Indagine sull'alfabetizzazione finanziaria e le competenze di finanza digitale in Italia: adulti*, in *Statistiche.*

BANCA D'ITALIA (2023), *Debt Advice for Consumers: Nature, European Debate and Implications for Italy*, Occasional Papers, n. 740.

BCE (2021) *Household Finance and Consumption Survey (HFCS)*, https://www.ecb.europa.eu/stats/ecb_surveys/hfcs/html/index.en.html.

BEDUK (2020), *Missing dimensions of poverty? Calibrating deprivation scales using perceived financial situation*, in *European Sociological Review.*

BRAUNSTEIN S., WELCH C. (2002), *Financial literacy: an overview of practice, research, and policy*, in *Federal Reserve Bulletin*, 88, pp. 445-457.

BRICKELL K., PICCHIONI F., NATARAJAN N., GUERMOND V., PARSONS L., ZANELLO G., BATEMAN M. (2020), *Compounding crises of social reproduction: Microfinance over-indebtedness and the COVID-19 pandemic*, in *World Development*.,.

DISNEY R., GATHERGOOD J. (2013), *Financial literacy and consumer credit portfolios*, in *Journal of Banking & Finance*, 37, pp. 2246-2254.

ELLIEHAUSEN G., LUNDQUIST C., STATEN M. (2007), *The impact of credit counseling on subsequent borrower behavior*, in *Journal of Consumer Affairs*, 41, pp. 1-28.

EUROPEAN COMMISSION (2023), *Study on European consumers'over-indebtedness and its implications*, in *Final Report*, June.

FERRETTI F., VANDONE D. (2019), *Personal debt in Europe. The EU Financial Market and Consumer Insolvency*, Cambridge University Press, Cambridge.

FRIGERIO M., OTTAVIANI C., VANDONE D. (2020), *A Meta-Analytic Investigation of Consumer Over-Indebtedness: The Role of Impulsivity*, in *International Journal of Consumer Studies*, 44(4), pp. 328-342.

GATHERGOOD J. (2012), *Self-control, financial literacy and consumer over indebtedness*, in *Journal of Economic Psychology*, 33, pp. 590-602.

IDRIS H., RAHIM F., KASSIM S. (2019), *The influence of digital technologies on consumer's over-indebtedness*, in *International Journal of Academic Research in Business and Social Sciences.*

LUSARDI A., TUFANO P. (2015), *Debt literacy, financial experiences, and overindebtedness*, in *Journal of Pension Economics and Finance*, 14, pp. 332-368.

LUSARDI A., MITCHELL O.S., CURTO V. (2010), *Financial Literacy among the Young*, in *Journal of Consumer Affairs*, 44 (2), pp. 358-380.

LUSARDI A., MICHAUD P.C., MITCHELL O.S. (2017), *Optimal financial knowledge and wealth inequality*, in *Journal of Political Economy*, 125(2), pp. 431-477.

OECD (2020), *OECD/INFE 2020 International Survey of Adult Financial Literacy*.

OECD (2021), *G20/OECD-INFE Report on Supporting Financial Resilience and Transformation through Digital Financial Literacy*.

OECD (2022), *OECD/INFE Guidance on Digital Delivery of Financial Education*.

OECD (2024), *Policy Note on Defining and Measuring Financial Well-being.*

OTTAVIANI C., VANDONE D. (2011), *Impulsivity and household indebtedness: Evidence from real life*, in *Journal of Economic Psychology*, 32(5), pp. 754-761.

OTTAVIANI C., VANDONE D. (2018), *Financial literacy debt burden and impulsivity: A mediation analysis*, in *Economic Notes: Review of Banking Finance and Monetary Economics*, 47(2-3), pp. 439-454.

PATEL A., BALMER N.J., PLEASENCE P. (2012), *Debt and disadvantages: The experience of unmanageable debt and financial difficulty in England and Wales*, in *International Journal of Consumer Studies*, 36(5), pp. 556-565.

REEVES A., MCKEE M., GUNNELL D., CHANG S.S., BASU S., BARR B., STUCKLER D. (2015), *Economic shocks, resilience, and male suicides in the Great Recession: cross-national analysis of 20 EU countries*, in *The European Journal of Public Health*, 25(3), pp. 404-409.

ROBB C.A. (2011), *Financial knowledge and credit card behavior of college students*, in *Journal of Family and Economic Issues*, 32, pp. 690-698.

STOLPER O.A., WALTER A. (2017), *Financial literacy financial advice and financial behavior*, in *Journal of Business Economics*, 87(5), pp. 581-643.

SUGAWARA N., ZALDUENDO J. (2011), *Stress-testing Croatian households with debt implications for financial stability*, in *World Bank Policy Research Working Paper*, no 5906.

VANDONE D. (2009), *Consumer credit in Europe: Risks and Opportunities of a Dynamic Industry*, Springer-Verlag, Berlin, pp. 1-134.

ZEHRA N., SINGH U.B. (2023), *Household finance: a systematic literature review and directions for future research*, in *Qualitative Research in Financial Markets*.

# Competenze digitali e fintech. Un confronto tra fasce di età

Lorenzo Gobbi [*]

SOMMARIO: 1. Introduzione. – 2. Il confronto europeo. – 3. I dati italiani. – 4. Conclusioni.

## 1. Introduzione

Il settore finanziario ha da sempre accolto con favore le opportunità offerte dallo sviluppo tecnologico. La spinta del digitale si è avvertita in particolar modo nell'ultima decina di anni, nei quali grazie alla tecnologia sono nati nuovi soggetti, prodotti, canali e modelli di business.

In una prima fase il fenomeno fintech è stato percepito come disruptive; l'idea diffusa era che i nuovi operatori sarebbero stati capaci di sostituire gli intermediari tradizionali grazie all'offerta di prodotti e servizi non solo più rapidi, meno costosi, più personalizzati, inclusivi, resilienti e trasparenti ma anche maggiormente continui e di più facile utilizzo, la cui richiesta era stimata in forte crescita [1].

In realtà il paventato rischio di sostituzione degli intermediari tradizionali da parte dei nuovi soggetti non si è mai concretizzato così come è stata limitata l'offerta di nuovi prodotti, circoscritta perlopiù al settore dei pagamenti, e sono invece nate forme di collaborazione fra incumbent e fintech, in risposta a una domanda sì con caratteristiche in rapida evoluzione ma che sembra aver privilegiato soprattutto la digitalizzazione dei canali.

Diverse possono essere le ragioni alla base di tale evoluzione (abitudini radicate, rapporti di fiducia consolidati, preferenza per l'interazione personale specie nella gestione del risparmio ne sono alcuni esempi) ma questa analisi si pro-

---

[*] Le opinioni contenute nel presente articolo sono espresse a titolo personale e non impegnano l'istituzione di appartenenza. Si ringrazia Romina Gabbiadini per gli utili commenti.

[1] Si veda anche Parlamento Europeo, risoluzione su "*Tecnologia finanziaria: l'influenza della tecnologia sul futuro del settore finanziario*" https://www.europarl.europa.eu/doceo/document/TA-8-2017-0211_IT.html.

pone in particolare di approfondire il tema delle competenze di finanza digitale degli utenti per valutarne la relazione con la domanda di prodotti digitali.

Non sempre infatti consumatori e imprese possiedono le competenze necessarie per fruire appieno dei benefici del digitale e per presidiare al contempo i rischi posti dalla tecnologia – sia quelli tradizionali, che si sono evoluti (si pensi alle truffe), sia quelli nuovi, in primis il rischio cyber [2]. Tali competenze possono essere utilmente analizzate scindendole in due componenti – ovvero la capacità basilare di usare dispositivi tecnologici (computer, tablet, smartphone) con cui poter accedere ai servizi digitali, e quella di presidiare le vulnerabilità connesse all'utilizzo online di prodotti o servizi finanziari.

Quando le competenze digitali mancano o sono carenti la fiducia nei mezzi tecnologici può venire meno e quindi la domanda di prodotti e servizi finanziari digitali ne può risentire, specie in alcune fasce della popolazione. Anziché favorire l'inclusione finanziaria, l'innovazione tecnologica potrebbe allora finire per emarginare ancor più alcuni soggetti, in particolare quelli appartenenti alle categorie più vulnerabili: sicuramente gli anziani, ma anche le fasce più giovani a reddito basso, specialmente se come è stato spesso rilevato [3] esiste una correlazione tra status sociale e conoscenze.

Anche per le sue ricadute sul benessere collettivo il tema delle competenze digitali è quindi all'attenzione delle istituzioni italiane ed europee, che conducono indagini ricorrenti e hanno pubblicato una pluralità di lavori di ricerca sull'argomento. La Commissione UE ha per esempio sviluppato un quadro di riferimento per le competenze digitali degli europei, noto comunemente come DigComp [4], nel cui contesto Eurostat e il Centro Comune di Ricerca si occupano delle attività di raccolta e analisi dei dati, anche in collaborazione con autorità nazionali (per l'Italia Istat); sempre la Commissione ha elaborato una "Digital Decade strategy" con obiettivi concreti e misurabili da raggiungere entro il 2030, pure in termini di competenze digitali dei cittadini. La Banca d'Italia conduce inoltre con cadenza triennale indagini campionarie sull'alfabetizzazione finanziaria e sulle competenze di finanza digitale della popolazione.

---

[2] La diffusione della tecnologia nel sistema finanziario ha anche modificato i rischi tradizionalmente presidiati dalle autorità, trasformandone alcuni – si pensi alla maggiore difficoltà nell'adattare la strategia aziendale a un contesto digitale o all'aumento del rischio reputazionale e alle sfide poste in termini di governance dei dati – e introducendone di nuovi, come quello di eccessiva dipendenza da terze parti https://www.bis.org/bcbs/publ/d575.pdf; https://www.bankingsupervision.europa.eu/press/speeches/date/2024/html/ssm.sp240322~7bbfe50962.en.html.

[3] https://op.europa.eu/webpub/eac/education-and-training-monitor-2020/en/chapters/chapter1.html "ICILS 2018 and ICILS 2013 reveal that digital competence is linked to socio-economic background".

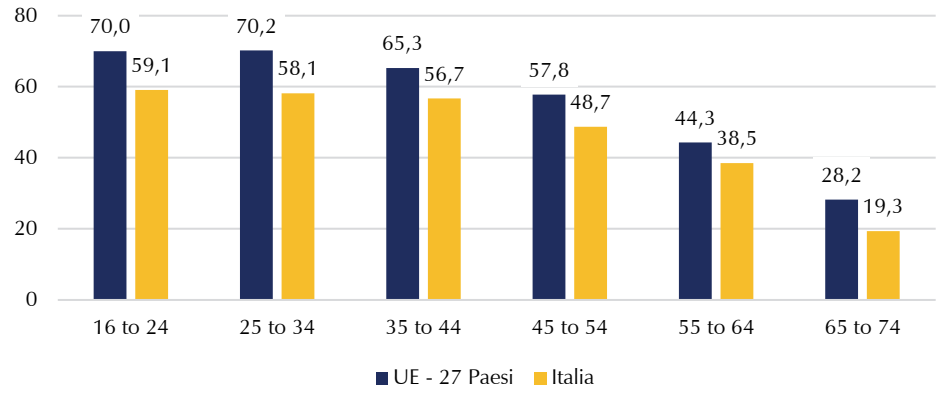
[4] https://ec.europa.eu/jrc/en/digcomp.

## 2. Il confronto europeo

Gli ultimi dati europei, pubblicati da Eurostat a dicembre 2023[5], mostrano che le competenze digitali degli italiani sono ancora carenti: nonostante l'88% della popolazione fra i 16 e i 74 anni utilizzi internet almeno una volta alla settimana solo il 46% è dotato di competenze digitali almeno di base, a fronte di una media europea del 56% e di valori molto più alti nei Paesi Bassi (83%), in Finlandia (82%) e in Irlanda (73%)[6]; fanno peggio dell'Italia solo Romania, Bulgaria, Polonia e Lettonia.

La quota di italiani con competenze digitali è al di sotto della media europea in ogni fascia d'età (cfr. grafico); il valore è pressappoco costante per chi ha fra i 16 e i 44 anni – intervallo che comprende Millennials (nati fra il 1980 e il 1994) e GenZ (nati fra il 1995 e il 2012) – e scende gradualmente nelle fasce più anziane della popolazione.

Figura 1 – Quota di individui con conoscenze digitali almeno di base (%)




*Fonte: Eurostat.*

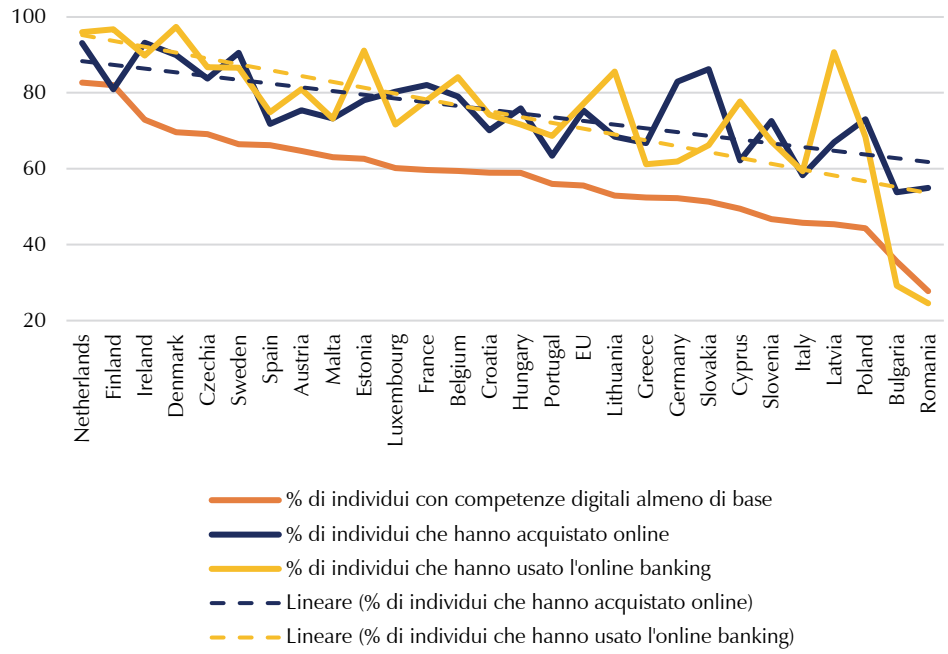
La mancanza di competenze digitali e finanziarie sufficienti potrebbe impedire ai consumatori di accedere a prodotti e servizi basati sulla tecnologia, anche quando questi sono meno costosi o hanno caratteristiche più coerenti con le loro esigenze.

[5] https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20231215-3; https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2023.

[6] Secondo la metodologia utilizzata ha competenze digitali di base chi è in grado di svolgere almeno una attività in ciascuna delle cinque aree di competenza individuate: informazione e alfabetizzazione dei dati (es. ricerca di dati online), comunicazione e collaborazione (es. invio di email), creazione di contenuti digitali (es. scrivere codice di programmazione), sicurezza (es. proteggere dati personali) e risoluzione dei problemi (es. installare software).

In effetti i dati sull'uso del commercio elettronico, che può essere indice dell'abitudine a utilizzare strumenti tecnologici, mostrano che in Italia la quota di chi acquista online (58%) è significativamente più bassa della media europea (75%) per tutte le fasce di età. Persino guardando ai più giovani, fra i quali ci si attenderebbe di cogliere cambiamenti di tendenza ispirati dalle iniziative intraprese per diffondere la conoscenza del digitale, si nota un ritardo notevole (il 67% di giovani under 24 acquista online in Italia contro la media EU dell'82%).

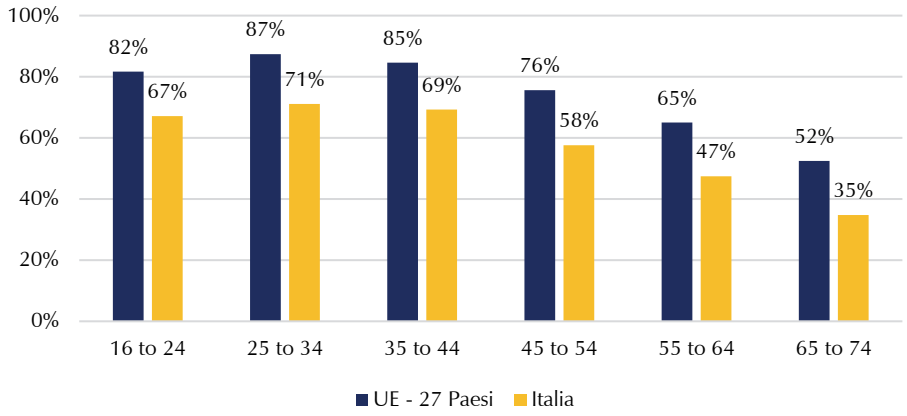
Figura 2 – Correlazione tra competenze digitali e uso di servizi tecnologici




*Fonte: Eurostat e rielaborazioni dell'autore.*

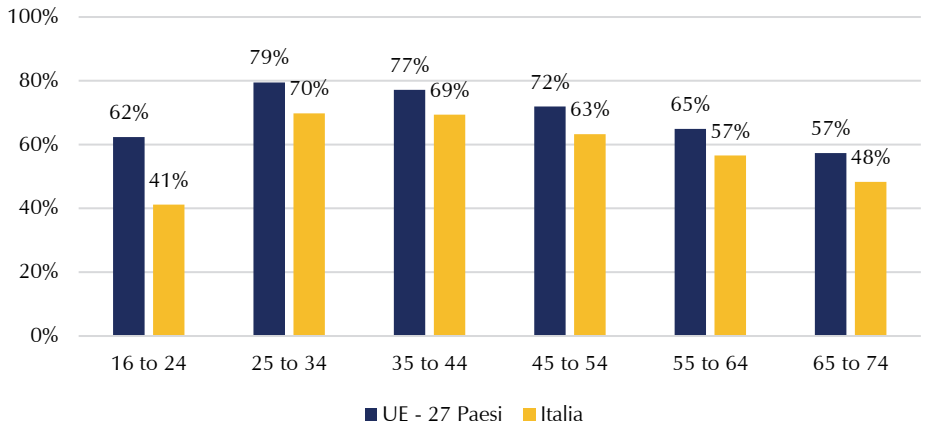
I dati sull'online banking confermano questa tendenza. In Italia l'accesso ai servizi bancari tramiti canali online è meno diffuso rispetto ad altri Paesi dell'Unione: solo il 41% degli italiani fra i 16 e i 24 anni ha usato internet per accedere ai servizi bancari nei tre mesi precedenti alla rilevazione, con una distanza di oltre 20 punti percentuali dai coetanei europei; nelle altre fasce di età l'uso dell'internet banking è più frequente e la distanza dalla media europea si riduce ma resta comunque rilevante, nell'intorno degli 8-10 punti percentuali.

Figura 3 – Uso del commercio online nei 12 mesi precedenti alla rilevazione (% di chi ha accesso a internet)




*Fonte: Eurostat.*

Figura 4 – Uso dell'internet banking (% di chi ha accesso a internet)




*Fonte: Eurostat.*

## 3. I dati italiani

Per approfondire il livello di competenze finanziarie digitali degli italiani può essere interessante analizzare anche i risultati di un'indagine che Banca d'Italia ha condotto nel 2023 su un campione di circa cinquemila persone[7].

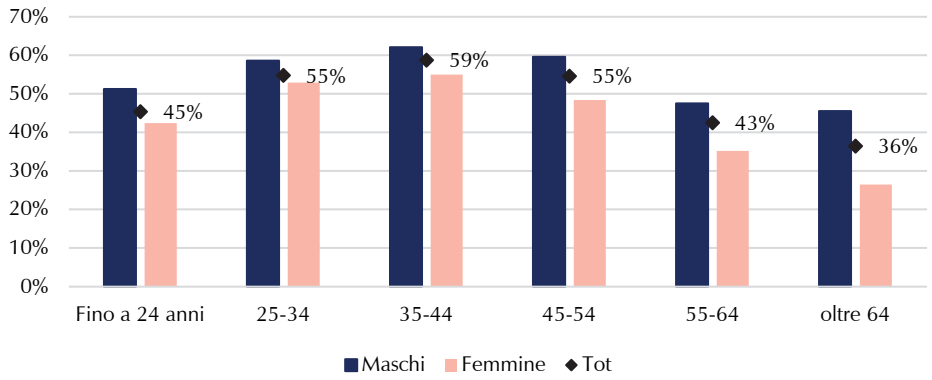
*Il settore dei pagamenti*

Un settore da osservare con attenzione è quello dei pagamenti, particolarmente significativo per almeno due motivi: è stato il primo in cui l'innovazione tecnologica si è manifestata ed – essendo pervasivo nella vita delle persone – è spesso considerato un volano per contribuire alla diffusione del digitale.

Le novità apportate dalla tecnologia in questo ambito sono molte e ormai introdotte da tempo: si pensi ai trasferimenti peer-to-peer, ai wallet digitali, ai wearables, ai bonifici istantanei, ma anche alle criptovalute.

I dati mostrano che nel nostro Paese i nuovi strumenti non hanno ancora raggiunto una diffusione generalizzata: poco meno della metà degli intervistati con accesso a internet ha usato il cellulare per pagare beni o servizi in negozi fisici, e il dato è ancora più basso fra la popolazione femminile. Si evidenzia inoltre che la quota di giovani fra i 18 e i 24 anni che non ha mai pagato tramite cellulare, diversamente da quanto ci si attenderebbe, è superiore alla media della popolazione.

Figura 5 – In negozi fisici ha effettuato pagamenti per beni e servizi tramite cellulare (% di intervistati)

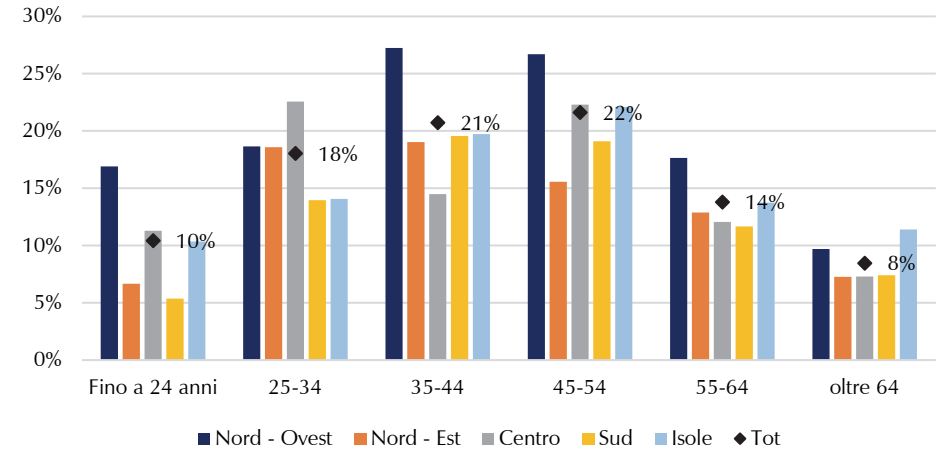



*Fonte: Dati Banca d'Italia elaborati dall'autore.*

[7] La rilevazione è condotta sulla base di una metodologia sviluppata dall'International Network on Financial Education (INFE) dell'OCSE.

Pure la sottoscrizione interamente online di prodotti e servizi di pagamento non è particolarmente diffusa, nemmeno tra i giovani. Solo il 16% di chi ha accesso a internet ha richiesto una carta di debito o di credito, oppure una carta per effettuare pagamenti con modalità interamente online. Il valore si ferma al 10% per chi ha fra i 18 e i 24 anni – con un'ampia forbice fra il 5% di chi risiede al Sud e il 17% di chi abita nel Nord-Ovest – mentre sale al 22% nella fascia d'età 45-54 anni. Nel complesso la componente di genere non sembra rilevare particolarmente: la popolazione maschile e quella femminile hanno grossomodo richiesto carte con la medesima frequenza (17% vs 15%).

Figura 6 – Ha richiesto con modalità interamente online una carta di debito o di credito, oppure una carta per effettuare pagamenti (% di intervistati)

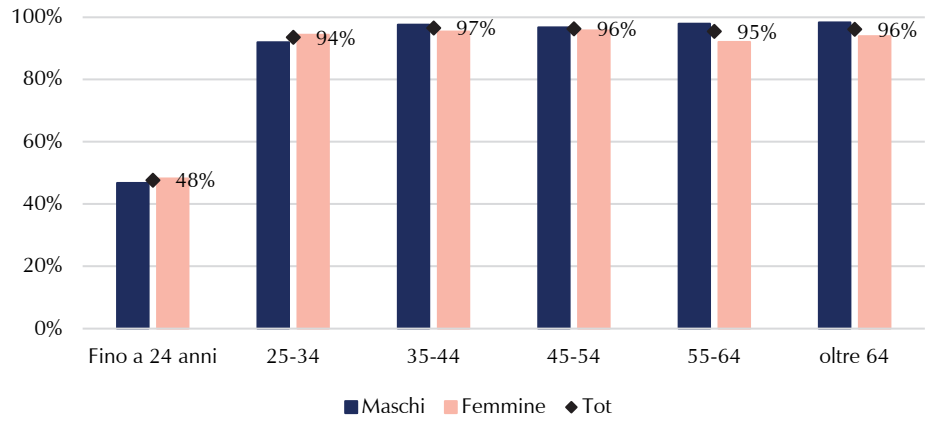



*Fonte: Dati Banca d'Italia elaborati dall'autore.*

Per capire quanto i consumatori siano abituati a operare online può essere utile analizzare le statistiche di utilizzo dell'internet banking. Poiché molti giovani non hanno un rapporto bancario o postale – fra i ragazzi con meno di 25 anni (generazione Z) solo il 48% dispone di un conto corrente – si considerano in queste statistiche unicamente gli intervistati che hanno dichiarato di possederne uno.

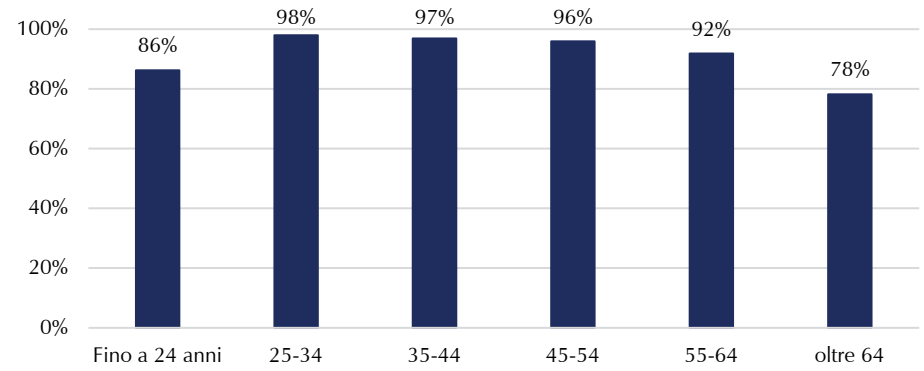
I risultati mostrano che, anche quando possiedono un conto corrente, gli under 25 ne sfruttano relativamente poco le funzionalità disponibili online: solo l'86% aveva controllato online il saldo e la movimentazione almeno una volta nei 12 mesi precedenti alla rilevazione, contro il 96% nella fascia 45-54, senza significative differenze di genere – probabilmente perché ancora poco abituati a gestire entrate, spese ed eventuali risparmi.

Figura 7 – Attualmente possiede un conto c/c bancario e/o postale (% di intervistati)




*Fonte: Dati Banca d'Italia elaborati dall'autore.*

Figura 8 – Controlla online il saldo e la movimentazione del c/c (% di soggetti che hanno un c/c)




*Fonte: Dati Banca d'Italia elaborati dall'autore.*

## *Il settore del credito*

L'utilizzo poco frequente di strumenti di pagamento digitale può avere conseguenze rilevanti anche su altri comparti, ad esempio sul credito.

Se usati spesso, infatti, strumenti di pagamento e conti correnti generano grandi quantità di dati che potrebbero utilmente alimentare i modelli di valutazione del merito creditizio, talvolta basati su algoritmi di intelligenza artificiale.

Sfruttando dati transazionali gli operatori potrebbero attribuire un credit score anche a soggetti privi di storia creditizia, che hanno maggiori difficoltà ad accedere ai finanziamenti – tipicamente i più giovani. In questo senso l'evoluzione

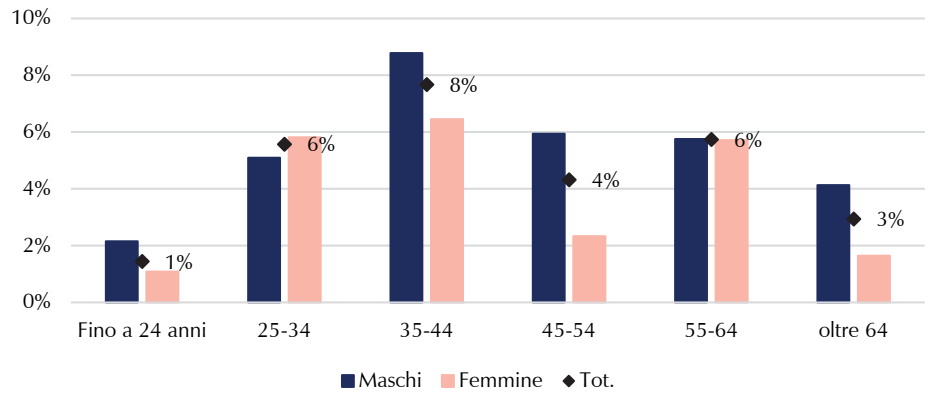
tecnologica potrebbe favorire l'inclusione finanziaria, ampliando la platea dei soggetti considerati meritevoli di prendere a prestito a individui (e imprese) che i modelli (e gli intermediari) tradizionali non sono in grado di valutare correttamente.

Quando, come nel caso italiano, gli strumenti di pagamento digitali – alternativi al contante – vengono accolti timidamente, il bacino dei dati che possono essere utilizzati per alimentare i modelli si restringe, col rischio che le stime di PD basate su dati alternativi non siano possibili o siano meno precise, e che ad alcuni soggetti continui a restare inibito l'accesso al credito.

Uno studio di CRIF mostra come in effetti nel nostro Paese avere un *track record* consultabile nel Sistema di Informazioni Creditizie (SIC) incrementi ancora oggi del 53% la possibilità di ottenere un prestito o un mutuo. Nel caso dei prestiti personali, per i quali non viene richiesta alcuna garanzia reale, la forbice tra chi possiede una storia creditizia e chi invece non la ha è ancora più ampia (+ 136%)[8].

Per fare considerazioni su quanto la tecnologia possa sostenere l'accesso al credito sarebbe anche utile fare un confronto tra il tasso di rifiuto dei prestiti richiesti attraverso canali digitali e quello dei prestiti richiesti attraverso altri canali, ma purtroppo questi dati non sono disponibili. Si può comunque rilevare che fra gli intervistati che hanno sottoscritto un prestito interamente online, il 18% ha dichiarato di avere ricevuto un rifiuto su altri affidamenti richiesti, con percentuali più elevate fra gli ultra 55enni e gli under 24, dato che potrebbe essere indicativo di una capacità inclusiva del canale digitale.

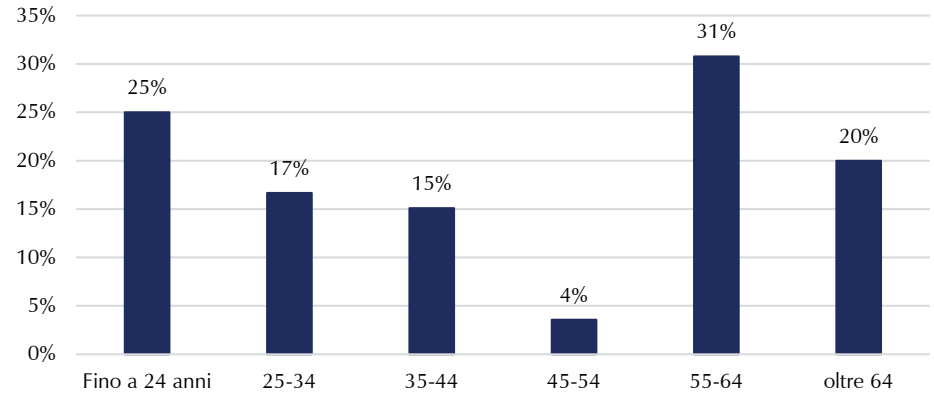
Figura 9 – Ha sottoscritto un prestito con modalità interamente online (% degli intervistati)




*Fonte: Dati Banca d'Italia elaborati dall'autore.*

[8] https://www.crif.it/area-stampa/ricerca-crif-nomisma-limpatto-positivo-del-sistema-di-informazioni-creditizie/.

Figura 10 – Ha subìto il rifiuto di un affidamento (% di chi ha sottoscritto un prestito online)




*Fonte: Dati Banca d'Italia elaborati dall'autore.*

## *L'importanza dei dati*

Il tema dei dati è importante e trasversale ai diversi ambiti della finanza; l'uso di strumenti digitali genera infatti grandi quantità di informazioni personali che gli istituti finanziari possono elaborare – anche attraverso sistemi di intelligenza artificiale – e poi usare per diverse finalità, previo ovviamente consenso dell'utente: profilazione, invio di offerte commerciali personalizzate, consulenza automatizzata, calcolo del merito creditizio sono solo alcuni esempi.

Il trattamento automatizzato da parte delle istituzioni finanziarie di dati personali può generare vantaggi per i consumatori, fra i quali offerte più customizzate, segmentate e meno costose e come già accennato valutazioni del merito creditizio più precise. Va tuttavia considerato che potrebbe pure determinare effetti negativi se ad esempio gli algoritmi – o i dati che li alimentano – contenessero errori o distorsioni, generando quindi discriminazioni[9]. Addirittura le imprese potrebbero fare ricorso a sistemi di intelligenza artificiale per estrarre dai dati pregiudizi comportamentali subconsci, per poi utilizzarli a fini manipolativi del comportamento dei consumatori – ad esempio inducendo l'acquisto di beni che provocano una gratificazione immediata ma dannosi nel lungo termine[10].

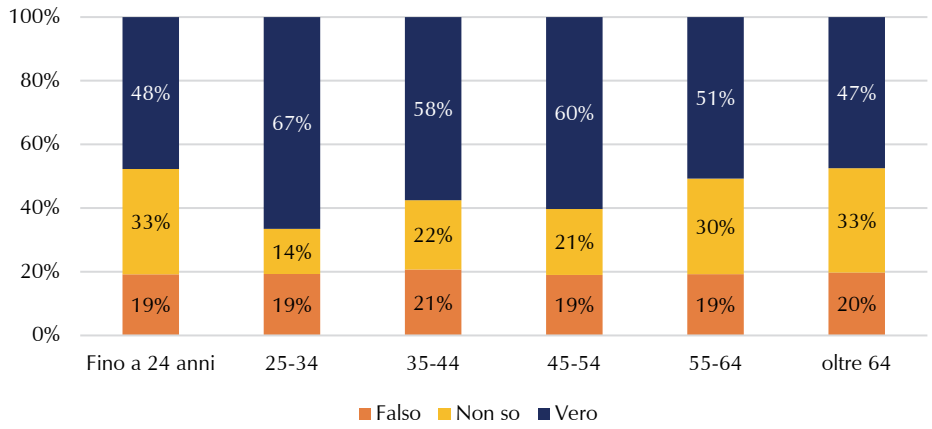
[9] Si veda anche il Regolamento (UE) 2024/1689 che stabilisce norme armonizzate sull'intelligenza artificiale. L'obiettivo del regolamento è promuovere un'IA affidabile, garantendo che i sistemi di IA rispettino i diritti fondamentali, la sicurezza e i principi etici dell'Unione. Per alcuni sistemi di IA il regolamento introduce, tra gli altri, l'obbligo usare in fase di addestramento serie di dati di alta qualità, al fine di ridurre al minimo i rischi e i risultati discriminatori. https://digital-strategy.ec.europa.eu/it/policies/regulatory-framework-ai.

[10] *The Economic Impacts and the Regulation of AI: A Review of the Academic Literature and Policy Actions* (imf.org).

È quindi importante che i consumatori siano consapevoli del valore dei propri dati personali, delle conseguenze che possono derivare dalla condivisione dei propri dati online e, più in generale, dei propri diritti. Sapere che è possibile scegliere quali dati condividere online, anche al fine di costruire un "io" digitale che sia espressione delle caratteristiche che si decide di rendere pubbliche, potrebbe aiutare a superare la diffidenza di alcuni verso l'uso di strumenti digitali.

L'indagine di Banca d'Italia rileva tuttavia che solo meno della metà degli under 25 e degli over 64 sa che i dati personali condivisi pubblicamente in rete possono essere utilizzati per finalità di profilazione e di invio di offerte commerciali personalizzate. La massima consapevolezza si ritrova nella fascia 25-34 anni (67% degli intervistati). Fra chi ha meno di 35 anni la popolazione femminile è più consapevole di quella maschile delle conseguenze che derivano dalla condivisione di dati online, viceversa per gli over 35.

Figura 11 – Domanda: I dati personali che condivido pubblicamente online possono servire a delineare le mie preferenze, e a farmi ricevere offerte commerciali personalizzate




*Fonte: Dati Banca d'Italia elaborati dall'autore.*

La domanda sull'utilizzo che può essere fatto dei dati personali condivisi pubblicamente in rete è usata nell'Indagine di Banca d'Italia per testare il livello di competenze di finanza digitale degli italiani[11]. Va messa in risalto la scarsa consapevolezza che emerge dalle risposte, che potrebbe facilitare la diffusione di informazioni personali che, anziché migliorare l'inclusione finanziaria, possono finire per limitarla. Questo rischio diventa ancor più significativo quando i consumatori si interfacciano con i grandi player tecnologici (BigTech) – la cui ope-

[11] Altre domande che hanno lo stesso obiettivo riguardano la validità dei contratti finanziari conclusi unicamente con strumenti digitali e il corso legale delle criptoattività.

ratività si estende in ambiti molto diversi, dal commercio elettronico alla prestazione di servizi finanziari – che sono in grado di raccogliere ed elaborare grandi quantità di informazioni in poco tempo anche grazie all'enorme disponibilità di tecnologia e di risorse.

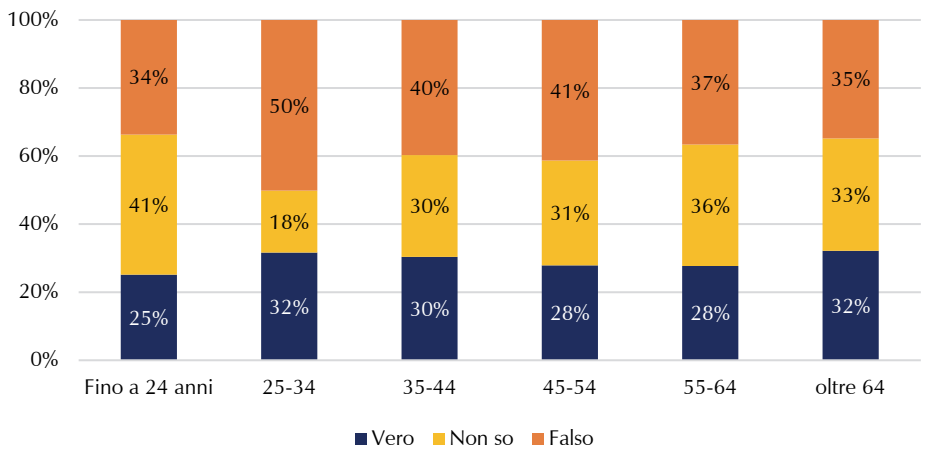
Per consumatori e imprese i dati rilasciati in rete sono quindi una sorta di arma a doppio taglio che se non si hanno le giuste competenze può diventare alquanto rischiosa: i dati possono infatti essere utili per allargare la platea dei soggetti finanziabili, ma se dalle tracce lasciate online emergesse una situazione di difficoltà finanziaria o di scarsità di risorse potrebbe determinarsi invece un problema di esclusione finanziaria e di sfiducia nei confronti del digitale.

*Il Buy Now Pay Later*

La mancanza di competenze in materia di finanza digitale unita a conoscenze finanziarie deboli potrebbe inoltre portare a concludere contratti senza comprenderne appieno le conseguenze o senza capirne la natura.

L'indagine di Banca d'Italia rileva che effettivamente gran parte degli italiani non conosce le conseguenze che derivano dalla stipula di contratti online: solo il 39% degli intervistati sa che un contratto finanziario sottoscritto digitalmente è valido anche quando non è disponibile una sua copia cartacea con la firma delle parti. La fascia d'età in cui la conoscenza è meno diffusa è quella degli under 25 (34%), mentre i più preparati sono gli intervistati fra i 25 e i 34 anni (50%), che come si è visto sono pure fra i più avvezzi all'uso di strumenti tecnologici in finanza.

Figura 12 – Domanda: Concludere un contratto finanziario con strumenti digitali ha valore solo se lo stesso contratto è disponibile anche in forma cartacea con la firma delle parti contraenti

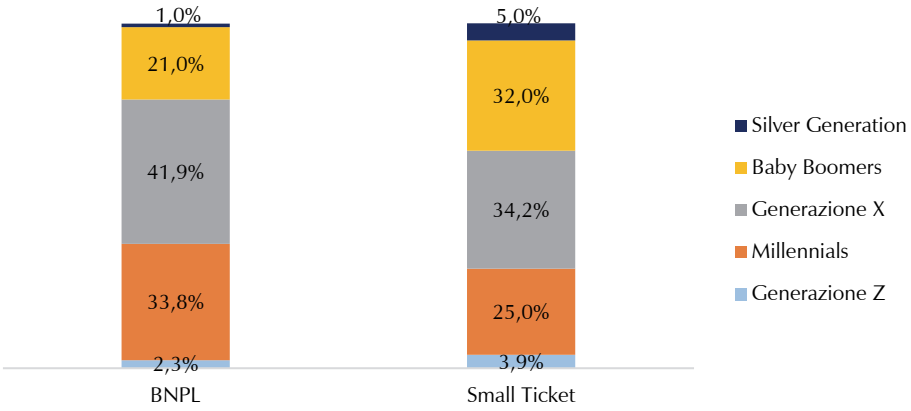



*Fonte: Dati Banca d'Italia elaborati dall'autore.*

Anche la natura del contratto sottoscritto non è sempre percepita in maniera corretta dai consumatori. Sono particolarmente significativi per fare considerazioni sotto questo aspetto i prodotti di "Buy Now Pay Later" (BNPL), che pur avendo natura di credito sono spesso percepiti come strumenti di pagamento. Il BNPL è invece un vero e proprio finanziamento – a breve termine e di importo contenuto – con il quale il consumatore fraziona il pagamento di un acquisto in un numero variabile di rate, generalmente senza interessi.

Un'analisi pubblicata da CRIF a marzo 2024 mostra che il Buy Now Pay Later (BNPL) è utilizzato prevalentemente da chi ha fra i 30 e i 59 anni (41,9% Generazione X – 40-59 anni; 33,8% Millennials – 30-44 anni). Anche se non giovanissima, la popolazione che usa il BNPL è mediamente più giovane di quella che fa ricorso a prestiti Small Ticket [12] più tradizionali.

Figura 13 – Uso di prodotti BNPL e di finanziamenti Small Ticket per fasce di età

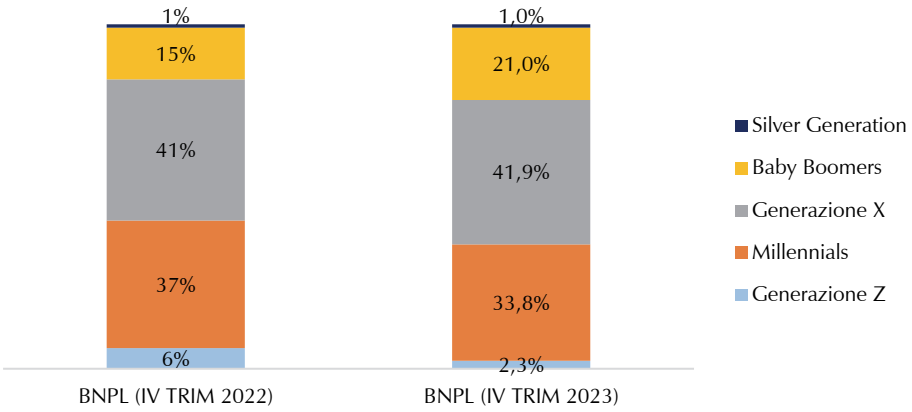



*Fonte: CRIF.*

Il trend – osservato anno su anno confrontando il quarto trimestre del 2023 con il quarto trimestre del 2024 – mostra un calo della quota di giovani della Generazione Z e Millennials che hanno usato il BNPL, principalmente ascrivibile alla crescita del suo utilizzo fra i Baby Boomers (50-78 anni).

[12] Per Small Ticket si intendono i prestiti personali e finalizzati con ticket inferiore a 5 mila Euro.

Figura 14 – BNPL – confronto fra generazioni sul IV TRIM 2022 vs 2023




*Fonte: CRIF.*

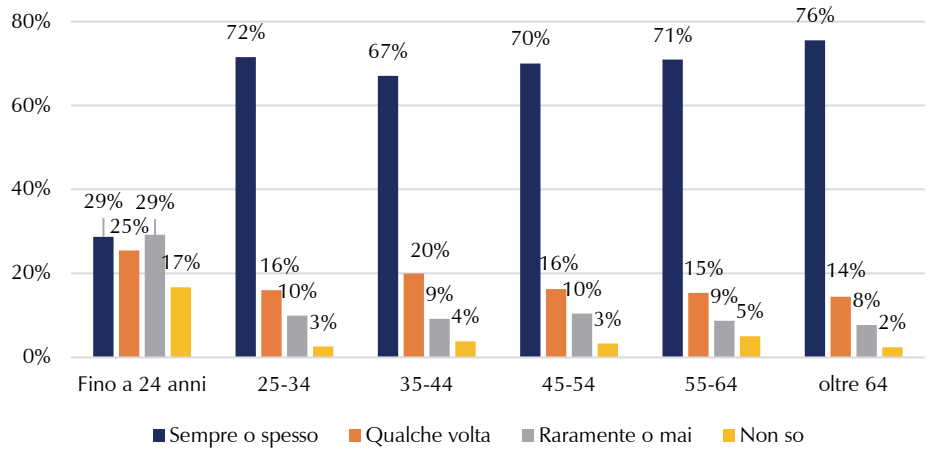
Il BNPL può aiutare ad avvicinare i consumatori al mercato del credito: l'indagine CRIF rileva che il 62% di chi richiede un finanziamento per la prima volta lo fa proprio attraverso prodotti di BNPL e che la quota di chi è senza storia creditizia all'interno del SIC è più alta fra i richiedenti di prodotti BNPL (13%) che fra i richiedenti di prestiti Small Ticket (8%).

Secondo la stessa indagine nel 2023 la rischiosità dei prodotti BNPL è peraltro rimasta contenuta – meno della metà di quella dei finanziamenti Small Ticket – e in calo rispetto al 2022.

Allo stesso tempo le piattaforme di BNPL – che sono di facile utilizzo, valutano le richieste di credito in tempi estremamente rapidi, spesso in maniera istantanea, e richiedono agli utilizzatori un numero esiguo di informazioni –potrebbero indurre i consumatori meno preparati ad accendere un finanziamento senza essere pienamente consapevoli delle conseguenze – per esempio in termini di interessi di mora –, oltre a favorire potenzialmente acquisti impulsivi ed eccessivi rispetto alle capacità di spesa determinando per gli utilizzatori l'accumulo inconsapevole di una quantità di debito complessivo non sostenibile.

I dati raccolti da Banca d'Italia mostrano che effettivamente solo il 29% degli under 24 dichiara di pagare regolarmente le rate dei propri finanziamenti o spese ricorrenti sempre o spesso, e fra le altre fasce d'età la media è di poco superiore al 70%, il che potrebbe essere sintomo di un generale problema di sovraindebitamento.

Figura 15 – Paga puntualmente l'affitto mensile, le rate di un debito, il mutuo, le bollette e altre spese ricorrenti (% di intervistati)



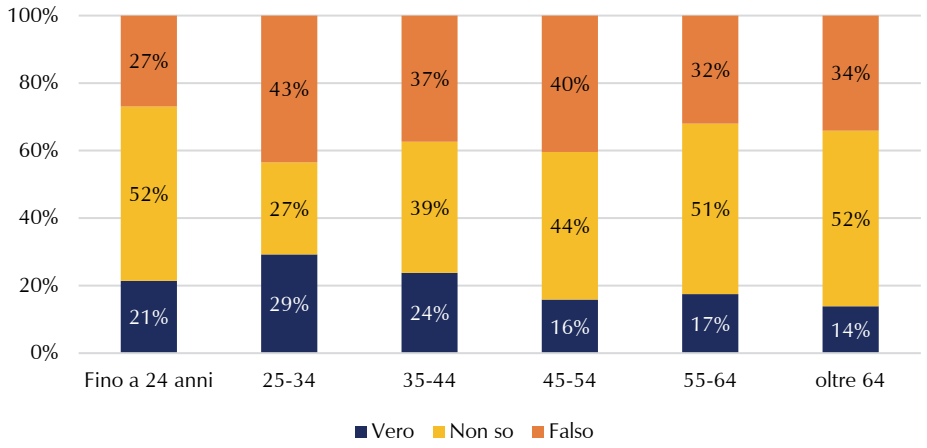

*Fonte: Dati Banca d'Italia elaborati dall'autore.*

## *Le competenze di finanza digitale*

La mancanza di competenze in materia di finanza digitale, oltre a determinare situazioni di sovraindebitamento e di possibile esclusione finanziaria, può contribuire anche a spiegare il timido accoglimento dei nuovi strumenti abilitati dalla tecnologia. Si è già detto della scarsa conoscenza fra gli italiani dell'uso che i terzi possono fare dei dati condivisi online e della limitata consapevolezza del valore contrattuale delle operazioni concluse in rete.

Pure la conoscenza dei nuovi strumenti tecnologici, come le criptovalute, appare nel complesso non adeguata. La maggior parte degli italiani non sa per esempio che le criptoattività – qualificate come moneta solo da fonti "commerciali" – non hanno in realtà un corso legale analogo a quello delle banconote: alla domanda hanno risposto correttamente solo 36 intervistati su 100 – e ancora meno (27%) fra gli under 25. Sorprende anche che la quota di giovani con meno di 24 anni che dichiarano di non sapere rispondere sia in linea con quella di chi ha più di 55 anni.

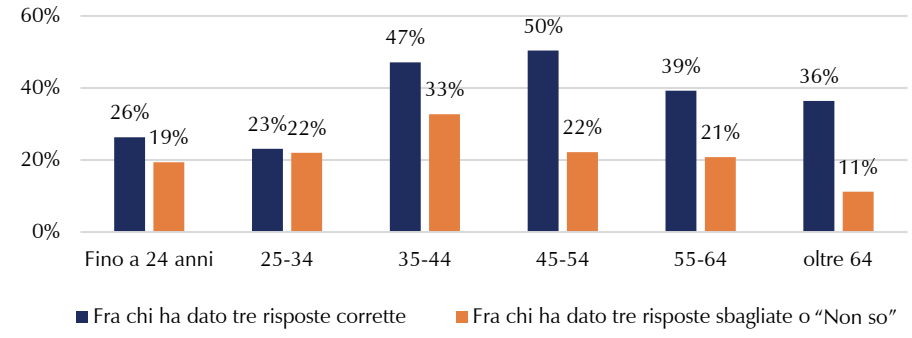
Figura 16 – Paga puntualmente l'affitto mensile, le rate di un debito, il mutuo, le bollette e altre spese ricorrenti (% di intervistati)




*Fonte: Dati Banca d'Italia elaborati dall'autore.*

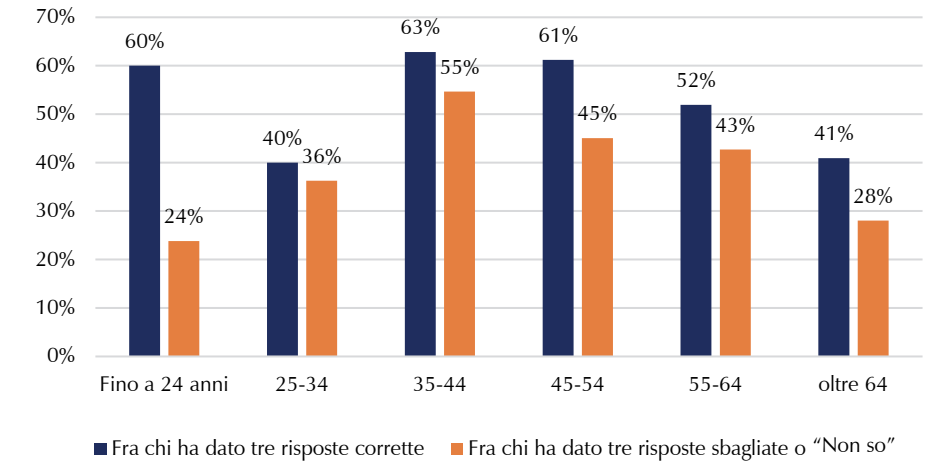
È confortante osservare che gli intervistati che hanno risposto correttamente alle tre domande che testano le competenze di finanza digitale (quella su corso legale delle criptoattività, quella sulle conseguenze della condivisione dei propri dati in rete e quella sulla validità dei contratti sottoscritti in rete) gestiscono online servizi e prodotti finanziari più frequentemente di quelli che non hanno saputo rispondere o hanno risposto in modo sbagliato. Fra chi ha risposto correttamente è anche più comune trasferire denaro online e aprire un conto o richiedere una carta con modalità interamente online. Indipendentemente dall'età, l'uso di prodotti e servizi tecnologici sembra dunque essere legato alle conoscenze in materia di finanza digitale.

Figura 17 – Gestisce online servizi e prodotti finanziari



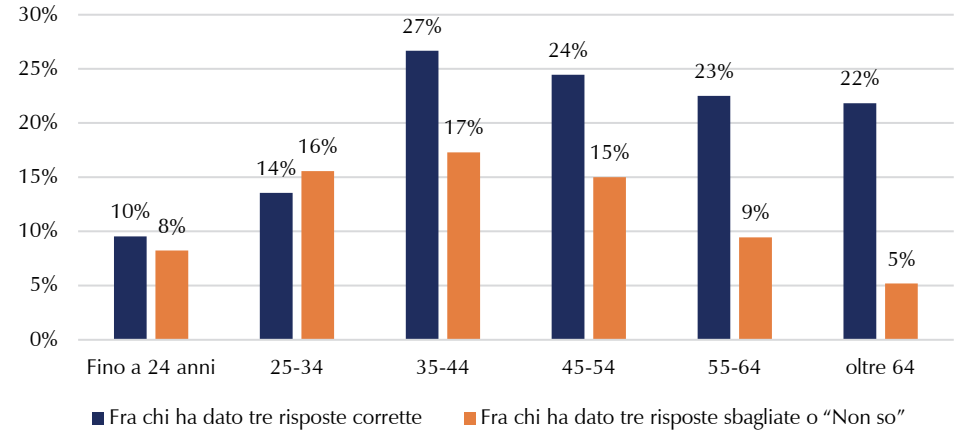

*Fonte: Dati Banca d'Italia elaborati dall'autore.*

Figura 18 – Ha trasferito online del denaro ad altri



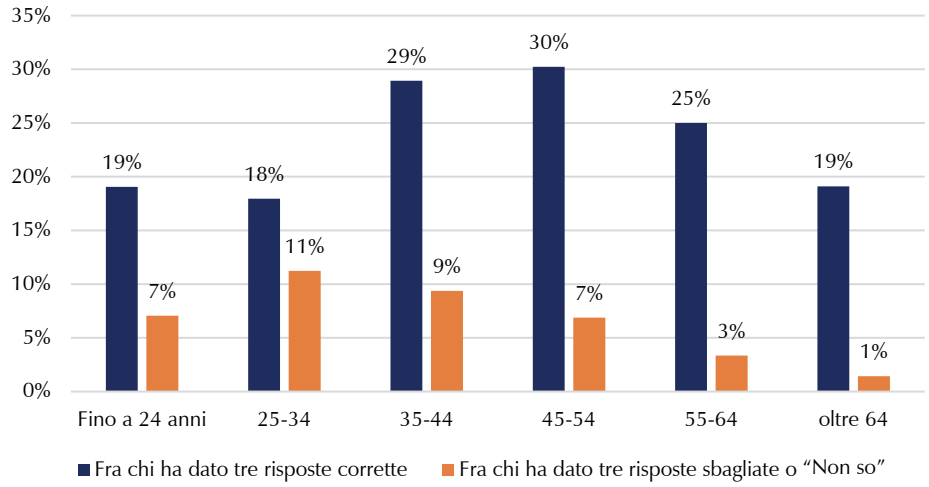

*Fonte: Dati Banca d'Italia elaborati dall'autore.*

Figura 19 – Ha aperto un c/c o di deposito con modalità interamente online




*Fonte: Dati Banca d'Italia elaborati dall'autore.*

Figura 20 – Ha chiesto con modalità interamente online una carta di debito o di credito, oppure una di pagamento

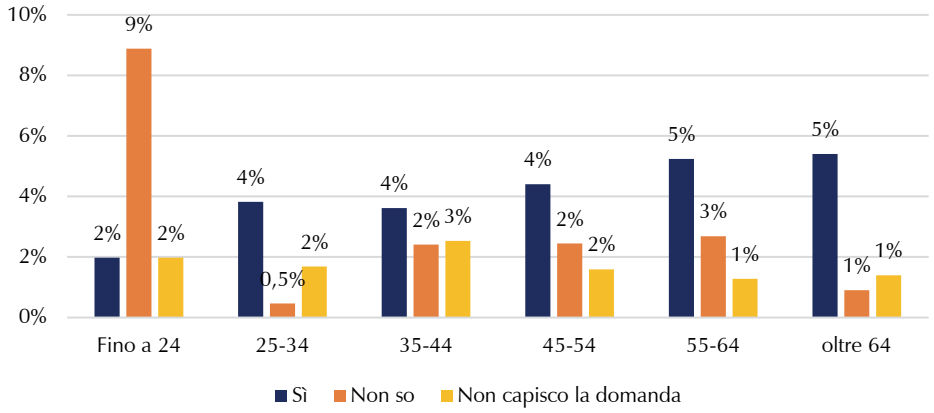



*Fonte: Dati Banca d'Italia elaborati dall'autore.*

Resta il fatto che, comunque, una quota non trascurabile di chi utilizza la rete per gestire prodotti e servizi finanziari ha risposto alle tre domande in modo sbagliato o ha dichiarato di non conoscere la risposta –indice di competenze finanziarie digitali non adeguate – e di conseguenza è maggiormente esposta al rischio di cadere vittima di truffe, di consentire inconsapevolmente all'utilizzo dei propri dati personali da parte di terzi, di sottoscrivere involontariamente contratti finanziari vincolanti o di acquistare prodotti finanziari non in linea con le proprie esigenze.

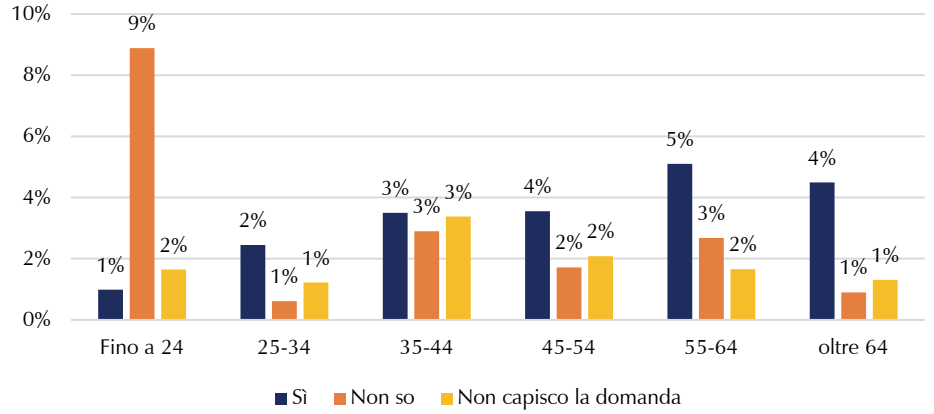
Il 4,4% degli intervistati ha in effetti dichiarato di avere scoperto che le proprie carte o i propri dati sono stati utilizzati senza autorizzazione per acquistare beni o servizi e il 3,7% ha rivelato di avere investito in qualcosa che si è poi rivelata una truffa. I numeri reali sono probabilmente persino più alti: il 4% circa degli italiani ha infatti affermato di non essere in grado di rispondere o di non avere capito la domanda, il che rende privo di senso un confronto fra fasce d'età.

Figura 21 – Domanda: Ho scoperto che qualcuno, senza essere autorizzato, ha utilizzato le mie carte (di credito, o bancomat, o prepagata) o i miei dati per acquistare beni o servizi.




*Fonte: Dati Banca d'Italia elaborati dall'autore.*

Figura 22 – Domanda: Ho accettato suggerimenti a investire in qualcosa che a seguito di accertamenti giudiziari si è rivelata una truffa (ad es. un prodotto che poggiava su uno schema piramidale fittizio)




*Fonte: Dati Banca d'Italia elaborati dall'autore.*

## 4. Conclusioni

L'analisi si è soffermata sul livello di conoscenze di finanza digitale degli italiani nelle sue due componenti: capacità basilare di usare dispositivi tecnologici per accedere ai servizi digitali e capacità di presidiare le vulnerabilità connesse all'utilizzo online di prodotti o servizi finanziari.

Il livello che risulta dai dati disponibili è nel complesso basso e comunque inferiore alla media europea; nonostante esista un'ampia offerta di strumenti di finanza digitale, la loro diffusione, sia nel settore dei pagamenti che in quello del credito, è ancora ben lontana da quella che si osserva nei Paesi digitalmente più avanzati in presenza di una domanda che stenta a crescere.

L'aspetto più da rimarcare, tuttavia, è che non si notano rilevanti segnali di inversione di tendenza, nemmeno nelle fasce più giovani della popolazione su cui da tempo si tenta di intervenire con programmi dedicati.

Le conseguenze della limitata diffusione degli strumenti di finanza digitale possono essere rilevanti: se il bacino dei dati utilizzabili non è adeguatamente alimentato dalle informazioni prodotte usando gli strumenti digitali, le istituzioni (finanziarie e non) potrebbero avere più difficoltà a offrire ai consumatori alcuni importanti benefici, fra i quali proposte più customizzate, segmentate e meno costose ma anche valutazioni del merito creditizio più precise e inclusive.

Si conferma quindi la necessità di investire nell'accrescimento delle competenze sui temi più rilevanti e con gli strumenti adatti, promuovendo fra cittadini e imprese una cultura del digitale che abbracci il cambiamento e supporti l'innovazione affinché tutti possano trarre vantaggio dalla digitalizzazione della finanza.

Sul fronte dell'educazione finanziaria, anche in chiave digitale, Banca d'Italia promuove iniziative da tempo. Una questione importante riguarda la capacità di tali iniziative di raggiungere efficacemente i destinatari. Per arrivare ai più giovani sarebbe auspicabile che questi temi diventino materia obbligatoria nelle scuole; la recente scelta della legge italiana [13] di inserire l'educazione finanziaria nell'educazione civica, insegnamento trasversale alle varie materie, va in questa direzione [14].

Come evidenziato in diversi lavori, tuttavia, perché ciò sia efficace è necessario anche che gli insegnanti possiedano le competenze da trasmettere [15]. Dal 2021 Banca d'Italia ha avviato un progetto sperimentale per inserire l'educazione finanziaria nei corsi di laurea in Scienze della formazione primaria. È un progetto con un grande potenziale perché, da un lato, si rivolge ai futuri inse-

[13] Legge 5 marzo 2024, n. 21, c.d. Legge sulla competitività dei capitali.

[14] Si veda anche M. Bianco, *L'educazione finanziaria nelle scuole. Indicazioni dall'esperienza internazionale e da quella della Banca d'Italia*, giugno 2024.

[15] R. De Bonis, M. Guida, A. Romagnoli, A. Staderini, QeF N.726, *Educazione finanziaria: presupposti, politiche ed esperienza della Banca d'Italia*, ottobre 2022.

gnanti quando sono ancora nel loro percorso di formazione, e dall'altro consentirà di raggiungere i destinatari finali nella scuola primaria, negli anni cioè più fruttuosi dell'apprendimento. In questo contesto sarebbe opportuno dedicare uno spazio anche alla formazione di una cultura digitale di base, fondamentale per contribuire alla cybersicurezza del sistema.

Se gli sforzi fatti per promuovere l'educazione finanziaria e la cultura digitale fra la popolazione avranno successo e rafforzeranno la domanda italiana di prodotti fintech, oltre ai già citati benefici per i consumatori si potrebbero determinare riflessi positivi anche sul livello degli investimenti nell'ecosistema fintech nazionale, le cui dimensioni oggi sono contenute e inferiori a quelle degli altri Paesi europei [16].

[16] STATISTA (2024), *Value of investment in the fintech sector in Europe in 2023*, by country.

# Il sogno e l'attuazione di una Banca Fintech: innovazione, accessibilità e futuro dei servizi bancari e finanziari

Paolo Martini



## 1. TNB: un modello pionieristico di Wealth Fintech Bank

L'ambizione di trasformare l'accesso ai servizi finanziari da privilegio a diritto universale ha ispirato il progetto di TNB (The Next Bank), la Banca Fintech nata da un'idea del management di Azimut. Questo "sogno" che sarà oggetto di una rapida esposizione in queste pagine, nasce dalla visione di una finanza innovativa, accessibile e sostenibile, capace di liberarsi dalle barriere tradizionali e guidare una nuova era dell'intermediazione patrimoniale.

Non sarà possibile descrivere nel dettaglio tutto il modello ma appare di interesse sottolineare come uno degli aspetti di maggiore interesse del progetto TNB è l'idea di una banca che evolve per diventare una piattaforma digitale fluida, dove la tecnologia più avanzata e la consulenza umana si fondono per creare soluzioni personalizzate, sicure e scalabili.

Questo contributo cerca di far comprendere come TNB incarni una nuova generazione di istituzioni finanziarie, radicata nel desiderio di realizzare un "sogno" condiviso: democratizzare la finanza e prepararla alle sfide di un futuro in rapida trasformazione.

L'innovazione tecnologica è ovviamente il cuore pulsante del progetto TNB, che si distingue per la sua natura ibrida rappresentata da una banca digitale costruita sulla sinergia tra intelligenza artificiale, automazione dei processi e competenza umana.

A differenza delle banche tradizionali, TNB mira a essere una piattaforma agile e scalabile, focalizzata su soluzioni modulari per il cliente, basandosi sulla combinazione di alcuni strumenti specifici che possiamo così enucleare:

• **ricorso all'Intelligenza artificiale per la personalizzazione dei portafogli**: algoritmi avanzati analizzano i dati del cliente per costruire portafogli su misura, riducendo i costi di gestione e migliorando la performance del capitale investito (Philippon 2016);

• **sfruttamento di tecnologie blockchain e smart contract**: per garantire sicurezza e trasparenza, TNB adotta ledger distribuiti, che automatizzano la verifica delle transazioni e permettono così di ridurre i tempi di esecuzione (Gomber et al. 2018);

• **architettura aperta e integrazione API**: la banca sfrutta un ecosistema fintech collaborativo, integrando servizi di terzi per ampliare l'offerta di prodotti.

Questi strumenti possono rivoluzionare il wealth management, rendendolo più accessibile, flessibile e personalizzato rispetto ai modelli tradizionali.

## 2. Accessibilità come strumento di democratizzazione finanziaria

Secondo la Banca Mondiale, circa 1,7 miliardi di persone non hanno accesso ai servizi bancari (Demirgüç-Kunt et al. 2018). Proprio questo dato e la sfida che esso rappresenta hanno spinto TNB ad affrontare questa sfida per implementare e garantire un sistema finanziario più inclusivo, in grado di ridurre le barriere all'ingresso.

A questo scopo, la scelta di TNB è stata quella di seguire i driver di sviluppo di seguito enuclati:

• **Mobile banking come canale principale**

I clienti potranno aprire conti e gestire investimenti senza la necessità di una presenza fisica. Questo approccio potrà anche essere particolarmente efficace nei mercati emergenti, dove le infrastrutture bancarie tradizionali sono carenti (Arner et al. 2015).

• **Costi ridotti per i servizi di pagamento e trasferimenti internazionali**

La disintermediazione può consentire tariffe più competitive rispetto a quelle garantite dagli istituti tradizionali.

• **Inserimento di piattaforme educative integrate**:

Queste piattaforme sono strumenti finalizzati a migliorare la conoscenza finanziaria e a supportare decisioni consapevoli. Questo approccio del resto è supportato da studi che evidenziano come la consapevolezza finanziaria riduca i rischi di indebitamento e miglioramenti nell'investimento a lungo termine (Beck et al. 2019).

• **Supporto alle PMI con riduzione dei costi e velocizzazione dei servizi attraverso la tecnologia.**

TNB utilizzerà tecnologie avanzate per abbattere i costi operativi e accelerare la fornitura di servizi bancari, offrendo soluzioni innovative che permettono alle PMI di accedere a finanziamenti, servizi di pagamento e consulenze con maggiore efficienza e a costi inferiori rispetto agli istituti bancari tradizionali. In particolare, la scelta di utilizzo di algoritmi per l'elaborazione automatica delle pratiche di prestito, la gestione delle transazioni e l'automazione dei servizi di assistenza clienti consentirà di ridurre i costi operativi.

Ad esempio, tramite l'AI, TNB potrà automatizzare l'analisi del rischio e la valutazione del credito, un processo tradizionalmente laborioso e costoso per le banche tradizionali. Ciò consentirà di offrire prestiti a tassi di interesse competitivi e con tempi di approvazione molto più rapidi (KPMG 2020).

Le tecnologie digitali permetteranno poi a TNB di raccogliere informazioni sulle PMI in tempo reale tramite l'analisi di dati alternativi, come transazioni bancarie, vendite online o dati provenienti da social media. Questo approccio consente di velocizzare il processo di valutazione del credito e abbattere le barriere burocratiche tipiche delle banche tradizionali (Berger, Udell 2006).

Attraverso questo approccio, TNB porterà il suo contributo all'obiettivo di rendere il sistema bancario più equo e accessibile.

## 3. Sfide normative e soluzioni innovative per la sicurezza

La sicurezza e la conformità normativa rappresentano le principali sfide per le banche fintech. TNB ha deciso di adottare un approccio proattivo, implementando tecnologie all'avanguardia e collaborando con i regolatori per garantire il rispetto delle leggi vigenti.

Del resto un ambiente normativo chiaro, abbinato a un'adozione tecnologica responsabile, è fondamentale anche per favorire la fiducia del mercato.

A tal fine TNB intende lavorare su tre strategie principali:

• **protezione dei dati personali**: le soluzioni crittografiche e i protocolli di autenticazione avanzati (come l'autenticazione biometrica) sono essenziali per prevenire accessi non autorizzati e garantire la privacy (Zetzsche et al. 2017);

• **prevenzione delle frodi con l'intelligenza artificiale**: i modelli di machine learning identificano comportamenti anomali e potenziali minacce, rafforzando i sistemi antifrode;

• **compliance dinamica**: attraverso l'uso di smart contracts, le normative possono essere applicate automaticamente alle transazioni, riducendo i rischi operativi.

## 4. Sostenibilità: il nuovo paradigma del banking

Infine ultimo ma non meno importante il tema della sostenibilità. La sostenibilità non è più soltanto un'opzione, ma una necessità per il settore finanziario.

TNB mira ad integrare la sostenibilità nelle sue strategie, promuovendo investimenti responsabili e pratiche aziendali ecologiche.

**• Finanziamenti green e sostenibili**

La banca offrirà strumenti come green bonds e fondi ESG, seguendo il trend di crescita dell'investimento responsabile (Schoenmaker, Schramade 2019).

**• Analisi del rischio ESG**

Algoritmi di valutazione del rischio considerano fattori ambientali, sociali e di governance per migliorare la gestione dei portafogli.

**• Riduzione dell'impatto ambientale**

Un modello completamente digitale elimina la necessità di filiali fisiche, riducendo il consumo di energia e risorse naturali.

Allo stesso tempo, verranno affrontate le sfide energetiche proprie della digitalizzazione, ed in particolare:

**• Ottimizzazione dei data center**

Investimento in data center efficienti dal punto di vista energetico, alimentati da fonti rinnovabili.

**• Modelli AI più sostenibili**

La ricerca su modelli di intelligenza artificiale meno energivori è in crescita. È necessario adottare quanto più possibile approcci basati su tecnologie di compressione dei modelli e apprendimento federato.

**• Cloud computing sostenibile**

Utilizzo di fornitori di servizi cloud impegnati nella sostenibilità.

Queste iniziative posizionano TNB come un esempio di banca sostenibile, pronta a guidare il cambiamento verso un'economia più resiliente e inclusiva.

Ogni grande innovazione nasce da un sogno. TNB rappresenta la materializzazione di una visione audace, dove la tecnologia è al servizio delle persone e la finanza diventa un ecosistema inclusivo, accessibile e sostenibile.

Come un ponte tra passato e futuro, l'obiettivo di TNB non è solo quello di integrare soluzioni digitali, ma immagina un sistema bancario in cui il cliente è al centro, con esperienze personalizzate, trasparenza e sicurezza.

Potremmo dire che questa banca fintech è la risposta concreta a una domanda che guida l'evoluzione del settore: come possiamo rendere la finanza più equa, innovativa e resiliente? Guardando avanti, il sogno che ha dato vita a TNB continuerà a ispirare nuovi modelli e opportunità, ridisegnando i confini della possibilità in un mondo sempre più interconnesso.

## 5. Una riflessione finale sull'equilibrio tra innovazione tecnologica ed esperienza dell'uomo

La digitalizzazione è la chiave per una banca moderna, efficiente e accessibile, capace di abbattere le barriere geografiche e democratizzare i servizi finanziari. Grazie all'intelligenza artificiale, ai big data e alla blockchain, le banche digitali possono offrire esperienze personalizzate, ridurre i costi operativi e migliorare la sicurezza delle transazioni.

Inoltre, l'evoluzione della consulenza finanziaria digitale, attraverso robot-advisor e piattaforme di wealth management basate su AI, permette di fornire strategie di investimento sofisticate e personalizzate a un pubblico più ampio. Tuttavia, l'elemento umano rimane essenziale e non può essere trascurato.

La fiducia, la consulenza personalizzata e l'inclusione finanziaria dipendono ancora dalla capacità di comprendere le esigenze specifiche dei clienti, evitare discriminazioni algoritmiche e garantire che la tecnologia sia utilizzata per il bene collettivo.

Una banca digitale di successo deve quindi trovare il giusto equilibrio tra innovazione tecnologica e centralità dell'esperienza umana, integrando strumenti avanzati con il supporto di esperti capaci di guidare scelte finanziarie consapevoli.

## Bibliografia

ARNER D.W., BARBERIS J., BUCKLEY R.P. (2015), *The Evolution of Fintech: A New Post-Crisis Paradigm?*, Paper No. 2015/047, University of Hong Kong Faculty of Law Research, Hong Kong.

ARNER D.W., BARBERIS J., BUCKLEY R.P. (2017), *FinTech, RegTech, and the Reconceptualization of Financial Regulation*, in *Northwestern Journal of International Law & Business*, 37(3), 371-413.

BECK T., DEMIRGÜÇ-KUNT A., LEVINE R. (2019), *Finance and Inequality: Theory and Evidence*, in *Annual Review of Financial Economics*, 11, pp. 145-163.

BERGER A.N., UDELL G.F. (2006), *A more complete conceptual framework for SME finance*, in *Journal of Banking & Finance*, 30(11), pp. 2945-2966.

DEMIRGÜÇ-KUNT A., KLAPPER L., SINGER D., VAN OUDHEUSDEN P. (2018), *The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution*, World Bank Group.

FENWICK M., KAAL W.A., VERMEULEN E.P. (2020), *Legal Innovation and Technology in Global Financial Markets*, in *Journal of Financial Regulation*, 6(1), pp. 45-62.

GOMBER P., KOCH J.A., SIERING M. (2018), *Digital Finance and Fintech: Current Research and Future Research Directions*, in *Journal of Business Economics*, 88, pp. 537-580.

KPMG (2020), *The rise of fintech and its impact on SMEs*, KPMG International.

MÖSLEIN F., GLOSTEN L.R. (2020), *Robo-Advisors and the Future of Financial Advice: Market Developments and Regulatory Challenges*, European Banking Institute Working Paper Series.

PHILIPPON T. (2016), *The FinTech Opportunity*, in *NBER Working Paper*, No. 22476.
SCHOENMAKER D., SCHRAMADE W. (2019), *Principles of Sustainable Finance*, Oxford University Press, Oxford.
SIRONI P. (2016), *FinTech Innovation: From Robo-Advisors to Goal Based Investing and Gamification*, Wiley.
VIVES X. (2019), *Digital Disruption in Banking*, in *Annual Review of Financial Economics*, 11, pp. 243-272.
WORLD BANK (2022), *The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19*, Washington, DC, World Bank Publications.
ZETZSCHE D.A., BUCKLEY R.P., ARNER D.W., BARBERIS J. (2017), *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*, in *Fordham Journal of Corporate & Financial Law*, 23, pp. 31-103.
ZUBOFF S. (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs.

# *Investment crowdfunding*: tra eccesso regolatorio e questioni aperte

Ugo Minneci

SOMMARIO: 1. La parabola normativa del crowdfunding. – 2. Il Regolamento UE 2020/1503 e le sue criticità. – 3. L'oggetto dell'offerta in sottoscrizione. – 4. La tutela dei sottoscrittori. – 5. L'assenza di un mercato secondario.

## 1. La parabola normativa del crowdfunding

*Mutatis mutandis* e con un certo grado di approssimazione l'evoluzione regolatoria dell'*investment crowdfunding* appare ricalcare quella dei monopattini elettrici, prestandosi ad essere idealmente suddivisa in tre fasi [1].

La prima è senz'altro quella dell'*entusiasmo*, indotta dal convincimento di avere trovato – grazie alla innovazione tecnologica – un principio di soluzione per una serie di problemi fino a quel momento considerati insuperabili: in un caso, la congestione del traffico urbano; nell'altro l'estrema difficoltà per le piccole-medie imprese (PMI) di reperire risorse al di fuori della ristretta compagine dei soci e del canale bancario. Tale *sentiment* ha indotto il nostro legislatore (che, una volta tanto, si è mosso prima degli altri) a creare un ambiente normativo più che amichevole attraverso l'introduzione di deroghe ed esenzioni rispetto alle regole vigenti.

La stagione successiva può definirsi quella del *dubbio*, rispettivamente legata da un lato ai problemi di sicurezza propria e altrui generati dall'utilizzo dei monopattini e dall'altro all'assedio dei vincoli di sistema che, specie con riguardo alle s.r.l., ha fin da subito circondato le prime esperienze di raccolta di capitali tramite piattaforme di crowdfunding. Nell'ambito di tale fase si sono moltiplicati gli interrogativi e le perplessità in ordine alla possibilità per i nuovi innesti di attecchire su un terreno già profondamente arato.

L'ultimo periodo è quello del *ripensamento* che ha spinto il legislatore (unionale e interno) ad intervenire di nuovo con l'introduzione di plessi normativi sem-

[1] Per un *excursus* storico sulla evoluzione normativa in materia, v. E. FREGONARA, *La dematerializzazione delle quote di piccole e medie imprese*, in *Riv. soc.*, 2024, I, 754 ss.

pre più corposi e onerosi per gli operatori del settore, ma lasciando – almeno con riferimento al fenomeno delle piattaforme di crowdfunding – ancora molte questioni aperte.

Nell'abbandonare un parallelismo che deve rimanere puramente impressionistico, non è forse superfluo ricordare che il crowdfunding si lascia declinare in quattro varianti: da una parte, il *donation-based crowdfunding* che consiste in una forma di raccolta di risorse per la realizzazione di un progetto ispirato da finalità esclusivamente altruistiche; dall'altra parte il *reward-based, l'investment based* e il *lending based crowdfunding* che prevedono rispettivamente, in contropartita della attribuzione erogata, il diritto a una controprestazione costituita da un bene o servizio; oppure la titolarità di una partecipazione sociale o di un credito incorporato in un titolo (a seconda dei casi, *equity* o *debt crowdfunding*), oppure ancora il diritto di credito alla restituzione della somma prestata con l'aggiunta degli interessi (*lending crowdfunding*) [2].

Ribadito che nel presente lavoro ci si soffermerà sull'*investment crowdfunding* [3], occorre fin da ora ricordare che il fenomeno in esame ha posto e pone

---

[2] Sulle varie declinazioni del crowdfunding cfr. l'ampio lavoro monografico di A. RENDA, *Donation-based crowdfunding: raccolte fondi oblative e donazioni di scopo*, Giuffrè, Milano, 2021.

[3] Per quanto di conio relativamente recente, la normativa in tema di *equity* e *lending crowdfunding* ha già formato oggetto di numerosi interventi da parte della dottrina. In particolare cfr. L. ENRIQUES, *La disciplina italiana uccide il crowdfunding nella culla*, in AA.VV., *Aspetti giuridici del crowdfunding*, a cura di G. MOSCO, Bologna, s.d.; A. TROISI, *Crowdfunding e mercato creditizio: profili regolamentari*, in *Contr. impr.*, 2014, p. 519 ss.; M. VITALI, *Equity crowdfunding: la nuova frontiera della raccolta del capitale di rischio*, in *Riv. soc.*, 2014, p. 371 ss.; A. GUACCERO, *La start-up innovativa in forma di società a responsabilità limitata: raccolta del capitale di rischio ed* equity crowdfunding, in *Banca borsa tit. cred.*, 2014, I, p. 699 ss.; V. SANTORO, E. TONELLI, *Equity crowdfunding ed imprenditorialità innovativa*, in *Riv. dir. banc.*, 2014, p. 1 ss.; M.L. PASSADOR, *Crowdfunding: tra profili di adeguatezza ed appropriatezza e profili di applicabilità all'aumento di capitale*, in *Banca impresa soc.*, 2015, p. 287; E. FREGONARA, *L'equity based crowdfunding: un nuovo modello di finanziamento per le start up innovative*, in *Giur. it.*, 2016, p. 2287 ss.; R. CARATOZZOLO, *L'utilizzo delle nuove tecnologie per il finanziamento delle imprese*, in AA.VV., *Fintech – Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi di finanziari*, a cura di M.T. PARACAMPO, Giappichelli, Torino, 2019, II, p. 147 ss.; N. DE LUCA, S. FURNARI, A. GENTILE, voce Equity crowdfunding, in *Dig. disc. priv.*, sez. comm. Agg., 2017, p. 159 ss.; E. MACCHIAVELLO, *La travagliata evoluzione normativa dell'equity crowdfunding in Italia*, in *Riv. dir. banc.*, 2018, p. 1 ss.; E. MACCHIAVELLO, *La problematica regolazione del lending-based crowdfunding in Italia*, in *Banca borsa tit. cred.*, 2018, I, p. 63 ss.; U. MINNECI, Equity crowdfunding: *gli strumenti a tutela dell'investitore*, in *Riv. dir. civ.*, 2019, I, p. 509 ss.; M. LAMANDINI-D. RAMOS MUNOZ, *La disciplina dell'equity crowdfunding nella prospettiva dell'emittente e del diritto societario: verso il sub-tipo emittente digitali*, in *Fintech: diritti, concorrenza, regole*, a cura di G. FINOCCHIARO e V. FALCE, ZANICHELLI**,** Bologna, 2019, p. 255 ss.; G. BALP, *P2P lending e invoice lending*, in *Diritto del fintech*, a cura di M. CIAN e C. SANDEI, Wolters Kluwer, Torino, 2020, p. 303 ss.; N. CIOCCA, *I portali per il crowdfunding*, in *Diritto del fintech*, cit., p. 243 ss.; V. DE STASIO, *Il crowdfunding*, in *Il Testo unico Finanziario*, a cura di M. CERA e G. PRESTI, Zanichelli, Bologna, 2022, II, p. 2325 ss.; P. SPOLAORE, *S.R.L. e offerta al pubblico di partecipazioni sociali*, Giuffrè, Milano, 2022; S. CORSO, A. LAUDONIO, *Le s.r.l. aperte al mercato tra* crowdfunding *e sperimentazione di nuovi ambienti digitali*, in *Orizzonti dir. comm.*, 2024, p. 119 ss.; P.P. PIRANI, *Verso la s.r.l. aperta: ultimo atto?*, in *Giur. comm.*, 2024, I, p. 108 ss.

tuttora al regolatore la seguente sfida: quella di creare un ambiente normativo idoneo allo sviluppo di uno strumento che, almeno sulla carta, dovrebbe facilitare per le piccole-medie imprese (PMI) il reperimento sul mercato di risorse aggiuntive (in termini di capitali tanto di rischio quanto di debito), senza travolgere i principi consolidati del diritto societario (specie con riguardo alle imprese costituite nella forma delle s.r.l.) e senza neppure lasciare gli investitori comuni privi di protezione. Il tutto però nella consapevolezza della necessità di concedere un allentamento dei vincoli e dei presidi richiesti all'uopo dal tradizionale diritto dei mercati finanziari: vincoli e presidi che, se mantenuti invariati e richiamati meccanicamente, finirebbero per risultare troppo gravosi per operatori economici le cui dimensioni risultano decisamente minori rispetto a quelle degli emittenti per i quali sono stati pensati.

## 2. Il Regolamento UE 2020/1503 e le sue criticità

Nell'oggi il cuore della disciplina dell'*investment crowdfunding* dovrebbe rinvenirsi nel Regolamento UE 2020/1503 che ha – come noto – introdotto una normativa *ad hoc* al duplice scopo di agevolare l'accesso delle PMI alla raccolta di capitali presso il pubblico e di creare all'interno del mercato europeo un contesto normativo il più possibile uniforme anche nell'ottica di favorire la prestazione transfrontaliera dei relativi servizi.

Nel perseguimento di tali obiettivi, il legislatore unionale ha *cercato* di introdurre regole di armonizzazione massima, ovvero regole destinate a prevalere su eventuali normative interne difformi; solo che la materia ha finito per sfuggirgli di mano, con la conseguenza che si è venuto a produrre una sorta di *monstre* giuridico.

In primo luogo, occorre segnalare come l'ampio utilizzo del meccanismo della delega legislativa abbia fatto sì che nel giro di un rapido torno di tempo siano stati adottati un numero impressionante di Regolamenti attuativi, con l'effetto di creare un plesso normativo di dimensioni gigantesche e in palese contraddizione con l'idea originaria di dettare un *corpus* normativo leggero, in quanto costruito su misura per imprese di minori dimensioni. In particolare, il riferimento corre al Regolamento delegato 2022/2018 in materia di elementi del metodo di valutazione del rischio di credito; al Regolamento delegato 2022/2112 in tema di requisiti e modalità per la domanda di autorizzazione come fornitore di servizi di crowdfunding; al Regolamento delegato 2022/2016 sulle misure e procedure di continuità operativa; al Regolamento delegato 2022/2115 con riguardo al metodo di calcolo dei tassi di default dei prestiti; al Regolamento delegato 2022/2011 con riferimento agli obblighi in materia di conflitto di interesse; al Regolamento delegato 2022/2113 avente ad oggetto i *regulatory technical standards* sullo scambio di informazioni tra autorità competenti ai fini dell'attività di vigilanza e di contrasto delle violazioni; al Regolamento delegato 2022/2118 sulla gestione individuale di portafogli prestiti; al Regolamento delegato 2022/2014 sul test di in-

gresso di verifica delle conoscenze e la simulazione della capacità di sostenere perdite per i potenziali investitori non sofisticati in progetti di *crowdfunding*; al Regolamento delegato 2022/2019 sul contenuto della scheda recante le informazioni chiave sull'investimento; al Regolamento delegato 2022/2117 sulle modalità di trattamento dei reclami; al Regolamento delegato 2022/2123 in materia di formulari, modelli e procedure standard per le notifiche all'ESMA delle prescrizioni nazionali concernenti il *marketing*.

A ciò deve aggiungersi che il Regolamento UE 2020/1503 ha rimesso ai Paesi membri alcune scelte di rilievo fondamentale, tra cui quella di includere o meno le quote di s.r.l. tra i tipi di partecipazione sociali suscettibili di formare oggetto di una offerta unitaria di sottoscrizione tramite portali on line e l'estensione del perimetro soggettivo della responsabilità verso gli investitori nell'ipotesi di divulgazione al pubblico di informazioni false e/o decettive in relazione all'investimento proposto [4]. Il tutto con il risultato di azzoppare – in larga misura – l'aspirazione di creare un ecosistema normativo di impronta unitaria.

Nel complesso, è venuto a formarsi un set di regole farraginoso, difficile da maneggiare, con la permanenza di accentuate caratterizzazioni nazionali, nonché contraddistinto da ampie zone di opacità.

Non è questa la sede per svolgere un esame approfondito dell'intera disciplina in materia. Circoscrivendo l'analisi al nostro Paese, ci si soffermerà sui punti che richiamano tuttora l'attenzione dell'interprete. Più precisamente, , i temi affrontati riguarderanno l'oggetto dell'offerta, gli strumenti di protezione per gli investitori, nonché le carenze strutturali che continuano a inficiare l'architettura normativa.

## 3. L'oggetto dell'offerta in sottoscrizione

È noto che, nell'adeguare la normativa nazionale al Regolamento UE 2020/1503, il d.lgs. 10 marzo 2023, n. 30 ha riscritto l'art. 100-ter t.u.f.

Rispetto alla precedente versione, facendo uso dello spazio di manovra concesso dal testo unionale, il legislatore italiano ha incluso, tra i «titoli ammessi» suscettibili – unitamente ai valori mobiliari – di formare oggetto di offerta in sottoscrizione tramite portali on line anche le quote di s.r.l., non solo PMI, ma pure di grandi dimensioni: il tutto in deroga all'art. 2468 c.c. e nei limiti previsti dal Regolamento 2020/1503 [5].

---

[4] Cfr. P. SPOLAORE, *Il regime del crowdfunding tra fonti europee e nazionali*, in *Nuova giur. civ. comm.*, 2024, p. 397 ss.

[5] Sul significato nell'oggi del divieto di offerta al pubblico di quote di s.r.l. di cui all'art. 2468 c.c.) v. P.P. PIRANI, *Verso la s.r.l. aperta*, cit., p. 1103 ss.; R. LENER, *Nuove quote o nuova s.r.l.? Pensare prima di legiferare*, in *An. giur. econ.*, 2024, p. 29 ss.; S. GUIZZARDI, *La s.r.l. che si apre al mercato,* in *Europa dir. priv.,* 2024, p. 148 ss.

La scelta compiuta, se da un lato si rivela apprezzabile nella misura in cui ha eliminato una limitazione all'utilizzo della tecnica del crowdfunding che, nell'essere basata sul mero superamento di una soglia dimensionale, non brillava per ragionevolezza, dall'altro lato, appare censurabile per il fatto di non essersi preoccupata di estendere alle s.r.l. grandi o grandissime le medesime deroghe alla disciplina del tipo (come quella di emettere categorie di quote con diritti diversi, con diritto di voto limitato o prive di diritti di voto o con riduzione, se non addirittura ablazione, dei diritti di controllo e/o della legittimazione all'esercizio individuale dell'azione sociale) che sono da tempo consentite alle s.r.l.-PMI.

È peraltro vero che, alla luce di una lettura sistematica del dato normativo, non sembra potersi mettere in discussione la possibilità anche per le s.r.l. diverse dalle PMI di canalizzare attraverso portali on line l'offerta di partecipazioni-tipo, ovvero di quote standardizzate, suscettibili a propria volta di essere qualificate come valori mobiliari. In effetti, sul punto una diversità di trattamento così marcata rispetto alle s.r.l.-PMI non avrebbe ragione di darsi [6].

La riscrittura dell'art. 100-ter t.u.f. ha altresì eliminato ogni riferimento al *debt crowdfunding*, ovvero all'offerta tramite portale di titoli di debito. Sicura la proponibilità di strumenti obbligazionari emessi dalle S.p.A. (trattandosi senza dubbio di valori mobiliari), qualche dubbio potrebbe sorgere rispetto ai titoli rilasciati dalle s.r.l. *ex* art. 2483 c.c. [7].

Vi è tuttavia da rilevare che, come osserva autorevole dottrina [8], «l'art. 2483 c.c. parla di titoli: il richiamo a frazionamenti in unità omogenee del capitale raccolto e a tecniche cartolari – vale a dire documenti idonei a circolare nella disciplina stabilita dagli artt. 1992 ss. – viene perciò naturale»; e con esso – preme aggiungere – l'inquadramento degli stessi nei valori mobiliari.

Del resto, prevedendo che «il gestore del portale assicura che per ciascuna offerta avente ad oggetto titoli di debito siano rispettati i limiti posti dall'art. 2483 c.d. ove pertinenti, nonché gli ulteriori limiti posti dalla disciplina speciale applicabile», lo stesso art. 13, comma 5-quinquies, punto *ii*) del Regolamento Consob sulla raccolta di capitali tramite portali on line (adottato con delibera n. 18592 del 26 giugno 2013 e aggiornato con delibera n. 21259 del 6 febbraio 2020) viene implicitamente ad ammettere la suscettibilità anche dei titoli di debito *ex* art. 2483 c.c. ad integrare l'oggetto di una offerta tramite portali on line.

---

[6] Il tema è approfondito da F. BRIZZI, *Offerta al pubblico e circolazione delle quote di s.r.l. in seguito alla novella dell'art. 100.ter t.u.f.: prime riflessioni*, in *Orizzonti dir. comm.*, 2023, p. 894 ss.

[7] Il punto è trattato da P. SPOLAORE, *Struttura finanziaria della s.r.l. e raccolta di capitali* online, in *Società*, 2024 p. 303 ss., il quale sottolinea che la raccolta di capitale di debito attraverso portali *on line* deve ritenersi comunque pacifica in virtù di quanto previsto dal Reg. UE 2020/1503. In senso analogo, M. GARCEA, *Società a responsabilità limitata e raccolta di capitale di credito,* in *Riv. dir. comm.*, 2023, p. 383 ss.

[8] LIBONATI, *Diritto commerciale. Impresa e società*, Giuffrè, Milano, 2005, p. 462. Per un primo catalogo dei problemi legati alla raccolta di capitale debito da parte della piccola e media impresa, v. M. MAUGERI, *Capitale di debito, minibond e informazione imperfetta del mercato*, in *Riv. dir. comm.*, 2015, I, p. 449 ss.

Semmai, il problema riguarda non tanto l'*an* ma il *quomodo* di una simile sollecitazione all'investimento. Nel fare salvi i limiti posti dall'art. 2483 c.c. ove pertinenti, proprio la norma regolamentare appena menzionata lascia aperta la questione se la relativa offerta debba essere riservata a investitori professionali soggetti a vigilanza, nonché gravati dal vincolo di garanzia della solvenza del soggetto emittente, nell'ipotesi di cessione successiva dei titoli in questione a investitori comuni.

Pur trattandosi di questione allo stato incerta [9], ragioni di coerenza sistematica inducono a propendere per una risposta negativa. E ciò per almeno tre ordini di ragioni.

In primo luogo, perché non avrebbe senso selezionare la platea dei potenziali destinatari dell'offerta dei titoli di debito *ex* art. 2483 c.c., quando non viene prevista alcuna limitazione di natura soggettiva nell'ipotesi di collocamento tramite portali on line delle quote di s.r.l. In altri termini, a ragionare in maniera opposta, si verrebbe a scontare un regime più rigoroso per una soluzione di investimento, la sottoscrizione di capitale di debito, reputata tradizionalmente meno pericolosa di una sollecitazione a sottoscrivere capitale di rischio.

Inoltre, è lo stesso già citato art. 13, comma 5-quinquies, punto *ii*) a lasciare uno spazio di manovra all'interprete – e dunque ad escludere ogni automatismo applicativo – attraverso l'uso dell'inciso "ove pertinenti".

Da ultimo, appare contraddittorio gravare il debt crowdfunding di vincoli che non trovano riscontro nel lending crowdfunding. Più precisamente, la natura cartolarizzata delle posizioni creditorie nel primo caso non sembra ragione sufficiente e idonea per giustificare una tale disparità di trattamento.

## 4. La tutela dei sottoscrittori

Come già accennato, il Regolamento UE 2020/1503 non prende una posizione netta in ordine al tema degli strumenti di tutela attivabili direttamente dai sottoscrittori di capitale di rischio o di debito tramite portali on line; fermo restando che il corretto adempimento delle molteplici regole di condotta poste a carico del gestore della piattaforma si presta a formare oggetto dell'attività di vigilanza da parte della Consob [10].

Dal canto suo, l'art. 100-ter t.u.f. si limita a stabilire al 7° comma che, nei casi previsti dall'art. 24, par. 10, del regolamento (UE) 2020/1503, il titolare del progetto è responsabile (del carattere impreciso o fuorviante) delle informazioni fornite in una scheda contenente le informazioni chiave sull'investimento, com-

[9] Ad avviso di E. FREGONARA, *Il* crowdfunding *dell'impresa innovativa sostenibile (PMI e S.R.L.): tipologie e novità*, in *Banca impr. soc.*, 2024, p. 234, l'allentamento rispetto all'art. 2483 c.c. riguarderebbe solo la possibilità di collocare i titoli di debito presso investitori professionali, anche se non sottoposti a vigilanza.

[10] Sottolinea tale aspetto P. SPOLAORE, *Il regime del crowdfunding*, cit., p. 425 ss.

prese le sue eventuali traduzioni. Nulla viene previsto a carico del fornitore dei servizi di crowdfunding.

È peraltro da reputare che la soluzione di circoscrivere al soggetto offerente la responsabilità da informazioni scorrette o decettive non sia in grado di scriminare compiutamente il comportamento del gestore della piattaforma che viene comunque gravato – a mente dell'art. 23, comma 12 del Regolamento UE – di un obbligo di controllo sul contenuto della scheda informativa redatta dall'offerente i titoli di *equity* o di *debt*. Sicché, tenuto conto della diretta applicabilità delle previsioni del Regolamento unionale, appare corretto ipotizzare se non altro una responsabilità concorrente – sul modello di quella dei sindaci per omessa vigilanza sull'operato degli amministratori – del prestatore dei servizi di crowdfunding per avere agevolato con la propria inerzia e/o negligenza l'illecito del soggetto offerente.

Nell'ipotesi di sottoscrittore non sofisticato, l'apparato di protezione si arricchisce di ulteriori presidi: da un lato, l'obbligo per il gestore della piattaforma di valutare l'appropriatezza dei servizi offerti prima di consentire l'avvio della operatività (acquisendo determinate informazioni e sottoponendo l'investitore a un test di ingresso), dall'altro lato il riconoscimento in favore del risparmiatore retail di una sorta di *ius poenitendi* esercitabile entro un dato termine e tale da permettergli di revocare la propria adesione senza incorrere in conseguenze negative.

Nel complesso, appare un ritorno al passato l'adozione in favore degli investitori di un modello di tutela essenzialmente basato sulla trasparenza (*rectius* sulla statuizione di specifici doveri di *disclosure*), anziché sulla verifica della adeguatezza dell'investimento ovvero sulla coerenza e/o plausibilità dello stesso rispetto al profilo ascrivibile al risparmiatore retail [11].

A ben vedere, l'esigenza di offrire ai sottoscrittori *retail* una protezione ido-

[11] È appena il caso di aggiungere che un simile approccio trovava il proprio antecedente culturale in quelle concezioni c.d. ordo-liberali, che individuando nelle situazioni di asimmetria informativa un'ipotesi di *market failure*, identificano l'antidoto appropriato nella previsione, con riferimento alla operazione da realizzare, di una pluralità di obblighi di trasparenza a carico del contraente esperto e in favore del soggetto profano, in modo da consentire a quest'ultimo di prestare un consenso consapevole: il tutto, naturalmente, muovendo dal presupposto dell'agire razionale del singolo operatore, una volta sorretto da tutti gli elementi necessari per valutare la convenienza di un determinato affare. Solo che sembrava potersi considerarsi il frutto di una stagione ormai archiviata (quella cioè delle Direttive 2003/71CE, 22/93 CEE e 2003/6/CE rispettivamente in tema di prospetto, servizi di investimento e abusi di mercato) il pensiero che in un mercato competitivo si potrebbero vendere anche uova marce, purché si dica al consumatore che sono tali; ovvero il convincimento di poter superare gli squilibri indotti dalla disparità di accesso alle informazioni attraverso la previsione di una serie di doveri di *disclosure* nei confronti dell'investitore comune. Vero è infatti che l'impianto normativo risultante dapprima dalla Mifid e poi dalla Mifid 2 appare riflettere con chiarezza il passaggio alla differente impostazione secondo cui, per risultare efficiente, la tutela del risparmiatore *retail* non possa limitarsi alla comunicazione in suo favore di determinati contenuti informativi ma richieda di verificare la *qualità* (*rectius* coerenza) dell'operazione rispetto al profilo del medesimo.

nea appare ancora insoddisfatta. In effetti, se è corretto assumere che la necessità di proteggere gli investitori comuni non possa andare disgiunta dall'esigenza di contenere i costi delle relative misure in modo da evitare che i soggetti emittenti siano disincentivati dall'utilizzo di tale forma di finanziamento, è altrettanto incontestabile che occorra impegnarsi per non cadere nell'errore opposto di creare un ambiente (non accogliente, ma) ostile per i risparmiatori [12].

Sul punto, occorrerebbe forse lavorare con maggiore fantasia, senza farsi scudo dietro vecchi paradigmi di tutela, come per l'appunto quelli incentrati sui doveri di *disclosure,* in relazione alla cui efficacia, anche in esito alla crisi finanziaria del 2008, appare lecito sollevare fortissime perplessità [13].

Una soluzione potrebbe essere quella di limitare l'operatività del singolo risparmiatore sotto il profilo quantitativo, prevedendo un vero e proprio divieto di destinare risorse oltre una certa soglia (salvo permettere di reinvestire quelle scaturenti da investimenti già effettuati attraverso la medesima piattaforma). Tale misura consentirebbe di contenere la perdita entro un ammontare modesto, così giustificando – sulla base del principio di proporzionalità – l'adozione di *standard* di tutela blandi e quindi con ridotto impatto rispetto ai costi di realizzazione della emissione [14].

Altra via percorribile sarebbe quella di innalzare al ruolo di gate-keeper il gestore della piattaforma di *crowdfunding*, anche intervenendo, a livello di diritto societario, sulla disciplina degli emittenti [15]; ma si tratterebbe di scelte che ver-

---

[12] Sulla necessità di escogitare modelli di tutela differenti da quelli ricavabili dalla disciplina di cui al T.u.f. – sia pure muovendo dalla diversa premessa secondo cui la s.r.l. con quote diffuse presso il pubblico non integrerebbe comunque il concetto tipologico e normativo di società aperta –, cfr. E. GINEVRA, *Le società di capitali "aperte", tra codice civile e Tuf*, in Governance *e mercati. Studi in onore di Paolo Montalenti*, I, Giappichelli, Torino, 2022, p. 486 ss.

[13] Quanto all'opportunità di riconsiderare l'attitudine della informazione a porsi come effettivo strumento di correzione delle imperfezioni di mercato, v. A. PERRONE, *Sistema dei controlli e mercato dei capitali*, in *Riv. soc.*, 2011, p. 845, laddove scrive che «l'enfasi sulla trasparenza riflette una risalente tradizione di autonomia dell'investitore, *caveat emptor* e di valutazione individuale del rischio nella disciplina dei mercati finanziari che risulta ormai fortemente in discussione. Pur presentando il vantaggio di favorire al massimo la libertà di impresa e di esonerare il regolatore dal difficile compito di operare un compromesso tra differenti preferenze, l'impostazione tradizionale presenta, infatti, rilevanti imperfezioni di struttura, nella misura in cui trascura la possibile rilevanza sistemica dei limiti cognitivi dei partecipanti al mercato e le molteplici dinamiche della liberà morale dell'individuo».

[14] Naturalmente, si potrebbe sollevare il timore di creare «zone franche». In realtà, non sembra azzardato accostarsi con un maggiore ottimismo, sia tenendo conto che i gestori dei portali on line resterebbero comunque soggetti vigilati (e, quindi, ad esempio tenuti in ogni caso a rispettare determinati requisiti organizzativi; sia osservando come la possibilità di investire – anche oltre la soglia ipoteticamente fissata – la ricchezza generata attraverso la piattaforma dovrebbe tradursi in un incentivo per i fornitori di servizi di crowdfunding a vagliare con attenzione le soluzioni d'investimento da veicolare al pubblico.

[15] Il riferimento è al pacchetto di interessanti proposte avanzate da M. LAMANDINI, D. RAMOS MUNOZ, *La disciplina dell'equity crowdfunding*, cit., p. 262 ss. diretto a costruire uno statuto *ad hoc* del c.d. emittente digitale anche attraverso una responsabilizzazione del gestore della piatta-

rebbero con ogni probabilità a richiedere un disegno organico di riforma delle s.r.l. [16]

Resterebbe infine l'opzione del c.d. risparmio gestito [17]. Incoraggiare tale forma di intermediazione determinerebbe il vantaggio di avere come destinatario dei titoli (il gestore in monte, ovvero) un soggetto non solo contraddistinto da elevata professionalità, ma anche con la capacità di muovere disponibilità notevoli. Ne discenderebbe il ridimensionamento delle questioni legate al *need of protection* dell'investitore e la stessa esigenza di avere un mercato secondario liquido si configurerebbe in termini meno urgenti.

Naturalmente, occorrerebbe mettere in conto il costo connesso alla remunerazione della attività di gestione collettiva, nonché il prevedibile interesse degli

---

forma in veste di *gate-keeper*. Più precisamente, si ipotizza, da un lato, l'introduzione in capo all'emittente dell'obbligo della revisione contabile con revisore nominato dal portale, l'attribuzione a quest'ultimo della titolarità sia dei poteri di controllo che le azioni di responsabilità previste dall'art. 2476 c.c., nonché della legittimazione ad impugnare le delibere dei organi sociali; dall'altro lato, l'adozione di regimi di responsabilità degli amministratori più «garbati», volti a limitare entro un tetto massimo rappresentato da un multiplo ragionevole dei compensi percepiti il danno risarcibile connesso a scelte effettuate in buona fede, una maggiore digitalizzazione della relazione organica tra investitori e società (specie con riguardo allo svolgimento dell'assemblea dei soci mediante la possibilità di partecipare al voto attraverso sistemi di accesso basati su crittografia) e l'obbligo per l'emittente di istituire un sito web che contenga in uno spazio facilmente accessibile e chiaramente organizzato (possibilmente in formato tabellare in modo da risultare agevolmente attingibile dai motori di ricerca) tutta l'informazione concernente *i)* gli assetti proprietari e di governo della società; *ii)* l'attività di impresa con pubblicazione dei dati di bilancio disponibili e indicazioni sintetiche circa l'indebitamento complessivo; *iii)* operazioni con parti correlate e infragruppo; *iv)* fatti o eventi rilevanti suscettibili di incidere sul valore della società e degli strumenti finanziari emessi.

[16] Mette peraltro conto di sottolineare che alcuni dei presidi architettati dalla normativa interna in tema di *crowdfunding* ma non ripresi dal Regolamento unionale meriterebbero in realtà di essere conservati, se del caso migliorandoli. In particolare, il pensiero va all'art. 24, comma 2 del Regolamento Consob il quale prevede che, ai fini del perfezionamento dell'offerta di azioni o quote rappresentative del capitale sociale sul portale, il gestore verifichi che una quota almeno pari al 5% degli strumenti finanziari offerti sia stata sottoscritta da investitori professionali o da fondazioni bancarie o da incubatori di start-up innovative … o a investitori a supporto delle piccole e medie imprese con requisiti tali da far presumere il carattere professionale dei medesimi. Pur essendo emendabile attraverso il duplice correttivo da un lato di estendere l'ambito del precetto anche alle sollecitazioni riguardanti titoli di debito, dall'altro lato di richiedere che la quota del 5% sia sottoscritta da un unico investitore professionale (in modo da evitare che il senso della cautela venga stemperato mediante una dispersione del rischio tra più operatori qualificati), si rivela senz'altro apprezzabile l'intuizione su cui la regola in esame si basa: ovvero l'idea di trarre una conferma indiretta della bontà dell'offerta dalla significatività dell'impegno assunto da un soggetto in grado di selezionare la serietà delle proposte di investimento rivolte al mercato. Anche se più pertinente rispetto ad operazioni di *equity crodfunding,* si rivela del pari meritevole di attenzione il congegno – di cui all'art. 24, comma 1, lett. *a* del Regolamento Consob – di prevedere il diritto di co-vendita nell'ipotesi di passaggio di mano del controllo dell'emittente.

[17] Che l'apertura delle PMI al mercato dei capitali possa consentire di ampliare la platea dei potenziali interessati anche a soggetti diversi dagli investitori *retail* quali investitori istituzionali, nonché operatori di *Venture Capital* o *Private Equity* è segnalato anche da S. ROSSI, *S.r.l.-P.M.I.: disciplina del capitale e tipologia delle società*, in *Riv. dir. soc.*, 2019, p. 528.

operatori del risparmio gestito solo per titoli attributivi anche di diritti di controllo e di informazione.

## 5. L'assenza di un mercato secondario

È noto che esiste un nesso di proporzionalità diretta tra appetibilità di una determinata soluzione di investimento e facilità del suo smobilizzo; ed è altrettanto risaputo che la creazione di un efficiente mercato secondario costituisce la migliore garanzia per un agevole e immediato disinvestimento.

Di per sé, la piattaforma di crowdfunding si configura come un mercato primario; non a caso, l'emittente costituisce una parte necessaria delle operazioni che si perfezionano al suo interno.

Ciò posto, un problema di «liquidità» dell'investimento viene concretamente a porsi quando vengono sottoscritte quote di s.r.l. o titoli di debito *ex* art. 2483 c.c. Invero, il gestore dei servizi di *crowdfunding* non è abilitato ad istituire una sede di negoziazione e non esistono – a differenza di quanto possa accadere per i titoli azionari o obbligazionari – circuiti alternativi presso i quali concentrare gli eventuali scambi su tali entità.

A ben vedere, un primo passo per facilitare la trasferibilità delle quote di s.r.l. sottoscritte tramite portali potrebbe ravvisarsi nella previsione di un regime di circolazione alternativo a quello delineato dall'art. 2470 c.c. Il riferimento è naturalmente al sistema delineato dall'art. 100-ter t.u.f. (dal comma 2 al comma 5) che introduce un modello di circolazione intermediata, parametrato sul paradigma della gestione accentrata, in quanto basato sulle annotazioni nei registri tenuti dagli intermediari e le certificazioni rilasciate da quest'ultimi al fine di legittimare il socio all'esercizio dei diritti sociali (pur senza recepire i tratti della circolazione di natura cartolare) [18].

Un passo ulteriore per incoraggiare la possibilità di un *exit* dall'investimento si rivela il meccanismo delle bacheche elettroniche all'interno delle quali le piattaforme possono consentire ai propri clienti di pubblicizzare l'interesse per l'acquisto e la vendita di valori mobiliari o di strumenti ammessi ai fini del crowdfunding inizialmente offerti sulla piattaforma.

È tuttavia scrupolo dell'art. 25, comma 2 del medesimo Regolamento vietare che la bacheca possa funzionare come sistema multilaterale di negoziazione, operando come sistema di abbinamento delle manifestazioni di interesse per l'acquisto e la vendita; sicché eventuali contratti non potranno che essere perfezionati ed eseguiti all'esterno della stessa.

Nel complesso, le misure adottate per consentire la liquidità dell'investimento appaiono modeste. Si tratta, questo, di un nervo scoperto della disciplina del

[18] Cfr. M. CIAN, *Le quote dematerializzate di s.r.l.*, in *Riv. dir. civ.*, 2024, p. 293.

crowdfunding. In effetti, una volta ammessa l'offerta delle quote standardizzate di s.r.l. (e, a nostro avviso, anche dei titoli *ex* art. 2483 c.c.) nell'ambito del pubblico indistinto, non può che apparire contraddittorio non adoperarsi per la formazione di un reale mercato secondario in modo da assicurare la liquidità dell'investimento realizzato. Il tutto con l'ulteriore precisazione che, nella prospettiva indicata, la soluzione più semplice sarebbe quella di avvalersi proprio dei portali on line, oltre che per l'offerta, anche per la successiva circolazione degli strumenti emessi.

# Garanzia pignoratizia e obbligo di conservazione del creditore. Il contributo della tecnologia digitale

Benedetta Bonfanti [*]



## 1. Garanzia mobiliare e tecnologia digitale

Nell'ultimo decennio l'applicazione delle tecnologie digitali nel contesto del comparto finanziario, il fenomeno del c.d. *FinTech* [1], ha occupato in grande misura l'attenzione e l'impegno ricostruttivo della letteratura in materia [2]. Come

[*] Lavoro svolto nell'ambito del progetto PNNR "Security and RIghts in the CyberSpace (SERICS), spoke 10. – PNRR MUR M4C2 -1.3 – CUP del progetto G43C22002580001 – Codice del progetto PE00000014.

[1] Secondo la nota definizione del *Financial Stability Board* può descriversi come «*the technology-enabled innovation in financial services that could result in new business models, applications, process or products with an associated material effect on the provision of financial services*»; il riferimento si appunta su ogni forma di innovazione finanziaria abilitata dalle diverse tecnologie disponibili, quali: *Artificial Intelligence (AI), machine learning, big data, distributed ledger technology, (DLT), cloud computing, biometrics, application program interface etc.* (*Financial Stability Implications from FinTech. Supervisory and Regulatory Issues that merit Authorities' Attention*, June 2017, p. 7 ss.)

[2] Cfr., tra i lavori domestici, AA.VV., *Fintech, Smart Technologies e governance dei mercati*, a cura di A. NUZZO, 2021, Luiss University Press, Roma; AA.VV., *Diritto del Fintech*, a cura di M. CIAN e C. SANDEI, 2020, Cedam-Wolters Kluwer, Milano-Padova; AA.VV., *FinTech: Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, a cura di M.T. PARACAMPO, Giappichelli, Torino, 2017; A. SCIARRONE ALIBRANDI, *Il Testo Unico finanziario alla prova del FinTech*, in *Il Testo Unico finanziario*, a cura di G. PRESTI e M. CERA, I, Zanichelli, Bologna, 2020, p. 29 ss.; AA.VV., *Fintech: diritti, concorrenza, regole*, a cura di G. FINOCCHIARO e V. FALCE, Zanichelli, Bologna, 2019.

ormai noto, l'avvento di questi supporti tecnologici (*distributed ledger technology (DLT)*, *machine learning*, *big data, etc.*) ha infatti condotto a profonde innovazioni nel settore, consentendo lo sviluppo di prodotti e di servizi nuovi e, correlativamente, di nuovi mercati [3].

Ciò non di meno, queste diverse applicazioni digitali hanno trovato impiego anche nella costruzione e nello svolgimento dei prodotti e dei servizi tradizionali, che storicamente formano e danno corpo alle attività tipiche dei diversi intermediari finanziari. Sul punto basti considerare l'implementazione dell'attività di valutazione del merito creditizio nell'ambito dei contratti di finanziamento ad opera soprattutto delle tecnologie di *machine learning* e dei protocolli algoritmici: alla valutazione compiuta dal singolo operatore, sulla base di un *set* informativo di carattere patrimoniale e finanziario, si assiste nell'oggi al passaggio ad un'automazione della procedura attraverso tecniche digitali in grado di elaborare un maggior numero di dati (anche non finanziari), con un'accuratezza più elevata, in un minor lasso di tempo [4]; oppure il servizio di consulenza finanziaria, nei tempi recenti sempre più affidato al supporto di processi automatizzati, e cioè svolto con *automated tools* ovvero con veri e propri *robo advisors* [5].

Soprattutto l'osservazione di tale ultimo contesto (: dei prodotti e delle attività tradizionali) svela, tuttavia, come tali supporti tecnologici non siano ancora utilizzati al pieno delle loro potenzialità. Nell'attuale permangono, cioè, dei settori – o parti degli stessi – nei quali l'uso di questi strumenti non gode ancora di ampia diffusione, venendosi così a precludere l'apprezzamento dei benefici che ne potrebbero derivare per l'impresa in termini di efficienza nello svolgimento delle diverse attività.

Da quest'angolo visuale, considerando l'ambito specifico dell'attività bancaria, viene in particolare rilievo la materia delle garanzie reali mobiliari connesse ai contratti di credito e, segnatamente, quella fase del rapporto di garanzia costituita dalla «gestione» del bene da parte del creditore durante il periodo di pendenza della relazione.

Secondo l'articolazione dell'istituto del pegno fatta propria dal codice civile, infatti, questa si compone, oltre che della fase finale – avente carattere eventuale – di escussione della garanzia nell'ipotesi di inadempimento da parte del debitore dell'obbligazione principale, anche di una fase antecedente, caratterizzata dalla

---

[3] G. ALPA, *Fintech: un laboratorio per i giuristi*, in *Contr. impr.*, 2019, p. 377 ss.

Sul punto basti pensare, tra i molteplici esempi possibili, all'attività di *crowdfunding*, il cui sviluppo è stato determinato anzitutto dalle nuove possibilità tecniche offerte dalle piattaforme digitali. Cfr. U. MINNECI, *Sviluppi normativi in tema di piattaforme di crowdfunding*, in *La finanza nell'età degli algoritmi*, a cura di L. AMMANNATI e A. CANEPA, Giappichelli, Torino, 2023, p. 83 ss.

[4] In materia di *credit scoring*, v. L. AMMANATI, G.L. GRECO, *Piattaforme digitali, algoritmi e big data: il caso del credit scoring*, in *Riv. trim. dir. ec.*, 2021, 2, p. 290 ss.; M. RABITTI, *"Credit scoring via machine learning" e prestito responsabile*, in *Riv. dir. banc.*, 2023, p. 175 ss.

[5] Cfr. F. SARTORI, *La consulenza finanziaria automatizzata: problematiche e prospettiva*, in *Riv. trim. dir. ec.*, 2018, p. 253 ss.; U. MORERA, *Consulenza finanziaria a "robo-advisor": profili cognitivi*, in *Dir. banc. mer. fin.*, 2019, p. 205 ss.

sussistenza in capo al creditore di un obbligo di conservazione del bene *ex* art. 2790 c.c. [6]

Considerando proprio questo segmento della relazione, specie nell'ipotesi in cui la garanzia abbia ad oggetto beni i cui valori di scambio siano mutevoli e soggetti ad oscillazioni frequenti (come, ad esempio, le azioni o gli strumenti finanziari), un maggiore sfruttamento delle tecnologie digitali potrebbe costituire un utile ed efficace ausilio per l'ente erogatore al fine dell'adempimento dell'obbligo conservativo.

Questi appunti saranno a ciò dedicati: nella prima parte del lavoro (parr. 2 e 3) si procederà ad una preliminare individuazione del contenuto dell'obbligo di conservazione gravante sul creditore pignoratizio *ex* art. 2790 c.c. Come si verrà ad analizzare, il tema ha vissuto negli ultimi anni degli sviluppi ricostruttivi che, da una prospettiva statica, incentrata sul mantenimento della mera esistenza giuridica e materiale del bene, hanno condotto ad una ricomprensione nell'alveo precettivo della disposizione anche condotte propedeutiche al mantenimento dell'utilità economica in esso incorporata. Nella seconda parte (parr. 4 e 5) si andrà a valutare il possibile contributo della tecnologia digitale nello svolgimento delle attività conservative. A partire dall'analisi del caso degli *NFT-backed loans*, nel quale una simile prospettiva risulta già concretamente applicata, verranno tratte delle considerazioni di più ampio respiro circa i vantaggi e i benefici derivanti dalla digitalizzazione della fase gestoria della garanzia di tipo mobiliare.

## 2. Il perimetro dell'obbligo di conservazione del creditore. La prospettiva tradizionale

L'obbligo di conservazione di cui all'art. 2790 c.c. ha ricevuto dalla letteratura tradizionale un'interpretazione per così dire «ristretta»; dagli scarsi passaggi che si riscontrano sul tema, infatti, sembra emergere l'idea che la condotta richiesta al creditore si sostanzi (ed esaurisca) nel mantenimento dell'integrità fisica della *res* e della sua esistenza giuridica [7].

---

[6] Cfr., per una ricostruzione di questa duplicità di momenti, con particolare riferimento a quello «gestorio», U. MALVAGNA, *Sulle clausole di rotatività nel pegno: funzione «conservativa» del valore della garanzia e strutture decisionali delle sostituzioni*, in *Banca borsa e tit. cred.*, 2014, I, p. 313 ss.

[7] Come si avrà modo di rilevare in più occasioni, il problema della conservazione del valore della cosa trova naturale terreno di sviluppo in relazione a beni, quali le azioni o gli strumenti finanziari, intrinsecamente soggetti a repentine e frequenti oscillazioni. Non è un caso, in effetti, che gli sporadici arresti giurisprudenziali sul tema abbiano ad oggetto fattispecie in cui il vincolo pignoratizio è appuntato proprio su questa tipologia di beni. Anche in letteratura il tema della rilevanza del valore economico del bene è stato svolto proprio in questo specifico ambito, per quanto non tanto con riferimento al problema della sua conservazione, bensì nel contesto di un'indagine dogmatica sull'oggetto della garanzia pignoratizia. Così, in relazione al pegno di azioni, si

Con riferimento all'alveo precettivo della disposizione, una tra le più autorevoli voci sull'argomento, scrive: «il creditore non è tenuto a migliorare la cosa, né ad evitare quei deprezzamenti e deterioramenti che siano conseguenza della natura stessa della cosa [...] egli è tenuto a preservare la cosa dagli agenti esteriori ma non anche da quelli interiori alla stessa» [8].

Attraverso la distinzione tra fattori intrinseci ed estrinseci alla cosa si individua dunque il *focus* della prestazione nella preservazione dell'integrità fisica del bene, escludendo che il comportamento dovuto si estenda all'impedimento del decremento del valore incorporato.

Frutto della medesima ricostruzione sembra l'affermazione per cui nell'ipotesi di pegno di azioni il creditore non sia tenuto ad attivarsi quando i titoli «perdano semplicemente valore sul mercato» [9].

Questa interpretazione trova seguito e applicazione nelle scarse occasioni in cui la giurisprudenza ha avuto modo di occuparsi del tema.

Tra queste, si consideri ad esempio un arresto della Corte d'Appello di Milano [10] che, in una fattispecie concreta in cui il cliente censurava l'inerzia del creditore di fronte alla riduzione del valore di azioni costituite in pegno, ha escluso la violazione dell'art. 2790 c.c. dal momento che «non è certo la diminuzione del corso di borsa a costituire un deterioramento imputabile al creditore pignoratizio». Seguendo la medesima impostazione concettuale diffusa in dottrina, per cui il creditore non è tenuto ad attivarsi nel caso in cui il deterioramento sia conseguenza della «natura» di bene (*i.e.* intrinseca dipendenza dall'andamento del mercato mobiliare), ne consegue la legittimità della condotta inerte del creditore laddove il decremento interessi in via diretta ed esclusiva il valore venale del bene [11].

---

afferma che il valore delle azioni costituisce l'«*oggetto sostanziale*» del pegno (S. POLI, *Il pegno di azioni*, Giuffrè, Milano, 2000, p. 97); anche C. ABATANGELO, *Le nuove garanzie mobiliari tra realità e obbligatorietà del vincolo*, Cedam-Wolters Kluwer, Milano-Padova, 2012, p. 9, approfondendo il tema delle garanzie «flottanti», pone l'interrogativo sulla «compatibilità di una garanzia avente ad oggetto non un bene specifico, ma un "valore" economico rispetto alla ricostruzione del pegno in termini di diritto reale limitato».

[8] D. RUBINO, *Il pegno*, in *Trattato Vassalli*, XIV, Utet, Torino, 1956, p. 243. Del medesimo tenore anche F. REALMONTE, *Il pegno*, in *Trattato Rescigno*, XIX, Utet, Torino, 1997, p. 797, e A. MONTEL, voce *Pegno (Diritto vigente)*, in *Noviss. Dig. it.*, XII, Utet, Torino, 1965.

[9] G. GORLA, P. ZANELLI, *Del pegno. Delle ipoteche*, in *Commentario Scialoja-Branca*, Roma-Bologna, 1992, p. 114.

[10] App. Milano, 13 aprile 2011, in *IlCaso.it*.

[11] Cfr. anche Trib. Milano, 21 gennaio 1991, in *Banca borsa e tit. cred.*, 1992, II, 94, con nota di E. Ginevra. La fattispecie concreta giunta al vaglio del giudice meneghino aveva ad oggetto un mutuo garantito da un pegno su titoli di Stato. A seguito dell'inadempimento della debitrice per l'intervenuto fallimento, l'istituto di credito aveva atteso circa un anno per procedere alla vendita dei titoli, i quali, nel frattempo, avevano perso parte del valore originario. La società adiva il giudice chiedendo il risarcimento del danno subito a seguito del comportamento della banca creditrice per violazione dei principi di correttezza e buona fede contrattuale. Il Tribunale respingeva la domanda dell'attrice affermando come sul creditore non gravi alcun obbligo di attivarsi per la

Tra le ragioni che hanno condotto alla ricostruzione delineata sembra potersi ravvisare la coincidenza contenutistica tra l'obbligazione di custodire la cosa oggetto del pegno *ex* art. 2790 c.c. e l'obbligazione di custodia di cui al tipo contrattuale del deposito regolare di cui agli artt. 1766 c.c. e ss.

A questo riguardo, si afferma tradizionalmente che «la custodia ha un carattere meramente statico ed un contenuto meramente materiale» e, ai fini dell'adempimento della prestazione, «il custode deve semplicemente limitarsi a mantenere la cosa nello stato in cui l'ha ricevuta, difendendola dai pericoli di materiale distruzione o danneggiamento» [12].

Come è facile notare, risuona in queste righe la ricostruzione riguardo al contenuto dell'obbligo di conservazione gravante sul creditore pignoratizio: se il baricentro dell'obbligo è individuato nella conservazione dell'integrità fisica del bene consegnato, l'attività dovuta dal custode si sostanzia nel mantenimento del «medesimo stato e modo di essere» [13] della cosa con riferimento al momento costitutivo del contratto. Correlativamente, rimane fuori dal perimetro oggettivo delle condotte dovute ogni attività strumentale alla conservazione del valore economico incorporato nel bene.

Deve osservarsi, tuttavia, – e tale rilievo riveste una posizione centrale – che nel rapporto di deposito l'obbligazione di custodia si conforma al perseguimento dell'interesse oggettivo sotteso al tipo contrattuale a cui inerisce; come correttamente affermato dalla migliore dottrina, il deposito «risponde al bisogno, sentito dal depositante, di allontanare da sé la cosa per un certo tempo [...] per raggiungere questo fine, non c'è che un possibile mezzo: quello di affidare la cosa ad altro soggetto, il quale assuma su di sé l'ingombro che essa comporta e il fastidio che la esigenza della sua conservazione impone» [14].

La fissazione dell'estensione dell'obbligo nei limiti di cui si discorre si attaglia dunque al perseguimento del fine a cui il contratto di deposito è oggettivamente preordinato.

E tuttavia, se il contenuto dell'obbligazione di custodia enucleato con riferimento al deposito viene trasposto e riferito senza alcun adattamento al contesto del rapporto pignoratizio, il rischio di un indebito appiattimento è davvero inevitabile.

---

vendita del bene, «dal momento che, essendone data la facoltà allo stesso costituente, sembrerebbe onere suo quello di evitare ogni depauperamento (vd. art. 2795, terzo comma, c.c.)».

Per quanto una simile fattispecie non sia sovrapponibile al caso del deterioramento del bene in corso di rapporto, avendo ad oggetto un'ipotesi di vendita esecutiva, segnala comunque la trascuratezza con cui si viene normalmente a ricostruire la posizione creditoria quanto al profilo della condotta dovuta.

[12] Così A. FIORENTINO, *Del deposito*, in *Commentario Scialoja-Branca*, Zanichelli-Soc. Ed. del Foro italiano, Bologna-Roma, 1953, p. 58. Del medesimo tenore le affermazioni di G. BALBI, *L'obbligazione di custodire*, Giuffrè, Milano, 1940, p. 13, secondo il quale «la custodia, tendendo a perpetrare uno stato attuale [...] implica, in modo esclusivo ed essenziale, un punto di vista statico».

[13] Così G. BALBI, *op. cit.*, p. 8.

[14] G.B. PORTALE, A. DALMARTELLO, voce *Deposito (Contratto di)*, in *Enc. dir.*, XII, Giuffrè, Milano, 1963, p. 245.

Ciò posto, diviene allora necessario verificare se, ferma l'esistenza di un nucleo minimo essenziale proprio della prestazione di custodia, esso non possa arricchirsi di contenuti o sfumature ulteriori nel momento in cui sia collocato in strutture contrattuali diverse.

## 3. (*Segue*) La rilevanza delle condotte strumentali alla conservazione dell'utilità economica incorporata nel bene

A questo proposito non sembra inutile riprendere, sul solco già tracciato dalla dottrina più autorevole, i criteri che permettono di adattare e modulare l'estensione dell'obbligo in discorso ai diversi tipi contrattuali a cui accede.

Come osservato tradizionalmente in dottrina, l'obbligazione di custodia, in astratto indeterminata nei singoli e concreti atti che la compongono, trova il proprio «criterio di determinabilità» [15] nella combinazione di due elementi basici: in primo luogo, nella tipologia di bene verso cui si dirige; in secondo luogo, nello scopo del negozio a cui accede.

Tralasciando di soffermarsi sul primo dei criteri, il quale si manifesta di più immediata comprensione (conservare un vaso è attività diversa da quella in cui si esprime, ad esempio, la custodia di titoli azionari), il punto centrale del discorso sembra proprio essere la messa a fuoco del secondo.

Limitando il ragionamento a quanto di interesse ai fini della ricostruzione dei contenuti dell'obbligazione di custodia del creditore pignoratizio, si tratta di individuare la condotta dovuta sulla base di un'indagine in ordine all'interesse tipico sotteso al rapporto.

Sul punto, è utile riprendere una recente sentenza della Suprema Corte che si volge proprio a ricostruire questo profilo [16]. Si tratta, per vero, di un momento ricostruttivo evolutivo della materia, che si pone in forte discontinuità con le osservazioni della tradizione appena riprese.

In una fattispecie concreta in cui il cliente censurava l'inerzia del creditore di fronte alla riduzione del valore di azioni costituite in pegno, la Corte afferma l'esistenza, in capo al creditore e al debitore, di un interesse convergente alla conservazione dell'integrità economica del bene a fronte di un suo significativo deterioramento; in specie, il primo manifesta l'interesse a «utilizzare liberamente il

---

[15] G. BALBI, *op. cit.*, p. 7; nello stesso senso, G.B. PORTALE, A. DALMARTELLO, *op. cit.*, p. 258.

[16] Cfr. Cass. civ., 15 maggio 2019, n. 12863.

La vicenda oggetto del provvedimento trae origine da un rapporto di mutuo tra una banca e un proprio cliente, garantito da un pegno su azioni quotate. In corso di rapporto, a seguito della progressiva perdita di valore delle azioni, il cliente si rivolgeva alla banca e ne chiedeva la vendita. Quest'ultima provvedeva a dare seguito a tale richiesta dopo circa due anni dalle prime sollecitazioni. Per il decorso del tempo, il ricavato della vendita risultava inferiore di circa due terzi rispetto al valore originario dei titoli al momento di costituzione della garanzia. Cfr., anche, in senso adesivo, Cass. civ., 6 marzo 2023, n. 6549.

corrispondente valore economico del bene in garanzia» una volta eseguita la propria prestazione, il secondo, invece, quello di mantenere una garanzia «efficiente». Per l'effetto, sotto il profilo teleologico, l'obbligo di custodia «risulta funzionale al sostanziale mantenimento di un valore economico sostanzialmente corrispondente a quello originario».

Il passaggio appena evidenziato esprime il dato per cui nel pegno — diversamente, appunto, dal contratto di deposito regolare — la conservazione del valore della *res* assume una dimensione immanente al rapporto di garanzia. Per meglio dire, essa si propone come momento costitutivo interno del medesimo, formando un dato strutturale della fattispecie normativa, che si esprime nella fase «gestoria» [17] del rapporto di pegno, in vista dell'intimo rischio di deterioramento del bene, che sussiste in particolare quando la garanzia insista su beni volatili quanto al loro valore.

In breve, l'interesse «sintetico» delle parti è individuato nella conservazione di un bene utile e (anche) economicamente integro [18].

Fissato correttamente nei termini che precedono l'interesse tipico sotteso a questa fase del rapporto, il valore di scambio incorporato nella *res* non può allora ritenersi del tutto estraneo all'obbligazione di custodia.

In particolare, senza giungere a configurare alcuna obbligazione di «mantenimento del valore», deve ritenersi, piuttosto, che gravi sul creditore pignoratizio l'obbligo di adottare un comportamento attivo e propositivo ai fini di una gestione efficace del rischio di deterioramento del valore di scambio del bene [19]. Dovere che si esprime nel corso dell'intero rapporto di garanzia: dal monitoraggio del valore, all'informazione e avviso al costituente in merito ad eventuali perdite di valore in atto.

---

[17] Cfr. U. MALVAGNA, *op. cit*., p. 319 ss.

[18] Con specifico riferimento al pegno di azioni, l'interesse convergente del creditore pignoratizio e del datore del bene alla conservazione del valore del bene trova ulteriore punto di emersione nell'art. 2352 c.c. Molte sono state le ricostruzioni in merito alla portata della norma (per una sintesi delle quali, cfr. il primo capitolo della monografia di S. POLI, *op. cit*., p. 19 ss.). Ciò che sembra essere punto acquisito in letteratura, quanto al profilo teleologico, attiene al dovere del creditore pignoratizio di esercitare il diritto di voto in assemblea dell'interesse comune (al costituente e al creditore pignoratizio) alla conservazione del valore patrimoniale delle azioni (sul punto, R. SACCHI, *L'intervento e il voto nell'assemblea della s.p.a. – Profili procedimentali*, in *Trattato Colombo-Portale*, 3, Utet, Torino, 1994, p. 131 ss.).

[19] Dal punto di vista della qualificazione strutturale di tali doveri, sembra corretto affermare che si tratta di obblighi di protezione accessori all'obbligo di prestazione costituito dalla custodia del bene: cfr. L. MENGONI, *Obbligazioni «di risultato» e obbligazioni «di mezzi» (Studio critico)*, in *Riv. dir. comm*., 1954, I, p. 185, ora in *Scritti II. Obbligazioni e negozio*, a cura di C. CASTRONOVO, A. ALBANESE e A. NICOLUSSI, Giuffrè, Milano, 2011, p. 166 ss.: «nei rapporti concernenti la restituzione di un corpo certo e determinato, la diligentia in custodiendo (artt. 1001, co. 2, 1026, 1587 n. 1, 1768, 1804, co. 1, 1961, co. 2, 2148, co. 2, 2167, co. 2, 2790) non designa un obbligo di carattere primario, bensì un obbligo integrativo strumentale».

## 4. L'applicazione delle tecnologie digitali nell'adempimento dell'obbligo di conservazione. Il caso degli *NFT-backed loans*

Fissato nei termini descritti il perimetro delle condotte richieste al creditore pignoratizio, si può ora passare a svolgere qualche osservazione in relazione al secondo profilo a cui si è fatto riferimento in apertura (in fine del par. 1). Ci si intende soffermare sull'apporto che le nuove tecnologie digitali possono offrire nell'adempimento dell'obbligo di conservazione, specie nell'ipotesi in cui la veste del creditore sia assunta da un soggetto che professionalmente svolge l'attività creditizia.

In questa prospettiva occorre porre l'attenzione sulle condotte strumentali e propedeutiche alla conservazione del bene; in via segnata sull'obbligo di monitoraggio del valore e su quello di avviso al debitore riguardo ad eventuali deprezzamenti in corso di rapporto.

Da quest'angolo visuale, un utile punto di partenza è costituito dall'analisi delle realtà operative in cui un simile ordine di idee risulta già concretamente attuato; contesti in cui, in altri termini, la fase di conservazione e gestione del rischio di deterioramento, con specifico riguardo al valore incorporato nel bene, viene supportata e implementata dalla tecnologia digitale.

In questa prospettiva, viene in rilievo quella particolare forma di finanziamento, diffusasi nel mondo dei *crypto-assets*, costituita dagli *NFT-backed loans*.

Dalla ricognizione dell'operatività delle principali piattaforme e dallo studio delle condizioni praticate [20], è possibile definire questa operazione come un prestito di moneta digitale (più raramente, anche di moneta avente corso legale), subordinato al deposito da parte del debitore di uno o più *Non-Fungible Token(s)* [21] in garanzia. Scontando un necessario grado di approssimazione, si trat-

---

[20] Le presenti osservazioni, nel ricostruire le regole che governano questi prodotti, si basano sullo studio delle condizioni generali di contratto (presenti normalmente nell'apposita sezione «*Terms and Conditions*») adottate dalle principali piattaforme.

[21] Secondo la definizione corrente, l'*NFT* rappresenta un certificato di autenticità e univocità di un bene fisico o digitale correlato, iscritto su una *blockchain*; pertanto consente che siano assicurate l'origine e le vicende circolatorie del bene (dall'emissione sino al suo eventuale trasferimento) e, correlativamente, specie con riferimento alle opere d'arte, che l'originale possa essere distinta da eventuali contraffazioni. Per un primo studio domestico in chiave qualificatoria v. A. GUACCERO, G. SANDRELLI, *Non-Fungible Tokens (NFTs)*, in *Banca borsa e tit. cred.*, 2022, II, p. 824 ss.

Per una ricognizione delle origini di questi *token* v. A. CANEPA, *Regulation of NFTs and Crypto Art Trading. Influencers, Gamification, and Emerging User Protection Issues*, in *American Research Journal of Humanities and Social Sciences*, 2023, p. 167 ss.; K. LOMMERS, J. KIM, M. BAIOUMY, *Market Making in NFTs*, reperibile all'indirizzo https://ssrn.com/abstract=4226987. U.W. CHOHAN, *Non Fungible Tokens: Blockchains, Scarcity, and Value*, in *Critical Blockchain Research Initiative (CBRI) Working Papers*, 2021; G. TROVATORE, *op. cit.*, p. 81 ss.; A. CALONI, *Blockchain e mercato dell'arte: spunti di diritto privato*, in *Arte e Diritto*, 2022, p. 183 ss.; B. XIAO, *Copyright Law and Non-Fungible Tokens: Experience from China*, in *International Journal of Law and Information Technology*, 2022, p. 444 ss.

ta di un'operazione strutturalmente assimilabile ad un contratto di mutuo, assistito da una garanzia reale di tipo mobiliare [22].

Nonostante la presenza di alcune differenze tra i prodotti offerti dalle diverse piattaforme, è possibile andare a isolare alcuni tratti «di base» comuni.

Riguardo al momento costitutivo del rapporto, il deposito dell'*asset* avviene attraverso una modalità tecnologica analoga. Secondo l'alternativa oggi ricorrente, l'*NFT* viene trasferito dal conto (*wallet*) del proprietario in uno *smart contract* (: *escrow smart contract*) ovvero, secondo una distinta variante, mantenuto nel portafoglio digitale del debitore senza che tuttavia gli venga reso tecnicamente possibile alcun atto di disposizione durante tutto il corso del finanziamento.

Un ulteriore tratto di comunanza si coglie poi nell'assenza, all'interno dell'articolazione propria di questa operazione, di una fase preordinata alla valutazione del merito creditizio del debitore. Secondo lo schema maggiormente diffuso, i connotati specifici del prestito, in specie, capitale e tasso di interesse, vengono a dipendere e ad essere proporzionati in via esclusiva sulla stima del bene offerto in garanzia. Più in dettaglio, ogni singola piattaforma definisce un coefficiente percentuale (*Loan to Value*) volto ad esprimere l'ammontare monetario che il debitore può ricevere in rapporto alla stima effettuata dell'*asset* digitale [23].

Di seguito, brevemente, i passaggi della procedura: il mutuatario deposita sulla piattaforma l'*NFT* che desidera porre in garanzia; la piattaforma, per il tramite di un protocollo algoritmico, aggrega i valori di scambio di quel particolare *token* emergenti dalle principali piattaforme del mercato secondario e ne estrae il dato mediano; individuato questo valore, sulla base di un ulteriore calcolo probabilistico circa il valore di realizzo del bene al momento della scadenza del termine di restituzione, definisce la somma mutuabile.

Ciò posto, il profilo rilevante ai fini del presente lavoro attiene agli specifici strumenti posti in campo da queste piattaforme per la gestione della fase di pendenza del rapporto e della correlativa attività di monitoraggio della garanzia mobiliare. Si consideri a questo proposito che il mercato degli *NFTs* si caratterizza strutturalmente per l'estrema volatilità dei prezzi di scambio che, dunque, subiscono sensibili oscillazioni in brevi lassi di tempo [24].

---

[22] Per un'analisi più articolata dei profili qualificatori dell'operazione sia consentito rinviare a B. BONFANTI, *NFT-backed loans. Spunti per un inquadramento giuridico*, in *Il mercato dei non fungible tokens, moda e gamification*, a cura di A. CANEPA, Milano University Press, Milano, 2023, p. 39 ss.

[23] Ad esempio, attraverso la piattaforma Nexo è possibile ottenere una somma in prestito corrispondente al 10% o al 20% del valore di mercato (*floor price*) del proprio *NFT*; la piattaforma Drops consente di ottenere una somma compresa tra il 30% e il 60%.

Secondo lo schema proposto da altre, invece, non deve sussistere alcun rapporto tra i due valori. Il mutuatario «carica» il proprio *NFT* sulla piattaforma e indica autonomamente l'ammontare del prestito, il tasso di interesse e il termine del finanziamento. Fissati questi elementi, la proposta contrattuale così formatasi viene diffusa attraverso la piattaforma presso il pubblico composto dagli altri utenti (v. ad es. la piattaforma Zharta).

[24] L'osservazione può stimarsi acquisita nell'ambiente. Cfr., per tutti, A. CANEPA, K.A. SHAH, A. VISCONTI, *NFTs and Crypto Art Marketplaces: New Risks for Investors and Financial Markets?*, in *Law and Economics Yearly Review*, 2022, vol. 11, p. 72.

Nella maggior parte delle piattaforme si può notare a riguardo la predisposizione di una struttura tecnologica finalizzata al costante controllo del valore della garanzia e di un articolato meccanismo di «salvaguardia» del valore dell'*asset* digitale nel caso di repentini deprezzamenti del bene.

In particolare, una volta instauratosi il rapporto, la piattaforma, per il tramite di un processo automatizzato, monitora che il rapporto tra il valore della garanzia e la somma erogata (*LTV*) si mantenga su linee costanti. In sostanza, che le oscillazioni di valore dell'*NFT* si collochino entro soglie preventivamente determinate.

Nel caso in cui si verifichino dei deprezzamenti che si pongano al di sotto degli *standards* fissati[25], viene attivata una particolare procedura, definita *liquidation protection*, volta a preservare l'utilità economica incorporata nel bene. In una prima fase, che può durare anche poche ore, sono inviate, secondo un processo automatico, delle notifiche al debitore (tramite *e-mail*), informandolo della perdita di valore dell'*asset* digitale[26]; nella seconda, che si apre nel caso in cui quest'ultimo non abbia provveduto alla sostituzione della garanzia o all'aggiunta di una ulteriore, l'*NFT* viene liquidato.

## 5. I vantaggi correlati alla digitalizzazione della fase gestoria della garanzia mobiliare

L'operazione appena tratteggiata, specie con riguardo alla fase gestoria della garanzia, offre come già anticipato lo spunto per formulare alcune considerazioni ad un livello di generalità maggiore in merito allo sfruttamento del supporto offerto dalle tecnologie digitali per l'adempimento dell'obbligo di conservazione gravante sul creditore pignoratizio.

Specie in relazione agli obblighi strumentali alla preservazione dell'utilità economica del bene, che – come già osservato – si sostanziano nel monitoraggio del valore e nella segnalazione al debitore delle eventuali perdite in corso, le nuove tecnologie digitali sembrano infatti costituire degli strumenti in grado renderne più efficiente lo svolgimento, nonché di ridurre fortemente per l'intermediario i costi connessi.

Riguardo al monitoraggio, la strutturazione di un processo automatizzato permetterebbe anzitutto una maggiore costanza e puntualità delle rilevazioni nel paragone con le procedure fondate sull'attività periodica dei singoli operatori o dei periti. Ciò risulta tanto più essenziale nell'ipotesi in cui i beni che formano oggetto della garanzia siano intrinsecamente soggetti a frequenti oscillazioni di valore e sia dunque necessario porre in essere un'attività di tratto continuativo.

---

[25] La piattaforma Nexo considera anche l'ipotesi in cui il valore di mercato della garanzia aumenti durante il corso del rapporto. In una simile ipotesi al debitore è concessa la facoltà di smobilizzare la garanzia, attraverso la sostituzione con un altro *asset* digitale, ovvero di richiedere un aumento della linea di credito.

[26] Per questa particolare forma di «*alert*», v. ad esempio la piattaforma Nexo.

In secondo luogo, sempre con particolare riferimento a beni «volatili», se il processo fosse implementato attraverso tecniche di *machine learning*, si potrebbe aprire la possibilità che siano sviluppati dei modelli predittivi relativi all'andamento dei valori di scambio del bene considerato, consentendo, nell'interesse di entrambe le parti del rapporto (debitore e creditore), una previsione sui possibili futuri deprezzamenti e, dunque, una gestione anticipata del relativo rischio.

Riguardo invece al distinto profilo della segnalazione al debitore delle perdite di valore in corso, la programmazione di un modello automatizzato attraverso la fissazione *ex ante* di soglie di allerta, consentirebbe l'invio di comunicazioni al debitore secondo tempistiche molto brevi, idonee a permettergli la sostituzione del bene concesso in garanzia e la pronta liquidazione dell'*asset.*

Per vero, una simile prospettiva ideale si pone in sintonia con le linee guida tracciate dall'*European Banking Authority* in materia di *loan origination and monitoring*[27].

Tale documento, orientato a fornire delle indicazioni agli enti creditizi riguardo alla strutturazione di idonei processi interni per la gestione del rischio di credito, si sofferma infatti con particolare grado di dettaglio sulle procedure di gestione delle garanzie eventualmente connesse al finanziamento.

Ai fini del presente lavoro viene in rilievo la Sezione dedicata alla valutazione e al monitoraggio delle garanzie reali, della quale occorre riprendere due passaggi[28].

Il primo riguarda la raccomandazione circa la necessità che l'attività di valutazione della garanzia concessa dal debitore non sia relegata al momento costitutivo del rapporto di finanziamento, ma si protragga per l'intero «*life cycle*» dello stesso. In altri termini, che le procedure volte ad attuare la fase di monitoraggio del valore del bene non si risolvano in episodiche rilevazioni, ma vengano strutturate in modo da porsi in via continuativa e costante durante l'intero corso del rapporto. A proposito, uno specifico riferimento è compiuto all'eventuale attività di rivalutazione della garanzia mobiliare al fine di consentire che la stima originaria venga costantemente aggiornata e il dato rappresenti dunque valore effettivo.

In secondo attiene, invece, alle modalità attraverso cui simili procedure devono essere strutturate da parte degli enti creditizi. A riguardo viene espressa l'esigenza che gli intermediari si dotino di «*adequate IT processes, systems, capabilities and sufficient data*» per l'esecuzione di questa fase di monitoraggio.

Anche l'Autorità europea di vigilanza del settore viene dunque ad affidare alle tecnologie digitali un ruolo centrale per lo sviluppo di processi interni adeguati ed efficienti per lo svolgimento della fase gestoria e conservativa della garanzia reale.

---

[27] Cfr. EUROPEAN BANKING AUTHORITY, *Guidelines on loan origination and monitoring,* del 29 maggio 2020.

[28] Cfr. EUROPEAN BANKING AUTHORITY, *op. cit.*, parr. 7 ss.

# Il *"FinTech"* e la *"Dark Finance"*: quali rischi per i risparmiatori

Mauro Lorenzoni, Giuseppe Frega [*]



## 1. Introduzione. Frodi finanziarie collegate a nuove tecnologie

Il continuo progresso delle tecnologie informatiche e delle loro applicazioni nel campo dei servizi e dei prodotti finanziari (*FinTech*) pone costantemente nuove sfide agli operatori di mercato, al legislatore e al regolatore, generando per i risparmiatori nuove opportunità ma anche nuovi rischi.

Alle forme di investimento tradizionali si sono sempre più affiancate offerte di nuovi prodotti e servizi finanziari che utilizzano tecnologie avanzate e operano in modi e contesti che spesso non garantiscono una tutela adeguata dei risparmiatori.

Il progresso tecnologico ha infatti favorito l'innovazione finanziaria e lo sviluppo di nuovi modelli di *business* basati sull'utilizzo di piattaforme digitali che consentono l'offerta di servizi integrati in ottica *open finance* (servizi di *trading* di strumenti finanziari, scambio di *crypto-asset*, *crowdfunding* e servizi di pagamento).

Tuttavia, tale sviluppo ha favorito, quale effetto collaterale, anche la crescita del fenomeno degli abusivismi e delle frodi finanziarie che è presente soprattutto *online* con schemi sempre più interconnessi con le nuove tecnologie e si è dif-

[*] Le opinioni espresse dagli autori sono personali e non impegnano in alcun modo la Consob.

fuso attraverso l'utilizzo di canali di comunicazione digitale caratterizzati da modalità di interazione a distanza.

Un recente studio pubblicato dalla Consob [1] ha mostrato che gli investitori *retail* (soprattutto i meno abbienti, i meno scolarizzati e quelli con una minore alfabetizzazione finanziaria) effettuano le loro scelte di investimento principalmente sulla base di informazioni acquisite attraverso *internet* e i *social network*. Ciò aumenta l'esposizione al rischio di cadere vittima di abusivismi e frodi finanziarie *online*.

Parliamo in questi ultimi casi di "*Dark Finance*", intesa come quel complesso di mercati e soggetti che offrono prodotti finanziari o servizi di investimento in assenza dei presupposti previsti dalla normativa per operare nel settore finanziario.

## 2. Competenze e poteri della Consob nel contrasto alle attività abusive e casi maggiormente ricorrenti

Con la crescita dei casi di abusivismo finanziario e delle frodi ad essi collegate – in parallelo con il progresso delle nuove tecnologie – si è sviluppata l'attività di contrasto della Consob in questo settore. La Consob svolge un'azione di contrasto al fenomeno degli abusivismi finanziari con un ufficio dedicato (che è l'Ufficio Vigilanza sui Fenomeni Abusivi) dal 2011. Il fenomeno dell'abusivismo finanziario è presente soprattutto on-line (il 75% circa dei casi esaminati). Gli operatori abusivi agiscono infatti prevalentemente tramite siti *web* e utilizzano, quali canali di contatto per promuovere le proprie iniziative presso i risparmiatori, soprattutto *e-mail*, *chat*, *social network* e sollecitazioni telefoniche (c.d. *cold calling*). Come ulteriore veicolo di tali iniziative negli ultimi tempi ha assunto una particolare rilevanza il ruolo dei c.d. *fin-fluencer*.

L'azione di contrasto della Consob in questo campo si sviluppa principalmente lungo due direttrici: 1) il contrasto alla prestazione in assenza di autorizzazione di servizi di investimento su strumenti finanziari (quali ad es. negoziazione, gestione di portafogli, collocamento ecc.) e la relativa attività pubblicitaria; 2) il contrasto alle abusive offerte al pubblico di prodotti finanziari (in quanto svolte in assenza del prescritto prospetto informativo) e la relativa attività pubblicitaria. Si consideri che secondo la legislazione italiana l'offerta al pubblico di prodotti finanziari può avere come oggetto non solo uno "strumento finanziario" rientrante nelle categorie definite dalla normativa di derivazione comunitaria (tra cui azioni, obbligazioni, quote di fondi comuni di investimento, contratti derivati finanziari), ma anche "ogni altra forma di investimento di na-

[1] Rapporto 2024 sulle scelte di investimento delle famiglie italiane (https://www.consob.it/web/area-pubblica/abs-rf/-/asset_publisher/Ir0V5xvz7Z8K/content/report-famiglie-2024/11973).

tura finanziaria". Infatti, la nozione italiana di prodotto finanziario è più ampia della nozione di strumento finanziario e comprende altri investimenti finanziari come i contratti di investimento. In proposito, la ricorrenza di un "*prodotto finanziario*", *sub specie* di "*investimento di natura finanziaria*", diverso da uno strumento finanziario, ai sensi della disciplina nazionale e alla luce del consolidato orientamento della Consob, si basa sulla valutazione, caso per caso, delle oggettive pattuizioni e/o meccanismi contrattuali correlati all'operazione di volta in volta considerata.

Un investimento ha natura finanziaria in presenza dei seguenti elementi: *i)* impiego di capitale; *ii)* promessa/aspettativa di un *rendimento di natura finanziaria*, ossia di un profitto consistente nell'accrescimento delle disponibilità investite, *prospettato già all'atto dell'instaurazione del rapporto contrattuale, derivante prevalentemente dalle azioni imprenditoriali o manageriali poste in essere da terze parti rispetto all'acquirente il prodotto*; *iii)* assunzione di un rischio direttamente correlato all'impiego di capitale.

Il rendimento di natura finanziaria è pertanto rappresentato dalla remunerazione del capitale conferito dall'investitore, generata prevalentemente dallo sforzo imprenditoriale o manageriale dell'offerente. In sostanza, *l'investitore affida una somma di denaro all'offerente che la fa rendere e corrisponde all'investitore la remunerazione promessa*. In tale caso si è in presenza di contratti di investimento che configurano prodotti finanziari "atipici" diversi dagli strumenti finanziari.

Per contrastare le suddette attività finanziarie abusive la Consob esercita: 1) il potere di ordinare la cessazione della violazione nei confronti di coloro che prestano/offrono abusivamente servizi di investimento via *internet* o che pubblicizzano detti servizi, nonché il potere di ordinare ai fornitori dei servizi di connessione a *internet* l'oscuramento in Italia dei siti *web* mediante i quali sono offerti/prestati abusivamente servizi di investimento o gli stessi sono pubblicizzati (in tale ambito il fenomeno prevalente è quello del c.d. *trading on line* abusivo); 2) il potere di sospendere e vietare le offerte abusive di prodotti finanziari e l'attività pubblicitaria di tali offerte nonché il potere di ordinare, anche in tal caso, ai fornitori dei servizi di connessione a *internet* l'oscuramento in Italia dei siti *web* mediante i quali sono svolte le anzidette attività di offerta e pubblicità. La Consob dispone altresì della potestà sanzionatoria in relazione alle fattispecie di abusiva offerta al pubblico di prodotti finanziari.

Nella grande maggioranza dei casi l'operatività dei soggetti che prestano abusivamente attività finanziarie riservate cela vere e proprie truffe che la Consob segnala regolarmente all'Autorità giudiziaria. La prestazione abusiva di servizi di investimento è, peraltro, di per sé un reato ai sensi dell'art. 166 del d.lgs. n. 58/1998 (Tuf).

Preme evidenziare come l'azione di contrasto agli abusivismi finanziari si sia fatta più incisiva proprio grazie all'introduzione del potere di chiedere ai fornitori dei servizi di connessione a *internet* l'oscuramento: a) dei siti *web* mediante i quali sono offerti/prestati abusivamente servizi di investimento (da lu-

glio 2019)[2]; b) dei siti *web* mediante i quali sono offerti al pubblico abusivamente (senza prospetto informativo) prodotti finanziari (da marzo 2020)[3]. Tali poteri consentono di bloccare in Italia l'accesso ai siti *web* mediante i quali vengono prestate attività di cui è stata accertata, ad esito di specifiche istruttorie, la natura illecita garantendo maggiore efficacia all'azione di contrasto e, quindi, innalzando i livelli di tutela per gli investitori.

In poco più di cinque anni, da luglio 2019 a febbraio 2025, sono stati oscurati oltre 1.230 siti *web* riconducibili a operatori finanziari abusivi.

I casi più ricorrenti di prestazione abusiva di servizi di investimento sono rappresentati dai servizi di *trading*/negoziazione, offerti agli utenti mediante piattaforme *web*, che hanno ad oggetto strumenti finanziari derivati (quali i *Contract for Difference* – CFD[4]) che hanno come sottostanti – oltre a valute, indici di borsa e materie prime – sempre più frequentemente, cripto-valute. Non di rado all'utente è, altresì, offerta la possibilità di farsi "gestire"/"movimentare" il conto di *trading* mediante un c.d. *account manager* oppure mediante un *software* che opera formulando e/o eseguendo operazioni di investimento secondo modalità automatiche. In tale ambito, i risparmiatori sono spesso indotti ad acquistare cripto-valuta al presunto scopo di alimentare i propri conti di *trading*.

L'impiego di modalità automatiche di esecuzione di operazioni di compravendita di strumenti finanziari sui conti degli investitori ha spinto ormai da tempo l'ESMA e la Consob ad adottare apposite comunicazioni interpretative con cui è stato precisato che il c.d. *mirror trading* è assimilabile al servizio di investimento di gestione di portafogli per il cui svolgimento è necessario essere autorizzati. In particolare, lo schema operativo in questione prevede che il fornitore del servizio, attraverso una piattaforma tecnologica presente su un sito *internet*, raccolga i segnali operativi (i segnali di *trading*/indicazioni su compravendite di strumenti finanziari) proposti da *trader* privati o da *software* (tipo *trading system* o *robo advisor*) selezionati dal cliente tra le liste presenti sul medesimo sito *internet* e ne assicuri l'esecuzione automatica in virtù di una specifica autorizzazione del cliente a veicolare i segnali di *trading* al negoziatore prescelto dal cliente stesso. In alternativa è anche possibile che il fornitore del servizio di *mirror trading* esegua esso stesso i segnali di *trading* per conto del cliente. Tale attività è assimilata alla prestazione del servizio di gestione di portafogli in quanto il cliente/investitore si spoglia della facoltà di scelta dell'operazione di investimento e

[2] In base alla legge n. 58 del 28 giugno 2019 (legge di conversione del c.d. "Decreto Crescita", art. 36, comma 2-terdecies).

[3] In base alla legge n. 8 del 28 febbraio 2020 (legge di conversione del c.d. "Decreto Milleproroghe", art. 4, comma 3-bis).

[4] Attraverso i "CFD" le parti si impegnano a scambiarsi la differenza di prezzo che un asset sottostante fa registrare tra il momento di apertura della posizione (acquisto/conclusione del contratto) e quello di chiusura della posizione (esecuzione del contratto). I "CFD" sono, quindi, liquidati in contanti in base al differenziale tra il prezzo di mercato del sottostante alla data di apertura e di chiusura della posizione.

non intervenire in fase di trasmissione della decisione di investimento all'intermediario negoziatore.

Altra forma di replicazione automatica delle operazioni investimento è rappresentata da una modalità operativa anch'essa assimilabile al servizio di investimento di gestione di portafogli denominata *Multi-Account Manager*. In tali casi in genere una persona fisica (italiana) invita investitori (italiani) ad attivare conti di *trading* presso imprese di investimento (in alcuni casi autorizzate) ove lo stesso soggetto ha un proprio conto di *trading*, per poi farsi autorizzare a collegare il proprio conto ai conti degli investitori. In tal modo le operazioni di *trading* effettuate da detto soggetto sul proprio conto principale (detto anche conto "*master*") sono replicate in automatico sui conti collegati degli investitori (c.d. conti "*slave*").

Il più delle volte i potenziali clienti – raggiunti attraverso pressanti, reiterati contatti telefonici[5] – vengono invitati a fornire i loro dati personali e a versare somme di denaro (tramite bonifici, carte di credito, carte prepagate) per aprire conti per il *trading* di 'titoli' presso la piattaforma *on line* (il portale/il sito) che l'operatore abusivo indica loro. Il cliente viene quindi irretito con la prospettiva di facili guadagni a fronte di investimenti iniziali di modica entità. Poi l'investitore viene pressantemente invitato ad investire sempre maggiori somme facendogli credere che sta gradualmente conseguendo consistenti rendimenti. Quando l'investitore prova a prelevare in tutto o in parte le somme di denaro che risultano presenti sul suo conto tale possibilità gli viene negata e gli vengono addotti i pretesti più disparati (economici, fiscali-contrattuali o semplicemente di opportunità).

Nella maggioranza dei casi, l'apertura del conto di *trading* consente solo apparentemente di operare effettuando acquisti e vendite di "titoli". In realtà, le operazioni di compravendita di "titoli" che il cliente dispone, e visualizza sullo schermo del suo *computer*, sono solo virtuali perché il *broker* abusivo non le esegue e, conseguentemente, anche i guadagni che il cliente visualizza sul suo conto sono solo virtuali, non reali.

Per quel che riguarda le offerte abusive di prodotti finanziari sono, invece, frequenti le proposte di investimenti finanziari "atipici" rappresentati da contratti di investimento con cui sono promessi mirabolanti rendimenti fuori mercato.

In tali casi agli investitori vengono di solito prospettati rendimenti predeterminati o predeterminabili sulla base di parametri predefiniti nonché in proporzione al capitale versato dall'investitore.

Non di rado le offerte di prodotti di investimento atipici sono associate a schemi di vendita di tipo piramidale. Secondo tali sistemi agli investitori sono prospettati ulteriori guadagni per il procacciamento di altri aderenti al sistema. Si è poi manifestato, nel tempo, un ulteriore schema illecito secondo cui, quando l'investitore ha ormai compreso di essere vittima di un operatore finanziario abusivo, viene contattato da una sedicente società di recupero crediti che – a volte anche utilizzando illegittimamente il logo o altri segni distintivi della

[5] Attraverso massicce campagne telefoniche effettuate da *call center* situati all'estero.

CONSOB o di altre Autorità – gli prospetta, a fronte di un corrispettivo in denaro, la possibilità di ottenere il rimborso delle somme già investite, salvo poi sottrargli anche queste ulteriori somme senza fornire alcun servizio. La Consob ha pubblicato avvisi sul fenomeno a beneficio del pubblico degli investitori. La Consob ha pubblicato avvisi per i risparmiatori anche in merito alla frequente pratica posta in essere da operatori finanziari abusivi che utilizzano impropriamente il nome e l'immagine di personaggi noti per indurre i risparmiatori, dietro promesse di facili guadagni, ad aderire a proposte di investimento.

Infine, oltre all'azione di contrasto svolta mediante l'assunzione di provvedimenti di *enforcement*, la Consob già da tempo – considerata la pericolosità del fenomeno per il pubblico risparmio – offre anche una tutela informativa nei confronti degli investitori, sia promuovendo iniziative di *investor education* sia pubblicando, nella sezione del proprio sito *web* denominata "Occhio alle truffe", informazioni idonee a mettere i risparmiatori in condizione di acquisire consapevolezza e, quindi, di individuare, evitando di aderirvi, iniziative abusive che sono, come detto, solitamente attività truffaldine.

## 3. I *crypto-asset*

I *crypto-asset* hanno assunto una sempre maggiore attrattività, canalizzando quote di risparmio crescenti, e si presentano, soprattutto nella percezione dei risparmiatori, come veicolo di possibile ritorno economico, soprattutto quando sono negoziabili su apposite piattaforme presenti *on-line*. Ciò risulta particolarmente rilevante se si considera che sul mercato si assiste ad intense campagne di *marketing*, spesso veicolate tramite i *social network*, che sollecitano il pubblico ad acquistare tali *asset*.

Dal 30 dicembre 2024 è pienamente applicabile il Regolamento (UE) 2023/1114 relativo ai mercati delle cripto-attività (MiCAR – *Markets in Crypto-Assets Regulation*), che ha introdotto nell'Unione europea una disciplina armonizzata per l'emissione, l'offerta, l'ammissione alla negoziazione e la prestazione di servizi aventi ad oggetto cripto-attività non riconducibili a strumenti finanziari o altri prodotti già regolamentati da atti legislativi dell'UE.

### 3.1. Tecnologie a registro distribuito (DLT) e *blockchain*

Prima di trattare più ampiamente la recente normativa comunitaria in materia di cripto-attività appare opportuno fornirne un breve inquadramento e fare cenno dell'ambiente digitale in cui esse vengono create e circolano.

Per *crypto-asset* o anche *digital token* si intende la rappresentazione digitale di un valore o di un diritto che viene creato, trasferito e conservato elettronicamente

attraverso un registro digitale distribuito/condiviso. Tale registro digitale si basa su tecnologie DLT, *Distributed Ledger Technology,* la cui applicazione più frequente è la *blockchain*. La *blockchain* altro non è che un registro *online* condiviso dai suoi partecipanti che sono i "nodi" che appunto condividono la gestione di questo registro procedendo alla validazione dei "blocchi" che contengono le informazioni relative alla creazione, alla gestione e alla circolazione di *crypto-asset*.

La *blockchain* è, quindi, un registro condiviso strutturato in blocchi consecutivi, cronologicamente ordinati in modo da formare una catena. Ogni blocco contiene le informazioni relative alla registrazione delle operazioni effettuate.

Questi blocchi di registrazioni/transazioni si formano attraverso la validazione dei partecipanti alla *blockchain*, i c.d. nodi. A questo riguardo, esistono *blockchain* di tipo *permissionless,* ove chiunque può partecipare (si tratta di *blockchain* aperte, completamente decentralizzate), e *blockchain* di tipo *permissioned*, governate da un'autorità centrale, ove l'accesso è riservato a un numero ristretto di utenti. Accanto a queste due macrocategorie si inseriscono alcune *blockchain* che adottano soluzioni ibride e che, pertanto, presentano caratteristiche miste, delle *blockchain* private e delle *blockchain* pubbliche.

Il processo di validazione di ogni singolo blocco si basa su un protocollo di consenso che può essere, solitamente, di due tipi: *Proof of work* e *Proof of stake*.

La *Proof of work* prevede la soluzione di un complesso problema di calcolo (c.d. "*mining*"). Il nodo che per primo riesce a risolvere il problema comunica la soluzione e il blocco creato agli altri nodi della rete che verificano la correttezza della soluzione. Se la maggioranza dei nodi ritiene che la soluzione sia valida, il nuovo blocco viene aggiunto alla catena ed il "*miner*" si aggiudica una ricompensa (rappresentata da una quota parte delle nuove cripto-attività create).

La *Proof of stake* prevede che venga di volta in volta individuato, in modalità prevalentemente casuale, un nodo o un gruppo di nodi della rete (c.d. *validator)* per validare le transazioni, ricevendo una ricompensa per l'attività svolta (anche in tal caso rappresentata da una quota parte delle nuove cripto-attività create). Per vedersi riconosciuta la qualifica di "validatori", i nodi vincolano parte dei propri *token* (tramite un sistema detto "*stake*"). Generalmente, quanto maggiore è l'ammontare degli *asset* "vincolati" dal "*validator*" e l'ampiezza del periodo in cui detti *asset* sono tenuti vincolati tanto maggiore è la possibilità che si venga scelti come validatori. La *Proof of stake* si fonda sulla presunzione che più *asset* un utente possiede e da più tempo li possiede, minore sarà il suo interesse ad attaccare o pregiudicare il sistema del quale fa parte.

## 3.2. Principali categorie di cripto-attività attualmente in circolazione

Nell'ambito della *blockchain* si possono quindi creare e trasferire varie cripto-attività. Senza alcuna pretesa di esaustività le principali categorie di *crypto-asset* che sono risultate essere le più diffuse in base all'osservazione della prassi applicativa sono:

• gli *utility token* che incorporano diritti a godere di beni o a usufruire di servizi messi a disposizione dall'emittente;

• gli NFT *(non fungible token*) che identificano univocamente un *asset* di riferimento (spesso un'opera d'arte digitale) e non sono tra loro fungibili, cioè intercambiabili, data l'intrinseca univocità del bene cui ciascun NFT si riferisce;

• i *payment token* che possiamo classificare per semplicità come cripto-valute in quanto assolverebbero almeno teoricamente alla funzione di mezzo di pagamento;

• i *security token* o *investment token* che sono assimilabili a prodotti finanziari;

• gli *hybrid token* che in genere combinano elementi degli *utility* ed elementi finanziari.

### 3.3. Operatività delle c.d. piattaforme di *exchange* di *crypto-asset*

Gli *asset* digitali, emessi e circolanti all'interno dei sistemi DLT, vengono depositati e trasferiti per il tramite di un "portafoglio digitale" (c.d. *e-wallet* o *wallet*, ossia un conto personale), al quale si accede mediante credenziali. La custodia può essere svolta: *i*) *online* da un *custodial wallet provider* (c.d. "*hot storage wallet*"), ossia da un soggetto che si pone come intermediario tra l'utente e il sistema basato su registri distribuiti fornendo un servizio di custodia; *ii*) *offline* direttamente dall'utente attraverso un sistema c.d. *noncustodial* (c.d. "*cold storage wallet*"), ossia tramite il salvataggio e la conservazione in remoto delle chiavi crittografiche (ad esempio sul PC, sullo *smart phone* o su altri apparecchi dell'utente).

È possibile scambiare gli *asset* digitali nell'ambito di "piattaforme di scambio" *online* che si distinguono in centralizzate e decentralizzate.

Nelle piattaforme centralizzate le attività di negoziazione dei *crypto-asset* tra gli utenti sono registrate presso la piattaforma di *exchange* ma non nella *blockchain*, che viene aggiornata esclusivamente per registrare le fasi di deposito e ritiro di *token* (in sostanza sono registrati in *blockchain* solo i saldi).

Nelle piattaforme non centralizzate l'utente, attraverso un *software* installato su un proprio dispositivo, negozia nella piattaforma di scambio e interagisce con la *blockchain* registrandovi direttamente le transazioni.

In tali ambienti di scambio i *crypto-asset* sono solitamente soggetti a repentine oscillazioni di valore e possono divenire oggetto di operazioni a carattere speculativo determinando le tipiche distorsioni dei mercati speculativi che presuppongono rialzi di valore basati sulla – non sempre ben riposta – fiducia che ci sia sempre una controparte disponibile ad acquistare ad un prezzo futuro più alto dell'attuale.

## 3.4. L'evoluzione del quadro normativo e il MiCAR

Il quadro normativo ha presto evidenziato i suoi limiti (che hanno posto problemi definitori e di disciplina) rispetto a processi e prodotti tecnologicamente innovativi quali l'emissione e la circolazione di *crypto-asset* mediante l'utilizzo delle tecnologie basate su registri elettronici distribuiti (c.d. sistemi DLT, come la *blockchain*) che si sono rapidamente imposti all'attenzione (non solo) del mondo finanziario. Per un lungo periodo le Autorità di controllo hanno infatti dovuto agire in assenza di un quadro normativo strutturato e specificamente tarato sul settore delle cripto-attività.

Ciò ha comportato la necessità che la normativa si evolvesse anche tenendo conto di tali nuove tecnologie per accompagnare il processo di cambiamento da queste determinato che porterà sempre più a un riposizionamento di operatori finanziari tradizionali e all'ingresso di nuovi operatori provenienti dai settori tecnologici.

In tal senso si sono quindi sviluppate varie iniziative legislative a livello europeo, nell'ambito dell'"*European Digital Finance Package*", tra le quali il Regolamento c.d. "MiCAR" (*Markets in Crypto-Assets Regulation*) [6], che disciplina, da un lato, i profili di trasparenza dell'offerta (e ammissione alla negoziazione) dei *crypto-asset* diversi dagli strumenti finanziari, attraverso la pubblicazione di un *white paper* e, dall'altro, la prestazione dei servizi su *crypto-asset*, tra i quali il servizio di gestione di piattaforme di scambio di *crypto-asset* e il servizio di *custodial wallet provider*, mediante un regime di autorizzazione per i prestatori di tali servizi. Sul piano nazionale, il d.lgs. n. 129 del 5 settembre 2024, identificando la Consob e la Banca d'Italia come Autorità competenti e delineando le rispettive competenze in ragione delle tipologie di cripto-attività di volta in volta considerate, ha completato l'*iter* di adeguamento al MiCAR che è applicabile nella sua interezza a far data dal 30 dicembre 2024 [7].

Il MiCAR contiene una definizione generale volutamente ampia di cripto-attività che viene identificata come una rappresentazione digitale di un valore o di un diritto che può essere trasferito e memorizzato elettronicamente utilizzando una tecnologia a registro distribuito o una tecnologia analoga.

Occorre, tuttavia, precisare che il MiCAR non disciplina tutto ciò che rientra nel "settore cripto" e infatti restano fuori dal suo perimetro, tra l'altro:

- le cripto-attività assimilabili agli strumenti finanziari e gli altri "prodotti" già disciplinati dall'esistente legislazione UE (es., depositi, fondi, cartolarizzazioni, prodotti assicurativi, prodotti pensionistici ecc.) indipendentemente dalla tecnologia utilizzata per la loro emissione o il loro trasferimento;
- i *Non-Fungible Tokens* (NFTs), a condizione che le cripto-attività siano real-

[6] Regolamento UE 2023/1114.

[7] I Titoli III (relativo agli ART) e IV (relativo agli EMT) sono applicabili dal 30 giugno 2024.

mente "uniche e non fungibili con altre cripto-attività" (condizione che, ad es., non ricorre quando si tratta di *token* frazionabili o emessi in una ampia serie);

• le *Central bank digital currency* (CBDC) come l'Euro digitale.

Prima dell'entrata in vigore in Italia del MiCAR, l'unica disciplina applicabile alla prestazione dei servizi su valute virtuali era quella in materia "anti-riciclaggio" che prevedeva l'iscrizione dei soggetti che intendevano prestare servizi su valute virtuali presso una sezione speciale del registro dei cambia-valute tenuto dall'OAM (Organismo Agenti in attività finanziaria e Mediatori creditizi).

Tale assetto è stato superato dal MiCAR.

Nel decreto di implementazione del MiCAR nell'ordinamento nazionale è previsto un regime transitorio per disciplinare il passaggio dalla disciplina della prestazione di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale alla disciplina della prestazione di servizi sulle cripto-attività prevista da MiCAR. In particolare, il regime transitorio prevede che i soggetti regolarmente iscritti al registro OAM al 27 dicembre 2024 possono continuare ad operare fino al 30 giugno 2025. Inoltre, a condizione che entro la predetta data presentino istanza di autorizzazione ai sensi del MiCAR in Italia o in un altro Stato membro, possono continuare a operare fino al 30 dicembre 2025 (o fino al rilascio o al diniego di un'autorizzazione ai sensi MiCAR se questa data è anteriore) ai sensi della previgente disciplina.

Analizzando le tipologie di cripto-attività espressamente prese in considerazione dal Regolamento si può subito notare che, per la loro individuazione e classificazione, il MiCAR ha adottato un criterio basato sul "rischio". Le cripto-attività vengono distinte in tre tipi che appunto si differenziano tra loro a seconda dei rischi che comportano. Maggiori sono i rischi individuati dal legislatore con riferimento ad una determinata tipologia di cripto attività, più sarà stringente la disciplina relativa alla sua emissione, offerta, e ammissione alla negoziazione.

In particolare, gli e-*Money Token* (EMT) mirano a mantenere un valore stabile facendo riferimento al valore di una valuta ufficiale. La funzione degli EMT è analoga a quella della moneta elettronica (come carte di credito, debito, applicazioni di pagamento ecc.) e sono utilizzati per effettuare pagamenti. Devono essere emessi necessariamente da un ente creditizio autorizzato o da un istituto di moneta elettronica. Gli emittenti dei *token* di moneta elettronica sono tenuti a garantire ai loro possessori di poter esercitare il diritto di ottenere in qualsiasi momento il rimborso dei *token* al valore nominale della valuta di riferimento.

Gli *Asset Referenced Token* (ART) mirano a mantenere un valore stabile facendo riferimento ad altri valori o diritti (o a una loro combinazione), comprese una o più valute ufficiali. Possono essere utilizzati come mezzo di scambio, per trasferire valore o per finalità speculative. A differenza degli EMT che vengono rimborsati al valore nominale della loro valuta di riferimento, gli ART conferiscono al possessore il diritto di ottenere il rimborso del *token* al suo valore di mercato (valore di mercato dell'*asset* di riferimento).

Dopo gli EMT e gli ART il regolamento individua una categoria residuale molto ampia che comprende (anche) gli *utility token*. Questa categoria residuale, denominata categoria dei *token other than,* comprende tutte le cripto-attività diverse dagli ART e dagli EMT al netto ovviamente di quelle cripto-attività che sono escluse dall'ambito di applicazione del Regolamento.

Non rientra direttamente nell'ambito applicativo del MiCAR il Bitcoin che senza dubbio è la più famosa delle criptovalute in circolazione ma il cui emittente non è individuabile. Infatti, nei "considerando" del MiCAR è ben chiarito che se le cripto-attività non hanno un emittente identificabile non devono rientrare nell'ambito di applicazione del regolamento almeno per ciò che concerne l'emissione e l'offerta al pubblico. Lo stesso MiCAR precisa, tuttavia, che queste cripto-attività prive di un emittente individuabile, come il Bitcoin, rientrano nell'ambito della regolamentazione sotto il profilo della prestazione di servizi su cripto-attività da parte dei CASP autorizzati (*crypto-asset service provider*) o in relazione alla richiesta di ammissione alla negoziazione su una piattaforma di *trading* per cui il soggetto richiedente l'ammissione è tenuto alla redazione di un *white paper*.

I servizi su cripto-attività possono essere prestati da soggetti che non siano già intermediari finanziari autorizzati e che siano appositamente autorizzati dall'autorità competente (in Italia, la Consob) oppure da soggetti che siano già sottoposti a vigilanza come Banche, SIM e IMEL (Istituti di Moneta Elettronica) che non avranno bisogno di un'ulteriore e apposita autorizzazione ma potranno operare previa semplice notifica all'autorità competente.

Per quanto riguarda l'emissione e l'offerta di cripto attività il MiCAR prevede, in via generale, che lo svolgimento di tali attività sia necessariamente assistito e preceduto dalla pubblicazione di un documento informativo chiamato *white paper* che deve contenere un *set* di informazioni relative all'emittente e alle caratteristiche della cripto-attività con l'indicazione dei diritti che essa attribuisce, degli obblighi in capo all'emittente e dei rischi sottostanti.

In particolare, gli EMT possono essere emessi solo dalle banche e dagli IMEL, quindi da soggetti qualificati e già ampiamente vigilati, previa notifica del *white paper* all'autorità competente.

Gli ART possono essere emessi e offerti dalle banche, previa notifica all'autorità competente e previa approvazione del relativo *white paper* oppure da altre entità giuridiche che però devono essere debitamente autorizzate all'emissione dall'autorità competente (in Italia, la Banca d'Italia) alla quale va sottoposto (per l'approvazione) il *white paper*.

Infine, per le cripto-attività "*other than*", il Regolamento introduce una disciplina meno stringente per l'offerta al pubblico e l'ammissione alla negoziazione e stabilisce che possono essere effettuate sulla base della semplice notifica del *white pape*r all'autorità competente (in Italia, la Consob).

### 3.5. Nuove responsabilità e poteri delle Autorità di controllo a seguito del MiCAR. Cenni

Il decreto di implementazione del MiCAR nell'ordinamento interno ha individuato la Banca d'Italia e la Consob come le Autorità responsabili degli atti delegati e delle norme tecniche di regolamentazione e di attuazione del MiCAR. Di conseguenza, i loro ambiti di competenza e i loro poteri generali di vigilanza e di indagine sono stati adeguati secondo le linee di specializzazione funzionale definite in via generale dalla normativa di settore: vigilanza prudenziale alla Banca d'Italia e vigilanza sulla trasparenza e correttezza degli operatori e dei mercati alla Consob.

La Banca d'Italia è primariamente responsabile per la supervisione degli emittenti di ART e EMT. La Consob supervisiona il rispetto delle regole di condotta applicabili ai CASP nella prestazione di servizi. Con riferimento ai medesimi CASP la Banca d'Italia è responsabile per i profili organizzativi, di gestione del rischio, prudenziali, etc.

La Consob è inoltre responsabile per l'applicazione delle regole che riguardano l'offerta di cripto-attività "*other than*" (diverse dagli ART e dagli EMT) e di quelle in materia di *market abuse*.

Spetta alla Consob il compito di gestire i procedimenti autorizzativi dei CASP che presentino istanza di autorizzazione in Italia; l'autorizzazione potrà essere rilasciata o rifiutata d'intesa con la Banca d'Italia, per i profili di competenza.

La prestazione di servizi per le cripto-attività, l'offerta o l'ammissione alla negoziazione di ART o EMT nonché l'emissione di EMT in violazione dei requisiti autorizzativi previsti dal MiCAR costituiscono attività soggette a sanzione penale, consistente nella reclusione da sei mesi a quattro anni e in una multa da Euro 2.066,00 a Euro 10.329,00.

La Consob esercita i poteri di vigilanza e di indagine di cui all'art. 94 del MiCAR al fine di adempiere ai compiti ad essa attribuiti dal medesimo Regolamento, compreso il potere di contrastare le iniziative abusive che si sostanziano principalmente in due macrocategorie: *i*) da un lato, la prestazione di servizi per le cripto-attività in assenza di autorizzazione e, *ii*) dall'altro l'offerta al pubblico e/o richiesta di ammissione alla negoziazione di cripto-attività *other than* in assenza di *white paper* notificato. In relazione a tali fattispecie, secondo quanto previsto dal MiCAR e dalla relativa disciplina nazionale di implementazione, la Consob dispone di poteri interdittivi e inibitori in forza dei quali può: *i*) vietare la prestazione di servizi per le cripto-attività in assenza di autorizzazione; *ii*) vietare l'offerta al pubblico e/o ammissione alla negoziazione di cripto-attività c.d. *other than* effettuata in assenza di *white paper* notificato alla Consob; *iii*) oscurare i siti *internet* mediante cui vengono prestati servizi per le cripto-attività in assenza di autorizzazione nonché dei siti *internet* mediante cui viene effettuata l'offerta di *token other than* in assenza di *white paper* notificato. Il decreto di implementazione del MiCAR specifica che le norme italiane in materia di pro-

dotti finanziari ("atipici") non trovano più applicazione alle cripto-attività soggette al MiCAR.

## 3.6. I rischi per i risparmiatori e i *warning* delle Autorità di vigilanza

Negli ultimi anni le Autorità di controllo, in assenza di uno specifico quadro normativo di riferimento, non hanno mancato di informare i risparmiatori in merito ai significativi rischi associati all'acquisto e/o alla detenzione di *crypto-asset*. A tale riguardo, particolarmente significativo appare il comunicato congiunto emesso il 9 marzo 2018 dall'Autorità europea degli strumenti finanziari e dei mercati (ESMA), dall'Autorità bancaria europea (ABE) e dall'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali (EIOPA)[8].

In tale comunicato le tre Autorità hanno affermato, tra l'altro, che "l*e valute virtuali attualmente disponibili sono una rappresentazione digitale di valore, non sono emesse né garantite da una banca centrale o da un'autorità pubblica e non godono dello status giuridico di valuta o di moneta"* e che *"l''acquisto di valute virtuali o di prodotti finanziari che forniscono un'esposizione diretta a tali valute comporta una serie di rischi",* tra i quali vengono evidenziati "*il rischio di volatilità estrema e di bolla speculativa", "l'assenza di protezione", "l'assenza di opzioni di uscita", "la mancanza di trasparenza sui prezzi", "le informazioni fuorvianti" e "l'inidoneità delle valute virtuali per la maggior parte degli scopi, tra cui la pianificazione d'investimenti o previdenziale",* per poi concludere che "*l'elevata volatilità delle valute virtuali, l'incertezza sul loro futuro e l'inaffidabilità delle piattaforme di negoziazione e dei fornitori di portafogli rende le valute virtuali inadatte per la maggior parte dei consumatori, inclusi quelli con un orizzonte d'investimento di breve periodo, e specialmente per coloro che perseguono obiettivi di lungo periodo come risparmiare per la pensione*".

Anche la Consob e la Banca d'Italia hanno in più occasioni messo in guardia i risparmiatori contro gli elevati rischi connessi alle cripto-attività, pubblicando a tale riguardo nel 2021 anche un comunicato congiunto[9] nel quale, tra l'altro, dopo aver segnalato che "*tali rischi assumono ora una maggiore rilevanza in relazione al diffondersi di forme di offerta attraverso il canale digitale che facilitano l'acquisto di cripto-attività da parte di una platea molto ampia di soggetti*", concludono che "*l'adesione a offerte di prodotti finanziari correlati a cripto-attività, quali ad esempio i cd. digital token, è un investimento altamente rischioso, tanto più qualora, come spesso riscontrato, le offerte siano effettuate da operatori abusivi, non autorizzati, non regolati e non vigilati da alcuna Autorità".*

Queste attività sono prive di un valore intrinseco e vengono spesso scambiate

---

[8] https://www.esma.europa.eu/sites/default/files/library/joint_esas_warning_on_virtual_currencies_it.pdf.

[9] https://www.bancaditalia.it/media/comunicati/documenti/2021-01/CS_Congiunto_BI_CONSOB_cryptoasset.pdf.

su circuiti opachi. Nonostante ciò, secondo l'analisi dei flussi trimestrali inviati all'Organismo Agenti e Mediatori (OAM) e di un sondaggio condotto in collaborazione con Banca d'Italia e Consob, nel primo trimestre 2024 vi erano oltre 1,3 milioni di individui che detenevano cripto-attività presso i prestatori di servizi su valute virtuali (Vasp) registrati in Italia nel registro dell'OAM per un controvalore complessivo di 2,7 miliardi, ovvero l'85% in più rispetto al quarto trimestre 2023. Inoltre, secondo quanto segnalato dalla Consob in un comunicato stampa del 30 luglio 2024, la quota di famiglie italiane con *crypto-asset* in portafoglio è salita in due anni dall'8 al 18% [10].

## 4. Conclusioni

Si è dato conto nei paragrafi precedenti di come all'evolversi delle tecnologie sia purtroppo conseguito anche un aumento dei casi di abusivismo finanziario e di truffe *on-line* e di quali siano i rischi connessi all'acquisto, detenzione e scambio di *crypto-asset*.

Questa situazione è stata sicuramente favorita dal fatto che molti risparmiatori sono sprovvisti delle conoscenze necessarie per valutare il grado di rischiosità intrinseca dell'investimento nonché lo scarso livello di liquidabilità dei *crypto-asset*.

Creare le condizioni perché i cittadini possano conseguire un adeguato livello di cultura finanziaria è alla base della tutela del risparmio garantita dalla Costituzione e rappresenta un dovere per tutte le Istituzioni che a diverso titolo sono chiamate ad offrire il proprio contributo, ivi incluse le Autorità di controllo.

Si tratta di un campo in cui negli ultimi anni sono stati fatti molti progressi, in particolare a seguito della creazione, presso il Ministero dell'Economia e delle Finanze, del "Comitato per la programmazione e il coordinamento delle attività di educazione finanziaria" [11], che opera prevalentemente in una prospettiva di medio-lungo termine.

Più recentemente, l'art. 45 della legge 5 marzo 2024 n. 21 [12] ha introdotto, nell'ambito dell'educazione civica, lo studio dell'educazione finanziaria tra le materie di insegnamento nelle scuole dell'obbligo, nel presupposto che l'istru-

[10] https://www.consob.it/documents/1912911/3990887/cs_20240730.pdf/9faf020a-e6c9-d98f-dfc1-3371b6503e91?t=1722321555814.

[11] Il Comitato, istituito nel 2017, è composto da: Ministero dell'Economia e delle Finanze, Ministero dell'Istruzione, Ministero dello Sviluppo Economico, Ministero del Lavoro, Banca d'Italia, Consob, Covip, Ivass, Ocf, Consiglio nazionale dei consumatori e degli utenti.

[12] Recante "*Interventi a sostegno della competitività dei capitali e delega al Governo per la riforma organica delle disposizioni in materia di mercati dei capitali recate dal testo unico di cui al decreto legislativo 24 febbraio 1998, n. 58, e delle disposizioni in materia di società di capitali contenute nel codice civile applicabili anche agli emittenti*".

zione scolastica rappresenti un canale fondamentale per veicolare la comprensione di concetti finanziari.

Nell'immediato quello che occorre è che i risparmiatori siano resi almeno coscienti del fatto che un investimento non deve essere inteso come una scommessa ma richiede ponderazione, informazioni accurate e verificabili e una chiara consapevolezza dei rischi.

A questo fine è raccomandabile quanto meno di avvalersi delle informazioni e del supporto messi a disposizione dalle Autorità di controllo preposte alla tutela del pubblico risparmio. I rispettivi siti *web* istituzionali, oltre a fornire un quadro informativo corretto e completo, sono anche ricchi di utili consigli e i canali di comunicazione con il pubblico sempre attivi.

# La cybersecurity in ambito bancario, finanziario e assicurativo nell'era dei crimini informatici e dell'intelligenza artificiale

Giovanni Ziccardi

SOMMARIO: 1. Il quadro attuale. – 2. Gli attacchi legati al fattore umano. – 3. Gli attacchi legati alle azioni criminali mirate. – 4. Gli attacchi legati alla mancanza di aggiornamenti e alla vulnerabilità dei sistemi. – 5. Alcune considerazioni conclusive sul futuro, sulla formazione e su DORA.

## 1. Il quadro attuale

Il tema della sicurezza informatica in ambito bancario e assicurativo si è manifestato particolarmente urgente durante la pandemia e nel periodo immediatamente successivo: vi era un timore diffuso, nelle istituzioni dell'Unione Europea, che un possibile attacco alle infrastrutture tecnologiche del Vecchio Continente potesse portare, in un periodo così delicato, a una crisi economica globale [1]. Allo stesso tempo, il livello di alfabetizzazione informatica e la consapevolezza in tema di cybersecurity da parte del mondo della politica, del settore pubblico e delle aziende era visto in Europa come carente anche rispetto all'attenzione, per questi temi, che era presente in altri Paesi [2].

Questo spiega il succedersi di importanti riforme normative che hanno preso il via agli inizi del decennio 2010 con il Regolamento europeo per la protezione dei dati (GDPR), si sono evolute in un quadro normativo specifico sulle infrastrutture critiche e la cyber sicurezza anche a livello dei singoli Paesi (ci si riferisce alla NIS e alla NIS2, due direttive che hanno disciplinato in Europa il quadro della cybersecurity), per, poi, spostarsi verso la normativa sull'intelligenza artificiale (AI Act del 2024) e, soprattutto, il regolamento DORA, che è stato

[1] Si veda sul punto, per un quadro introduttivo e alla portata anche del non esperto, P. IEZZI, *Cyber e potere. L'escalation delle ostilità digitali e i nuovi rischi per le infrastrutture strategiche*, Mondadori, Milano, 2023.

[2] Sul punto sia consentito il rinvio a G. ZICCARDI, *Dati avvelenati*, Raffaello Cortina, Milano, 2024.

specificamente pensato per le infrastrutture tecnologiche economiche e finanziarie in Unione Europea.

Proprio il regolamento DORA, che vedrà la sua attuazione completa dal gennaio del 2025, è il provvedimento più interessante nel nostro contesto, dal momento che è stato pensato proprio per l'ambito finanziario, bancario e assicurativo.

È sempre, però, necessario coordinare questi provvedimenti (che disciplinano in maniera "verticale" il mondo delle tecnologie) con provvedimenti più generali che comunque, da tempo, individuano le questioni di cybersicurezza e le vulnerabilità nell'ambito *de quo*.

Tutti questi provvedimenti evidenziano, *prima facie*, possibili attacchi informatici e vulnerabilità che si possono dividere in tre specifiche categorie.

Per tradizione, si individuano, innanzitutto, attacchi o incidenti informatici che possono essere generati dall'interno, attacchi o incidenti che possono essere causati dal dolo di criminali informatici che vogliono attaccare quella determinata realtà e la prendono come obiettivo e vulnerabilità che nascono, invece, dal mancato aggiornamento del sistema informatico o da problematiche che si potrebbero dire "insite" nel sistema informatico stesso e che spesso sono utilizzate dai criminali per avere accesso al sistema informatico di un determinato ente o contesto aziendale.

Circa la prima "famiglia", ossia quella degli attacchi provenienti dall'interno, è prassi distinguere solitamente tra attacchi causati da un dipendente che lo fa per dolo (quindi volontariamente "malicious"), un dipendente che è invece *incauto* e non segue le regole che sono stabilite all'interno della realtà (si pensi a un soggetto che non segue le *policy* di sicurezza in una determinata realtà aziendale oppure sovrastima le proprie competenze tecnologiche) e, infine, un dipendente cosiddetto "compromesso" (gli sono state sottratte le credenziali o ha rivelato le credenziali di accesso alla sua posta elettronica o al sistema dell'azienda a terzi e un criminale informatico sta utilizzando le sue credenziali per entrare nel sistema e vedere ciò che succede).

Circa il secondo gruppo di attacchi provenienti *dall'esterno* troviamo quei comportamenti che sono portati da organizzazioni criminali. Il crimine informatico è diventato, negli ultimi anni un business importantissimo, e questi attacchi sono portati tendenzialmente per finalità estorsive (con correlata richiesta di denaro) [3].

Questi tipi di attacco operano in maniera simile. Innanzitutto, il criminale cerca di ottenere l'accesso al sistema. Entra, quindi, nel sistema, e inizia uno "spostamento laterale" (ossia cerca di individuare tutti i computer che sono collegati al computer nel quale è entrato, per spostarsi all'interno del sistema e compromettere ulteriori computer). A questo punto, inizia a "scalare i privilegi", ossia cerca di rubare delle credenziali, o passare in computer di utenti, che

[3] Per un quadro storico completo si veda G. WHITE, *Crime dot com. Il potere globale dell'hacking dai virus ai brogli elettorali*, Odoya, Bologna, 2022.

hanno più poteri sul sistema. Si pensi, ad esempio, a utenze che hanno il potere di disattivare un antivirus, di eliminare un firewall o di togliere altre protezioni di sicurezza. Quando il criminale ha ottenuto il potere "massimo" all'interno di un sistema può cifrare i dati, esfiltrare le informazioni e domandare un riscatto.

Oggi le azioni criminali di questo tipo sono stratificate in più organizzazioni che si prendono cura, ognuna, di una determinata azione. Vi sono organizzazioni criminali più esperte che aiutano a entrare nel sistema, e criminali che domandano il riscatto, altri soggetti che attivano servizi di pagamento, altri ancora che si occupano del cash-out e della monetizzazione del profitto per far perdere le tracce o del riciclaggio del denaro.

Non si deve più pensare a un crimine informatico come a un attacco portato da un adolescente dalla sua cameretta di notte con particolari competenze informatiche ma vi è alle spalle una vera e propria stratificazione di organizzazioni criminali coinvolte nello stesso attacco che hanno reso il crimine informatico particolarmente insidioso.

Nel terzo, e ultimo, tipo di attacchi abbiamo invece delle modalità di aggressione che sono legate a azioni connesse a "difetti" del sistema attaccato, ossia alla presenza di vulnerabilità, mancanze di aggiornamenti o "porte d'ingresso" lasciate aperte in siti web, app o sistemi.

Il quadro informatico odierno della cyber security in ambito bancario lo possiamo fare rientrare, pur con qualche piccola eccezione che vedremo, in questi tre grandi ambiti. In questo breve scritto li andremo ad analizzare tutti e tre per, poi, comprendere quali possano essere le strategie di difesa più corrette e quali possano essere i punti di debolezza.

## 2. Gli attacchi legati al fattore umano

Nel settore bancario, assicurativo e finanziario, il *fattore umano* rappresenta una delle principali vulnerabilità per la sicurezza informatica.

I dipendenti, infatti, possono facilmente diventare vittime inconsapevoli di attacchi mirati come il *phishing* e il *social engineering*, che altro non sono che tecniche di manipolazione che sfruttano la fiducia e la disattenzione delle persone per indurle a rivelare informazioni sensibili o a cliccare su link dannosi.

Allo stesso tempo, una gestione superficiale delle *credenziali*, come l'uso di password deboli o la condivisione non autorizzata di informazioni riservate, può creare punti di accesso pericolosi nei sistemi aziendali. Questa facilità con cui gli attaccanti riescono a sfruttare tali debolezze rappresenta un problema di grande rilevanza, dato che gli errori umani sono alla base della maggioranza degli incidenti di sicurezza.

Il phishing si manifesta comunemente attraverso e-mail, messaggi o telefonate apparentemente affidabili, spesso mascherate da comunicazioni di colleghi, partner commerciali o, persino, di istituzioni bancarie stesse. Gli attaccanti stu-

diano il comportamento e il contesto lavorativo delle vittime, creando messaggi credibili e personalizzati che ispirano fiducia, rendendo così difficile distinguere il falso dal reale.

Questi messaggi, apparentemente innocui, inducono il dipendente a compiere azioni pericolose, come cliccare su link malevoli, scaricare allegati infetti o rivelare informazioni sensibili, come le proprie credenziali d'accesso. Le conseguenze possono essere gravi: una singola e-mail di phishing può aprire un varco nei sistemi aziendali, consentendo ai criminali informatici di accedere a dati riservati e di compromettere intere reti informatiche.

La Polizia Postale, nel suo rapporto del 2022, descrive ad esempio l'uso dell'idea di autorità come leva perfetta per fare vittime[4]:

> "Operazione "KAFKA" – La Polizia di Stato, a conclusione di una delicata attività d'indagine condotta dal Servizio Polizia Postale e delle Comunicazioni, ha eseguito 16 decreti di perquisizione personale e domiciliare, emessi dalle Procure della Repubblica di Brescia e Vicenza, con l'ausilio dei Compartimenti di Polizia Postale di Milano, Torino, Pescara, Trieste, Venezia e Roma. Proprio come nel libro "Il processo" dello scrittore boemo, ignari utenti della rete hanno scoperto di essere stati accusati, processati e condannati per delitti mai commessi; l'indagine trae spunto dall'invio massivo di mail estorsive, apparentemente provenienti da Autorità istituzionali, contenenti una falsa citazione in Tribunale per fatti afferenti alla pedopornografia. Solo nel periodo di circa 2 mesi i proventi illeciti sono stati di oltre mezzo milione di euro. La corrispondenza telematica oggetto di indagine riproduce un falso documento governativo e presenta nell'intestazione falsi loghi di Forze di polizia e di Ministeri italiani, tra i quali il Ministero dell'Interno e il Ministero della Difesa – affiancati a quelli di Agenzie internazionali quali Europol ed Interpol. Il falso documento a firma di vertici di Istituzioni statuali quali il Capo della Polizia Lamberto Giannini, piuttosto che del Comandante Generale dell'Arma dei Carabinieri, Teo Luzi, dal Direttore del Servizio Polizia Postale, pro tempore, Nunzia Ciardi e dall'attuale Direttore Supplente del Servizio Polizia Postale, Ivano Gabrielli. L'atto fraudolento contesta all'utente violazioni gravissime, commesse attraverso la rete Internet, legate a condotte penalmente rilevanti riferite a delitti di molestie sessuali su minori. Il documento minaccia di inoltrare le prove ad un non meglio specificato "Procuratore" ed ai media, invitando a fornire giustificazioni entro 72 ore. Il passo successivo è una richiesta di denaro per far "decadere" le accuse e l'indicazione delle coordinate bancarie verso le quali corrispondere le somme estorte. Il fenomeno che ha una rilevanza europea, colpisce in particolare Francia, Austria, Spagna, Belgio e Italia. Sono in corso i rituali accertamenti tecnici sul materiale informatico oggetto di perquisizione, al fine di delineare le responsabilità dei soggetti indagati nell'attività delittuosa e la rete dei contatti coinvolti nell'invio delle mail estorsive con particolare attenzione ai collegamenti con l'estero".

[4] Si veda in Internet all'indirizzo https://www.commissariatodips.it/notizie/articolo/resoconto-attivita-2022-della-polizia-postale-e-delle-comunicazioni-e-dei-centri-operativi-sicurezz/index.html.

Il *social engineering*, dal canto suo, va oltre il semplice invio di comunicazioni ingannevoli: sfrutta le relazioni umane per ottenere informazioni riservate. In questo caso, gli attaccanti cercano di costruire un rapporto con la vittima, fingendo di essere una figura di fiducia o, addirittura, creando uno scenario di emergenza per far leva sull'urgenza.

In una banca o in un'azienda assicurativa, ad esempio, un cybercriminale potrebbe presentarsi come un responsabile informatico (o amministratore di sistema) e, con una giustificazione plausibile, chiedere a un dipendente di fornire informazioni o di eseguire procedure per risolvere asseriti problemi tecnici. La persona presa di mira, magari colta di sorpresa, è così indotta a collaborare e ad abbassare le difese, permettendo all'attaccante di acquisire informazioni preziose o di introdursi nei sistemi informatici aziendali.

Queste tecniche si basano spesso sulla gestione superficiale delle credenziali da parte dei dipendenti, un fattore che amplifica le vulnerabilità aziendali.

L'utilizzo di password deboli o facilmente intuibili, come combinazioni comuni o legate alla vita privata del dipendente, apre spesso la porta agli attaccanti. Inoltre, la condivisione non autorizzata di credenziali, magari fra colleghi o con fornitori esterni, espone i sistemi a potenziali intrusioni. Spesso i dipendenti non si rendono conto che tale leggerezza può comportare l'accesso indesiderato di soggetti terzi, i quali sfruttano questa vulnerabilità per infiltrarsi nei sistemi. A ciò si aggiunge la pratica, purtroppo comune, di riutilizzare le stesse password per diversi account aziendali e personali, il che rende ancora più facile il lavoro dei cybercriminali, i quali possono utilizzare credenziali già violate in passato per accedere a nuove reti.

Le aziende del settore finanziario, per loro natura, gestiscono dati estremamente sensibili e riservati, e l'imperizia nella gestione delle credenziali rappresenta un grave rischio per l'integrità dell'intero sistema.

In questi contesti, anche il minimo errore umano può comportare danni significativi e, una volta che l'attaccante ottiene le credenziali di un dipendente, il percorso verso l'accesso a informazioni finanziarie o a dati personali dei clienti diventa veramente semplice. Appare, quindi, cruciale adottare pratiche rigorose nella gestione delle password e formare costantemente il personale sui pericoli legati alla manipolazione psicologica e alla gestione sicura delle informazioni.

La minaccia non si limita, però, alla verifica di comportamenti negligenti: vi è un'altra categoria di rischi che proviene da "insider" malevoli, ovvero dipendenti che intenzionalmente utilizzano il loro accesso privilegiato per sottrarre dati o compromettere i sistemi dell'azienda. Tali minacce interne possono derivare da motivazioni economiche, vendette personali o influenze esterne, e sono particolarmente insidiose perché spesso il danno viene scoperto solo dopo che sono state compromesse seriamente le operazioni aziendali.

Questi attacchi interni sono particolarmente insidiosi perché si fanno risalire a figure già integrate nell'organizzazione, persone che conoscono le dinamiche e le vulnerabilità dell'azienda, e che hanno un accesso diretto alle risorse più preziose e sensibili. In questo caso, il rischio non è rappresentato dall'errore uma-

no, ma da una volontà deliberata di danneggiare l'azienda, mossa da motivazioni che possono essere di varia natura.

Le ragioni alla base di tali atti dolosi possono spaziare da incentivi economici a vendette personali. In alcuni casi, un dipendente insoddisfatto o in conflitto con l'azienda potrebbe agire per risentimento, cercando di colpire la propria organizzazione per rivalsa o per danneggiarne la reputazione. In altri casi, possono intervenire fattori economici esterni: non sono rari gli episodi in cui dipendenti vengano "comprati" da *competitor* o gruppi criminali, attratti da offerte economiche che li spingono a cedere informazioni sensibili o a sabotare i sistemi aziendali per favorire interessi esterni. Esiste anche il rischio che questi insider vengano manipolati o ricattati da entità esterne che sfruttano eventuali vulnerabilità personali per ottenere la loro collaborazione forzata.

Simili attacchi interni, dettati da intenzioni dolose, sono particolarmente difficili da rilevare e spesso il danno emerge solo quando il sistema è già stato gravemente compromesso. Poiché l'insider agisce dall'interno, riesce a muoversi nei sistemi aziendali in modo da suscitare meno sospetti, operando in zone e con procedure a cui ha normalmente accesso.

Le operazioni aziendali possono subire danni gravissimi da queste minacce, compromettendo in modo irreversibile la fiducia dei clienti e la posizione sul mercato, oltre a mettere a rischio i dati finanziari e sensibili gestiti dall'azienda.

Di fronte a questi rischi, risulta evidente come la protezione da minacce interne richieda un sistema di monitoraggio avanzato e una cultura della sicurezza che incoraggi la segnalazione di comportamenti sospetti, anche se provenienti da figure interne e apparentemente affidabili.

La sottrazione di credenziali, si diceva poco sopra, è un'altra tattica prediletta dagli attaccanti per ottenere accesso non autorizzato ai sistemi finanziari. Attraverso tecniche di attacco come il "credential stuffing", gli attaccanti sfruttano combinazioni di username e password già violate in precedenti attacchi. Altre tecniche, come il cosiddetto "Business Email Compromise" (BEC), mirano invece a compromettere direttamente gli account e-mail aziendali. Quest'ultimo metodo, diffuso soprattutto nel settore finanziario, si basa sull'uso fraudolento di account compromessi per inviare false istruzioni relative a trasferimenti di fondi, danneggiando sia l'azienda che i suoi clienti, inviando comunicazioni come se provenissero da una figura interna all'organizzazione, spesso con un alto grado di autorità.

In particolare, nel settore finanziario, dove le istruzioni relative a operazioni di trasferimento di fondi sono all'ordine del giorno, il rischio è amplificato. Attraverso un account e-mail compromesso, i criminali inviano messaggi fasulli contenenti richieste di trasferimento di somme di denaro o modifiche alle coordinate bancarie dei fornitori. Poiché queste richieste sembrano provenire da una fonte attendibile, i destinatari, spesso responsabili di operazioni finanziarie, sono portati a eseguire le istruzioni senza sospetti.

Le conseguenze di questi attacchi sono importanti. Non solo compromettono la sicurezza dell'azienda, ma minano anche la fiducia dei clienti, i quali vedo-

no a rischio i propri dati e le proprie risorse. Ogni attacco di questo tipo non è solo un danno alle finanze aziendali, ma anche un danno alla reputazione, dato che le vittime principali sono proprio i clienti, ai quali spesso vengono sottratti fondi o informazioni personali. Di fronte a queste minacce, diventa essenziale adottare misure preventive, come l'autenticazione a più fattori, che rende più difficile per gli attaccanti accedere agli account aziendali, e l'educazione continua del personale per riconoscere segnali di compromissione degli account e-mail.

## 3. Gli attacchi legati alle azioni criminali mirate

Gli attacchi portati alle banche e alle compagnie di assicurazione da organizzazioni criminali informatiche si configurano oggi come operazioni *altamente sofisticate*, spesso organizzate su scala globale e condotte con una precisione che ricorda le strategie militari.

Questi gruppi di criminalità informatica non sono più composti da *singoli attori isolati*, ma da organizzazioni strutturate e ben coordinate, che operano da diverse parti del mondo, con una forte concentrazione di attività in regioni come l'Europa orientale, l'Asia e, in misura crescente, anche l'Africa e il Sud America. Si tratta di vere e proprie *imprese del crimine digitale*, con gerarchie, compiti specifici e obiettivi chiari, che collaborano per portare a termine attacchi su vasta scala, mirando a colpire infrastrutture finanziarie critiche con precisione chirurgica.

Queste organizzazioni si avvalgono di metodologie diversificate, adattando le loro tattiche in base al tipo di bersaglio e alla struttura dell'organizzazione.

Una delle tecniche più comuni è la produzione e l'uso di *ransomware*, un attacco in cui i criminali riescono a bloccare l'accesso ai sistemi aziendali, cifrando i dati e rendendoli inutilizzabili fino a quando non viene pagato un riscatto.

In particolare, gli attacchi ransomware contro banche e assicurazioni possono paralizzare intere sezioni operative, poiché i dati finanziari e le informazioni sensibili diventano irraggiungibili, costringendo l'azienda a interrompere i servizi, con un danno immediato sia economico che reputazionale.

Spesso i riscatti richiesti per "liberare" questi sistemi sono esorbitanti, e le aziende si trovano davanti a una scelta difficile tra la perdita economica diretta, nel caso accettino di pagare il riscatto, e il danno prolungato causato dall'impossibilità di riprendere subito l'attività.

Il ransomware ha subito (purtroppo) un'evoluzione significativa dai suoi primi casi, risalenti alla fine degli anni Ottanta del secolo scorso, fino ai sofisticati software odierni, che rappresentano una delle minacce più temute nel panorama della sicurezza informatica.

Ogni fase di questa evoluzione riflette sia i progressi tecnologici sia la crescente abilità e organizzazione delle gang di cybercriminali, che hanno trasformato il ransomware in una vera e propria industria del crimine digitale.

Il primo caso documentato di ransomware risale al 1989, con un virus, diffu-

so tramite floppy disk, che cifrava i nomi dei file sul computer della vittima e richiedeva un pagamento di riscatto inviato a un indirizzo fisico per riottenere l'accesso ai dati. Questo attacco pionieristico era rudimentale, sia per la tecnologia di cifratura utilizzata che per le modalità di pagamento, ma stabiliva già il modello di base del ransomware: *blocco dei dati* e *richiesta di riscatto*.

Nei primi anni 2000, con la diffusione di Internet, il ransomware iniziò a diventare più sofisticato. I criminali informatici iniziarono a utilizzare tecniche di crittografia più avanzate per cifrare i file delle vittime, rendendo il riscatto necessario per il recupero dei dati. I pagamenti iniziarono a essere richiesti in modalità più *anonime*, anche se la diffusione su larga scala era ancora limitata dalla scarsa conoscenza del ransomware tra le vittime e dalla minore diffusione delle transazioni digitali. In questa fase, gli attacchi ransomware erano meno frequenti e si concentravano più su individui che su aziende.

Il periodo tra il 2010 e il 2015 ha segnato un punto di svolta. I criminali hanno iniziato a sviluppare il modello del "ransomware-as-a-service" (RaaS), offrendo kit di ransomware pronti all'uso che chiunque può acquistare e distribuire *senza particolari competenze tecniche*. Questo modello ha permesso di abbassare la barriera di ingresso, portando a un aumento esponenziale degli attacchi ransomware. Inoltre, in questo periodo iniziarono a emergere attacchi mirati a organizzazioni e aziende, non solo a singoli individui, con richieste di riscatto molto più elevate. Gli attaccanti iniziavano a prendere di mira specifiche aziende o settori vulnerabili, come quello *sanitario* e quello *finanziario*, sapendo che le potenziali perdite di dati critici avrebbero reso più probabile il pagamento del riscatto.

Nel 2017, due attacchi ransomware, WannaCry e NotPetya, segnarono un'altra svolta. WannaCry utilizzava un exploit chiamato EternalBlue, sviluppato dall'NSA e poi trapelato online, per diffondersi autonomamente tra i computer Windows non aggiornati, causando danni su scala globale e colpendo ospedali, aziende e istituzioni governative. WannaCry non solo cifrava i file, ma si *diffondeva rapidamente* in tutta la rete, aumentando esponenzialmente la velocità e la portata dell'attacco.

NotPetya, apparentemente un ransomware, era in realtà un attacco distruttivo che cancellava i dati senza possibilità di recupero, colpendo principalmente l'Ucraina ma diffondendosi anche ad aziende multinazionali.

Questi attacchi dimostrarono il potenziale devastante del ransomware e spinsero le aziende e i governi a prendere più seriamente la minaccia. Durante questi anni, inoltre, le criptovalute, come il Bitcoin, iniziarono a essere utilizzate quasi esclusivamente come metodo di pagamento per i riscatti, poiché garantivano l'anonimato e la rapidità delle transazioni.

Negli anni recenti, il ransomware si è evoluto ulteriormente, con l'introduzione del modello di "doppia estorsione".

In questo schema, i criminali non solo cifrano i file delle vittime, ma li *rubano* anche, minacciando di pubblicare o vendere i dati sottratti se il riscatto non viene pagato. Questo nuovo approccio ha portato a un aumento delle richieste di riscatto e ha spinto molte aziende, preoccupate per la propria reputazione e per

le implicazioni legali, a pagare. Un esempio emblematico è l'attacco alla *Colonial Pipeline* negli Stati Uniti nel 2021, che bloccò un'importante infrastruttura energetica e causò gravi disagi economici, spingendo la società a pagare milioni di dollari per evitare la diffusione dei propri dati.

Nel frattempo, il ransomware-as-a-service è diventato ancora più strutturato e professionale.

Le gang di cyber criminali ora forniscono ransomware chiavi in mano ad "affiliati", che si occupano di distribuire il malware in cambio di una percentuale sui riscatti.

Questo modello di business ha permesso di espandere ulteriormente la portata degli attacchi, rendendoli accessibili anche a criminali informatici meno esperti, e creando veri e propri *ecosistemi criminali* con supporto tecnico e aggiornamenti continui.

## 4. Gli attacchi legati alla mancanza di aggiornamenti e alla vulnerabilità dei sistemi

Gli attacchi informatici basati sulle vulnerabilità dei sistemi rappresentano una minaccia altrettanto seria per il settore finanziario e assicurativo, e si basano principalmente sullo sfruttamento di *falle* nei software e nei sistemi operativi che non sono stati adeguatamente aggiornati o, come si dice in gergo tecnico, "patchati".

Ogni sistema informatico, infatti, è composto da una complessa serie di applicazioni, reti e infrastrutture hardware, tutte costantemente sottoposte a possibili evoluzioni tecnologiche e a nuove minacce. I fornitori di software rilasciano regolarmente *patch di sicurezza*, cioè aggiornamenti che risolvono falle identificate, ma se queste patch non vengono applicate in modo tempestivo, le vulnerabilità rimangono aperte, diventando un facile bersaglio per gli attaccanti.

Si veda, in particolare, questo caso recente sanzionato dal Garante per la Protezione dei Dati italiano[5]:

> "Il Garante Privacy ha applicato una sanzione di 900mila euro a Postel Spa che per quasi un anno non è intervenuta su una già nota e segnalata vulnerabilità dei propri sistemi, attraverso la quale ha poi subito una violazione dei dati personali. Nell'agosto del 2023, la società è stata oggetto di un attacco informatico di tipo ransomware che ha causato il blocco dei server e di alcune postazioni di lavoro. In particolare l'attacco ha comportato l'esfiltrazione – e in alcuni casi la perdita di disponibilità – dei file contenenti i dati personali di circa 25mila interessati, fra dipendenti, ex dipendenti, congiunti, titolari di cariche societarie, candidati a posizioni lavorative e

[5] Si veda in Internet all'indirizzo https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10066116.

> rappresentanti di imprese che intrattenevano rapporti commerciali con Postel. Le informazioni, successivamente pubblicate nel dark web, riguardavano dati anagrafici e di contatto, dati di accesso e identificazione, dati di pagamento, nonché dati relativi a condanne penali e reati e, tra quelli appartenenti a categorie particolari, dati che rivelano l'appartenenza sindacale e relativi alla salute. Nonostante la vulnerabilità fosse stata segnalata, prima dal produttore del software (settembre 2022, con la messa a disposizione degli aggiornamenti necessari a novembre 2022) e poi dall'Agenzia per la cybersicurezza nazionale (novembre 2022), Postel non aveva aggiornato, come raccomandato, i propri sistemi. […] Nel provvedimento adottato, il Garante ha ingiunto a Postel, oltre al pagamento della sanzione di 900mila euro, di effettuare un'azione straordinaria di analisi delle vulnerabilità dei propri sistemi, di predisporre un piano per rilevare e gestire tali vulnerabilità e di individuare tempistiche di rilevamento e di risposta adeguate al rischio".

Gli attacchi alle vulnerabilità dei sistemi si basano spesso su *exploit*, programmi creati appositamente per sfruttare specifiche falle di sicurezza.

Questi exploit vengono impiegati dai cybercriminali per penetrare nei sistemi aziendali, installare malware, ottenere accesso non autorizzato ai dati o, persino, prendere il controllo completo delle risorse informatiche.

In un contesto bancario o assicurativo, dove sono gestiti dati sensibili e operazioni finanziarie, il rischio è amplificato: anche una singola vulnerabilità non "patchata" può fornire un punto d'ingresso pericoloso, consentendo agli attaccanti di sottrarre informazioni riservate, compromettere la privacy dei clienti o manipolare transazioni finanziarie a loro favore.

Una delle tipologie di attacco più temute in questo ambito è quella del cosiddetto "zero-day", che sfrutta una vulnerabilità appena scoperta e per la quale non esiste ancora una patch di sicurezza.

In questi casi, gli attaccanti approfittano del ritardo inevitabile tra l'individuazione della vulnerabilità e la distribuzione di una correzione da parte del fornitore, lanciando attacchi prima che le aziende abbiano il tempo di proteggere i propri sistemi.

Gli zero-day sono tra gli attacchi più difficili da prevenire, poiché nessuno, nemmeno i team di sicurezza, è a conoscenza della falla fino a quando questa non viene scoperta. Spesso, per contrastare i rischi associati a questi attacchi, le aziende si affidano a strumenti di rilevamento avanzati, in grado di monitorare costantemente il traffico di rete per individuare attività sospette, ma la prevenzione rimane complessa.

I sistemi bancari e assicurativi sono inoltre composti da architetture *stratificate* e *integrate*, in cui operano molteplici software e applicazioni spesso interconnessi, e questo rende difficile applicare regolarmente aggiornamenti senza interrompere i servizi. I dipartimenti IT si trovano quindi davanti a una sfida costante: da un lato, la necessità di garantire la continuità operativa, dall'altro, l'obbligo di mantenere sistemi e applicazioni sempre aggiornati. Tuttavia, rinviare l'implementazione delle patch di sicurezza per non interrompere i servizi può aprire falle che diventano veri e propri punti d'accesso per gli attaccanti, i

quali sanno bene come approfittare di queste debolezze per infiltrarsi nei sistemi aziendali.

Un ulteriore rischio è rappresentato dai dispositivi e dai software *di terze parti*, come quelli forniti dai partner commerciali o dai fornitori esterni, che spesso non dispongono di controlli di sicurezza altrettanto rigorosi. I criminali informatici possono sfruttare le vulnerabilità nei sistemi dei fornitori per accedere indirettamente all'infrastruttura delle banche o delle assicurazioni, utilizzando una sorta di "porta sul retro". Questa strategia permette agli attaccanti di infiltrarsi senza essere rilevati e di mantenere l'accesso ai dati aziendali per lunghi periodi, con il rischio di arrecare danni gravi e *persistenti*.

Le conseguenze di questi attacchi possono essere importanti: una vulnerabilità sfruttata in un sistema bancario o assicurativo può esporre dati sensibili, compromettere interi sistemi e creare interruzioni di servizio che incidono sulla fiducia dei clienti e sul rispetto delle normative di settore.

## 5. Alcune considerazioni conclusive sul futuro, sulla formazione e su DORA

Negli ultimi anni, come abbiamo scritto poco sopra, la sicurezza informatica nel settore bancario e finanziario a livello globale si è trovata ad affrontare sfide sempre più complesse e sofisticate.

L'evoluzione delle tecnologie digitali ha portato a una *maggiore esposizione* a minacce cibernetiche, richiedendo alle istituzioni finanziarie di adottare misure avanzate per proteggere i propri sistemi e, soprattutto, i dati dei clienti.

Le organizzazioni criminali informatiche hanno intensificato gli attacchi contro le istituzioni finanziarie in pieno periodo di pandemia, utilizzando tecniche come il *ransomware*, il *phishing* mirato e il *Business E-mail Compromise*. Questi attacchi mirano contemporaneamente a sottrarre dati sensibili, a compromettere le operazioni e a ottenere guadagni illeciti.

Si veda, nel resoconto 2023 delle attività della Polizia Postale [6], il più importante caso italiano di *Business E-mail Compromise* che ha colpito la società sportiva della Cremonese calcio:

> "Operazione "Cremonese Calcio" Gli specialisti del Servizio Polizia Postale e delle Comunicazioni si sono attivati il 9 ottobre u.s. in seguito alla denuncia presentata dall'U.S. Cremonese Calcio per una patita frode informatica di tipo B.E.C. Fraud (Business Email Compromise). In particolare, gli ignoti autori del reato, mediante la violazione dei sistemi di posta elettronica aziendali, si inserivano nella corrispondenza intrattenuta tra la U.S. Cremonese Calcio e l'omologa Belga del Genk, riuscendo a

[6] In Internet all'indirizzo https://www.commissariatodips.it/docs/RESOCONTO_ATTIVITA_2023.pdf.

> modificare le coordinate bancarie per il pagamento della seconda rata dell'acquisto del calciatore belga Cyriel Dessers. Indotta in errore, la U.S. Cremonese Calcio disponeva in data 28 settembre 2023, un bonifico di euro 1.719.500,00 su un conto corrente attestato presso la banca belga ING di Avenue Marnix 24 – Bruxelles. L'immediata attivazione dei canali di cooperazione internazionale di polizia, ha consentito il blocco cautelativo del conto corrente contenente l'intera somma frodata".

Per contrastare queste minacce, le autorità di regolamentazione hanno introdotto normative più stringenti. La direttiva europea NIS2 e il *Digital Operational Resilience Act* (DORA) impongono, infatti, requisiti rigorosi in materia di sicurezza informatica per le istituzioni finanziarie, obbligandole a implementare misure di protezione avanzate e a garantire la resilienza operativa

Tuttavia, l'adeguamento a queste normative comporta costi significativi, sollevando preoccupazioni sulla reale sostenibilità economica di tali operazioni legislative.

Le minacce cibernetiche, al contempo, si stanno evolvendo in diverse direzioni: sempre maggiore *sofisticazione degli attacchi* (gli attaccanti utilizzano tecniche avanzate per eludere le difese tradizionali), *automazione e intelligenza artificiale* (l'uso di strumenti automatizzati e dell'intelligenza artificiale consente di condurre attacchi su larga scala con maggiore precisione, riducendo il tempo necessario per compromettere i sistemi target) e *attacchi mirati* (cresce il numero di attacchi personalizzati che sfruttano informazioni specifiche sulle vittime per aumentare l'efficacia).

Tra le nuove tipologie di attacchi che sono emersi nel 2024 si evidenziano, in particolare, il *phishing-as-a-Service*, o PaaS (modello in cui i criminali informatici offrono kit di phishing completi e personalizzabili, abbassando le barriere d'ingresso per gli attaccanti meno esperti), gli attacchi alle *criptovalute* (gli attaccanti sviluppano kit di phishing specifici che clonano pagine di login di piattaforme di criptovalute per sottrarre credenziali agli utenti), lo sfruttamento dell'intelligenza artificiale (gli attaccanti utilizzano l'intelligenza artificiale per creare e-mail e siti web falsi altamente convincenti, aumentando l'efficacia degli attacchi di phishing e social engineering) e, infine, gli attacchi alla *supply chain* (gli attaccanti compromettono fornitori terzi per infiltrarsi nelle reti delle istituzioni finanziarie, sfruttando le relazioni di fiducia esistenti).

L'aumento e l'evoluzione delle minacce cibernetiche richiedono così alle banche e alle compagnie di assicurazione di adottare strategie di sicurezza più *robuste* e *proattive*.

È fondamentale, in particolare, implementare programmi di *formazione continua* per il personale, adottare tecnologie avanzate di rilevamento e risposta alle minacce e collaborare con le autorità competenti per condividere informazioni sulle minacce emergenti. Solo attraverso un approccio integrato e dinamico è possibile mitigare i rischi associati a un panorama di minacce in continua evoluzione.

Per affrontare il crescente rischio di attacchi informatici, sono spesso lanciate campagne di sensibilizzazione rivolte ai cittadini e ai dipendenti del settore finanziario, per educare il pubblico a riconoscere e prevenire le truffe online. Que-

ste iniziative mirano a rafforzare la consapevolezza e la preparazione contro le minacce cibernetiche.

Un'azione di formazione e sensibilizzazione dei dipendenti nel settore bancario e assicurativo per abbassare il rischio di minacce cibernetiche dovrebbe essere progettata in modo strategico e personalizzato, considerando le specificità e le criticità di questi ambienti ad alto rischio.

L'obiettivo dovrebbe essere quello di creare una *cultura aziendale* attenta alla sicurezza informatica, dove ogni dipendente diventi un "difensore" della sicurezza e sia in grado di riconoscere e rispondere ai tentativi di attacco.

La formazione dovrebbe partire con una base introduttiva, che renda i dipendenti consapevoli delle principali minacce informatiche, del contesto attuale e della loro crescente complessità. In questa fase si dovrebbero trattare temi come il significato e l'importanza della cybersecurity nel settore finanziario, introducendo concetti essenziali come phishing, social engineering, ransomware e Business E-mail Compromise. È cruciale che i dipendenti comprendano quanto queste minacce possano compromettere dati sensibili e sistemi operativi e abbiano chiaro il ruolo fondamentale che loro stessi svolgono nella prevenzione di tali rischi.

Una parte fondamentale del programma dovrebbe poi riguardare il *riconoscimento* delle minacce. I dipendenti dovrebbero essere abituati a identificare e-mail e messaggi di phishing, a distinguere comunicazioni sospette da quelle autentiche e a capire quali azioni possono risultare rischiose. Attraverso esercitazioni pratiche e simulazioni, si dovrebbe insegnare ai partecipanti ai percorsi di formazione a riconoscere i segnali di allarme tipici, come link strani, errori grammaticali nelle e-mail, mittenti non attendibili, o richieste *urgenti* di accesso a dati sensibili. Simulazioni periodiche di phishing sono anch'esse molto efficaci per valutare la capacità dei dipendenti di resistere a questi attacchi e per rafforzare la loro attenzione alle comunicazioni in entrata.

La gestione sicura delle *credenziali* è, ancora, un elemento chiave nel settore finanziario. Si dovrebbe affrontare il tema delle migliori pratiche per creare password robuste e dell'uso corretto di strumenti di gestione delle password, sensibilizzando sull'importanza di non riutilizzare le stesse credenziali in contesti diversi. Inoltre, si dovrebbero incentivare pratiche di *autenticazione multifattoriale* (MFA) e spiegare come questa funzione protegga ulteriormente l'accesso ai sistemi, rendendo più difficile per un attaccante ottenere accessi non autorizzati.

I dipendenti dovrebbero poi essere informati sui rischi legati all'uso dei dispositivi aziendali e sull'importanza di mantenere un alto livello di sicurezza anche nei dispositivi *personali*, che spesso possono accedere a risorse aziendali. Si pensi all'importanza di aggiornare i software e di applicare le patch di sicurezza, dell'uso sicuro delle reti Wi-Fi pubbliche, e della corretta gestione dei dispositivi mobili. La policy di accesso da remoto, ormai essenziale con l'aumento dello smart working, dovrebbe essere spiegata in dettaglio, con *focus* sulle procedure di accesso sicuro e sui rischi legati all'uso di reti non protette.

Per evitare danni derivanti da minacce interne, d'altro canto, occorrerebbe

sensibilizzare i dipendenti anche sull'importanza di comportamenti *etici* e del rispetto delle policy aziendali. Sarebbe opportuno elaborare *linee guida* su come evitare pratiche pericolose, come la condivisione non autorizzata di informazioni, e promuovere l'etica della sicurezza. È importante che i dipendenti comprendano che, anche senza intenzioni dolose, comportamenti imprudenti possono mettere a rischio l'azienda e la propria sicurezza.

I dipendenti dovrebbero poi essere informati sulle procedure di segnalazione di comportamenti sospetti o di eventuali incidenti. Fondamentale è chiarire a chi rivolgersi in caso di sospette attività informatiche come, ad esempio, un possibile tentativo di phishing o una violazione dei dati. È fondamentale che i dipendenti sappiano come rispondere a un attacco in corso, come isolare un dispositivo compromesso e come evitare di compromettere altri sistemi.

Per rafforzare le conoscenze acquisite, sarebbe anche utile organizzare esercitazioni pratiche e *scenari simulati* che riproducano le situazioni di rischio più comuni e realistiche. I partecipanti potrebbero essere messi alla prova con simulazioni di phishing, richieste di accesso a dati sensibili o tentativi di social engineering, per valutare e migliorare la loro prontezza e capacità di rispondere. Le simulazioni sono particolarmente efficaci perché aiutano i dipendenti a *familiarizzare* con situazioni di rischio reale senza conseguenze, aumentando la loro sicurezza e reattività.

Infine, la formazione dovrebbe essere un processo continuo. Le minacce informatiche evolvono rapidamente e una sensibilizzazione aggiornata è fondamentale per mantenere alta la capacità difensiva dell'azienda. Questo significa prevedere sessioni periodiche di aggiornamento, condividere le nuove informazioni sulle minacce emergenti e promuovere una *cultura della sicurezza* in cui i dipendenti siano costantemente informati e pronti a collaborare per mantenere sicuro l'ambiente di lavoro.

La cooperazione tra istituzioni finanziarie, autorità governative e organismi internazionali è diventata, si diceva, fondamentale per affrontare le minacce informatiche.

A tal fine, il *Digital Operational Resilience Act* (DORA), entrato in vigore nell'Unione Europea per rafforzare la *resilienza operativa* delle istituzioni finanziarie, ci sembra un ottimo *esempio normativo* capace di imporre un insieme di requisiti chiave che banche, assicurazioni e altre entità finanziarie dovranno implementare per proteggersi al meglio dagli attacchi informatici e per garantire continuità operativa.

DORA, in estrema sintesi, richiede alle istituzioni di integrare il concetto di "resilienza operativa digitale" nella loro *governance* complessiva. Ciò implica che i consigli di amministrazione e la leadership aziendale saranno ritenuti responsabili della gestione del rischio informatico e della resilienza operativa. Dovranno, in particolare, stabilire chiare linee guida, monitorare i progressi e assegnare risorse sufficienti per garantire che le policy di sicurezza informatica siano implementate correttamente.

Le istituzioni finanziarie dovranno così implementare processi per identifica-

re, valutare e mitigare i rischi informatici *in modo proattivo*. Ciò include l'obbligo di condurre valutazioni e analisi regolari del rischio su tutti i sistemi informatici, sulle infrastrutture e sulle tecnologie utilizzate, valutando le vulnerabilità potenziali e assicurandosi che vi siano meccanismi di controllo adeguati. I rischi devono essere *documentati* e monitorati *costantemente* per identificare eventuali lacune o aree a rischio.

DORA impone anche che le banche e le assicurazioni stabiliscano piani di continuità operativa e piani di ripristino dei sistemi in caso di *incidente*, assicurandosi che tutti i soggetti siano pronti per *situazioni di emergenza*. Questi piani devono essere testati periodicamente attraverso prove, test ed esercitazioni, per garantire che l'organizzazione possa continuare a operare e fornire servizi anche durante, o dopo, un attacco informatico.

Interessante il punto del provvedimento dove si stabilisce come le istituzioni dovranno condurre regolari test di resilienza operativa, inclusi stress test e simulazioni di attacco, per valutare la capacità di *resistere* a potenziali incidenti informatici. DORA richiede che queste simulazioni non si limitino a testare singoli sistemi, ma si concentrino su scenari di attacco realistici che potrebbero compromettere l'intera operatività dell'istituzione. I test servono così a valutare sia la resistenza delle infrastrutture informatiche che la capacità di risposta dei team interni.

Uno degli aspetti centrali di DORA è, poi, l'obbligo di monitorare attentamente i *fornitori terzi* di servizi ICT, dato che questi rappresentano un potenziale punto di vulnerabilità.

Le istituzioni finanziarie devono assicurarsi che i fornitori rispettino standard di sicurezza informatica altrettanto rigorosi e che siano incluse nei contratti clausole per gestire il rischio di *interruzione dei servizi*. Devono essere predisposti accordi che garantiscano accesso ai dati e ai sistemi in caso di necessità, e le istituzioni devono esercitare un'adeguata supervisione e revisione sui fornitori critici.

DORA introduce, inoltre, un sistema di *segnalazione degli incidenti informatici*, con obblighi stringenti di notifica.

Le istituzioni finanziarie devono segnalare tempestivamente alle autorità competenti qualsiasi incidente rilevante, fornendo dettagli chiari sull'accaduto, sulle conseguenze e sulle misure adottate. Questa procedura di notifica consente una rapida *condivisione* delle informazioni con le autorità, che possono così aiutare a prevenire altri attacchi simili e offrire supporto, se necessario.

Di particolare interesse, e pregio, è la promozione della collaborazione e della condivisione delle informazioni tra le istituzioni finanziarie, incentivando così la costruzione di una rete di condivisione delle minacce ("threat intelligence") e delle migliori pratiche. Le banche e le assicurazioni dovrebbero scambiarsi informazioni utili sui rischi emergenti, sugli attacchi subiti e sulle misure di difesa, costruendo così una *conoscenza condivisa* per migliorare la sicurezza complessiva del settore.

Un ulteriore punto chiave, già si è visto nel corso di questo contributo, è la

*formazione continua* dei dipendenti in materia di sicurezza informatica e resilienza operativa. DORA richiede che le istituzioni finanziarie offrano programmi di formazione regolare, adattando i contenuti alle nuove minacce e alle migliori pratiche. Il personale deve essere costantemente aggiornato non solo su come prevenire le minacce ma, anche, su come reagire in modo appropriato in caso di incidente.

Le banche e le compagnie di assicurazione devono, infine, garantire una protezione rigorosa dei *dati personali e finanziari* dei clienti. DORA richiede l'implementazione di misure avanzate di sicurezza per la protezione e la gestione dei dati, assicurando che i dati sensibili siano protetti da accessi non autorizzati, perdite o alterazioni.

Nonostante gli sforzi compiuti, e l'avvento di DORA, il settore finanziario continua a confrontarsi con sfide significative.

L'adozione di nuove tecnologie come l'intelligenza artificiale e il *quantum computing* introduce ulteriori rischi, richiedendo un costante aggiornamento delle strategie di sicurezza. Inoltre, la crescente *interconnessione* tra istituzioni finanziarie e fornitori esterni amplia la superficie di attacco, rendendo necessaria una gestione attenta della sicurezza lungo l'intera catena di fornitura.

La sicurezza informatica nel settore bancario e finanziario è caratterizzata, in conclusione, da un panorama in continua evoluzione, con minacce sempre più sofisticate e con una crescente pressione normativa, a volte criticata [7].

Le istituzioni finanziarie dovrebbero, pertanto, adottare un approccio proattivo, investendo in tecnologie avanzate, formazione del personale e collaborazioni strategiche per proteggere al meglio i propri sistemi e i dati dei clienti.

[7] Ci si riferisce, in particolare, a frequenti accuse che provengono dal mondo imprenditoriale e politico e che sostengono che un quadro normativo così articolato possa in qualche modo *soffocare* la spinta innovativa tecnologica in Europa.

Sezione II

# *I servizi finanziari tra Distributed Ledger Technology (DLT) e intelligenza artificiale*

# Dalla dematerializzazione al DLT Pilot: verso il decentramento della gestione titoli

Gian Luca Greco

SOMMARIO: 1. *Distributed Ledger Technology* e finanza: un matrimonio che "s'ha da fare". – 2. Il regolamento europeo 858/2022: "Avanti, DLT, con giudizio, se puoi". – 3. DLT, finanza e *sandbox*: un esperimento regolatorio all'insegna della proporzionalità.

## 1. *Distributed Ledger Technology* e finanza: un matrimonio che "s'ha da fare"

Nella loro funzione di strumenti per il trasferimento di fondi tra soggetti in *surplus* (generalmente, famiglie) a soggetti in *deficit* (principalmente imprese e Stato), gli strumenti finanziari sono tanto più efficienti – a parità di altre condizioni – quanto più la loro circolazione è rapida, sicura e economica.

Una tappa fondamentale in questa direzione è rappresentata dal passaggio da una forma di documentazione e movimentazione dei diritti cartacea ed individuale (incorporazione), tipica dei titoli di credito, ad una di registrazione e movimentazione contabile (e telematica), massificata ed accentrata, intermediata da soggetti specializzati [1].

Tale processo, detto comunemente "dematerializzazione", ebbe inizio in Italia a metà degli anni Ottanta, quando una società per azioni, Monte Titoli, fu costituita d'imperio (con legge n. 289/1986), su impulso di Banca d'Italia, per rendersi disponibile a ricevere in deposito i certificati rappresentativi dei titoli, registrando sui conti di banche, agenti di cambio e società emittenti (quest'ultimi per i soli titoli propri) quantità e specie dei titoli di loro proprietà o depositati dai propri clienti e ivi subdepositati.

Poco più di dieci anni dopo, con l'emanazione del d.lgs. n. 58/1998, Monte Titoli perde l'originaria posizione di monopolio e viene qualificata come la prima (e al tempo l'unica) tra le "società di gestione accentrata degli strumenti finanziari", soggetti autorizzati da Consob e vigilati congiuntamente da Banca d'Italia.

---

[1] M. CIAN, *La dematerializzazione degli strumenti finanziari*, in *Banca, borsa, tit. cred.*, 2007, pp. 641 e 655 ss.

Pochi mesi più tardi, in occasione dell'emanazione della normativa di adeguamento all'euro (d.lgs. n. 213/1998), viene previsto che la gran parte degli strumenti finanziari debbano essere gestiti in via accentrata in regime di dematerializzazione obbligatoria.

Quello che alla fine degli anni Novanta fu considerato, a ragione, un vero cambiamento epocale apportato dall'utilizzo pervasivo di tecniche di custodia e amministrazione a contenuto contabile e telematico [2], oggi potrebbe dirsi superato in ragione dello sviluppo di tecnologie innovative, quali la tecnologia a registro distribuito (*Distributed Ledger Technology* o DLT) [3].

Inizialmente adottata per le c.d. criptovalute (non può non richiamarsi, a tal proposito, la *blockchain permissionless* dei *bitcoin*) [4], la DLT è stata oggetto di limitate applicazioni nel settore finanziario tradizionale, dapprima nel credito documentario (*trade finance*), ove si riscontrano significative e storiche difficoltà pratiche nella gestione dei documenti contrattuali, che ne rallentano il funzionamento e ne aggravano i costi [5]. Più di recente, la tecnologia a registro distribuito è stata utilizzata anche nel contesto dell'emissione di prestiti obbligazionari [6] e della cartolarizzazione di *Non-Performing Loans* [7]. A livello interbancario, la DLT è stata

---

[2] Si consenta sul punto il rinvio a G.L. GRECO, *La metamorfosi del deposito titoli, tra dematerializzazione e direttive Mifid*, in *Dir. banc.*, 2, 2021, p. 217.

[3] Come si legge all'art. 1, n. 1), 2) 3) e 4), del Reg. (UE) 2022/858 del 30 maggio 2022, la DLT può essere definita come «una tecnologia che consente il funzionamento e l'uso dei registri distribuiti», ognuno dei quali è, a sua volta, un «archivio di informazioni in cui sono registrate le operazioni e che è condiviso da una serie di nodi di rete DLT ed è sincronizzato tra di essi, mediante l'utilizzo di un meccanismo di consenso». Il nodo di rete DLT è «un dispositivo o un'applicazione informatica che è parte di una rete e che detiene una copia completa o parziale delle registrazioni di tutte le operazioni eseguite tramite il registro distribuito» e il meccanismo di consenso rappresenta «le regole e le procedure con cui si raggiunge un accordo, tra i nodi di rete DLT, sulla convalida di un'operazione».

[4] Si è soliti distinguere tra protocolli DLT "pubblici" (o *permissionless*) a gestione interamente decentrata su internet, attraverso l'azione di soggetti specializzati detti *miners*, come appunto nella *blockchain* di *bitcoin*, e protocolli DLT "privati" (o *permissioned*), ove i "nodi" sono abilitati dal gestore del protocollo informatico (questa classe di DLT può operare anche senza i *miners*).

[5] La prima operazione reale basata su DLT è stata effettuata da Barclays nel 2016. Si trattava di una lettera di credito emessa a fronte di esportazione di partite di formaggio e burro da Israele a Isole Seychelles. La blockchain è stata utilizzata per la consegna della documentazione alle parti coinvolte nella transazione. Gli effetti positivi sono stati riscontrati nella trasparenza e velocità del processo, i cui tempi sono stati ridotti da 7/10 gg. a 4 ore. Analoghe operazioni sono state poi poste in essere da Deutsche Bank, nel 2017, e Unicredit, nel 2018.

[6] Si ha notizia che la DLT sia stata utilizzata per la negoziazione delle condizioni del prestito in un'operazione strutturata da Banco Bilbao Vizcaya con riferimento all'emissione di Bund tedeschi per 220 milioni di euro.

[7] Nel 2021 è stata sviluppata in Italia (da SIA e WizKey) una piattaforma basata su DLT che consente di gestire l'intero processo di negoziazione e cessione dei crediti, anche nell'ambito di operazioni di cartolarizzazione di NPL (*Non-Performing Loans*). Ciascun portafoglio di crediti presente sulla piattaforma è dotato di una propria *data room* permanente in cui sono resi disponibili la storia, i documenti e tutte le risultanze delle attività di due diligence; la tecnologia DLT consente di rendere immodificabili i dati e le informazioni, evitando i rischi di asimmetria informativa a tutela delle parti coinvolte nel processo. Tramite l'utilizzo di *smart contracts*, il credito

poi adottata per la riconciliazione delle partite di debito/credito tra le banche [8].

Anche in ambito eurounionale è da tempo aperta la discussione sui possibili impatti dell'utilizzo della DLT nel settore finanziario [9]. Dal lato dei possibili benefici si suggerisce la semplificazione dei processi, la riduzione dei costi di intermediazione, la sicurezza delle transazioni associata al contenimento dei relativi costi e il miglioramento della trasparenza; d'altro canto, si è anche sostenuto che l'adozione di tale tecnologia potrebbe comportare perturbazioni nell'intermediazione e nell'infrastruttura finanziaria, minacce alla tutela dei dati personali, un possibile utilizzo per evasione ed elusione fiscale, riciclaggio del denaro/finanziamento del terrorismo nonché, soprattutto nelle DLT *permissionless*, la violazione dei meccanismi tecnologici che effettuano la convalida, la salvaguardia e la conservazione delle transazioni e accelerano la compensazione e il regolamento di alcune operazioni in titoli [10].

In sede istituzionale pare emergere dunque un particolare interesse all'applicazione della DLT nella gestione, compensazione e regolamento delle operazioni in titoli, in quanto aspetti cruciali del funzionamento del sistema finanziario [11]. Anche la dottrina da tempo auspica l'utilizzo della DLT in detto contesto, per i potenziali guadagni in termini di efficienza che potrebbero scaturire dall'applicazione di tale tecnologia, in particolare grazie alla semplificazione del regolamento e delle relative attività di riconciliazione [12].

---

viene digitalizzato sull'infrastruttura di SIA consentendo a tutti gli attori della filiera di strutturare aste competitive private e pubbliche e trasferire portafogli di crediti.

[8] Assieme ad un gruppo di 18 banche italiane, l'ABI ha promosso il progetto «Spunta», ossia l'istituzione di una DLT *permissioned* per la riconciliazione delle partite di debito/credito tra le banche. La rendicontazione dei conti reciproci delle banche è un processo di nicchia, che si basa tradizionalmente sulla logica della partita doppia. Si parla, in gergo, di spunta, in quanto una banca comunica all'altra le proprie scritture ed esse devono essere accoppiate, «spuntate» appunto. Il processo di riconciliazione delle partite bancarie è tradizionalmente regolato da un Accordo interbancario del 1978, sotto l'egida dell'ABI.

[9] Per una breve ma interessante rassegna cfr. EBA, *Uses of DLT in the EU banking and payments sector: banking and payments sector: EBA monitoring and convergence work*, 24 April 2024, in https://www.eba.europa.eu.

[10] Sul punto cfr. PARLAMENTO EUROPEO, *Blockchain e tecnologie di registro distribuito: la risoluzione del Parlamento europeo*, Risoluzione, 3 ottobre 2018.

[11] In argomento cfr. BANK FOR INTERNATIONAL SETTLEMENTS (BIS), *Distributed ledger technology in payment, clearing and settlement*, February 2017.

[12] In argomento si vedano: A. PINNA, W. RUTTENBERG, *Distributed ledger technologies in securities post-trading*, ECB Occasional Paper 172, April 2016; R. PRIEM, *Distributed ledger technology for securities clearing and settlement: benefits, risks, and regulatory implications*, in *Financial Innovation*, 6:11, 2020; M. BAPTISTE, *The use of blockchain in clearing and settlement*, Neoma Business School, Paris**,** 2017; J. CAYTAS, *Developing Blockchain Real-Time Clearing and Settlement in the EU, U.S., and Globally*, in *Columbia Journal of European Law: Preliminary Reference*, 2016. E. MICHELER, L. VON DER HEYDE, *Holding, Clearing and Settling Securities Through Blockchain Technology Creating an Efficient System by Empowering Asset Owners*, 2016; J. LEE, *Distributed ledger technologies (blockchain) in capital markets: risk and governance*, 2018; G. PETERS, E. PANAY, *Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money*, 2015, tutti in *SSRN*.

Non può sorprendere dunque che proprio alle infrastrutture del mercato finanziario sia dedicata la prima iniziativa legislativa europea con la quale si regolamenta l'utilizzo della tecnologica a registro distribuito.

## 2. Il regolamento europeo 858/2022: "Avanti, DLT, con giudizio, se puoi"

Il regolamento (UE) 858/2022 (c.d. DLT Pilot) introduce appunto un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito (DLT), modificando la dir. 2014/65/UE (MIFID II) e il reg. (UE) 600/2014 (MIFIR) sui mercati finanziari nonché il reg. (UE) 909/2014 sui depositari centrali di titoli (CSDR), per consentire a tali infrastrutture di essere temporaneamente esentate da alcuni requisiti specifici previsti dalla normativa sopra richiamata, che altrimenti potrebbero impedire agli operatori di sviluppare soluzioni innovative basate su tecnologie trasformative, senza indebolire i requisiti o le garanzie esistenti applicati alle infrastrutture di mercato tradizionali [13].

Circa l'ambito di applicazione del DLT Pilot, l'ammissione alla negoziazione o alla registrazione in un'infrastruttura di mercato DLT è concessa: a) per le sole azioni il cui emittente ha una capitalizzazione di mercato inferiore a 500 milioni di euro; b) per obbligazioni, altre forme di debito cartolarizzato, comprese le ricevute di deposito, o strumenti del mercato monetario, con un'entità di emissione inferiore a 1 miliardo di euro; c) per quote di organismi di investimento collettivo il cui valore di mercato delle attività gestite è inferiore a 500 milioni di euro. In ogni caso, il valore di mercato aggregato di tutti gli strumenti finanziari DLT non deve superare i 6 miliardi di euro [14].

Sul piano soggettivo, il DLT disciplina le infrastrutture di mercato attive nella negoziazione su base multilaterale e nel regolamento delle transazioni su strumenti finanziari emessi, registrati, trasferiti e stoccati mediante la tecnologia a registro distribuito (ossia, gli strumenti finanziari DLT). Si tratta dei sistemi mul-

---

[13] Reg. (UE) 2022/858 del 30 maggio 2022, considerando 1 e 6. In dottrina si vedano: R. PRIEM, *A European distributed ledger technology pilot regime for market infrastructures: finding a balance between innovation, investor protection and financial stability*, in *Journal of Financial Regulation and Compliance*, Vol. 30, No. 3, 2022, pp. 371-390; D.A. ZETZSCHE, J. WOXHOLTH, *The DLT sandbox under the Pilot-Regulation*, in *Capital Markets Law Journal*, 2022, Vol. 17, No. 2, pp. 212-236; F. ANNUNZIATA, A.C. CHISARI, P.A. AMENDOLA, *DLT-Based Trading Venues and EU Capital Markets Legislation: State of the Art and Perspectives Under the DLT Pilot Regime*, in *The Italian Law Journal*, Vol. 9, 2023, pp. 141-160; F. BASSAN, *Digital Platforms and Blockchains: The Age of Participatory Regulation*, in *Business Law Review*, 34, No. 7, 2023, pp. 1103-1132; P. MAUME, F. KESPER, *The EU DLT Pilot Regime for Digital Assets*, in *European Company Law Journal*, 20, No. 6, 2023, pp. 118-126.

[14] DLT Pilot, art. 3. Nel caso in cui il valore di mercato aggregato di tutti gli strumenti finanziari DLT ammessi alla negoziazione su un'infrastruttura di mercato DLT o registrati in un'infrastruttura di mercato DLT raggiunga i 9 miliardi di euro, il gestore dell'infrastruttura di mercato DLT deve attivare una strategia per la riduzione dell'attività di una determinata infrastruttura di mercato DLT o per la transizione o la cessazione dell'attività di una determinata infrastruttura di mercato DLT (la c.d. "strategia di transizione").

tilaterali di negoziazione DLT (MTF DLT), che ammettono alla negoziazione solo strumenti finanziari DTL; dei sistemi di regolamento DLT (SS DLT), che regolano operazioni in strumenti finanziari DLT e che permettano la registrazione iniziale degli strumenti finanziari DLT o consentano la prestazione di servizi di custodia in relazione a strumenti finanziari DLT; e, infine, dei sistemi di negoziazione e regolamento DLT (TSS DLT), che combinano i servizi prestati dalle infrastrutture precedentemente ricordate.

Il DLT Pilot prevede un regime differenziato di minor rigore per i sistemi di regolamento titoli e i sistemi multilaterali di negoziazione operanti su criptoattività che rientrano nella definizione di strumenti finanziari e sono emesse, trasferite e conservate con tecnologia a registro distribuito nonché la possibilità di istituire infrastrutture di mercato DLT che combinino i suddetti servizi. In osservanza del principio di proporzionalità e della necessità di assicurare, a tendere, pari condizioni concorrenziali con gli operatori tradizionali, gli "sconti" sui requisiti organizzativi e di autorizzazione per le infrastrutture operanti nel regime pilota sono temporanei, compensati da requisiti supplementari specifici riguardo la tecnologia utilizzata e circoscritti all'operatività nel regime pilota, che prevede importanti limitazioni sulla tipologia e sul valore di mercato aggregato degli strumenti finanziari ammessi.

In particolare, gli operatori di una infrastruttura di mercato DLT devono, tra l'altro: a) stabilire regole di funzionamento della loro tecnologia, piani aziendali chiari e dettagliati e documentazione scritta a disposizione del pubblico, aggiornata e dettagliata; b) fornire ai membri, ai partecipanti, agli emittenti e ai clienti informazioni chiare e inequivocabili; c) garantire dispositivi informatici e cibernetici trasparenti, disponibili, affidabili e sicuri; d) disporre di procedure specifiche di gestione del rischio operativo; e) separare i fondi, le garanzie reali e gli strumenti finanziari DLT in custodia, assumendosi la responsabilità di eventuali perdite; f) calcolare mensilmente il valore medio delle proprie partecipazioni e trasmettere i dati all'autorità nazionale competente, che ha il potere di fissare limiti inferiori a quelli previsti dal regolamento; g) operare in stretta collaborazione con le autorità competenti designate dagli Stati membri dell'Unione e presentare una relazione ogni sei mesi [15].

L'ordinamento italiano è stato adeguato al DLT Pilot con il d.l. n. 25/2023, convertito con legge n. 52/2023, di seguito anche "Decreto Fintech" [16].

In primo luogo, il Decreto Fintech si preoccupa di definire gli aspetti privatistici dell'emissione e della circolazione degli strumenti finanziari DLT, richiamando e adattando le pertinenti disposizioni del TUF [17], e di individuare Banca

[15] DLT Pilot, artt. 3, 7 e 11.

[16] D.l. 17 marzo 2023, n. 25, convertito con legge 10 maggio 2023, n. 52, recante disposizioni urgenti in materia di emissioni e circolazione di determinati strumenti finanziari in forma digitale e di semplificazione della sperimentazione FinTech.

[17] Si vedano in particolare gli artt. 3-10 del Decreto Fintech, ove si individuano le caratteristiche dei registri per la circolazione digitale, gli effetti della scritturazione su di essi, le modalità di costituzione dei vincoli sui titoli e della tenuta dei libri sociali, le eccezioni opponibili dall'emittente, i titolari dei diritti di intervento in assemblea, dell'esercizio del voto, dei diritti patrimoniali.

d'Italia e Consob come autorità competenti per l'autorizzazione delle infrastrutture di mercato DLT in Italia [18], chiarendone i rispettivi poteri [19].

D'altro canto, il legislatore nazionale coglie l'occasione per introdurre, andando anche oltre l'ambito del DLT Pilot, una disciplina complessiva degli strumenti finanziari DLT, introducendo la figura del "responsabile del registro", al quale è riservata la tenuta dei registri a tecnologica distribuita su cui sono emessi strumenti finanziari digitali non scritturati presso un TSS DLT o un SS DLT, dunque negoziabili su base bilaterale *over the counter* [20].

Senza soffermarsi su tutti i profili di dettaglio del DLT Pilot e del Decreto Fintech, occorre quanto meno osservare che, pur dichiaratamente ispirandosi ai principi di neutralità tecnologica, nella configurazione del regime pilota il regolatore europeo ha provveduto a bilanciare l'interesse all'innovazione imprenditoriale proprio degli operatori con i tradizionali interessi pubblici immanenti del mercato finanziario [21] e i diritti fondamentali rappresentati dalla tutela della vita privata e dei dati personali.

In tale prospettiva, nell'ambito delle possibili opzioni già disponibili della tecnologia a registro distribuito il legislatore ha implicitamente selezionato per il regime pilota la sola DLT *permissioned* o "privata", ove i nodi sono diversamente abilitati con riguardo alla validazione, ai controlli e all'aggiornamento del registro condiviso. I requisiti supplementari previsti per le infrastrutture di mercato DLT includono infatti una serie di obblighi posti a carico dei gestori in merito, tra l'altro, alla trasparenza delle regole della DLT, alla disciplina dei diritti, dei requisiti, delle responsabilità e degli obblighi di gestori e partecipanti, delle modalità di risoluzione delle controversie, alla sicurezza cibernetica, alla strategia di transizione o alla eventuale cessazione delle attività [22]. Tali requisiti, volti a garantire la tutela degli investitori, l'integrità del mercato e la stabilità finanziaria, sembrano sostanzialmente incompatibili con DLT *permissionless* o "aperte" (come la nota *blockchain*), ove il consenso sulla validità delle registrazioni si for-

---

[18] L'art. 29 del Decreto Fintech prevede che la Banca d'Italia abbia la competenza principale per autorizzare le infrastrutture operanti all'ingrosso di titoli di Stato, mentre in tutti gli altri casi spetta alla Consob rilasciare l'autorizzazione, d'intesa con la Banca d'Italia. Per quel che concerne la vigilanza, il Decreto Fintech replica le attribuzioni, i poteri e le finalità rispettivamente assegnati alle predette autorità nella parte III del TUF.

[19] Ai sensi dell'art. 27 del Decreto Fintech, Consob esercita la vigilanza con riguardo alla trasparenza e alla tutela degli investitori, mentre Banca d'Italia è competente per quanto riguarda la stabilità e il contenimento del rischio degli intermediari vigilati e dei responsabili dei registri per la circolazione digitale di maggiore rilevanza.

[20] In questo senso P. CIPOLLONE, *Audizione sul disegno di legge n. 605 di conversione in legge del decreto-legge 17 marzo 2023, n. 25, recante disposizioni urgenti in materia di emissioni e circolazione di determinati strumenti finanziari in forma digitale e di semplificazione della sperimentazione FinTech*, Banca d'Italia, Roma, 4 aprile 2023, p. 8.

[21] DLT Pilot, considerando 10, ove si accenna alla necessità di difendere «i valori di trasparenza, equità, stabilità, tutela degli investitori, rendicontabilità e integrità del mercato».

[22] DLT Pilot, art. 7.

ma con algoritmi di tipo *proof of work* o *proof of stake*[23] e nelle quali è tecnicamente impossibile individuare soggetti responsabili della correttezza delle transazioni e della sicurezza e integrità dell'infrastruttura, facendosi esclusivo affidamento sulla "robustezza" della tecnologia crittografica utilizzata[24].

Come suggerito da alcuni studi[25] ed esperienze internazionali[26], la DLT *permissioned* – che vede l'attribuzione a specifici nodi di funzioni delicate ed essenziali, come quelle di validazione e di amministratore di sistema – parrebbe avere caratteristiche idonee a soddisfare gli attuali profili funzionali e istituzionali dei sistemi di pagamento, *clearing* e *settlement*. La DLT privata consente infatti di preservare il ruolo istituzionale di alcuni nodi, affidando agli stessi funzioni esclusive, sovente riservate per legge a soggetti autorizzati in via amministrativa. Si pensi, in Italia, al ruolo di Monte Titoli nella gestione accentrata e della Cassa di Compensazione e Garanzia come controparte centrale[27].

Tale esigenza assume ulteriore rilievo nell'ambito del DLT Pilot, che introduce la possibilità che un'infrastruttura di mercato (il c.d. "DLT *trading and settlement system*" o DLT TSS) presti al contempo servizi di regolamento e servizi di negoziazione su strumenti finanziari, così concentrando in un'unica piattaforma fasi diverse del ciclo di vita di un'attività finanziaria[28].

Le caratteristiche peculiari della DLT consentono infatti alle sedi di esecuzione (quali gli MTF, i sistemi multilaterali di negoziazione) di emanciparsi dai depositari centrali al fine del trasferimento definitivo degli strumenti finanziari

---

[23] In argomento si rinvia, per tutti, a M. MARCHESI, *Blockchain pubbliche e permissioned: una questione di fiducia*, in *Federalismi*, 2, 2021, 140 ss.; A. VISCONTI, A. FRISONI, *Consenso e* mining *nella blockchain*, in L. AMMANNATI, A. CANEPA, *Tech Law: il diritto di fronte alle nuove tecnologie*, Napoli, 2021, p. 188 ss.

[24] Sul punto si consenta il rinvio a G.L. GRECO, *Tecnologia a registro distribuito e infrastrutture dei mercati finanziari: più riforma che rivoluzione*, in L. AMMANNATI, A. CANEPA, *Tech Law*, cit., p. 194 s.

[25] BANK FOR INTERNATIONAL SETTLEMENTS (BIS), *Distributed ledger technology in payment, clearing and settlement*, cit., p. 7; COMMITTEE ON CAPITAL MARKETS REGULATION, *Blockchain and Securities Clearing and Settlement*, April 2019, 7 ss.; M. MARCHESI, *Blockchain pubbliche*, cit., p. 150.

[26] Nell'ottobre 2019 la SEC ha autorizzato una società (la Paxos Trust Company, LLC) a sperimentare l'utilizzo di una piattaforma di *settlement* (c.d. Paxos Settlement Service o PSS), basato su una DLT "privata" e *permissioned*. La SEC ha esentato temporaneamente Paxos dall'obbligo di autorizzazione come clearing agency (*no-action relief*), limitando l'attività della PSS in ordine al numero dei partecipanti (7) e al numero delle operazioni giornaliere (300). Nella piattaforma i partecipanti al sistema sono tenuti a detenere strumenti finanziari e denaro su conti aperti presso la PSS. A deposito avvenuto, Paxos crea rappresentazioni digitali degli strumenti finanziari e del denaro depositati, che vengono utilizzati per adempiere agli obblighi di consegna previsti dal regolamento. Sono previsti obblighi di marginazione giornalieri a presidio del rischio di regolamento.

[27] G.L. GRECO, *Tecnologia a registro distribuito*, cit., p. 205.

[28] P. CIPOLLONE, *Audizione*, cit., p. 5, che sottolinea altresì come l'introduzione del DLT TSS superi la necessità di separare tali fasi in diversi contesti tecnologici, amministrativi e normativi, «grazie al potenziale intrinseco dei registri distribuiti, che sono in grado di garantire strutturalmente la certezza, l'accessibilità e l'immutabilità delle informazioni e dei dati connessi con le operazioni effettuate dai partecipanti alla rete».

negoziati, dando una spinta fondamentale all'auspicata possibilità di tokenizzare il titolo, registrandolo direttamente sulla DLT [29].

D'altro canto, l'accesso al regime pilota non è limitato agli operatori esistenti, in quanto nuovi operatori potrebbero prestare attività quali infrastrutture di mercato DLT sulla base di uno specifico regime autorizzativo in parziale esenzione dai requisiti ordinari previsti da MIFID II e CSDR [30]. È evidente però che non venga mai posto in discussione il fatto che le attività di regolamento titoli, ad esempio, restino riservate a soggetti autorizzati, pur temporaneamente e fruendo di "sconti" regolatori [31].

## 3. DLT, finanza e *sandbox*: un esperimento regolatorio all'insegna della proporzionalità

Il DLT Pilot rappresenta l'esempio recente più significativo di *regulatory sandbox* previsto nella legislazione europea.

Il tema della qualità della regolazione è entrato prepotentemente nell'agenda europea nei primi anni duemila e oggi copre tutto il ciclo politico dell'Unione Europea: programmazione, proposta della Commissione, approvazione da parte del Consiglio e del Parlamento; attuazione, valutazione, revisione della legislazione [32].

Nelle valutazioni d'impatto effettuate con riguardo alle azioni dell'Unione Europea – che dal 2015 sono riviste a campione da un comitato indipendente che si avvale anche di esperti esterni, il Regulatory Scrutiny Board – viene tra l'altro esaminata la corretta applicazione dei principi di sussidiarietà e di proporzionalità [33].

Tra gli approcci più recenti utilizzati in ambito UE per raggiungere gli obiettivi della *better regulation* merita attenzione lo strumento della *regulatory sandbox*, grazie alla quale i regolatori intendono affrontare le sfide poste dalla tra-

---

[29] Così ancora P. CIPOLLONE, *Audizione*, cit., p. 7.

[30] DLT Pilot, considerando 11, ove si precisa che, in tali casi, «l'autorità competente non dovrebbe valutare se tale soggetto soddisfi i requisiti del regolamento (UE) n. 909/2014 o della direttiva 2014/65/UE per i quali è stata richiesta un'esenzione a norma del presente regolamento».

[31] DLT Pilot, considerando 18. Sul punto si consenta di rinviare a G.L. GRECO, *La metamorfosi del deposito titoli*, cit., p. 227 s., ove si è osservato che nel passaggio alla dematerializzazione forte risulta fortemente ridotto, se non ormai residuale, il perimetro delle attività di custodia e amministrazione titoli non riservato a intermediari vigilati, in armonia con quanto previsto per le attività di regolamento titoli.

[32] Gli interventi della Commissione sulla *better regulation* sono ormai numerosissimi. Ci limitiamo qui a citare alcuni dei più recenti e importanti, quali le *Better Regulation Guidelines* del 3 novembre 2021(SWD (2021) 305 final) e il *Better Regulation Toolbox*, anch'esso del 2021, che hanno lo scopo di fornire un concreto aiuto alle istituzioni europee quando predispongono nuove iniziative legislative o revisionano e rivalutano i provvedimenti esistenti.

[33] Si vedano, in proposito, gli *Annual Report* pubblicati dal Regulatory Scrutiny Board, ove sono riportate le attività di carattere generale svolte dal Comitato, anche sul piano della consulenza e comunicazione istituzionale, e le valutazioni d'impatto della normativa effettuate nel periodo di riferimento.

sformazione tecnologica e l'affermarsi di nuovi prodotti, servizi e modelli di *business*[34]. La *regulatory sandbox* può essere descritta, in senso ampio, come uno schema organizzato su base individuale, a regole "affievolite", che consente alle imprese di sperimentare prodotti e servizi innovativi in un ambiente reale controllato, nell'ambito di un piano specifico sviluppato e monitorato dall'autorità competente, salvaguardando sicurezza e protezione dei consumatori[35]. La scelta di istituire una *regulatory sandbox* in un determinato ambito deve rispondere al criterio di proporzionalità, per cui il regolatore dovrà tenere conto di vari aspetti – dal grado di innovazione di mercato, alla flessibilità delle regole applicabili, ai criteri di accesso, al *design*, alle risorse necessarie – confrontando tale opzione con le altre astrattamente disponibili (quale ad esempio l'emanazione di linee guida, con le quali si riducono le incertezze regolatorie senza intervenire con esenzioni temporanee o sperimentazioni)[36].

In linea con l'approccio *regulatory sandbox* è previsto che i risultati del regime pilota DLT siano relazionati dall'ESMA alla Commissione entro marzo 2026, che a sua volta predisporrà un'analisi costi/benefici a favore del Parlamento europeo e del Consiglio per decidere se prorogare, modificare, sopprimere o rendere permanente il regime pilota, mediante adeguate modifiche alla legislazione sui servizi finanziari[37].

Il regolamento DLT Pilot costituisce una significativa applicazione del principio di proporzionalità nel processo di costruzione di una regolazione che miri a coniugare le potenzialità dello sviluppo tecnologico con gli imprescindibili in-

---

[34] La dottrina che si è occupata delle *regulatory sandboxes* è ormai ampia. Tra i molti, si vedano L. AMMANNATI, *Regolare o non regolare, ovvero l'economia digitale tra 'Scilla e Cariddi'*, in AA.VV., *I servizi pubblici. Vecchi problemi e nuove regole*, Giappichelli, Torino, 2018, p. 101 ss.; A. ATTREY, M. LESHER, C. LOMAX, *The role of sandboxes in promoting flexibility and innovation in the digital age*, OECD Going Digital Toolkit Policy Note n. 2, 2020; B.R. KNIGHT, T.E. MITCHELL, *The Sandbox Paradox: Balancing the Need to Facilitate Innovation with the Risk of Regulatory Privilege*, Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, March 2020; V. LEMMA, *La regolazione del fintech tra 'same supervision' e 'sandbox'*, in M. PASSALACQUA (a cura di), *Diritti e mercati nella transizione economica e digitale*, Wolters Kluwer, Milano, 2021, p. 385 ss.; M. LESHER, *Bringing new digitally enabled products and services to market: Sandboxes and the role of policy experimentation*, VoxEU, CEPR, 2020; M. MACCHIAVELLO, *FinTech. Problematiche e spunti per una regolazione ottimale*, in *Mercato Concorrenza Regole*, 3, 2019, p. 435 ss.; S. RANCHORDAS, *Experimental regulations for AI: sandboxes for morals and mores*, in *Morals and Machines*, 2021; D.A. ZETZSCHE, J. BUCKLEY, D. ARNER, R. BARBERIS, *Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation*, European Banking Institute Working Paper Series, No. 11, 2017.

[35] La sperimentazione Fintech è stata disciplinata nel nostro paese con il d.l. 30 aprile 2019, n. 34, convertito in legge 28 giugno 2019, n. 58, e recentemente rivista, nell'ottica della semplificazione, con il d.l. 17 marzo 2023, n. 25, grazie al quale è stato chiarito che lo svolgimento temporaneo di attività che rientrano nella nozione di servizi e attività d'investimento nell'ambito della sperimentazione non implica l'esercizio di attività riservate e che spetta alle autorità di vigilanza di settore stabilire i limiti qualitativi e quantitativi dell'attività di partecipazione alla sperimentazione.

[36] In argomento si vedano anche EUROPEAN SUPERVISORY AUTHORITIES JOINT COMMITTEE, *FinTech: Regulatory sandboxes and innovation hubs*, Report, 2019; EUROPEAN COMMISSION, *'Better regulation' toolbox*, 2021, p. 597 ss.

[37] DLT Pilot, art. 14.

teressi pubblici connaturati al sistema finanziario e le esigenze di tutela dei diritti fondamentali degli investitori.

I "paletti" posti dal legislatore sul piano amministrativo, tecnico e organizzativo portano a escludere un approccio *one size fits all*, ossia l'idea che qualunque DLT, soprattutto "aperta", possa essere utilizzata per la gestione dei sistemi di pagamento, *clearing* e *settlement*[38]. D'altra parte, il rispetto del principio di neutralità tecnologica traspare nella rinuncia a imporre un modello "legale" di registro distribuito, delegando alle autorità di vigilanza, nel dialogo con gli operatori, il compito di individuare un equilibrio sostenibile tra vantaggi e rischi della tecnologia applicata.

Così pare essersi orientato il legislatore italiano, prevedendo che la Consob, «tenuto conto del principio di proporzionalità», possa prevedere disposizioni attuative con riguardo alla strategia di transizione e agli obblighi del responsabile del registro a tecnologia distribuita[39].

Nel dare attuazione alla delega, l'Autorità ha previsto che nella relazione tecnica illustrativa allegata all'istanza di iscrizione nell'apposito elenco dei registri per la circolazione digitale, la società richiedente descriva le regole di funzionamento e le modalità di attribuzione dei permessi per le principali funzioni svolte dalla DLT, specificando quelle relative all'esecuzione dei protocolli di consenso e chiarendo, a tal proposito, se la DLT è *permissionless*, *permissioned* o ibrida (ossia tale per cui alcune fasi dell'operatività sono *permissionless* e altre *permissioned*)[40].

Se in astratto, dunque, non vi sono preclusioni all'uso di una DLT *permissionless*, si è dell'avviso che, in concreto, allo stato dell'arte, tale tecnologia non consenta di assicurare la piena conformità ai requisiti tecnici previsti dal Decreto Fintech, con riferimento a: l'integrità, l'autenticità, la non ripudiabilità, la non duplicabilità e la validità delle scritturazioni; l'identificabilità dei soggetti a favore dei quali sono effettuate le registrazioni; la correttezza, la completezza e l'aggiornamento continuo delle evidenze relative alle informazioni sull'emissione; l'integrità e la sicurezza del sistema; la continuità operativa e il ripristino dell'attività[41].

La Consob non ha infatti fatto ricorso al principio di proporzionalità prevedendo una disapplicazione, totale o parziale, dei suddetti requisiti tecnici, considerandoli, giustamente, un presupposto indispensabile per la tutela dei rilevanti interessi pubblici sottesi alla circolazione digitale dei titoli.

Ciò posto, non può invece escludersi che una DLT ibrida possa incontrare il favore dell'Autorità, nella misura in cui sia configurata attribuendo a specifici nodi le funzioni essenziali dell'infrastruttura, alla luce dei rischi rilevati circa le possibili compromissioni del corretto funzionamento della stessa.

---

[38] G.L. GRECO, *Tecnologia a registro distribuito*, cit., p. 208.

[39] Decreto Fintech, art. 28.

[40] CONSOB, *Regolamento sull'emissione e circolazione in forma digitale di strumenti finanziari*, Delibera n. 22923 del 6 dicembre 2023, art. 8 e all. 2.

[41] Decreto Fintech, artt. 4, 13 e 23; CONSOB, *Regolamento sull'emissione e circolazione in forma digitale di strumenti finanziari*, cit., all. 2.

# Criptovalute. Quadro regolamentare nazionale e prospettive future: il ruolo dell'Organismo degli Agenti in attività finanziaria e dei Mediatori creditizi (OAM)

Federico Luchetti, Francesco Ruggiero

SOMMARIO: 1. Introduzione. – 2. L'evoluzione normativa sulle criptovalute in Italia: il Decreto del Ministero dell'Economia e delle Finanze del 2022 e il ruolo dell'Organismo degli Agenti in attività finanziaria e dei Mediatori creditizi. – 3. Uno sguardo al mercato delle criptovalute in Italia. – 4. Il d.lgs. del 5 settembre 2024: le nuove regole e il regime transitorio. – 5. Conclusioni.

## 1. Introduzione

Le criptovalute sono emerse come risposta alle inefficienze e alle limitazioni dei sistemi finanziari tradizionali, per aumentare l'efficienza e la sicurezza delle transazioni finanziarie, rappresentando, quindi, una rivoluzione nel panorama finanziario globale, offrendo soluzioni innovative e adattabili alle numerose sfide dei sistemi tradizionali.

La capacità delle valute virtuali di eliminare intermediari, preservare la *privacy*, permettere transazioni rapide e globali, nonché incrementare il controllo individuale, ha catalizzato un interesse crescente e una loro adozione sempre più diffusa. Inoltre, la natura inclusiva degli *asset* digitali permette l'accesso ai servizi finanziari anche in nazioni sottosviluppate, mentre le tecnologie emergenti come la *blockchain* e gli *smart contract* potrebbero trasformare molti altri settori: in particolare la *blockchain* ha enormi potenzialità di applicazione, dalla tracciabilità della filiera alimentare, a quella della movimentazione delle merci, alla condivisione delle informazioni sanitarie nel pieno rispetto delle *privacy*, solo per fare qualche esempio. Quanto agli *smart contract* trovano la loro naturale collocazione in quelle attività dove un pagamento è collegato al verificarsi di una condizione: il campo assicurativo, solo per citarne uno.

Focalizzando tuttavia l'attenzione sulle valute virtuali, va subito segnalato

che tali valute si contraddistinguono non solo per i molteplici vantaggi offerti agli utilizzatori ma anche per gli elevati rischi associati alle non sempre adeguate misure di sicurezza adottate dagli *exchange* per proteggere i fondi dei propri clienti. Inoltre, l'utilizzo delle criptovalute ha sollevato anche preoccupazioni legate alla regolamentazione, all'uso illegale (come in alcune attività criminali), alla *privacy* e alla sicurezza delle transazioni che hanno portato, soprattutto negli ultimi anni, ad ampi dibattiti politici e all'implementazione di dettagliate regolamentazioni.

Con riferimento alla regolamentazione sulle criptovalute, l'introduzione del Regolamento MiCAR (*Markets in Crypto-Assets*) mira a mitigare questi rischi fornendo un quadro normativo armonizzato per le cripto-attività in tutta l'Unione Europea, aumentando la protezione per i consumatori e gli investitori, promuovendo un ambiente di mercato più sicuro e stabile. L'assenza di una disciplina unica in Europa avrebbe potuto facilitare l'uso delle criptovalute per attività come il riciclaggio di denaro proveniente da attività illecite e il finanziamento del terrorismo, a causa delle difficoltà nel tracciare le transazioni e nell'identificare gli utenti.

In attesa della completa applicazione del Regolamento MiCAR, che avverrà a dicembre 2025, al termine di un periodo di transizione che verrà in seguito illustrato, il quadro normativo risulta frammentato e differente nei singoli Paesi EU, passando dall'assenza di normativa nazionale, a forme di regolamentazione poco stringenti e volte ad informare gli utilizzatori sui rischi delle criptovalute e a imporre presidi *anti-money laundering* e *combating the financing of terrorism* (AML/CFT), sino al rilascio di licenze (o alla registrazione) dei soggetti che operano professionalmente nel mercato. In alcune giurisdizioni, queste attività sono vietate.

In Italia, il settore è stato regolamentato dal Decreto del Ministero dell'Economia e delle Finanze n. 40, del 13 gennaio 2022.

## 2. L'evoluzione normativa sulle criptovalute in Italia: il Decreto del Ministero dell'Economia e delle Finanze del 2022 e il ruolo dell'Organismo degli Agenti in attività finanziaria e dei Mediatori creditizi

Il settore delle criptovalute in Italia, prima dell'entrata in vigore del Decreto del Ministero dell'Economia e delle Finanze n. 40, del 13 gennaio 2022, risultava essere caratterizzato da tentativi interpretativi di inquadramento da parte della giurisprudenza: i principali interventi hanno riguardato l'utilizzo delle criptovalute, gli obblighi di adeguata verifica e gli adempimenti in materia di antiriciclaggio, la fiscalità e il settore bancario-finanziario.

Giova ricordare, con riferimento all'utilizzo delle criptovalute, l'avvertenza pubblicata da Banca d'Italia il 30 gennaio 2015 con la quale viene specificato che "*esse non rappresentano in forma digitale le comuni valute a corso legale (eu-*

*ro, dollaro, ecc.); non sono emesse o garantite da una banca centrale o da un'autorità pubblica e generalmente non sono regolamentate. Le valute virtuali non hanno corso legale e pertanto non devono per legge essere obbligatoriamente accettate per l'estinzione delle obbligazioni pecuniarie, ma possono essere utilizzate per acquistare beni o servizi solo se il venditore è disponibile ad accettarle*". Inoltre, viene indicato come "*in Italia, l'acquisto, l'utilizzo e l'accettazione in pagamento delle valute virtuali debbono allo stato ritenersi attività lecite; le parti sono libere di obbligarsi a corrispondere somme anche non espresse in valute aventi corso legale. Si richiama tuttavia l'attenzione sul fatto che le attività di emissione di valuta virtuale, conversione di moneta legale in valute virtuali e viceversa e gestione dei relativi schemi operativi potrebbero invece concretizzare, nell'ordinamento nazionale, la violazione di disposizioni normative, penalmente sanzionate, che riservano l'esercizio della relativa attività ai soli soggetti legittimati (artt. 130, 131 TUB per l'attività bancaria e l'attività di raccolta del risparmio; art. 131 ter TUB per la prestazione di servizi di pagamento; art. 166 TUF, per la prestazione di servizi di investimento)*".

Per quanto concerne gli ambiti di applicazione degli adempimenti in materia Antiriciclaggio, l'Italia, in attuazione prima della Quarta e poi della Quinta Direttiva Antiriciclaggio dell'Unione Europea (IV e V AMLD), ha implementato norme per contrastare il riciclaggio di denaro e il finanziamento del terrorismo nel settore delle criptovalute. In particolare, il d.lgs. 25 maggio 2017, n. 90, ha modificato l'art. 3, comma 5, del d.lgs. n. 231/2007 prevedendo tra i destinatari di tutti gli obblighi AML i prestatori di servizi relativi all'utilizzo di valuta virtuale, limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso. Il successivo d.lgs. n. 125/2019 ha poi esteso i suddetti obblighi anche a carico dei prestatori di servizio di portafoglio digitale, ampliando altresì la nozione di prestatori di servizi relativi all'utilizzo di valuta virtuale ai "servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute". Tali disposizioni sono entrate in vigore rispettivamente il 4 luglio 2017 ed il 10 novembre 2019.

Relativamente all'ambito fiscale delle criptovalute in Italia, occorre precisare che le valute virtuali non sono considerate come una vera e propria valuta fiat ai fini fiscali, ma piuttosto come redditi diversi di natura finanziaria rientranti tra "*le plusvalenze e gli altri proventi realizzati mediante rimborso o cessione a titolo oneroso, permuta o detenzione di cripto-attività, comunque denominate*" (*ex* art. 67, comma 1, lett. *c*-sexies del TUIR). Pertanto, la permuta tra cripto-attività non assume rilevanza fiscale, mentre il passaggio da valuta virtuale a valuta fiat, oppure l'utilizzo della valuta per acquistare beni o servizi assume rilevanza fiscale. Pertanto, eventuali guadagni derivanti dalla vendita o dallo scambio di criptovalute possono essere soggetti a tassazione come plusvalenze, a seconda delle circostanze specifiche dell'investitore; a tal fine, è stata prevista una soglia di esclusione da imposizione pari ad euro 2.000 per

anno d'imposta e l'imposta sostitutiva è stabilita nella misura del 26%. Tale regime è stato modificato con la legge di Bilancio 2025 che ha innalzato a regime, a partire dal 2026, l'aliquota al 33% escludendo la soglia di non imponibilità di 2.000 euro. Tale esclusione vale anche per il 2025, anno per il quale è stata però confermata l'aliquota al 26%. La tassazione avviene tramite modello Redditi PF nell'apposito quarto RT, sezione II-B "Plusvalenze derivanti dalla cessione di cripto-attività".

Infine, le banche e le altre istituzioni finanziarie che operano in Italia devono seguire rigorose normative in relazione alle criptovalute, soprattutto per quanto riguarda il monitoraggio e la segnalazione delle transazioni. In linea generale, merita ricordare che la Banca d'Italia è intervenuta, in data 15 giugno 2022, con una propria Comunicazione in materia di tecnologie decentralizzate nella finanza e cripto-attività, con la quale viene richiamata *l'attenzione degli intermediari vigilati, dei soggetti sorvegliati e di quelli che operano a vario titolo negli ecosistemi decentralizzati, anche come utenti, sia sulle opportunità sia sui rischi connessi con l'uso di tali tecnologie e con l'operatività in cripto-attività, evidenziando alcuni profili rilevanti per il loro presidio.*

## 3. Uno sguardo al mercato delle criptovalute in Italia

Dalla data di avvio della sezione speciale del Registro dei Cambiavalute tenuto dall'OAM (16 maggio 2022) alla data di chiusura del primo semestre 2024, risultano iscritti 150 prestatori di servizi relativi all'utilizzo di valuta virtuale e di servizi di portafoglio digitale (*Virtual Asset Service Providers* – VASP), di cui 134 nella forma di persone giuridiche e 16 nella forma di persone fisiche. Con riferimento alla tipologia di attività svolta dagli operatori iscritti, al 30 giugno 2024 circa il 27% svolge esclusivamente l'attività di prestatore di servizi relativi all'utilizzo di valuta virtuale, circa il 4% effettua solo l'attività di prestatore di servizi di portafoglio digitale e circa il 69% svolge entrambe le attività. Nella Tabella 1, di seguito riportata, è fornito il dettaglio, in dati aggregati, delle tipologie di attività e di servizi offerti, nonché il luogo di svolgimento e la concentrazione territoriale degli iscritti. In estrema sintesi, alla data del 30 giugno 2024, degli attuali n. 150 iscritti, la quasi la totalità (n. 145) ha comunicato quale tipologia di attività, la prestazione di servizi relativi all'utilizzo di valuta virtuale e, sempre in via prevalente (n. 139), ha comunicato, quale tipologia di servizi, quelli funzionali all'utilizzo e allo scambio di valute virtuali e/o alla loro conversione da ovvero in valute. Ulteriormente, si segnala la comunicazione da parte degli iscritti di n. 167 siti *web* e n. 61 punti fisici, di cui n. 100 con ATM.

Tabella 1

| Dati Registro | 30/06/2024 | P.F. | P.G. |
|---|---|---|---|
| Iscritti | **150** | 16 | 134 |
| Cancellati | **16** | 3 | 13 |
| **Tipologia attività** | | | |
| Prestatore di servizi relativi all'utilizzo di valuta virtuale | **145** | 16 | 129 |
| Prestatore di servizi di portafoglio digitale | **109** | 4 | 105 |
| **Tipologia Servizi** | | | |
| Servizi funzionali all'utilizzo e allo scambio di valute virtuali e/o alla loro conversione da ovvero in valute | **139** | 14 | 125 |
| Servizio di emissione | **87** | 6 | 81 |
| Servizi trasferimento e compensazione in valute virtuali | **104** | 7 | 97 |
| Ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio | **117** | 12 | 105 |
| Servizi di portafoglio digitale | **110** | 4 | 106 |

| Luogo di svolgimento | Siti Web | Tot. Punti fisici | (ATM) |
|---|---|---|---|
| **Dislocazione Punti fisici** | **167** | **61** | **100** |
| Nord | | 18 | 54 |
| Centro | | 27 | 24 |
| Sud | | 16 | 22 |

| | Concentrazione Punti fisici | | |
|---|---|---|---|
| **Concentrazione Punti fisici** | **Provincia** | **Comune** | **N°** |
| 44% di Punti fisici al Nord | Roma | Roma | 10 |
| 32% di Punti fisici al Centro | Firenze | Firenze | 8 |
| 24% di Punti fisici al Sud | Venezia | Venezia | 4 |

| | Concentrazione ATM | | |
|---|---|---|---|
| **Concentrazione ATM** | **Provincia** | **Comune** | **N°** |
| 54% di ATM al Nord | Roma | Roma | 15 |
| 21% di ATM al Centro | Milano | Milano | 14 |
| 24% di ATM al Sud | Bologna | Bologna | 7 |

Conformemente a quanto previsto dall'art. 5, commi 1 e 2, del Decreto del Ministero dell'Economia e delle Finanze n. 40, del 13 gennaio 2022, successivamente all'istituzione della sezione speciale del Registro dei Cambiavalute, l'Organismo, tramite il suo Portale, ha abilitato il servizio per la trasmissione dei dati relativi alle operazioni effettuate sul territorio della Repubblica Italiana. I prestatori di servizi relativi all'utilizzo di valuta virtuale e i prestatori di servizi di portafoglio digitale trasmettono, con cadenza trimestrale, all'OAM per via telematica i dati relativi alle operazioni effettuate sul territorio della Repubblica Italiana, tra cui quelli identificativi del cliente (cognome e nome; luogo e data di nascita; residenza; codice fiscale/partita IVA, ove assegnato; estremi del documento di identificazione) e i dati sintetici relativi all'operatività complessiva di ciascun prestatore di servizi relativi all'utilizzo di valute virtuali e prestatore di servizi di portafoglio digitale per singolo cliente, come di seguito specificati:

- controvalore in euro, alla data dell'ultimo giorno del trimestre di riferimento, del saldo totale delle valute legali e delle valute virtuali riferibili a ciascun cliente;
- numero e controvalore complessivo in euro, alla data dell'ultimo giorno del trimestre di riferimento, delle operazioni di conversione da valuta legale a virtuale e da virtuale a legale riferibili a ciascun cliente;
- numero delle operazioni di conversione tra valute virtuali riferibili a ciascun cliente;
- numero delle operazioni di trasferimento di valuta virtuale in uscita e in ingresso da/verso il prestatore di servizi relativi all'utilizzo di valuta virtuale riferibili a ciascun cliente;
- numero e controvalore in euro, alla data dell'ultimo giorno del trimestre di riferimento, dell'ammontare delle operazioni di trasferimento di valuta legale in uscita e in ingresso da/verso il prestatore di servizi relativi all'utilizzo di valuta virtuale, riferibili a ciascun cliente e suddivise per trasferimenti in contante e strumenti tracciabili.

Dalla data di abilitazione del servizio per la trasmissione dei dati al 30 giugno 2024, sono stati trasmessi all'Organismo cinque flussi segnaletici trimestrali relativi alle operazioni effettuate sul territorio della Repubblica Italiana dal 1° gennaio 2023 al 31 marzo 2024. Con riferimento al quinto flusso segnaletico trasmesso all'Organismo, relativo al primo trimestre del 2024, sono stati 112 gli iscritti che hanno trasmesso all'Organismo, per via telematica, i dati relativi alle operazioni effettuate sul territorio della Repubblica, pari al 77% degli iscritti al 31.03.2024. Con tale flusso informativo, sono stati trasmessi all'Organismo i dati identificativi e relativi all'operatività in criptovalute di 1.803.653 clienti. Rispetto al totale dei clienti trasmessi, il 75% deteneva, all'ultimo giorno del trimestre di riferimento, criptovalute in portafoglio, per un controvalore in euro pari a 2.760.388.407. Pertanto, il valore medio delle criptovalute detenute dai clienti è pari a 2.030,81 euro; sono state effettuate 3.320.172 operazioni di conversione da valuta legale a virtuale (in media 9,4 operazioni per cliente) e 2.977.422 ope-

razioni di conversione da valuta virtuale a legale (in media 9,3 operazioni per cliente) [1].

L'OAM, su richiesta, è tenuto a fornire al Ministero dell'Economia e delle Finanze, alle Autorità di vigilanza di settore, all'Unità di Informazione Finanziaria per l'Italia, alla Guardia di Finanza e alla Direzione Nazionale Antimafia e Antiterrorismo ogni informazione e documentazione detenuta in forza della gestione della sezione speciale del Registro, compresi i dati relativi alla clientela degli operatori che ha fatto operazioni in Italia. Ai fini del contrasto all'abusivismo il Nucleo speciale di polizia valutaria della Guardia di Finanza e le forze di polizia possono richiedere all'OAM i dati e le informazioni sui prestatori di servizi relativi all'utilizzo di valuta virtuale e ai prestatori di servizi di portafoglio digitale, ivi compresi quelli relativi ai soggetti che non hanno integrato correttamente la comunicazione all'Organismo.

## 4. Il d.lgs. del 5 settembre 2024: le nuove regole e il regime transitorio

Come anticipato in premessa, è ormai imminente l'applicazione della riforma introdotta dal c.d. Regolamento MiCAR – *Markets in Crypto Assets* – finalizzata ad uniformare i requisiti e le legislazioni vigenti ed evitare arbitraggi normativi, prevedendo la possibilità di operatività transfrontaliera di un prestatore di servizi relativi all'utilizzo di valuta virtuale e di servizi di portafoglio digitale (nell'ambito dell'intero territorio UE, previa presentazione di istanza di autorizzazione al proprio Paese *home* seguita dall'iscrizione nel Registro ESMA).

Con l'introduzione del Regolamento MiCAR, l'Unione Europea mira a creare un quadro normativo più omogeneo e completo per le criptovalute, affrontando questi ed altri problemi in modo più sistematico e armonizzato a livello di tutti gli Stati membri. Come riportato al Considerando 6 del Regolamento "Si rende pertanto necessario un quadro specifico e armonizzato per i mercati delle cripto-attività a livello dell'Unione, allo scopo di definire norme specifiche per le cripto-attività e i servizi e le attività correlati non ancora coperti da atti legislativi dell'Unione in materia di servizi finanziari. Un simile quadro dovrebbe sostenere l'innovazione e la concorrenza leale, garantendo nel contempo un elevato livello di tutela dei detentori al dettaglio e l'integrità dei mercati delle cripto-attività. Un quadro chiaro dovrebbe consentire ai prestatori di servizi per le cripto-attività di espandere la loro attività su base transfrontaliera e facilitarne l'accesso ai servizi bancari, in modo da consentire loro di svolgere le loro attività in modo agevole. Un quadro dell'Unione per i mercati delle cripto-attività dovrebbe prevedere un trattamento proporzionato degli emittenti di cripto-attività e dei prestatori di servizi per le cripto-attività, dando così luogo a pari opportunità

[1] Per approfondimenti: https://www.organismo-am.it/documenti/Analisi_e_Ricerche/Analisi_Quarta_e_Quinta_Trasmissione_Flussi_VASP.pdf

per quanto riguarda l'ingresso nel mercato e lo sviluppo attuale e futuro dei mercati delle cripto-attività. Esso dovrebbe inoltre promuovere la stabilità finanziaria e il regolare funzionamento dei sistemi di pagamento e far fronte ai rischi di politica monetaria che potrebbero scaturire dalle cripto-attività che mirano a stabilizzare il loro prezzo in relazione a un'attività specifica o a un paniere di attività. Una regolamentazione adeguata mantiene la competitività degli Stati membri sui mercati finanziari e tecnologici internazionali e offre ai clienti vantaggi significativi in termini di accesso a una gestione patrimoniale e a servizi finanziari più economici, più veloci e più sicuri. Il quadro dell'Unione per i mercati delle cripto-attività non dovrebbe disciplinare la tecnologia sottostante. Gli atti legislativi dell'Unione dovrebbero evitare di imporre un onere normativo superfluo e sproporzionato sull'uso della tecnologia, poiché l'Unione e gli Stati membri si prefiggono di salvaguardare la competitività sul mercato mondiale".

Pertanto, le ragioni alla base della formulazione di una disciplina unionale delle criptovalute, come quella proposta nel Regolamento MiCAR, sono molteplici e riflettono sia le opportunità che le sfide presentate da questo settore in rapida evoluzione, quali:

✓ armonizzazione regolamentare: una delle principali motivazioni è la necessità di un quadro normativo armonizzato a livello europeo. Prima del Regolamento MiCAR, le criptovalute erano soggette a regolamentazioni diverse e a volte contraddittorie tra i vari stati membri. Una regolamentazione unionale fornisce chiarezza e coerenza, facilitando le attività delle imprese e proteggendo meglio i consumatori in tutta l'Unione Europea;

✓ migliorare la protezione dei consumatori e degli Investitori: la crescente popolarità delle criptovalute ha aumentato la necessità di proteggere i consumatori e gli investitori dai rischi associati, come frodi, volatilità del mercato e perdita di fondi. Il Regolamento MiCAR mira a stabilire *standard* di trasparenza e divulgazione per le emittenti e per i prestatori di servizi in cripto attività;

✓ garantire stabilità Finanziaria e Integrità del Mercato: la disciplina unionale cerca di prevenire l'utilizzo delle criptovalute per scopi illeciti come il riciclaggio di denaro e il finanziamento del terrorismo. Allo stesso tempo, mira a preservare la stabilità finanziaria riducendo i rischi sistemici che potrebbero emergere da questo settore;

✓ promuovere l'Innovazione e la Competitività: un quadro normativo chiaro ed equilibrato può anche promuovere l'innovazione e la competitività all'interno del mercato unico europeo. Fornendo linee guida chiare, il Regolamento MiCAR può incoraggiare lo sviluppo di nuove tecnologie e servizi legati alle criptovalute, mantenendo l'Unione Europea competitiva a livello globale;

✓ fornire risposta alle evoluzioni del Mercato: le criptovalute rappresentano un settore in rapida evoluzione, con nuovi prodotti e servizi che emergono costantemente. Una disciplina unionale consente di rispondere in modo flessibile e tempestivo a queste evoluzioni, garantendo al tempo stesso un monitoraggio e una regolamentazione efficaci.

La disciplina dell'Unione Europea sulle criptovalute mira quindi a bilanciare la necessità di regolamentare e mitigare i rischi con l'obiettivo di promuovere l'innovazione e la crescita in questo settore dinamico.

Le modalità di applicazione del Regolamento sono state stabilite dal d.lgs. del 5 settembre 2024, n.129, pubblicato in Gazzetta Ufficiale il 13 settembre 2024, che individua Banca d'Italia e Consob quali autorità competenti, sia ai fini autorizzativi che di vigilanza, e stabilisce un periodo transitorio nel corso del quale continuerà a essere attiva la sezione speciale del Registro dei Cambiavalute gestito dall'Organismo. Viene quindi regolamentata la transizione dall'attuale disciplina della prestazione di servizi relativi all'utilizzo di valuta virtuale e di portafoglio digitale alla disciplina della prestazione di servizi sulle cripto-attività prevista da MiCAR. Il Governo, in linea con le raccomandazioni pervenute dall'Autorità europea degli strumenti finanziari e dei mercati (ESMA) ha ridotto a 12 mesi il periodo transitorio a fronte dei 18 mesi previsti in via ordinaria dal Regolamento, ritenendo che il quadro normativo nazionale applicabile ai prestatori di servizi per le cripto-attività prima del 30 dicembre 2024 sia meno rigoroso di quello previsto da MiCAR.

Con l'applicazione del Regolamento MiCAR possono continuare a operare per un periodo di sei mesi – ossia fino al 30 giugno 2025 – ai sensi della disciplina attualmente prevista i soli soggetti regolarmente iscritti nella sezione speciale del Registro dei Cambiavalute tenuto dall'OAM al 27 dicembre 2024. Ove i medesimi soggetti presentino istanza di autorizzazione come CASP (*Crypto-Asset Service Providers*), in Italia o in un altro Stato membro, entro il 30 giugno 2025, sarà consentito agli stessi di continuare a operare nelle more dello svolgimento del procedimento di autorizzazione, fino al rilascio o rifiuto della medesima e comunque non oltre il 30 dicembre 2025. In caso di rigetto dell'istanza di autorizzazione, sono previsti termini ad hoc per consentire l'ordinata chiusura dei rapporti con la clientela italiana. Vengono anche definiti i flussi di comunicazione tra i soggetti iscritti nella sezione speciale del Registro dei Cambiavalute, l'OAM e l'autorità nazionale competente.

## 5. Conclusioni

L'applicazione del Regolamento europeo, che introduce una normativa più rigorosa e presidi a tutela degli utenti e dei risparmiatori, rappresenta un punto di svolta per il settore. Bisognerà attendere la fine del periodo transitorio per capire quanto gli operatori riterranno interessante il mercato italiano. A tal proposito, Banca d'Italia e Consob, in collaborazione con l'Organismo degli Agenti in attività finanziaria e dei Mediatori creditizi, hanno condotto, nel quarto trimestre 2023, un'indagine conoscitiva proprio per comprendere il potenziale livello di interesse a svolgere in Italia attività rientranti nell'ambito applicativo del Regolamento MiCAR. L'indagine è stata rivolta a: banche, Istituti di moneta

elettronica, Istituti di pagamento, intermediari finanziari *ex* art. 106 TUB, SIM, gestori di OICVM e FIA, depositari centrali di titoli e gestori di mercati regolamentati; i soggetti iscritti nel Registro dei Prestatori di servizi relativi all'utilizzo di valuta virtuale e di servizi di portafoglio digitale e tenuto dall'OAM che attualmente svolgono servizi e attività che saranno regolate dal Regolamento MiCAR; i soggetti diversi da quelli di cui ai precedenti punti che sono intenzionati a svolgere servizi o attività regolate dal Regolamento MiCAR. Con riferimento ai soggetti iscritti nel Registro dei Prestatori di servizi relativi all'utilizzo di valuta virtuale e di servizi di portafoglio digitale tenuto dall'OAM, l'Organismo ha condotto l'indagine, nei confronti dei prestatori di servizi relativi all'utilizzo di valuta virtuale e di servizi di portafoglio digitale nella forma di persone giuridiche. Il questionario trasmesso agli operatori risulta costituito da una scheda anagrafica (Informazioni generali) e da un'ulteriore sezione (Regolamento MiCAR Servizi ed emissione) relativa all'intenzione di svolgere attività o prestare servizi disciplinati dal Regolamento MiCAR dopo l'entrata in vigore del regolamento, tra cui: la prestazione di servizi in cripto-attività; l'emissione di *token* collegati ad attività (*asset-referenced token*, ART); l'emissione di *token* di moneta elettronica (*e-money token*, EMT); l'offerta al pubblico o richiesta di ammissione alla negoziazione per *crypto*-attività diverse da ART e EMT. L'indagine ha rilevato come molti VASP stiano considerando di presentare istanza di autorizzazione alla prestazione di servizi per le cripto-attività in Italia entro il primo semestre del 2025, in particolare con riferimento alle attività di scambio di cripto-attività con fondi, allo scambio di cripto-attività con altre attività e all'esecuzione di ordini di cripto-attività per conto di clienti[2].

In attesa di capire quali saranno le scelte definitive dei CASP (*Crypto-asset Service Provider*) è invece possibile tracciare un bilancio degli effetti prodotti dalla normativa delineata con il Decreto del Ministero dell'Economia e delle Finanze n. 40, del 13 gennaio 2022 che verrà sostituita dal Regolamento MiCAR. L'attività svolta dall'OAM negli oltre due anni di gestione della sezione speciale del Registro dei Cambiavalute, ha prodotto risultati di rilievo per quanto attiene gli obiettivi posti dalla normativa antiriciclaggio. Come riportato dall'Unità di Informazione Finanziaria per l'Italia (UIF) in un aggiornamento sulla collaborazione attiva nel comparto dei *virtual asset* e sui progressi della normativa in materia, l'introduzione del censimento dei prestatori di servizi relativi all'utilizzo di valuta virtuale e prestatori di servizi di portafoglio digitale operanti in Italia, ol-

[2] Inoltre, al fine di comprendere se l'intenzione di svolgere attività o prestare servizi disciplinati dal Regolamento MiCAR dopo l'entrata in vigore del regolamento da parte dei VASP rispondenti all'indagine potesse essere influenzata dall'attuale operatività degli operatori, è stata condotta un'analisi per cluster. Quest'ultimi sono stati definiti in base alla dimensione dell'operatività dei VASP, misurata in termini di numero medio di clienti (record) trasmessi trimestralmente all'OAM, classificando gli operatori in tre classi come di seguito indicato: a) Exchange piccolo (n. clienti < 500); b) Exchange medio (500 < n. clienti < 50.000); c) Exchange grande (n. clienti > 50.000). Per approfondimenti: https://www.organismo-am.it/documenti/Analisi_e_Ricerche/Analisi_Quarta_e_Quinta_Trasmissione_Flussi_VASP.pdf.

tre a promuovere una maggiore trasparenza nel settore e a ridurre i rischi connessi, sta contribuendo ad aumentare il numero di soggetti registrati in RADAR (Raccolta e Analisi Dati per l'Anti Riciclaggio) per la segnalazione di operazioni sospette. I principali sospetti riguardanti le valute virtuali si riferiscono all'origine dei fondi utilizzati per il loro acquisto, spesso legati a potenziali reati fiscali, frodi informatiche o episodi di *ransomware*[3]. Sono stati riscontrati casi di truffe nel *trading online* e investimenti effettuati dalle vittime attraverso piattaforme estere, spesso non autorizzate, a seguito di insistenze telefoniche o con l'intermediazione di presunti consulenti finanziari. L'investimento in *virtual asset* viene frequentemente proposto con basse commissioni, giustificate da presunte collaborazioni con i principali *exchanger*. Altre situazioni comuni includono lo svolgimento dell'attività di *exchanger* senza adeguate strutture organizzative a protezione dei clienti e la mancata osservanza delle normative antiriciclaggio[4].

La sezione speciale del Registro dei Cambiavalute tenuto dall'OAM dedicata ai Prestatori di servizi relativi all'utilizzo di valuta virtuale e di servizi di portafoglio digitale ha inoltre consentito la conoscenza della dimensione del mercato nazionale delle criptovalute e dell'atteggiamento degli italiani nei confronti di questi strumenti, creando così un prezioso bagaglio informativo.

[3] Trattasi di attacchi informatici che bloccano l'accesso ai dati dei computer colpiti; per il recupero degli stessi viene chiesto il pagamento, in *virtual asset*, di un "riscatto".

[4] https://uif.bancaditalia.it/pubblicazioni/newsletter/2022/newsletter-2022-5/Newsletter_5_2022.pdf.

# La disciplina degli abusi di mercato nel MiCAR con particolare riferimento alla gestione e comunicazione al pubblico delle informazioni privilegiate concernenti cripto attività

Paolo Maggini, Andrea Pantaleo [*]



## 1. Premessa

Il Regolamento relativo ai mercati delle cripto-attività ("MiCAR") è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea ("GUUE") il 9 giugno 2023 [1] ed il quadro normativo europeo è in completamento con l'emanazione della relativa normativa di esecuzione [2]Nell'ambito della strategia europea in

---

[*] Per quanto il lavoro sia riferibile nel complesso ad entrambi gli Autori, dopo la condivisa Premessa, i paragrafi 2 a 3 sono da attribuire a Andrea Pantaleo e quelli da 4 a 9 a Paolo Maggini, le cui opinioni sono ivi espresse a titolo personale e non impegnano l'Istituzione di appartenenza.

[1] Nell'*incipit* della Relazione alla proposta del MiCAR del 24 settembre 2020 (p. 1), la Commissione indica che questa: "*fa parte del pacchetto sulla finanza digitale, un pacchetto di misure volte a consentire e sostenere l'ulteriore sfruttamento del potenziale della finanza digitale in termini di innovazione e concorrenza, attenuando nel contempo i rischi*".

[2] Nel presente lavoro saranno, in particolare, esaminate le disposizioni del Regolamento di esecuzione (UE) 2024/2861 della Commissione ("Regolamento 2024/2861" o "Regolamento di esecuzione") che stabilisce norme tecniche di attuazione per l'applicazione del MiCAR "*per quanto ri-*

materia di finanza digitale, tale disciplina può essere considerata "*one of the major milestones achieved*" [3].

Successivamente, il legislatore nazionale con il d.lgs. 5 settembre 2024, n. 129, pubblicato in Gazzetta Ufficiale il 13 settembre 2024, ha adeguato la normativa nazionale al MiCAR, delineando anche il riparto di competenze tra la Banca d'Italia e la Consob per l'esercizio dei relativi poteri di vigilanza, come anche rappresentato in una nota ricognitiva congiunta pubblicata il 29 ottobre 2024 dalle due Autorità, che hanno successivamente stipulato nel 2025 uno specifico Protocollo d'Intesa.

Il presente lavoro non tratterà, se non per brevi richiami, le tematiche concernenti il funzionamento delle *Distributed Ledger Technologies* ("DLT") [4], tra cui la più nota *blockchain*, così come le tipologie di cripto attività [5] e le problematiche connesse alla *tokenizzazione di azioni e* (alle) *azioni tokens* [6].

---

*guarda gli strumenti tecnici per l'adeguata comunicazione al pubblico delle informazioni privilegiate e la comunicazione al pubblico tardiva di tali informazioni*", pubblicato nella GUUE il 13 novembre 2024.

[3] Alice GUEDEL e Giuseppe SCIASCIA, *The state of digital finance in Europe*, in *Digital Finance in the EU: drivers, risks, opportunities*, a cura di Thorsten BECK, Leonardo GIANI e Giuseppe SCIASCIA, European University Institute (*e-book*), San Domenico di Fiesole (FI), 2023, p. 16.

[4] Per un esame delle differenze tra le caratteristiche delle DLT e quelle dei regimi cartolari e dematerializzati dei titoli si vedano, in particolare, Michele DE MARI, Giorgio GASPARRI e Tommaso Nicola POLI *La natura giuridica delle cripto-attività*, in *Tokenizzazione di azioni e azioni tokens* (a cura di Paolo CARRIÉRE, Nicola DE LUCA, Michele DE MARI, Giorgio GASPARRI e Tommaso Nicola POLI), Quaderni Giuridici Consob (25), 2023, p. 26.

[5] Il MiCAR assoggetta alla propria disciplina tre tipologie di cripto-attività, ovvero *e-money token* ("EMT"), *asset-referenced tokens* ("ART") e *other non asset-referenced tokens* ("OTHR"). Quanto agli EMT ed ART, trattasi delle c.d. *stablecoins* che si prefiggono l'obiettivo di mantenere il proprio valore stabile con riferimento ad un *asset* di riferimento. Mentre gli EMT ancorano il proprio valore ad una ed una sola moneta *fiat* – e devono prevedere il diritto di riscatto *at par value* analogamente alla moneta elettronica tradizionale – gli ART fanno riferimento al valore di più monete *fiat*, *commodities*, altre cripto-attività, strumenti finanziari od un paniere di questi. La categoria degli OTHR, invece, è di carattere residuale ed abbraccia tutte le restanti cripto-attività che non hanno un meccanismo di stabilizzazione del proprio valore.

Le caratteristiche distintive di tali tipologie di cripto-attività sono ampiamente riprese dalle pubblicazioni citate nel presente lavoro. Si veda anche Raffaele LENER, Salvatore Luciano FURNARI, *Cripto-attività: prime riflessioni sulla proposta della commissione europea. Nasce una nuova disciplina dei servizi finanziari "crittografati"?*, in *dirittobancario.it*, ottobre 2020 e, con particolare riferimento alle *stablecoin*, Mattia SUARDI, *Revisione della PSD2 e coordinamento con il MiCAR: evoluzione o rivoluzione della disciplina sui servizi di pagamento?*, Collana *Mercati, infrastrutture, sistemi di pagamento* della Banca d'Italia, ottobre 2024, p. 17 ss. Tale Autore ricorda che: "*il concetto di EMT corrisponde alle stablecoin riferite a una valuta ufficiale, mentre agli ART sono riconducibili tutte le altre stablecoin riferite, in particolare, a commodities come l'oro, panieri di valute ufficiali, altre cripto-attività o anche una combinazione delle precedenti. La terza categoria è rappresentata dalle cripto-attività diverse dalle precedenti (cosiddette crypto other than) e include sia le cripto-attività unbacked, ossia non garantite da attività sottostanti, sia gli utility token*".

[6] Si rinvia, al riguardo, al già citato quaderno giuridico della Consob n. 25, pubblicato nel gennaio 2023.

## 2. L'ambito di applicazione della disciplina sugli abusi di mercato di cui al Regolamento (UE) 2023/1114

Al fine di esaminare i contenuti del Titolo VI di MiCAR, intitolato "*prevenzione e divieto degli abusi di mercato relativi alle cripto-attività*", è opportuno analizzare preliminarmente l'ambito di applicazione dell'intero Regolamento MiCAR.

Il Regolamento – e dunque anche la disciplina degli abusi di mercato – trova applicazione solamente alle cripto-attività che ricadono all'interno del suo perimetro.

Ne consegue che le cripto-attività escluse dal perimetro applicativo saranno parimenti esenti dalle regole sugli abusi di mercato, o perché ricadenti sotto altra disciplina, ad esempio quella del Regolamento (UE) n. 596/2014 ("MAR") nel caso di strumenti finanziari tokenizzati, o perché non regolati, come i *non fungible token* ("NFT"), salvo quanto in seguito si dirà.

Il Titolo VI si applica "*agli atti compiuti da qualsiasi persona in relazione a cripto-attività ammesse alla negoziazione o in relazione alle quali è stata presentata una richiesta di ammissione alla negoziazione*" (art. 86 del MiCAR).

Per definire la portata applicativa della disciplina di cui al Titolo VI di MiCAR, è necessario prima identificare quali cripto-attività ricadono nel perimetro applicativo del Regolamento. A tale riguardo, possiamo certamente individuare cripto-attività che:

– ricadono sotto l'integrale disciplina di MiCAR;
– ricadono parzialmente sotto la disciplina di MiCAR, ma sono comunque soggette alla disciplina sugli abusi di mercato;
– a determinate condizioni sono catturate da MiCAR, rimanendo altrimenti o prive di regolamentazione o sotto la disciplina del MAR in quanto strumenti finanziari.

Si è già indicato in Premssa che il MiCAR assoggetta alla propria disciplina tre tipologie di cripto-attività, ovvero gli *e-money token*, *asset-referenced tokens* ed *other non asset-referenced tokens*; quest'ultima categoria incontra nel MiCAR determinate esenzioni che ne determinano la parziale applicazione: a titolo esemplificativo, le cripto-attività che sono distribuite quale ricompensa per il funzionamento e la messa in sicurezza del *network* – come *Bitcoin* ed *Ethereum* – sono esentate dal titolo II sul regime di offerta al pubblico[7].

Più complessa è invece la categoria delle cripto-attività che a determinate condizioni ricadono nel perimetro applicativo di MiCAR mentre, in presenza di alcune caratteristiche, rimangono non regolamentate o ricadono sotto il perimetro del MAR poiché classificabili come strumenti finanziari.

---

[7] Ciò non toglie, tuttavia, che laddove queste cripto-attività siano oggetto di servizi da parte dei prestatori, troverà applicazione sia il Titolo V, sugli obblighi dei prestatori di servizi, che il Titolo VI, sugli abusi di mercato, considerato il rischio che i relativi andamenti possano essere oggetto di intenti manipolativi su talune *trading venues* rilevanti per la disciplina.

È il caso, ad esempio, degli NFT che sono generalmente esentati dall'applicazione di tutto il MiCAR, e dunque anche del Titolo VI sugli abusi di mercato, a condizione che rappresentino *asset* effettivamente e sostanzialmente infungibili (unici) tra di loro.

Al contrario, NFT che presentino elementi di fungibilità, come potrebbero essere ad esempio quelli emessi nell'ambito di collezioni o serie su ampia scala, non godranno del regime di esenzione e potrebbero essere, dunque, soggetti all'applicazione di MiCAR, nell'ambito della categoria degli OTHR.

Ancora più delicata è l'identificazione delle cripto-attività classificabili come strumenti finanziari e, pertanto, soggetti alla disciplina del MAR per quanto attiene agli aspetti degli abusi di mercato. A tale riguardo, è bene sin da ora distinguere tra:

– strumenti finanziari tradizionali in forma tokenizzata, ovvero rappresentati da *token* emessi e registrati su DLT e;

– cripto-attività non direttamente rappresentative di strumenti finanziari, ma che presentino caratteristiche similari agli strumenti finanziari e pertanto siano da considerarsi come tali ai fini dell'individuazione della corretta normativa applicabile.

Alla luce del dibattito già ampiamente svolto sulla prima delle categorie sopra indicate, ci si soffermerà, in particolare, sulle cripto-attività che, pur non essendo concepite per rappresentare strumenti finanziari tradizionali, ciò nondimeno presentino caratteristiche similari a quelle degli strumenti finanziari così da classificarle come tali.

Trattasi in particolare delle cripto-attività che sono idonee a ricadere nella residuale categoria delle c.d. *transferable securities*, ovvero gli strumenti finanziari che siano categorie di valori mobiliari – esclusi gli strumenti di pagamento – negoziati nei mercati di capitali.

Le peculiarità di talune cripto-attività e la loro programmabilità e molteplicità di diritti assegnabili ai titolari può infatti, in alcuni casi, determinarne l'attrazione verso la categoria delle *transferable securities*, motivo per il quale nel MiCAR è stato previsto un mandato all'*European Securities and Markets Authority* (di seguito, anche "ESMA") per elaborare delle linee guida rivolte alle autorità di vigilanza dei singoli Stati Membri e volte ad individuare i maggiori indicatori in presenza dei quali una cripto-attività possa essere qualificata come strumento finanziario in quanto *transferable security*.

In ottemperanza al proprio mandato, dunque, il 29 gennaio 2024 ESMA ha posto in consultazione [8] e successivamente pubblicato in data 17 dicembre 2024 le

[8] *Consultation Paper* dell'ESMA sulle *Guidelines on the qualification of crypto-assets as financial instruments*. Si sottolinea che le linee guida sono elaborate esclusivamente ai fini della qualificazione dei *crypto-asset* come strumenti finanziari e nell'ambito del mandato di cui al MiCAR, mentre non intendono fornire delle linee interpretative generali per la classificazione di altri *asset*, diversi dalle cripto-attività, come strumenti finanziari.

"*Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments*" che contengono i principi in base ai quali una cripto-attività può essere qualificata come strumento finanziario.

Pur di natura non vincolante per le Autorità degli Stati Membri trattandosi di strumento di *soft law* non direttamente applicabile e senza efficacia cogente [9], le linee guida di ESMA sono in ogni caso cruciali per definire i parametri che i *crypto-asset* devono rispettare per poter rientrare nella categoria delle *transferable securities*:

– fungibilità: le categorie di *crypto-asset* devono essere tra loro fungibili e conferire ai titolari i medesimi diritti;

– negoziabilità: il concetto di negoziabilità – per quanto riguarda i *crypto-asset* – coincide di fatto con quello di trasferibilità; i *crypto-asset* sono considerati negoziabili nel momento stesso in cui siano tecnicamente e concretamente trasferibili; in altri termini, l'astratta negoziabilità sui mercati dei capitali – derivante dalla loro possibile trasferibilità – è sufficiente per integrare il requisito pur in assenza di un *listing* ufficiale su una piattaforma di scambio;

– negoziabilità sul mercato di capitali: la astratta negoziabilità rileva nel momento in cui è possibile ritenere che i *crypto-asset* siano liberamente trasferibili su piattaforme di scambio, con conseguente esclusione dei *crypto-asset* che – pur trasferibili – prevedano delle limitazioni o restrizioni per il *listing* su *trading venues*; le autorità nazionali sono chiamate a interpretare in modo estensivo il concetto di mercato di capitali, includendo "*all contexts where buying and selling interests in securities meet, and simultaneously assess the differences between traditional venues and trading platforms for crypto-assets*".

Il punto però cruciale è quello dell'individuazione dei diritti che le cripto-attività, se fungibili e negoziabili, devono avere per essere classificate come strumenti finanziari, tema che pone maggiori dubbi interpretativi.

I criteri indicati da ESMA possono essere riassunti in questi termini:

– non sono classificabili come strumenti finanziari le cripto-attività che presentino unicamente diritti di utilità (i.e. possono essere utilizzati esclusivamente nei confronti dell'emittente per l'accesso a beni o servizi) o che siano portatrici di mere aspettative economiche non azionabili nei confronti dell'emittente;

– sono invece rilevanti le caratteristiche delle cripto-attività che conferiscano diritti di *ownership* o *governance* sull'emittente [10], a maggior ragione se attribuiscono un diritto a profitti derivanti dall'attività dell'emittente o dalla sua liquidazione;

– rimane invece incerta la natura dei *crypto-asset* che attribuiscono diritti azionabili nei confronti dell'emittente rispetto a profitti decorrelati rispetto all'atti-

[9] Le autorità competenti nazionali dovranno comunque comunicare ad ESMA se non intendono aderire alle linee guida proposte e, in tal caso, comunicare le ragioni a sostegno della propria scelta.

[10] Con esclusione, però, dei diritti di *ownership* o *governance* che non conferiscano poteri – ad esempio di voto – nell'ambito delle scelte di direzione strategica dell'emittente.

vità dell'emittente o alla sua liquidazione, per la quale viene in rilievo il principio generale di ESMA per cui "*NCAs should evaluate whether the rights granted by the crypto-assets are equivalent to those typically granted by a specific type of transferable security*", rimandando dunque ad una analisi comparativa con le tipiche caratteristiche degli strumenti finanziari elencati in via esemplificativa nei punti (a) (b) (c) dell'art. 4(1), punto (44) di MiFID II.

Per completezza, per le cripto-attività c.d. ibride – ovvero che presentino caratteristiche di utilità e al contempo finanziarie – dovrà essere condotta un'analisi di prevalenza per determinarne la natura, fermo restando che le caratteristiche tipiche degli strumenti finanziari (come diritti ai dividendi o interessi derivanti dalla detenzione per un determinato periodo di tempo) saranno sempre da considerarsi prevalenti.

In ultimo, merita un approfondimento *ad hoc* la categoria degli strumenti finanziari derivati aventi come sottostante cripto-attività. Ferma la loro classificazione come strumenti finanziari, il MiCAR prevede espressamente che "gli strumenti derivati qualificabili come strumenti finanziari quali definiti nella direttiva 2014/65/UE e la cui attività sottostante è una cripto-attività sono soggetti al MAR se negoziati in un mercato regolamentato, un sistema multilaterale di negoziazione o un sistema organizzato di negoziazione".

Parallelamente, le cripto-attività che rientrano nell'ambito di applicazione di MiCAR e che sono le attività sottostanti di strumenti derivati "*dovrebbero essere soggette alle disposizioni sugli abusi di mercato di cui al presente regolamento*" [11] (cioè del MiCAR), circostanza che evidenzia una scissione tra la normativa sugli abusi di mercato applicabile allo strumento derivato (MAR) e quella applicabile al sottostante (MiCAR), con le differenze – e le aree di possibile sovrapposizione – che verranno in seguito illustrate.

## 3. I servizi rilevanti ai fini dell'applicabilità della disciplina sugli abusi di mercato

Oltre all'individuazione delle cripto-attività soggette alla disciplina degli abusi di mercato di cui al MiCAR, è necessario evidenziare che questa si applica soltanto a quelle cripto-attività che, pur comprese nel perimetro applicativo, siano negoziate su piattaforme autorizzate o per le quali è stata fatta richiesta di ammissione alla negoziazione.

È necessario, quindi, ripercorrere le caratteristiche dei singoli servizi contemplati da MiCAR per individuare cosa si intenda per "*ammissione alla negoziazione*" ed a quale servizio – *rectius infra*struttura – si faccia riferimento.

[11] Cfr.: Considerando n. 97 del MiCAR.

In forte similitudine con il regime MiFID II, il MiCAR contempla, infatti, una serie di servizi [12], tra i quali, appunto la gestione di una piattaforma di negoziazione di cripto-attività, ovvero la gestione di sistemi multilaterali che consentono o facilitano l'incontro di molteplici interessi di terzi per l'acquisto o la vendita di cripto-attività, scambiando cripto-attività con fondi o cripto-attività con altre cripto-attività.

Per "ammissione alla negoziazione", nella tassonomia dei servizi previsti da MiCAR, si deve intendere, dunque la "quotazione" (c.d. *listing*) della cripto-attività sulle piattaforme di negoziazione ora richiamate, ovvero sistemi multilaterali – in regime MiFID II mercati regolamentati, MTF e OTF – che agevolano l'incontro tra interessi in acquisto e vendita di cripto-attività.

È bene precisare che la disciplina sugli abusi di mercato trova applicazione per il solo fatto che una cripto-attività sia scambiata su piattaforme di negoziazione, a prescindere dal fatto che "*l'operazione, ordine o condotta avvenga in una piattaforma di negoziazione*" (art. 86, Par. 2). Rilevano dunque non solo le condotte compiute – nell'Unione o in paesi terzi (vedi *infra*) – nell'ambito di transazioni su piattaforme di negoziazione, ma anche quelle poste in essere al di fuori di esse, ad esempio, l'utilizzo di una informazione privilegiata per acquistare o vendere una cripto-attività *over the counter* al di fuori dei mercati di negoziazione.

Rimangono, viceversa, escluse dalla disciplina sugli abusi di mercato le crip-

---

[12] Si riporta di seguito l'elenco di detti servizi:

– la custodia e amministrazione di cripto-attività per conto dei clienti, consistente nella custodia o il controllo, per conto di clienti, delle cripto-attività o dei mezzi di accesso anche del caso sotto forma di chiavi crittografiche private;

– la gestione di una piattaforma di negoziazione di cripto-attività, ovvero la gestione di sistemi multilaterali che consentono o facilitano l'incontro di molteplici interessi di terzi per l'acquisto o la vendita di cripto-attività, scambiando cripto-attività con fondi o cripto-attività con altre cripto-attività;

– lo scambio di cripto-attività con fondi e altre cripto-attività, che presuppone la conversione in proprio di fondi in cripto-attività o cripto-attività in altre cripto-attività mediante utilizzo di capitale proprietario del prestatore di servizi;

– l'esecuzione di ordini di cripto-attività per conto dei clienti, ovverosia l'esecuzione di contratti di acquisto o vendita per conto dei clienti di una o più cripto-attività in sedi di negoziazione, compresa la conclusione di contratti per la vendita di cripto-attività al momento della loro offerta al pubblico o dell'ammissione alla negoziazione;

– il collocamento di cripto-attività, rappresentata dalla commercializzazione di cripto-attività agli acquirenti, a nome o per conto dell'offerente o di una parte a esso connessa;

– la ricezione e trasmissione di ordini di cripto-attività per conto dei clienti, che è rappresentata dalla ricezione da una persona di un ordine di acquisto o di vendita di una o più cripto-attività e la trasmissione di tale ordine a una terza parte a fini dell'esecuzione sul mercato;

– la prestazione di consulenza sulle cripto-attività, ovvero la raccomandazione personalizzata di investimento in una determinata cripto-attività;

– la gestione di portafogli di cripto-attività, cioè la gestione su base discrezionale e individualizzata di portafogli di investimento che includano una o più cripto-attività nell'ambito di un mandato conferito dai clienti;

– il trasferimento di cripto-attività per conto dei clienti, ovvero lo spostamento, per conto di una persona fisica o giuridica, di cripto-attività da un *address* DLT ad un altro.

to-attività che non sono ammesse alla negoziazione su piattaforme di scambio nei termini descritti sopra, come ad esempio quelle negoziate esclusivamente *over the counter*.

Ciò, del resto, è in linea con le disposizioni del MAR, che da un lato trova applicazione, in relazione agli strumenti finanziari ammessi alle negoziazioni su mercati regolamentati, MTF e OTF, indipendentemente dalla sede di esecuzione delle operazioni, dall'altro non è applicabile agli strumenti finanziari negoziati esclusivamente *over the counter*, salvo che tale negoziazione non sia idonea ad incidere – come nel caso dei derivati – sul prezzo di strumenti finanziari negoziati sulle *trading venues* prima richiamate (art. 2, Par. 1, lett. *d*, del MAR).

Le cripto-attività interessate dalla disciplina sugli abusi di mercato sono quelle negoziate su piattaforme di scambio europee soggette agli obblighi di MiCAR, con esclusione invece di ogni altro mercato di scambio di giurisdizioni non europee, salvo naturalmente futuri specifici accordi di cooperazione internazionale nella prevenzione degli abusi.

Tale aspetto è di rilievo, perché l'industria dei prestatori di servizi su cripto-attività, per la maggior parte di derivazione extra-UE, sembrava aver pianificato la propria attività in Europa secondo un modello *broker/dealer*, quindi di svolgimento sotto il regime MiCAR dei soli servizi di ricezione e trasmissione ordini o esecuzione per conto dei clienti, mantenendo invece le proprie piattaforme di scambio, verso cui veicolare gli ordini della clientela europea per la relativa esecuzione, al di fuori dell'Unione Europea e quindi sottratte agli obblighi previsti dal MiCAR.

Tale modello, non preordinato al sottrarsi dagli obblighi previsti per le piattaforme di negoziazione, bensì a creare delle strutture meno complesse nell'Unione Europea senza necessità di spostare tutte le *infra*strutture di scambio nel territorio dell'Unione, non ha trovato, comunque, il favore di ESMA.

Infatti, con l'*opinion* del 31 luglio 2024, ESMA ha proprio preso in considerazione, ed in via generale censurato, i *modelli di broker / dealer* strutturati, *inter alia*, nei seguenti termini:

– ottenimento di autorizzazione MiCAR per la prestazione dei servizi di ricezione e trasmissione ordini o esecuzione di ordini per conto dei clienti da parte di una società stabilita in UE;

– *routing* sistematico degli ordini della clientela europea, ricevuti tramite il prestatore autorizzato MiCAR, verso una piattaforma di negoziazione o negoziatore in conto proprio (c.d. *execution venues*) di gruppo situato extra-UE;

– mancata valutazione – nell'ambito della c.d. *execution policy* – di sedi di esecuzione diverse in funzione dei criteri di *best execution* individuati dal prestatore di servizi;

– concentrazione dei profitti nella piattaforma di negoziazione extra-UE.

L'*opinion* di ESMA, pur confermando in astratto la possibilità per i prestatori di servizi soggetti al MiCAR di utilizzare *execution venues* extra-UE, ha di fatto disincentivato i modelli basati sull'utilizzo sistematico di sedi di negoziazione

di gruppo prive di autorizzazione MiCAR, salvo che tale modello riesca a rispettare gli obblighi di *best execution* e, soprattutto, di efficace gestione dei conflitti di interesse, peraltro difficilmente prevenibili.

Tale orientamento di ESMA, come prevedibile, sta inducendo i prestatori di servizi a riconsiderare i propri modelli operativi e dunque a spostare le proprie *execution venues* in Europa, in modo da rispettare i criteri dettati da ESMA.

Così facendo, si assisterà verosimilmente ad una crescita delle piattaforme di negoziazione autorizzate MiCAR e dunque una consequenziale espansione della portata applicativa *in concreto* della disciplina sugli abusi di mercato, che, come detto, trova applicazione rispetto alle cripto-attività negoziate su piattaforme operanti nel territorio dell'Unione Europa sotto la regolamentazione del MiCAR.

## 4. Un parallelismo tra la disciplina del MiCAR e quella del MAR in tema di abusi di mercato

Nel contesto di una disciplina di mercato e, ai fini che qui interessano, nello specifico di mercato secondario, saranno approfondite le tematiche in tema di abusi di mercato, con particolare riferimento alle modalità di gestione e comunicazione delle informazioni privilegiate secondo la disciplina disegnata per le cripto-attività.

In particolare, nei paragrafi che seguono, verrà analizzata la disciplina della *disclosure* al pubblico, che ha attinto in maniera pressoché totale, salvo alcuni alleggerimenti, a quella delineata nel per i mercati finanziari (di seguito anche "disciplina tradizionale") [13].

È stata una scelta precisa del legislatore eurounitario, tra l'altro attento a non onerare eccessivamente le piccole e medie imprese ("PMI"), che potrebbero trovare nel contesto delle cripto-attività un ambiente innovativo e inclusivo al finanziamento, come riporta il Considerando n. 2 del MiCAR [14]; questa esigenza di bilanciamento è, del resto, ben descritta nel Considerando n. 95 del medesimo Regolamento [15].

---

[13] Nello stesso senso si è espressa già la dottrina che ha approfondito dette tematiche e, come si vedrà, anche l'ESMA. Salvatore Luciano FURNARI, *Le norme che disciplinano il settore DeFi*, in *La Finanza Decentralizzata*, *cripto attività, Protocolli, questioni giuridiche aperte*, a cura dello stesso Autore, Minerva Bancaria, Roma, 2023, p. 98, ha indicato che la soluzione adottata "*non si può non sottolineare*".

[14] Considerando n. 2 del MiCAR: "*(…) Grazie alla semplificazione dei processi di raccolta di capitali e al rafforzamento della concorrenza, le offerte di cripto-attività potrebbero rappresentare un approccio innovativo e inclusivo al finanziamento, anche per le piccole e medie imprese (PMI) (…)*".

[15] Considerando n. 95 del MiCAR: "*È importante garantire la fiducia nei mercati delle cripto-attività e l'integrità di tali mercati. È pertanto necessario stabilire norme volte a scoraggiare gli abusi di mercato per le cripto-attività ammesse alla negoziazione. Tuttavia, poiché gli emittenti di cripto-attività e i prestatori di servizi per le cripto-attività sono molto spesso PMI, sarebbe sproporzionato*

Gli approfondimenti in merito alla rilevanza della diffusione delle informazioni per ciò che concerne l'efficienza del mercato delle cripto-attività trarrà beneficio ed attingerà, dunque, sicuramente dagli approfondimenti pluridecennali della giurisprudenza, della dottrina e degli operatori del mercato, che a dire il vero sono stati nelle ultime decadi particolarmente prolifici [16], in funzione dell'evoluzione della normativa europea concernente i mercati finanziari.

Da ciò, però, consegue un'algida constatazione: la normativa MiCAR è stata redatta a specchio, attingendo da una normativa che, specie in tema di individuazione e comunicazione al pubblico delle informazioni rilevanti, ha mostrato negli anni recenti alcune difficoltà interpretative ed oneri applicativi, tali da renderne necessaria una marcata rivisitazione.

Il riferimento, in particolare è al diverso *timing* per la comunicazione al pubblico delle informazioni privilegiate ed ai suoi riflessi sulla procedura del ritardo di cui all'art. 17, Par. 1 e 4 del MAR [17], che il c.d. *Listing Act* ha disegnato in maniera diversa da quello del MAR ad oggi vigente.

Il MiCAR, dunque, nella misura in cui è stato disegnato sull'impronta del MAR, poggia sulla *efficient capital markets hypothesis* ("ECMH") nella quale la

---

*applicare loro tutte le disposizioni del regolamento (UE) n. 596/2014 del Parlamento europeo e del Consiglio. È pertanto necessario stabilire norme specifiche che vietino determinati comportamenti che potrebbero indebolire la fiducia dell'utente nei mercati di cripto-attività e l'integrità di tali mercati, compresi l'abuso di informazioni privilegiate, la divulgazione illecita di informazioni privilegiate e la manipolazione del mercato in relazione alle cripto-attività (…)*".

[16] Nello stesso senso Stefano LOMBARDO, *I mercati di cripto-attività e la disciplina degli abusi di mercato*, in *Cripto-Attività*, a cura di Filippo ANNUNZIATA e Antonella SCIARRONE ALIBRANDI, Il Mulino, Bologna, 2024, p. 194 ss., indica che "*è indubbio che l'apparato interpretativo, dottrinario e giurisprudenziale, sviluppato su MAR, possa essere, con le dovute differenze e gli accorgimenti del caso, utilizzato per l'interpretazione degli abusi di mercato nel contesto MiCAR*". L'Autore prefigura anche le problematiche connesse alla possibile contemporanea applicazione della disciplina MAR e MiCAR in presenza di un emittente che abbia sia strumenti finanziari che cripto-attività negoziati sui relativi mercati. In tali (futuri ed eventuali) casi, "*la prassi operativa fra le due discipline con la possibile contemporanea applicazione di entrambe porterà ad una verifica della ratio della tenuta della segmentazione attualmente imposta dalla disciplina*" (p. 195), considerata, *de facto* la sovrapposizione (p. 210) delle stesse.

Anche in Michele BENCINI, Luca FANFANI, *Prevenzione degli abusi di mercato relativi alle criptoattività*, in *Crypto-Asset, Regolamento MiCA e DLT Pilot Regime*, a cura di Stefano CAPACCIOLI e Marco Tullio GIORDANO, Giuffrè, Milano, 2023, p. 250 ss., si rileva che "*la scelta del legislatore europeo è stata quella di replicare per quanto possibile la normativa già esistente in materia di mercati finanziari. In particolare, tanto sul piano delle definizioni che su quello delle condotte vietate è agevole rilevare il tendenziale adattamento alle criptoattività delle disposizioni esistenti*" sugli abusi di mercato.

[17] Il testo del "*Regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) 2017/1129, (UE) n. 596/2014 e (UE) n. 600/2014 per rendere i mercati pubblici dei capitali nell'Unione più attraenti per le società e facilitare l'accesso delle piccole e medie imprese ai capitali*" (c.d. *Listing Act*) pubblicato nella GUUE il 13 novembre 2024, al Considerando n. 5 fa esplicito riferimento a "*onerosi obblighi di comunicazione continuativa di cui al regolamento (UE) n. 596/2014*", mentre il successivo Considerando n. 67 tratteggia la diversa tempistica per la comunicazione al pubblico delle informazioni privilegiate, disciplinata dal novellato art. 17 del MAR.

diffusione di informazioni corrette per il pubblico – per permettere ad un investitore ragionevole di investire con cognizione– è un pilastro fondante [18].

Ciò, immaginando anche che molte delle dinamiche che caratterizzeranno le negoziazioni sui mercati di cripto-attività saranno influenzate da *human behaviours* e dai connessi *bias* cognitivi [19], approfonditi dalla finanza comportamentale.

L'euforia e il panico che hanno caratterizzato storiche crisi finanziarie come ben ha insegnato Kindleberger [20] decenni fa, hanno del resto già contribuito a creare cicli alternati di entusiasmo e gelo nei confronti delle cripto-attività, questi ultimi noti appunti come fasi di *crypto-winter* [21], tali da far temere il passaggio paradossale da mercati senza regole a regole senza mercati, se gli operatori avessero rivolto al contempo altrove i propri investimenti per mancanza di fiducia, privando, tra l'altro, le imprese di innovative fonti di finanziamento. MiCAR si può prefigurare, appunto, come un intervento pubblico per la tutela di detta fiducia [22].

---

[18] Filippo ANNUNZIATA, *The Market Abuse Regulation and the Use of General Clauses Thereunder*, *Bocconi Legal Studies Research Paper Series*, Milano, 2024, p. 11, ricorda al riguardo che "*the fundamental point of intersection between the ECMH and the MAR is the assumption that the market is expected to behave according to an ideal model of efficient functioning in which operators act on the basis of paradigms of predictable rationality. In an efficient market, investment decisions are closely based on the assessment of relevant information available to investors and the ability of investors to process and translate this information into useful evaluations for investment choice*".

[19] Se ne veda la sistematica illustrazione in Nadia LINCIANO, *Errori cognitivi e instabilità delle preferenze nelle scelte di investimento dei risparmiatori retail*, in Quaderni di Finanza Consob (66), 2010, p. 6 ss. (in particolare nella Tav. 2).

[20] Charles P. KINDLEBERGER, *Euforia e panico, storia delle crisi finanziarie* (edizione italiana), Laterza, Bari, 1981. Si vedano anche i relativi brani riportati in P. SAVONA, *Kindleberger visto da Paolo Savona*, Collana *I momenti d'oro dell'economia*, Luiss University Press, Roma, 2009. L'Autore ricorda che il "*il processo che parte dalle bolle speculative e porta al panico e alla crisi, sempre a detta di CPK* (Charles Poor Kindleberger, nda), *prende avvio da impulsi esogeni, come l'introduzione di innovazioni tecnologiche (è il caso recente dell'information technology)*" (p. 53).

[21] I *crypto-winter* verificatisi all'inizio del corrente decennio a seguito di crisi di fiducia nei confronti del mercato delle cripto-attività conseguenti a fenomeni patologici e truffe, hanno corroborato l'avvio di iniziative di regolazione di tale ecosistema a livello trasnazionale. Ricorda detti *crypto-winter* Filippo ANNUNZIATA, *An overview of the Market in Crypto-Assets Regulation (MiCAR)*, *EBI Working Series*, 2023, p. 5 ss.

[22] Considerando n. 5 del MiCAR: "*L'assenza di un quadro generale dell'Unione per i mercati delle cripto-attività può portare gli utenti a non avere fiducia in tali attività, il che potrebbe rappresentare un notevole ostacolo allo sviluppo di un mercato delle cripto– attività e condurre alla perdita di opportunità in termini di servizi digitali innovativi, strumenti di pagamento alternativi o nuove fonti di finanziamento per le imprese dell'Unione*".

## 5. La nozione di informazione privilegiata concernente cripto-attività

Il Titolo VI del MiCAR si apre con l'individuazione dell'ambito di applicazione delle norme di tale titolo[23], a cui segue, all'art. 87, la definizione delle informazioni privilegiate rilevanti per la prevenzione e il divieto degli abusi di mercato relativi alle cripto-attività.

Al di là della declinazione al plurale ("informazioni privilegiate") in luogo di quella al singolare utilizzata nel MAR all'art. 7, i tratti distintivi delle due nozioni sono, come ampiamente anticipato, sovrapponibili.

Se, però, nella disciplina tradizionale le informazioni privilegiate concernono – direttamente o indirettamente – "*uno o più emittenti o uno o più strumenti finanziari*", nella disciplina del MiCAR queste riguardano non solo "*uno o più emittenti di cripto-attività*" e "*una o più cripto-attività*", ma anche gli "*offerenti o persone che chiedono l'ammissione alla negoziazione*" delle stesse.

Tale specifica è presente in entrambe le fattispecie dell'art. 87, Par. 1 del MiCAR, di cui alle lett. *a*, di riferimento per la *disclosure* al pubblico e *b*, relativa alle "*informazioni di natura precisa trasmesse da un cliente e commesse ad ordini pendenti in cripto-attività*" nel caso di persone incaricate dell'esecuzione di ordini; quest'ultima tipizzazione concerne, dunque le informazioni privilegiate sfruttate indebitamente nel c.d. *front running*.

Fatta questa premessa, i caratteri principali dell'informazione privilegiata concernente cripto-attività *sub* art. 87, Par. 1, lett. *a* del MiCAR sono analoghi a quelli della disciplina tradizionale e cioè l'informazione: (*i*) non è stata resa pubblica, (*ii*) concerne direttamente o indirettamente i soggetti sopra riportati, (*iii*) è precisa e (*iv*) se resa pubblica avrebbe un impatto sui prezzi delle cripto-attività o sul prezzo di una cripto-attività collegata[24].

Sarebbe difficile, se non impossibile, spiegare dette caratteristiche senza rifarsi alle indicazioni ampiamente approfondite in relazione all'art. 7 del MAR. Si rinvia, al riguardo, tra i tanti testi esplicativi, alle Linee Guida della Consob per la gestione e comunicazione al pubblico delle informazioni privilegiate dove tali caratteri sono ampiamente approfonditi (Sezione IV).

---

[23] Giuseppe Matteo MIRODDI, in *Tutela dell'integrità del mercato: le regole per prevenire gli abusi di mercato*, in *Il MICAR, Guida al Regolamento Europeo sui mercati delle cripto*, Giuffrè, Milano, 2023, p. 100 ss., ricorda che l'applicabilità del titolo VI del MiCAR è subordinata a presupposti di natura (*i*) personale, (*ii*) materiale e (*iii*) territoriale.

L'art. 86 del MiCAR ("*Ambito di applicazione delle norme in materia di abusi di mercato*") recita: "*(1) Il presente titolo si applica agli atti compiuti da qualsiasi persona in relazione a cripto-attività ammesse alla negoziazione o in relazione alle quali è stata presentata una richiesta di ammissione alla negoziazione. (2) Il presente titolo si applica a qualsiasi operazione, ordine o condotta relativi alle cripto-attività di cui al paragrafo 1, indipendentemente dal fatto che tale operazione, ordine o condotta avvenga in una piattaforma di negoziazione. (3) Il presente titolo si applica alle azioni e alle omissioni, nell'Unione e nei paesi terzi, riguardanti le cripto-attività di cui al paragrafo 1*".

[24] Non, però, ad un derivato ai sensi della disciplina c.d. Mifid II e perciò ricondotto sotto il cono d'ombra della *market abuse regulation* (vedi *supra*).

Anche la declinazione del concetto di precisione di cui all'art. 87, Par. 2 del MiCAR – si noti qui il riferimento al termine "natura" e non "carattere" viceversa presente nel MAR – avviene attingendo pressoché letteralmente dalla disciplina tradizionale.

Le informazioni, dunque, hanno natura precisa se (*i*) fanno riferimento a una serie di circostanze esistenti o che si può ragionevolmente ritenere che vengano a prodursi o a un evento che si è verificato o del quale si può ragionevolmente ritenere che si verificherà e se (*ii*) sono sufficientemente specifiche da permettere di trarre conclusioni sul possibile effetto di detta serie di circostanze o di detto evento sui prezzi delle cripto-attività.

In base all'opzione legislativa adottata, la disciplina MiCAR, dunque, è destinata prima a introiettare e poi a proiettare tutte le difficoltà interpretative della nozione dell'art. 7 del MAR[25].

La disciplina del MiCAR riprende (art. 87, Par. 3) anche la nozione di processo prolungato, con le relative tappe intermedie che possono rilevare come informazioni privilegiate autonome, se in possesso dei criteri descritti al Par. 2 ora richiamato.

Anche su tale profilo, dunque, gli interpreti delle norme del mercato delle cripto-attività dovranno attingere, a proprio supporto, alla dottrina ed alla giurisprudenza formatasi sui casi paradigmatici accaduti nei mercati finanziari tradizionali, come il celebre caso *Daimler*[26].

Proprio in relazione alle informazioni privilegiate caratterizzate da un processo prolungato articolato in tappe intermedie si è innestato il germoglio normativo che ha disegnato il nuovo *timing* di comunicazione al pubblico prefigurato nel *Listing Act*[27] – richiesto a valle del processo prolungato medesimo quando si verifica il c.d. evento finale – che differenzierà temporalmente, dunque, tale adempimento nel MAR rispetto al MiCAR.

Peraltro, il mancato esplicito riferimento in MiCAR, alla disciplina del ritardo della comunicazione al pubblico delle tappe intermedie di un processo pro-

---

[25] L'art. 7 del MAR a sua volta aveva elevato al primo livello normativo europeo le analoghe caratteristiche dell'informazione privilegiata stabilite all'art. 1 della previgente Direttiva 2003/124/CE della Commissione, di esecuzione della direttiva 2003/6/CE (nota anche come *market abuse directive* o MAD).

[26] Se ne veda il richiamo in Michele BENCINI, Luca FANFANI, *op. cit.*, p. 254.

[27] Considerando n. 67 del *Listing Act*: "*(…) L'obbligo di comunicare informazioni privilegiate mira principalmente a consentire agli investitori di assumere decisioni informate. Se le informazioni sono comunicate in una fase molto precoce e sono di natura preliminare, potrebbero indurre in errore gli investitori, piuttosto che contribuire a una formazione efficiente dei prezzi e a risolvere l'asimmetria informativa. Pertanto, in un processo prolungato, l'obbligo di comunicazione non dovrebbe riguardare gli annunci di semplici intenzioni, i negoziati in corso o, a seconda delle circostanze, i progressi dei negoziati, ad esempio una riunione tra rappresentanti di società. L'emittente dovrebbe comunicare solo le informazioni relative alle particolari circostanze o al particolare evento che si intendono concretizzare con il processo prolungato o che risultano da quest'ultimo ("evento finale"), il prima possibile dopo il verificarsi di tali circostanze o tale evento (…)*".

lungato ha corroborato interpretazioni evolutive concernenti la generale tempistica di comunicazione al pubblico ivi stabilita (vedi *infra*),[28] in linea con quella che sarà prevista nel MAR per gli emittenti strumenti finanziari.

## 5.1. Sul concetto di possessore di cripto-attività ragionevole

Con riferimento all'ultima delle caratteristiche prima riportate (*sub* iv), vale a dire l'idoneità delle informazioni se rese pubbliche ad avere un effetto significativo sui prezzi delle cripto-attività, questa si si rifà a ciò che un loro possessore "*ragionevole probabilmente utilizzerebbe come uno degli elementi su cui basare le proprie decisioni d'investimento*".

È stato rimarcato anche di recente, con riferimento alla disciplina tradizionale, che lo sfocato perimetro di detta nozione stride con la netta tipizzazione che dovrebbe assistere una normativa presidiata da un poderoso sistema sanzionatorio, in MAR anche di natura penale[29].

Con specifico riferimento alla disciplina MiCAR si rileva un'ulteriore peculiarità: a differenza dell'"*investitore ragionevole*", evocato nel MAR, viene individuata una diversa figura: quella del "*possessore di cripto-attività ragionevole*".

Anche per le cripto-attività vi è il riferimento, come sopra riportato, ad un soggetto ragionevole che effettua "*decisioni di investimento*"; tuttavia, concetti approfonditi e scandagliati dalla dottrina per la disciplina tradizionale, come quello dell'investitore *medio* ("*average investor*")[30] sembrano attagliarsi in maniera meno intuitiva: si pensi al concetto di *possessore medio*.

È stato anche posto in evidenza, al riguardo, con riferimento agli *utility token*[31], come "*la realizzazione di un guadagno da negoziazione non solo si presenta*

---

[28] Stefano LOMBARDO, *op. cit*., p. 201 ss. Lo stesso Autore, nel contesto, ipotizzava che l'ESMA nell'implementare le norme tecniche di attuazione sulla comunicazione ed il ritardo potesse "*colmare eventuali lacune dovute all'assenza di disciplina*", come poi avvenuto a livello esplicativo in sede di *assessment* normativo nella predisposizione dei progetti di norme tecniche di attuazione del MiCAR (vedi *infra*).

[29] Filippo ANNUNZIATA, in *The Market Abuse Regulation and the Use of General Clauses Thereunder*, cit., p. 18, riporta che "*the apparent vagueness of the concept, set in a regulatory context marked by a significant repressive apparatus whose effects can lead to criminal consequences, also raised the problem, in Italy, of the constitutionality of the regime, for violation of the principle of legal certainty due to an insufficient clarity and lack of defined criteria*". L'Autore ricorda anche che la Corte costituzionale, nel 2004, aveva valutato inammissibili (da un punto di vista procedurale) le censure di alcuni giudici ordinari *a quibus* in merito all'insufficiente determinatezza della parte rilevante della disciplina sull'*insider trading* all'epoca contenuta nel Testo Unico della Finanza (art. 180).

[30] Si vedano gli approfondimenti di Matteo ARRIGONI, in *Informazioni privilegiate e funzionamento dei mercati finanziari*, Giuffrè, Milano, 2022, p. 100 ss.

[31] Ai sensi dell'art. 3, Par. 1, comma 9 del MiCAR gli *utility token* sono "*un tipo di cripto-attività destinato unicamente a fornire l'accesso a un bene o a un servizio prestato dal suo emittente*".

*del tutto eventuale, ma risulta svincolata dall'andamento del valore «oggettivo» o «intrinseco» dell'impresa emittente, dipendendo piuttosto dalle oscillazioni di un valore «soggettivo» ed «esterno»: quello convenzionalmente attribuito al token dalla comunità di utenti e di partecipanti al mercato in cui esso viene negoziato*" [32].

Si può ipotizzare che il legislatore europeo abbia inteso enfatizzare il fatto che la scelta di *possedere* talune tipologie di cripto-attività possa essere determinato da motivazioni prevalenti rispetto a quella speculativa: si pensi agli *utility token* aventi caratteristiche di *fan token*, i cui possessori beneficiano dei servizi e prestazioni del proprio *team* sportivo del cuore o dei propri artisti preferiti (vedi anche *infra*) [33].

Per altro verso, avendo a mente anche la definizione di informazione privilegiata concernente cripto-attività, "*il riferimento al «reasonable holder», pur confermando l'irriducibilità dell'ecosistema digitale alla logica dell'investitore ragionevole, appare al tempo stesso talmente sfumato da diventare quasi evanescente e da compromettere la concreta operatività del concetto di informazione privilegiata, ove rapportata alle cripto-attività*" [34].

Il concetto di possessore di una cripto-attività potrebbe, comunque, essere inteso in senso ampio, così da ricomprendere sia chi detiene (o intendesse detenere) cripto-attività per finalità di investimento, sia chi le detiene (o intendesse farlo) per prevalenti ragioni non speculative, in quest'ultimo caso senza negare che questi possa comunque beneficiare economicamente da una negoziazione delle stesse.

In questo senso, la dicotomia concettuale tra possessore ragionevole ed investitore ragionevole verrebbe ad elidersi, perché il secondo sarebbe comunque ricompreso nel primo.

---

[32] Marco MAUGERI, *Cripto-attività e abusi di mercato*, Osservatorio del diritto civile e commerciale, Il Mulino Rivisteweb, Bologna, settembre 2022 (fascicolo speciale), p. 431.

[33] Peraltro, anche i possessori di titoli azionari talvolta sono attraversati da sentimenti di affezione e appartenenza alla *societas*, beneficiando anche di correlati servizi e benefici.

[34] Marco MAUGERI, *op. cit.*, p. 432. Lo stesso Autore, ha altresì indicato che "*non è dubbio che anche il titolare di utility-token possa perseguire un profitto «da negoziazione», e quindi un «investimento in senso lato», mediante la cessione sul mercato della cripto-attività. La trasferibilità del token e la conseguente esposizione del possessore a un rischio di natura finanziaria – all'eventualità, cioè, di conseguire in sede di vendita una somma inferiore all'importo di capitale inizialmente impiegato – costituisce, anzi, un tratto ineliminabile della fattispecie, senza il quale viene meno l'esigenza stessa di applicare la disciplina MiCAR in tema di abusi di mercato. Tuttavia, neppure accedendo a questa lettura si avrebbe un accostamento strutturale o funzionale del token di «pura» utilità alle azioni e alle obbligazioni o, più in generale, ai security-token: in vero, di là dalla questione se nel caso delle cripto-utilità negoziabili prevalga il fine speculativo o invece quello di consumo, devono comunque dirsi estranei alla causa tipica degli utility-token sia uno scopo di finanziamento dell'emittente (atteso che non ricorre un diritto alla restituzione del capitale versato), sia uno scopo di investimento nell'emittente (atteso che non ricorre un interesse alla percezione periodica dei flussi di cassa generati dall'impresa)"* (p. 428 ss.).

## 5.2. Alcune ipotesi di informazioni privilegiate concernenti cripto-attività

Le informazioni privilegiate concernenti cripto-attività presentano notevoli elementi di interesse, perché alcune di queste sono specifiche e correlate all'infrastruttura tecnologica di supporto dell'*asset* digitale di cui si discute, alla scrittura del relativo codice ed alle possibili modifiche al protocollo: si pensi al mal funzionamento, rallentamento o addirittura attacco malevolo ad una *block-chain*, alle implementazioni di *layer* di secondo livello che aggiungono nuove funzionalità o migliorano le transazioni sul protocollo principale, alle modifiche al meccanismo di consenso (con conseguenti impatti sulla sicurezza della rete) o alle modalità di emissione di nuovi *token*.

Naturalmente per una *software-house* con titoli negoziati in Borsa, la notizia di un *bug* della *blockchain* di proprietà in generale potrebbe rilevare ai fini degli adempimenti informativi dell'art. 17 del MAR, considerato anche il presumibile impatto di una simile informazione sull'andamento dei titoli azionari.

Per gli *utility token*, specifiche informazioni privilegiate possono essere collegate alla maggiore o minore appetibilità dei beni o servizi prestati dal loro emittente. Nei *token* dedicati ai *fan* sportivi o *fan* token (qualora venissero ammessi alle negoziazioni su piattaforme di scambio rilevanti per il MiCAR) – o comunque per gli *utility token* aventi caratteristiche analoghe – ad esempio, ciò che incide sulle prestazioni del *team* sportivo (l'acquisto o cessione di un atleta chiave, ad esempio[35]), potrebbe incidere sulla loro domanda e offerta su un mercato secondario[36].

Specifiche ipotesi di informazioni privilegiate sembrano individuarsi nell'art. 30 del MiCAR, che prevede alcuni obblighi di *Informazione continua dei possessori di token collegati ad attività*, il cui Par. 3, dispone che: "*Fatto salvo l'articolo 88, gli emittenti di token collegati ad attività pubblicano in una posizione del proprio sito web facilmente accessibile al pubblico, non appena possibile e in modo chiaro, preciso e trasparente, informazioni su qualsiasi evento che abbia o possa avere un effetto significativo sul valore dei token collegati ad attività o sulla riserva di attività di cui all'articolo 36*".

L'articolo ora citato fa, appunto, salva l'applicazione dell'art. 88: dunque, eventi potenzialmente pregiudizievoli delle riserve di attività degli *asset referenced token* sono inquadrabili, in presenza delle caratteristiche dell'art. 87 del MiCAR, tra le informazioni privilegiate; su tale disciplina di tornerà anche in seguito.

---

[35] Michele De Mari, *Le cripto-attività nella disciplina MiCAr e la finanziarietà delle "cripto-attività non finanziarie"*, in *Dialoghi di Diritto dell'Economia*, II, 2023, p. 197, a proposito dei riflessi finanziari correlati all'apprezzamento (o al deprezzamento) dei *fantoken*, cita proprio il caso del notevole aumento di valore di un *token* di una importante squadra di calcio francese registrato nell'agosto del 2021 in occasione dell'acquisto di un notissimo calciatore.

[36] Qualora la stessa società sportiva avesse titoli negoziati, così da essere assoggettata anche al MAR, le stesse informazioni potrebbero rilevare ai sensi degli artt. 7 e 17 del medesimo Regolamento, prefigurando una possibile sovrapposizione delle due discipline, come segnalato nel presente lavoro.

È stato già rilevato come "*appare limitata la rilevanza delle informazioni concernenti i dati contabili e finanziari degli emittenti*"[37], quanto meno quando queste non concernino aspetti vitali degli stessi tali da impattare sulla loro esistenza o ordinaria attività di impresa.

Viceversa, talune vicende delle persone fisiche di riferimento degli emittenti (come degli offerenti o di coloro che chiedono l'ammissione alla negoziazione di una cripto-attività) – si pensi ad esempio a quelle giudiziarie – potrebbero rilevare ai sensi dell'art. 88 di MiCAR, specie se arrivassero ad intaccare le formali e sostanziali capacità di amministrare l'impresa emittente.

Infine, è stato rilevato che ulteriori speciali tipologie di informazioni privilegiate concernenti cripto-attività possono essere detenute – se non anche generate – da determinati *miners* in qualità di soggetti potenzialmente in una posizione privilegiata nell'ambito, ad esempio, di modifiche al funzionamento dei protocolli. Tali informazioni possono integrare la fattispecie di cui all'art. 87 del MiCAR, mentre bisognerà valutare, la riferibilità diretta di dette informazioni ai soggetti tenuti agli obblighi informativi di cui al seguente art. 88, ai fini della eventuale loro *disclosure*[38].

## 6. La disciplina sulla comunicazione al pubblico di informazioni privilegiate

L'art. 88 del MiCAR è il cuore della disciplina sulla *disclosure* in continua al pubblico delle informazioni privilegiate che, come anticipato, si applica a (*i*) gli emittenti (*ii*) gli offerenti e (*iii*) le persone che chiedono l'ammissione alla negoziazione di cripto-attività. L'obbligo di comunicazione al pubblico riguarda le informazioni che "*riguardino direttamente*" tali soggetti (vedi anche *infra* per i chiarimenti forniti dall'ESMA).

Come ereditato dalla disciplina tradizionale[39], detto riferimento restringe la tipologia di informazioni privilegiate di cui all'art. 87 del MiCAR che devono essere oggetto di comunicazione al pubblico o, come si vedrà tra poco, che possono essere oggetto della procedura di ritardo.

Se, con riferimento alla disciplina tradizionale, sono contemplate le categorie di *corporate information* e di *market information*, in MiCAR la più ampia categoria di soggetti tenuti agli obblighi informativi potrebbe portare a non ritenere

---

[37] Marco MAUGERI, *op. cit.*, p. 419.

[38] Marco MAUGERI, *op. cit.*, p. 418 ss. L'Autore cita anche il caso dei *wallet providers*, in quanto possibili conoscitori degli ordini degli utenti, ipotesi specialmente rilevante per ciò che concerne le condotte di *front running* (art. 87, Par. 1, lett. *b* del MiCAR) piuttosto che per l'adempimento ad obblighi informativi.

[39] Anche in questo caso forniscono un valido ausilio le Linee Guida della Consob per la gestione delle informazioni privilegiate (Par. 4.2).

esaustivo il richiamo alle informazioni c.d. *corporate* in senso stretto e tale nozione non si attaglierebbe del tutto agli offerenti ed alle persone che chiedono l'ammissione alle negoziazioni.

Per altro verso, oggetto dell'obbligo informativo sono le informazioni privilegiate di cui all'art. 87 comunque riferite alle cripto-attività, dovendo riguardare, ad esempio, circostanze o un evento in maniera sufficientemente specifica da permettere di trarre conclusioni sul loro possibile effetto sui prezzi delle cripto-attività, come prima riportato.

Da un punto di vista temporale, inoltre, è plausibile ritenere che gli obblighi di informativa continua per gli offerenti ed i soggetti che chiedono l'ammissione alle negoziazioni di una cripto-attività nel corso del tempo si affievoliscano fino a scomparire, anche se la formulazione comunque ampia dell'art. 87 della nozione di informazione privilegiata sconsiglia sul punto eccessiva assertività; nell'ipotesi, ad esempio di un contenzioso giudiziario sorto successivamente all'avvio delle negoziazioni per vicende connesse alle cripto-attività, pare potersi ammettere che i soggetti prima citati debbano fornire i relativi aggiornamenti al pubblico (o possano attivare la procedura di ritardo nella comunicazione, se le condizioni lo consentono), se in presenza dei caratteri dell'informazione privilegiata sopra descritti.

Ai sensi di MiCAR, le informazioni devono essere comunicate "quanto prima" e non "quanto prima possibile"; il testo in inglese del MiCAR, indica, però, che l'obbligo informativo deve essere adempiuto "*as soon as possible*" [40].

Si tratta dunque di una mera disarmonia in sede di traduzione dei testi che ragionevolmente verrà corretta in futuro dal legislatore eurounitario che sconsiglia ulteriori considerazioni circa una diversa tempistica di comunicazione al pubblico prevista nel MiCAR rispetto a quella del MAR.

Le informazioni devono essere comunicate in modo da consentire al pubblico di accedervi rapidamente e di valutarle in modo completo, corretto [41] e tempestivo.

Il Regolamento 2024/2861, come anticipato, stabilisce le norme tecniche di attuazione per l'applicazione del MiCAR "*per quanto riguarda gli strumenti tecnici per l'adeguata comunicazione al pubblico delle informazioni privilegiate e la comunicazione al pubblico tardiva di tali informazioni*" [42].

---

[40] Non potendo qui approfondire la tematica della tempistica attesa per la pubblicazione delle *insider information*, si rinvia all'ampia disamina offerta, anche in termini di una comparazione linguistica tra le varie versioni del MAR sul tema, in Filippo ANNUNZIATA, *'Madamina, il catalogo è questo ...' la disclosure delle informazioni privilegiate, tra regole speciali e disciplina dell'organizzazione d'impresa*, in *Diritto della banca e del mercato finanziario*, 3/2020, p. 438 ss.

[41] Una declinazione esplicita dell'obbligo di correttezza si ritrova nella necessità che "*gli emittenti, gli offerenti e le persone che chiedono l'ammissione alla negoziazione non coniugano la comunicazione di informazioni privilegiate al pubblico con la commercializzazione delle loro attività*" come recita lo stesso art. 88, Par. 1 del MiCAR.

[42] Tale Regolamento è stato pubblicato dopo che l'ESMA, chiamata ad elaborare e presentare alla Commissione i progetti di norme tecniche di attuazione ai sensi dell'art. 88, Par. 4, del Mi-

Tale disciplina, all'art. 1, specifica che tali strumenti tecnici devono consentire una diffusione delle informazioni: (a) su base non discriminatoria a una platea il più possibile ampia, (b) a titolo gratuito e (c) simultaneamente in tutta l'Unione.

Fermo considerata la necessità di rispettare quanto ora riportato, l'art. 2, in maniera innovativa rispetto al MAR, valorizza come strumenti per la *dissemination* delle informazioni privilegiate, non solo (*i*) i *media* tradizionali su cui fa affidamento il pubblico, ma anche i (*ii*) *social media* e (*iii*) le piattaforme basate sul web che raccolgono e diffondono dati e informazioni sulle cripto-attività.

A questi mezzi di comunicazione, in maniera opzionale, può aggiungersi l'utilizzo delle (*iv*) le piattaforme di *trading* di cripto-attività [43].

Nel documento di consultazione del 5 ottobre 2023 l'ESMA aveva così motivato queste innovative soluzioni [44]: "*taking into consideration the sources normally used by the crypto community to collect information, ESMA proposes in the ITS*

---

CAR, ha prima pubblicato il 5 ottobre 2023 un *Consultation Paper – Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation (MiCA) – second consultation paper* e, il 3 luglio 2024, a valle della consultazione, ha diffuso il relativo *Final Report* di sintesi e valutazione delle osservazioni pervenute, con la definizione del progetto di norme finale.

[43] Art. 1, Par. 2, del Regolamento 2024/2861: "*Per garantire una diffusione efficace, gli emittenti, gli offerenti e le persone che chiedono l'ammissione alla negoziazione comunicano le informazioni privilegiate, direttamente o tramite terzi, ai mezzi di informazione sui quali il pubblico fa ragionevole affidamento, tra cui uno o più dei seguenti: a) mezzi di informazione tradizionali; b) social media che consentono la pubblicazione in forma scritta; c) piattaforme basate sul web che consentono la pubblicazione di notizie relative a emittenti, offerenti o persone che chiedono l'ammissione alla negoziazione di cripto-attività. Le informazioni privilegiate relative a cripto-attività ammesse alla negoziazione su una piattaforma di negoziazione di cripto-attività possono essere pubblicate sul sito web di tale piattaforma quando tale pubblicazione è messa a disposizione degli emittenti o degli offerenti dalla piattaforma stessa*".

[44] Cfr. *Consultation Paper*, cit., p. 69 ss. ed in particolare i Parr. 292 e ss. Nei precedenti Parr. 273 e 274 l'ESMA si è invece soffermata, come anticipato, sulle strette analogie tra la disciplina MAR e quella MiCAR, in tema di informazioni privilegiate e loro comunicazione e gestione, indicando che: "*(274). The definitions of inside information provided in both Article (87)(1)(a) of MiCA and Article 7(1)(a) of MAR are nearly identical (the only difference being the instruments in scope, i.e., financial instruments vs. crypto-assets). The duty of relevant parties to inform the public about inside information is also analogous in nature in both Article 17(1) of MAR and Article 88(1) of MiCA. (…). (275) Furthermore, MiCA and MAR have comparable requirements regarding the delayed disclosure of inside information (…)".* Sempre con riferimento ai chiarimenti di carattere generale, inoltre l'ESMA ha indicato che ciascun soggetto tenuto a comunicare le informazioni privilegiate deve limitarsi a rendere note solo quelle lo concernono direttamente, anche per scongiurare il rischio di molteplici e potenzialmente nel complesso poco chiare comunicazioni pubbliche sulle medesime informazioni: "*(280) In addition, the MiCA text diverges from MAR by extending the scope of parties subject to the disclosure obligation to include "offerors and persons seeking admission to trading" (in addition to issuers). As Article 88(1) of MiCA provides for all the three categories of persons to disclose information that "directly concerns them", ESMA is of the view that the provision requires each relevant party to disclose only information about facts regarding them directly. Any different reading foreseeing also the disclosure of information regarding the other relevant parties would result in potentially multiple disclosures by different sources on to the same fact, with messages potentially not fully aligned, to the detriment of publications clarity*".

*to add some specific media for dissemination of inside information related to crypto assets, which are not foreseen under the MAR ITS* (…). *In particular, the MiCA ITS specifies that the media reasonably relied upon by the public could also be social media and web-based platforms. In respect to social media, ESMA notes that they are often the fora where crypto investors engage in discussions to exchange information on crypto assets. In this respect, they may represent a useful tool to reach the relevant public for the purpose of communicating inside information*" (Parr. 292 e 293) [45].

All'attività di *dissemination* deve affiancarsi la pubblicazione delle stesse informazioni sul sito internet dei soggetti tenuti all'adempimento informativo, da potersi raggiungere anche tramite *link* per poter effettuare il *download* del relativo testo. Il Par. 4 del Regolamento di esecuzione, infatti, recita che: "*La pubblicazione di informazioni privilegiate sui social media, sulle piattaforme basate sul web o sul sito web di una piattaforma di negoziazione di cripto-attività contiene un link alla dichiarazione scritta pubblicata sul sito web dall'emittente, dall'offerente o dalla persona che chiede l'ammissione alla negoziazione*".

Il Regolamento (art. 2, Par. 1, lett. *e*) fornisce anche indicazioni circa la lingua che deve essere utilizzata per la predisposizione di tali comunicati, indicando che il richiamato sito web "*fornisce le informazioni privilegiate nella lingua in cui è redatto il White Paper sulla cripto-attività e, ove possibile, in una lingua comunemente utilizzata negli ambienti della finanza internazionale* [46].

## 7. Il ritardo della comunicazione al pubblico di informazioni privilegiate

La disciplina sul ritardo della comunicazione al pubblico di informazioni privilegiate è collocata nei Parr. 2 e 3 dell'art. 88 del MiCAR ed anche in questo caso ricalca quella prevista per i mercati finanziari all'art. 17, Par. 4, del MAR; ciò, sia con riferimento alle condizioni per poter attivare la procedura di ritardo, vale a dire (*i*) possibile pregiudizio di un legittimo interesse, (*ii*) probabile assenza di effetti fuorvianti per il pubblico e (*iii*) tenuta della riservatezza delle informazioni, sia per ciò che concerne la notifica all'Autorità competente, a valle

[45] Sempre nel medesimo documento è riportato che (Par. 294): "*ESMA also acknowledges that one of the main tools used by crypto investors to make informed decisions are web-based platforms that aggregate information and/or data on crypto-assets. (…). As investors regularly use such web-platforms to collect information on crypto-assets, the ITS includes them within the means for dissemination, in those cases where the platform provides for the possibility to publish news (i.e., a real-time news feed related to a crypto-asset)*".

[46] Tale prescrizione è spiegata al Par. 289 del *Consultation Paper* dell'ESMA, dove è riportato, tra l'altro, che "*It is worth noting that at the time of writing the English language is the language customary in the sphere of international finance. The provision is included to facilitate the access to inside information by investors who do not speak the national language of the issuers, offerors and persons seeking admission to trading*".

della comunicazione al pubblico delle informazioni privilegiate, della precedente attivazione della procedura di ritardo in parola [47].

L'art. 18, comma 2, del d.lgs. n. 129/2024, analogamente a quanto previsto dall'art. 114, comma 3, del TUF, ha al riguardo specificato che i soggetti che hanno ritardato la comunicazione al pubblico delle informazioni privilegiate trasmettano la documentazione comprovante l'assolvimento degli obblighi previsti da MiCAR (cioè, il rispetto delle condizioni richieste dalla normativa), solo su richiesta della Consob.

Come parzialmente anticipato, non tutta la disciplina del ritardo descritta nel MAR è stata trasposta in MiCAR.

Si fa, in particolare riferimento a (*i*) a quanto previsto per il c.d. processo prolungato, che ha portato un Autore anche ad ipotizzare che le c.d. fasi intermedie, in MiCAR, non debbano essere oggetto di comunicazione al pubblico, anticipando, nell'ottica di agevolare le PMI, il *timing* di comunicazione che, come detto, il *Listing Act* scandirà nel novellato art. 17 del MAR [48].

Lo stesso commentatore ha segnalato come la disciplina del ritardo, in MiCAR, sia priva di ulteriori "*due elementi capisaldi che nel MAR garantiscono il rispetto del principio fondante e ispiratore della disciplina market abuse di stampo europeo*" [49], vale a dire (*ii*) la circostanza che la presenza di voci o indiscrezioni accurate, riferibili ad informazioni privilegiate, sia un indice di rottura della riservatezza così da imporre la pubblicazione delle stesse e (*iii*) il fatto che la comunicazione lecita di informazioni privilegiate a chi non sia tenuto alla confidenzialità determini anch'esso l'obbligo di pubblicare dette informazioni.

Un ulteriore importante elemento di distinzione tra la disciplina di MiCAR e quella del MAR concerne il c.d. ritardo sistemico (non presente nel primo), di cui si dirà in seguito.

In entrambe le ipotesi *sub* ii e iii l'emittente, ai sensi del MAR, deve procedere con la comunicazione al pubblico delle informazioni privilegiate.

L'ESMA, nell'*assessment* della disciplina di MiCAR nel documento di consultazione prima citato, si è comunque espressa nel senso di ricondurre la tempistica della comunicazione al pubblico delle informazioni privilegiate concernenti cripto-attività secondo il metronomo del MAR, con riferimento alle tappe intermedie di un processo prolungato ed alla presenza di *rumours* specifici che siano indici di una rottura della confidenzialità [50].

---

[47] La disciplina del ritardo della comunicazione al pubblico delle informazioni privilegiate nei mercati finanziari presenta vari degli aspetti di interesse, ampiamente approfonditi dalla dottrina. Si veda, al riguardo, Matteo ARRIGONI, in *Informazioni privilegiate e funzionamento dei mercati finanziari*, cit., p. 139 ss., e, con particolare riferimento alla configurabilità di un ritardo *solo* tecnico, in funzione degli adempimenti necessari alla *disclosure*, Filippo ANNUNZIATA, *'Madamina, il catalogo è questo ...'*, cit., p. 437 ss.

[48] Stefano LOMBARDO, *op. cit*., p. 201.

[49] *Ibidem*.

[50] *Consultation paper*, cit., p. 71: "*(277) Although MiCA does not address delayed disclosures in*

Con riferimento alla *disclosure* selettiva di informazioni privilegiate ad un soggetto che non sia tenuto ad un obbligo di confidenzialità, per quanto la soluzione indicata nel MAR prevenga in anticipo il rischio di una rottura, anche sostanziale, della confidenzialità, tale soluzione porterebbe ad un aggravio operativo non richiesto per le società– tra cui le PMI – assoggettate agli obblighi informativi in MiCAR.

Naturalmente, una *manifesta* rottura della confidenzialità dell'informazione – con la conseguente propalazione di voci sul mercato – determinerebbe comunque l'obbligo di effettuare una comunicazione al pubblico in base a quanto indicato in precedenza (nel presupposto indefettibile, almeno dal punto di vista del corretto modo di agire, che sia stata attivata in precedenza la procedura di ritardo). A ben vedere, tuttavia, ciò dovrebbe accadere anche in MAR, qualora l'obbligo di confidenzialità venisse in concreto poi disatteso e ne conseguisse la diffusione di indiscrezioni specifiche.

Preso anche atto di tali varie ipotesi interpretative, con riferimento al differente trattamento del MiCAR rispetto a quello del MAR nell'ipotesi ora descritta, "*the reasons for this omission are not fully understandable*" [51].

In maniera ancor più eclatante, MiCAR non contempla la speculare procedura di ritardo della comunicazione al pubblico delle informazioni privilegiate di possibile impatto sistemico, attivabile ai sensi dell'art. 17, Par. 5, del MAR, dagli enti creditizi o istituti finanziari nei mercati finanziari.

Quanto meno per i *token* di moneta elettronica, la cui offerta al pubblico ed ammissione alle negoziazioni è riservata dall'art. 48, Par. 1, lett. *a* del MiCAR agli enti creditizi ed agli istituti di moneta elettronica, una disciplina analoga potrebbe essere, viceversa, prefigurabile, così come per i *token* collegati ad attività [52], consi-

---

*the case of a 'protracted process' (as is the case in Article 17(4) of MAR), Article 87 of MiCA does bring protracted processes and their intermediate steps within the scope of 'inside information'. Therefore, ESMA concludes that under MiCA the same conditions applicable to the delay of disclosure of inside information would apply in cases of a protracted process. (278) Rumours are not addressed in the same way in the two regulations. In case of delayed disclosure, Article 17(7) of MAR explicitly requires issuers to immediately disclose the inside information whenever the confidentiality of that inside information is no longer ensured. While under MiCA confidentiality remains a condition for the relevant parties to delay the disclosure, it is worth noting that the Level 1 text does not include a specific paragraph on breach of confidentiality or rumours. (279) However, ESMA's reading of the provision for delayed disclosure under MiCA remains that a breach of confidentiality would require the relevant party to proceed with the disclosure of inside information to the public as soon as possible. As delayed disclosure is an exception to the general obligation to ensure transparency, the delay is possible only when the relevant conditions are met throughout the delayed disclosure process. When one of these conditions – in this case confidentiality – is no longer met, the exemption is no longer applicable and the general obligation to disclose applies. Consequently, any case of breach of confidentiality, including the occurrence of rumour which explicitly relates to inside information under delay, would require immediate disclosure from the relevant party*".

[51] Filippo ANNUNZIATA, *An overview of the Market in Crypto-Assets Regulation,* cit., p. 65.

[52] Il Considerando n. 4 del Regolamento delegato (UE) 2024/1506 della Commissione che integra il MiCAR precisando taluni criteri per classificare i *token* collegati ad attività e i *token* di moneta elettronica come significativi, indica, tra l'altro, che "*le operazioni transfrontaliere, in particolare quelle associate agli usi come mezzo di scambio, sono le operazioni a carattere internazionale*

derato che anch'essi possono essere inquadrabili nel novero delle c.d. *stable-coins*, su cui anche la relazione alla proposta di MiCAR della Commissione Europea si era soffermata, riconoscendone la possibilità per talune di queste diventare ampiamente accettate e, dunque, "*potenzialmente sistemiche*" [53].

Del resto, già da tempo sono stati indagati i fondamenti teorici e storici della pericolosità sistemica delle critpo monete [54].

Anche per questo motivo è stato indicato che la mancanza di tale specifica disciplina "*is not to justify*" [55].

Rimane infine, sullo sfondo, la possibile sovrapposizione delle due discipline con conseguenze ad oggi non ancora valutabili [56].

## 8. Cenni sulla ulteriore disciplina del Titolo VI del MiCAR

Il Titolo VI del MiCAR concerne, come anticipato, sia la prevenzione che il divieto degli abusi di mercato relativi alle cripto-attività.

Con riferimento alle c.d. *preventive measures*, si segnala l'assenza di una disciplina analoga a quella prevista per il registro delle persone che hanno accesso ad informazioni privilegiate (art. 18 del MAR) e della comunicazione delle operazioni effettuate da persone che esercitano funzioni di amministrazione, di controllo o di direzione (art. 19 del MAR).

Venendo invece alle condotte vietate, gli artt. 89 e 90 del MiCAR prevedono il divieto di abuso di informazioni privilegiate, reprimendo le tre *classiche* con-

---

*che presentano maggiori probabilità di comportare rischi per la stabilità finanziaria, la trasmissione della politica monetaria e la sovranità monetaria dell'Unione. Tali operazioni riflettono anche l'attività internazionale di un emittente di token collegati ad attività o di token di moneta elettronica su scala internazionale al di fuori dell'Unione in relazione al loro utilizzo per pagamenti e rimesse*".

[53] Relazione alla proposta del MiCAR, p. 3. In tale documento si legge che uno degli obiettivi della proposta stessa "*è garantire la stabilità finanziaria. Le cripto-attività sono in continua evoluzione. Mentre alcune hanno una portata e un uso piuttosto limitati, altre, come la categoria emergente degli stablecoin, hanno le capacità per diventare ampiamente accettate e potenzialmente sistemiche. La proposta comprende misure di salvaguardia per far fronte ai potenziali rischi per la stabilità finanziaria e la politica monetaria ordinata che potrebbero scaturire dagli stablecoin*".

[54] Cfr. Paolo SAVONA, *Criptomonete, al di là della sovranità monetaria*, Milano Finanza, Milano, 2021, p. 69 ss.

[55] Filippo ANNUNZIATA, *An overview of the Market in Crypto-Assets Regulation*, cit., p. 64: "*This is an omission that is not to justify, since MiCAR itself assigns to certain subjects, in particular issuers of ARTs and EMTs, a risk profile of even systemic importance. Moreover, the regulation of such entities is, as already mentioned, strongly modelled on the classic standards of prudential supervision, which would have made it logical to extend the relevant MAR rules also to the regulatory environment of markets in crypto-assets*".

[56] Stefano LOMBARDO, *op. cit*., p. 202, ipotizza il caso di un istituto di credito che ritardi la comunicazione al pubblico di informazioni privilegiate ai sensi dell'art. 17, Par. 5, del MAR che possono riguardare anche cripto-attività.

dotte di *insider trading*[57], *tuyautage* (art. 89) e *tipping* (art. 90); quest'ultimo ampiamente oggetto di approfondimento dalla dottrina per ciò che concerne l'ammissibilità di flussi comunicativi selettivi nei mercati finanziari, ad esempio nei confronti dei soci di controllo[58].

È stato già illustrato entro quali (stretti) limiti la disciplina di MiCAR trovi applicazione anche per gli NFT. L'esperienza oltreoceano ha peraltro evidenziato come anche queste particolari cripto-attività possono essere oggetto di condotte di abuso, quanto meno analoghe all'*insider trading*[59].

Considerato che le sanzioni amministrative sono perseguibili anche in ragione di condotte colpose, chissà, al riguardo, se le nuove tecnologie non possano, in generale, fornire uno strumento privato di prevenzione di nuova generazione. Ci si riferisce in particolare al *Zero Knowledge Proof* ("ZKP"), "*strumenti/protocolli che offrono una possibilità a prima vista paradossale, cioè consentono ad un soggetto di dimostrare ad un altro di conoscere un'informazione con certe proprietà, senza rivelare l'informazione*"[60].

---

[57] Ricordando i primi dibattiti sulla materia, ed a prescindere dalla negoziabilità o meno di certe tipologie di cripto attività su MiCAR, Andrew VERSTEIN, in *Crypto Assets and Insider Trading Law's Domain*, in *Iowa L. Rev*. 1 (2019), p. 17 ss., ricordava che "*It is common to believe that insider trading law and crypto assets do not fit together. The main insider trading theories for securities require the breach of a duty of trust or confidence and material non-public information, but many crypto assets seem to lack "issuers" or "shareholders" whose trust can be betrayed, or officers or directors who can commit a betrayal*". Tali considerazioni sono state riprese anche da Marco MAUGERI, *op. cit*., p. 431. La conclusione a cui Verstein giunge è che "*the point is that cryptocurrency is a perfectly sensible subject of insider trading regulation, and it is a policy decision whether to ratify that existing status*".

[58] Si ricordano, al riguardo, le Q&A della Consob pubblicate 18 marzo del 2021, intitolate "*Q&A sull'informazione selettiva nei confronti dei soci e, in particolare, del socio di controllo, nonché sulla pubblicazione delle informazioni privilegiate relative ai piani industriali*".

[59] Nicola MAINIERI, Nico Di GABRIELE, in *Utilizzi a scopi illeciti delle criptovalute: recenti profili giurisprudenziali e normativi italiani ed internazionali e riferimenti al mercato degli NFT*, in *Giurisprudenza Penale WEB*, 2022 (6), p. 11 ss., ricordano che il 1° giugno 2022 il Dipartimento della Giustizia americano ha annunciato la richiesta di rinvio a giudizio a carico di un *ex dirigente* di una società attiva nella commercializzazione di NFT, denominata OpenSea, per frode perpetrata con strumenti di comunicazione (c.d. '*wire fraud*') e riciclaggio. Il Dipartimento della Giustizia ha contestato all'indagato l'acquisto di 45 NFT prima che gli stessi – o altre opere d'arte digitale del medesimo *creator* – venissero pubblicizzati sulla pagina web della OpenSea e, pertanto, prima che il loro prezzo di mercato crescesse significativamente. "*L'indagato avrebbe frodato il suo datore di lavoro con l'uso indebito di informazioni confidenziali cui aveva accesso in ragione del suo ruolo di incaricato della gestione delle aste di NFT*". Successivamente, nel 2023, lo stesso *ex dirigente* è stato condannato per tali fatti ed i proventi dell'illecito sono stati confiscati.

[60] I protocolli ZKP, ove specificamente sviluppati, potrebbero un domani supportare i sistemi di tenuta della confidenzialità delle informazioni anche degli emittenti negoziati nei mercati finanziari. Di tali protocolli tratta diffusamente Francesco BRUSCHI, *Decentralizzare o regolamentare? Il paradosso apparente dei mercati secondari su blockchain*, in *La tecnologia blockchain come strumento per la democratizzazione dell'accesso alla gestione dei capitali* (*discussion paper)*, FutureW3B, 2023, p. 33.

I protocolli ZKP sembrano avere potenzialità tali da prevenire una divulgazione colposa di informazioni privilegiate, in tutti quei casi un soggetto può aver necessità di dimostrare la lecita conoscenza di specifiche informazioni aventi le caratteristiche prima richiamate, senza bisogno di doverle rilevare.

L'art. 91 concerne invece le fattispecie della manipolazione – informativa o operativa – del mercato, che potrebbero anche combinarsi in forme miste. Con riferimento alla prima, in analogia al MAR, l'art. 91, Par. 2, lett. *c*, del MiCAR reprime il "*diffondere informazioni attraverso i media, compreso Internet, o qualsiasi altro mezzo che forniscano, o è probabile che forniscano, segnali falsi o fuorvianti in merito all'offerta, alla domanda o al prezzo di una o più cripto-attività, o che fissino, o è probabile che fissino, il prezzo di una o più cripto-attività a un livello anormale o artificiale, compresa la diffusione di informazioni non confermate, qualora la persona responsabile della diffusione sapesse, o avrebbe dovuto sapere, che le informazioni erano false o fuorvianti*".

Considerato che i canali messi a disposizione dal *web* (siti internet, forum di discussione, etc.) ed i *social media* costituiscono i principali strumenti per il reperimento e lo scambio di informazioni e notizie su cripto-attività – come anche ha evidenziato l'ESMA (vedi *supra*), tale ipotesi di illecito evoca, per le cripto-attività, le problematiche inerenti alle *fake news* ed ai *deep fake*, anche con riguardo ai *fake social media accounts*, in maniera più marcata di quanto non accada per la disciplina concernente i mercati finanziari [61].

---

[61] Senza poter approfondire qui la tematica, MASSIMILIANO MEZZANOTTE, *Fake news, deepfake e sovranità digitale nei periodi bellici*, in *Federalismi* (33), 2022, p. 53, ricorda che: "*nell'informazione tramite web, oltre alla circolazione di notizie false, si prospetta anche la diffusione di foto, video ed audio manipolati, ossia creati grazie a un software di intelligenza artificiale; questi modificano contenuti reali, ricreando immagini, video e suoni. Sono questi i c.d. deepfake, espressione coniata dalla piattaforma social reddit, il cui scopo iniziale era quello di fare principalmente satira, ma che poi ha trovato applicazione anche in altri ambiti, come nelle arti o nella formazione*". Tale tematica, ha naturalmente rilievo anche per le condotte manipolative sui mercati finanziari., come si evince da uno studio dell'Autorità di vigilanza francese AMF. Alexander NEYRET, *Stock Market Cybercrime, definition, cases and perspective*, 2020, p. 45, ricorda che: "*the rapid emergence of artificial intelligence or, at the very least, of sophisticated learning techniques or machine learning, also opens up new opportunities for the cyber dissemination of false information. The opportunity afforded by the many easily accessible tutorials on the internet to falsify videos by 'making anyone say anything in any way' (known as 'deepfake') makes false information even more credible and therefore its dissemination even more effective. Governments, and particularly the US government, are already seriously concerned about the potential for misinformation from this new threat in the context of elections*". Secondo Jon BATEMAN, *Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios*, in *Cyber Policy Iniziative Working Paper Series*, Carnegie Endowment for international peace, n. 7, 2020, p. 4, "*Deepfakes are thus a subset of synthetic media, a broad category including all AI-generated video, images, sound, and text*". Tra questi, nello stesso lavoro, si descrivono anche i profili *social* falsi che potrebbero essere generati dall'intelligenza artificiale: "*Synthetic social botnets, another broadcast threat, are also of primary concern. Fake social media accounts could be constructed from synthetic photographs and text and operated by AI, potentially facilitating a range of financial harm against companies, markets, and regulators. Synthetic botnets would be more effective and harder to expose than the bots existing today. It seems likely that social bots will incorporate more AI over time, intensifying the technology competition between social media platforms and bad actors*" (ivi, p. 7).

Con riferimento alla manipolazione operativa, oltre a venire tratteggiati gli schemi manipolativi tradizionali, la disciplina riporta in maniera innovativa alcune forme di manipolazione specifiche poste in essere per vulnerare il corretto funzionamento delle piattaforme di negoziazione. Infatti, l'art. 91, Par. 3, lett. *b*, vieta le seguenti condotte che, influenzano il corretto processo di formazione dei prezzi attraverso: (*i*) "*la compromissione o il ritardo del funzionamento della piattaforma di negoziazione di cripto-attività o l'esecuzione di qualsiasi attività che possa avere tale effetto*" e (*ii*) "*l'esecuzione di azioni intese a ostacolare l'individuazione di ordini autentici sulla piattaforma di negoziazione di cripto-attività da parte delle altre persone o qualsiasi attività che possa avere tale effetto, anche mediante l'inserimento di ordini che determinano la destabilizzazione del normale funzionamento della piattaforma di negoziazione di cripto-attività*".

Il MiCAR non prevede, ad oggi, un porto sicuro (*safe harbour*) per gli emittenti che effettuino operatività sulle proprie cripto-attività per determinate finalità e rispettando limiti operativi ed adempimenti informativi, a differenza di quanto previsto dall'art. 5 del MAR o di quanto potrebbe essere stabilito da prassi di mercato ammesse, ai sensi dell'art. 13 del MAR, ma indica all'art. 91, Par. 2, lett. *a*) che talune condotte astrattamente manipolative sono vietate "*salvo che per motivi legittimi*" (vedi anche *infra*, in tema di sanzioni amministrative).

Il Titolo VI del MiCAR si chiude con l'art. 92, che dispone che chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività si doti di sistemi per la rilevazione di ordini e operazioni sospetti di abusi di mercato per la successiva segnalazione all'Autorità di vigilanza competente, in analogia a quanto prevede l'art. 16 del MAR per i mercati finanziari. È, al riguardo, prevista anche una specifica tipologia di segnalazione ove venissero individuate condotte atte ad incidere su "*aspetti del funzionamento della tecnologia a registro distribuito, come il meccanismo di consenso*".

Tale ipotesi sembra evocare il"*51 percent attack*", che altera il meccanismo di validazione delle DLT catturando "*la maggior parte del potere computazionale di una rete blockchain per usarlo al fine di alterare a proprio beneficio gli esiti*" [62], o anche il c.d. *Maximum Extractable Value* (o MEV), fenomeno che in linea teorica permette ai *miners* di alterare il normale ordine delle transazioni da aggiungere al blocco, anteponendone o postponendone alcune a vantaggio di altre, al fine di trarne un profitto.

In materia di abusi di mercato le Autorità nazionali competenti possono esercitare l'ampio spettro di poteri previsto dall'art. 94 del MiCAR, tra i quali, ai fini che qui interessano, si ricordano quelli indicato al Par. 1, lett. *s* "*di rendere pubbliche, o esigere che l'offerente, la persona che chiede l'ammissione alla negoziazione di una cripto– attività o l'emittente di un token collegato ad attività o di un token di moneta elettronica renda pubbliche tutte le informazioni rilevanti che possono influire sulla valutazione della cripto-attività offerta al pubblico o ammes-*

[62] Marco MAUGERI, *op. cit.*, p. 421, nt. 36.

*sa alla negoziazione al fine di garantire la tutela degli interessi dei possessori di cripto-attività, in particolare dei detentori al dettaglio, o il regolare funzionamento del mercato*" ed al Par. 3, lett. *h* "*di adottare tutte le misure necessarie a garantire che il pubblico sia correttamente informato con riguardo, tra l'altro, alla correzione di informazioni false o fuorvianti divulgate, anche imponendo all'offerente, alla persona che chiede l'ammissione alla negoziazione, all'emittente o ad altri che abbiano pubblicato o diffuso informazioni false o fuorvianti di pubblicare una dichiarazione di rettifica*" [63].

L'art. 4, comma 9, del d.lgs. n. 129/2024, mutuando la disciplina prevista all'art. 114, comma 6, del TUF, ha previsto che i destinatari della richiesta formulata ai sensi dell'art. 94, Par. 1, lett. *s*, del MiCAR (disposizione richiamata dal precedente comma 8) possano presentare reclamo alle Autorità mittenti [64].

Con specifico riferimento ai poteri di contrasto agli abusi di mercato concernenti cripto-attività, inoltre, l'art. 18, comma 1, del medesimo decreto legislativo stabilisce che: "*In qualità di autorità competente ai sensi del titolo VI del regolamento (UE) 2023/1114, la Consob esercita i poteri di cui all'articolo 4 del presente decreto, nonché gli ulteriori poteri previsti dall'articolo 187-octies del TUF, secondo le modalità ivi stabilite*".

In questo caso, con riferimento ai poteri esercitabili della Consob, vi è dunque un diretto rinvio alla disciplina sugli abusi di mercato applicabile nei mercati finanziari.

Per ciò che concerne l'apparato sanzionatorio, l'art. 111 del MiCAR prevede, delle sanzioni, anche specifiche (al Par. 5), per le violazioni delle disposizioni prima richiamate.

Il legislatore delegato ha poi specificato l'ammontare di dette sanzioni agli artt. 32 e 33 del citato decreto legislativo, oltre alla previsione specifica, all'art. 34, per la responsabilità dell'ente [65].

A differenza della disciplina tradizionale, non sono previste in Italia sanzioni

---

[63] Il potere da ultimo richiamato è uno dei più incisi in materia di *enforcement* sulla corretta informativa al pubblico ai sensi di MAR, richiamato anche esplicitamente nel Testo Unico della Finanza dall'art. 187-*octies*, comma 6, lett. *b* del TUF.

[64] Art. 4 del d.lgs. n. 129/2024: "*8. Ai fini dell'esercizio del potere di cui all'articolo 94, paragrafo 1, lettera s), del regolamento (UE) 2023/1114, la Consob e la Banca d'Italia secondo le rispettive competenze possono alternativamente: a) provvedere a rendere pubbliche le informazioni direttamente; b) esigerne la comunicazione al pubblico, secondo le modalità da esse stabilite.*

*9. Nell'ipotesi di cui al comma 8, lettera b), qualora l'offerente, la persona che chiede l'ammissione a negoziazione di una cripto-attività o l'emittente di un token collegato ad attività o di un token di moneta elettronica oppongano, con reclamo motivato, che dalla comunicazione al pubblico delle informazioni possa derivare loro un grave danno, gli obblighi di comunicazione sono sospesi. L'Autorità che ha imposto la comunicazione, entro sette giorni, può escludere anche parzialmente o temporaneamente la comunicazione delle informazioni, sempre che ciò non possa indurre in errore il pubblico su fatti e circostanze essenziali. Trascorso tale termine, il reclamo si intende accolto*".

[65] Per la quantificazione delle sanzioni si rinvia, per brevità, alle citate disposizioni.

penali in materia di abusi di mercato e dunque non ha trovato applicazione l'opzione prevista dall'art. 111, Par. 1 del MiCAR[66].

Con riferimento alla manipolazione del mercato, l'art. 33, comma 2, del d.lgs. n. 129/2024, indica che: "*non può essere assoggettato a sanzione amministrativa per violazione dell'articolo 91 del regolamento (UE) 2023/1114 chi dimostri di avere agito per motivi legittimi*" (vedi anche *supra*). Sarà interessante esaminare la portata applicativa di tale disposizione, rimessa, almeno in prima battuta, alle valutazioni della Consob, in assenza di una cornice dispositiva in materia di *safe harbour* o di prassi di mercato ammesse.

Infine, con un ulteriore collegamento con la disciplina collocata nel Testo Unico della Finanza, alle violazioni in materia di abusi di mercato, di competenza della Consob, è applicabile la disciplina sugli *impegni* di cui all'art. 196-*ter* del TUF.

## 9. La peculiare disciplina dell'art. 30, Par. 3, del MiCAR

Come anticipato, al di fuori del Titolo VI del MiCAR vi è un ulteriore disposizione in materia di obblighi informativi – specificamente concernenti i *token* collegati ad attività – meritevole di illustrazione.

L'art. 30 del MiCAR, titolato "*Informazione continua dei possessori di token collegati ad attività*", riporta al Par. 3 che "*fatto salvo l'articolo 88, gli emittenti di token collegati ad attività pubblicano in una posizione del proprio sito web facilmente accessibile al pubblico, non appena possibile e in modo chiaro, preciso e trasparente, informazioni su qualsiasi evento che abbia o possa avere un effetto significativo sul valore dei token collegati ad attività o sulla riserva di attività (…)*".

Detta disposizione, di cui si è già fatto cenno con riferimento alle ipotesi specifiche di informazioni privilegiate (vedi *supra*) è di interesse per le ragioni di seguito esposte.

In primo luogo, l'art. 30, Par. 3 del MiCAR potrebbe trovare applicazione anche quando, viceversa, non vi sia un obbligo per la comunicazione al pubblico di informazioni privilegiate, ad esempio, per difetto di uno dei caratteri dell'art. 87 del MiCAR prima tratteggiati[67].

In secondo luogo, viceversa, potrebbero trovare applicazione entrambe le discipline, quanto meno per gli emittenti di cripto-attività in questione, gli unici a cui si rivolge, come già descritto, l'art. 30, Par. 3, del MiCAR a differenza di quanto stabilito dall'art. 88 del MiCAR, a cui sono assoggettati, come detto, an-

---

[66] L'art. 111, Par. 1, comma 2 del MiCAR prevede che "*Gli Stati membri possono decidere di non stabilire norme relative alle sanzioni amministrative se le violazioni (…) sono già soggette a sanzioni penali nel rispettivo diritto nazionale al 30 giugno 2024 (…)*".

[67] Tra l'altro, il concetto di valore, richiamato all'art. 30 del MiCAR, non è uguale a quello di prezzo, richiamato all'art. 87 del medesimo Regolamento, per quanto nella sostanza dovrebbero tendere a coincidere. Cfr.: Filippo ANNUNZIATA, *An overview of the Market in Crypto-Assets Regulation (MiCAR)*, cit., p. 64.

che gli offerenti e le persone che chiedono l'ammissione alla negoziazione [68]; ciò potrebbe portare l'emittente alla "*pubblicazione contemporanea di due comunicati*" [69] per rispettare entrambe le discipline, o quanto meno all'inserimento di un comunicato unico sul proprio sito web che esplicitamente richiami i due articoli citati.

Ancor più interessante sarebbe il caso dell'attivazione di una eventuale procedura di ritardo della comunicazione al pubblico delle informazioni privilegiate, ai sensi dell'art. 88, Par. 2, del MiCAR, che, in base ai caratteri dell'art. 87 del MiCAR, potrebbe antecedere il verificarsi dell'evento, dunque, prima che sia sorto l'obbligo di cui all'art. 30, Par. 3, del MiCAR.

In tali casi, occorre domandarsi se l'emittente possa procrastinare il ritardo della comunicazione al pubblico anche dopo il verificarsi del citato evento, considerato, tra l'altro, che l'*incipit* dell'art. 30, Par. 3, del MiCAR, fa salva la disciplina dell'art. 88 del MiCAR. Premesso che la sussistenza di un legittimo interesse a ritardare la comunicazione di una informazione privilegiata oltre il verificarsi di un evento, ai sensi della disciplina del MAR ad oggi vigente, sembra una ipotesi eccezionale (anche se non si può escludere *a priori*), in base all'attuale formulazione della normativa una tale dilazione del ritardo potrebbe comunque avere l'effetto di fuorviare il pubblico e difettare così di una delle ulteriori condizioni richieste dall'art. 88, Par. 2, del MiCAR [70].

Alla luce delle novità del *Listing act* per la tempistica di comunicazione al pubblico delle informazioni privilegiate, che riverbereranno i propri effetti anche sulla gestione del ritardo della comunicazione medesima *ex* art. 17, Par. 4, del MAR, non è escluso, peraltro, che il rapporto tra i due adempimenti informativi ora descritti nel MiCAR possa essere oggetto di rivisitazione da parte del legislatore eurounitario.

In conclusione, parafrasando il paradosso di Zenone, quanto meno con riferimento alla presumibile evoluzione della regolamentazione su tale materia, non solo la tartaruga (il mercato finanziario) ad oggi è davanti ad Achille (il mercato delle cripto-attività), ma dovrebbe, almeno nel prossimo futuro, continuare ad indicare a questo la via.

---

[68] Da ciò consegue, naturalmente, l'applicabilità del solo art. 88 del MiCAR in presenza di informazioni che possono avere un effetto significativo sul valore dei *token* collegati ad attività che riguardano direttamente gli offerenti o le persone che chiedono l'ammissione alla negoziazione.

[69] Stefano LOMBARDO, *op. cit.*, p. 203.

[70] Ad esempio, in ragione delle precedenti informazioni già fornite dall'emittente su tali particolari cripto-attività, come esplicitamente indica l'Esma per la disciplina tradizionale nei propri orientamenti relativi al MAR.

# Acquisto di token e onboarding clienti

Fabrizio Vedana

SOMMARIO: 1. Natura e fisionomia dei token. – 2. La disciplina normativa. – 3. Acquisto e onboarding del cliente. – 3.1. La possibile detenzione di token attraverso una fiduciaria.

## 1. Natura e fisionomia dei token

Nel presente contributo, partendo dalla definizione che ne viene data come «rappresentazione digitale di un valore o di un diritto» nel Regolamento MiCA, si indaga sul suo significato dando un contributo per il corretto inquadramento dei «token» da una prospettiva meramente civilistica e, quindi, considerandoli come un particolare formato che assume l'informazione in ambiente digitale tale che, a seconda del contenuto di tale informazione, i token siano considerati come titolo al portatore ai sensi dell'art. 1992 ss. c.c. (es.: token collegati ad attività e token di moneta elettronica), come mero supporto virtuale per la riproduzione di un contenuto più o meno creativo (es.: NFT di opere dell'ingegno) o, infine, come generico bene *ex* art. 810 c.c. (es.: criptovalute e land di metaverso o di altri beni virtuali). Nella seconda parte ci si sofferma sulle modalità di on-boarding che mutano in ragione della diversa natura giuridica che agli stessi viene attribuita.

La tecnologia blockchain (o, più in generale, la DLT) ha sostanzialmente introdotto in ambiente digitale il concetto di unicità e originalità (resilienza e storicizzazione). Un token può definirsi, innanzi tutto, un asset digitale (un bene immateriale, potremmo dire), proprio perché sempre distinguibile dagli altri in quanto indelebilmente collocato in uno o più specifici punti nella sequenza cronologica delle transazioni. Caratteristiche, queste, che nel mondo fisico definiscono le "cose", ovvero i beni materiali che, anche quando sono prodotti in serie, sono rivali, possono cioè sempre essere distinti gli uni dagli altri per caratteristiche intrinseche e non riproducibili, oppure per la particolare posizione nello spazio e nel tempo che assumono. I caratteri di unicità e originalità delle cose non sono elementi trascurabili nella nostra vita di tutti i giorni. Il collezionismo si basa su di essi. Ma anche la ricerca scientifica è per lo più indagine di fenomeni, eventi e reperti unici e originali (se non addirittura irripetibili e perduti). In ambito giuridico unità e originalità sono alla base della finanza globale e del

mercato degli strumenti finanziari che operano attraverso modalità semplificate e tradizionali di trasferimento di crediti e altri diritti attraverso il fenomeno dell'incorporazione di questi in un documento [1]. Unicità e originalità sono anche alla base del mercato dell'arte e dei beni culturali, delle commodity e dei preziosi. Nonché sono gli elementi che caratterizzano titoli di vario genere, dal denaro contante, ai biglietti del cinema, dalle polizze di carico ai voucher di sconto o acquisto merce, dai titoli di viaggio alle sentenze con formula esecutiva. Si tratta in tutti i casi di "documenti" che, se non fossero unici e originali, non potrebbero costituire titolo del possessore per pretendere il pagamento di un credito, per esercitare un diritto, per pretendere una determinata prestazione o per attribuirgli un particolare status. Riprodurre pertanto le caratteristiche di unicità e originalità in ambiente digitale vuol dire compiere un passo decisivo verso un pieno "isomorfismo" del mondo virtuale con quello reale: da qui la necessità del giurista di definire con i propri strumenti civilistici la natura dei token.

Quale asset digitale unico e originale, un token si presta ad avere contenuti diversi. In esso, infatti, può essere scritta una dichiarazione, come ad esempio l'impegno ad eseguire una determinata prestazione a favore del portatore, ovvero il riconoscimento in capo a questo di un diritto di voto [2]. In un token, poi, possono essere rappresentate opere dell'ingegno o disegni e modelli, come negli NFT [3]. Ma un token può anche essere privo di contenuto, come lo sono i bitcoin. Può cioè essere solo un asset digitale scarso, nulla di più.

I token si possono quindi dividere in quattro macrocategorie [4]:

*i*) token a contenuto dichiarativo, i quali contengono una dichiarazione di volontà, ovvero l'impegno dell'emittente a dare o fare qualcosa in favore del portatore;

---

[1] Oppure attraverso l'intervento di un terzo che agisce da garante per la custodia e corretto aggiornamento di informazioni, per lo più consistenti in annotazioni di carattere contabile. In tal caso si parla di titolo dematerializzato che, tuttavia, non è propriamente un titolo, inteso come documento digitale in cui è incorporato un diritto, ma un rapporto tra debitore e creditore intermediato da un terzo fiduciario.

[2] Il contenuto dichiarativo di un token deve essere "al portatore", deve cioè attribuire il diritto (es.: di ricevere la prestazione o di esercitare il voto) al portatore del token. Solo in tal modo, infatti, il diritto può circolare con il trasferimento del token. Costituire invece un token che attribuisce un diritto ad un soggetto determinato, o determinabile, ma senza alcuna relazione con l'identità del portatore (i cc.dd. chirografi di credito), non avrebbe alcuna ragione pratica essendo sufficiente, in tal caso, a voler comunque mantenere il formato digitale, utilizzare i più comuni documenti informatici con firma elettronica avanzata.

[3] I file in questione sono fuori dalla DLT (fatto che può creare non pochi problemi di certezza del contenuto dell'NFT) e possono essere file di qualsiasi formato per supporto di immagini in 2D e 3D, oppure per filmati, tracce audio, o quant'altro possibile. Conseguentemente, un NFT può "contenere" una fotografia, un videoclip, un disegno, un brano musicale o anche un articolo sportivo o di arredo, e un land di metaverso perfino.

[4] Vedasi in tal senso il position paper "La natura giuridica delle cripto-attività" realizzato dall'Italian Blockchain Association.

*ii*) token a contenuto descrittivo, i quali contengono una dichiarazione di scienza che non importa un vincolo del dichiarante, ma, al limite, solo una sua responsabilità in ordine alla veridicità delle dichiarazioni rese;

*iii*) token a contenuto espressivo, i quali contengono un'opera dell'ingegno o del design industriale;

*iv*) token privi di contenuto, i quali sono in genere frazionabili e assumono valore solo in ragione della loro scarsità.

## 2. La disciplina normativa

La prima norma italiana che ha previsto una definizione di valuta virtuale è il d.lgs. n. 90/2017, modificativo del d.lgs. n. 231/2007. L'art. 1, lett. *qq* la definisce come «la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente». La stessa definizione è stata poco dopo ripresa dal d.lgs. 8 novembre 2021, n. 184, in tema di «lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti» (in recepimento della Direttiva (UE) 2019/713)[5]. Qualsiasi cosa voglia dire l'espressione «rappresentazione digitale di valore», non c'è dubbio che una criptovaluta è un token privo di contenuto dichiarativo o espressivo e che, come tale, ha senz'altro valore in sé in quanto emesso con una scarsità intrinseca (programmata). Facendo propria la definizione di «valuta virtuale» di cui sopra (che è poi quella prevista, a livello europeo, dalla Quinta Direttiva antiriciclaggio), il Regolamento (UE) 2023/1114 (noto anche come Regolamento MiCA o MiCAR, dall'acronimo del titolo «Markets in Crypto Assets Regulation»)[6], ha esteso la nozione di token anche a quelli che non rappresentano solo «valori», ma anche «diritti», adottando a tal fine il termine «cripto-attività»[7] ovvero quello di «rappresentazione digitale di un valore

[5] Precede le definizioni normative citate, quella dell'EBA del 2017: «Virtual currencies is a digital representation of value that is neither issued by a central bank or public authority, nor necessarily attached to a legal tender». Si vedano anche gli orientamenti Financial Action Task Force (FATF (2020), Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets, FATF, Paris, France,) e dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE (2022), Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard, OECD, Paris, Sez. IV, nn. 2 e 3).

[6] Tale regolamento è stato recepito in Italia con il d.lgs. n. 129 del 5 settembre 2024, pubblicato sulla Gazzetta Ufficiale, Serie Generale n. 215 del 13 settembre 2024.

[7] Nel Regolamento MiCA i termini token e cripto-attività sono utilizzati come sinonimi, eppure il ricorso a quest'ultimo neologismo (che è la traduzione in italiano del termine originale inglese «criypto-asset») tradisce l'enfasi finanziaria e regolamentare. Intento del legislatore, infatti, non è stato quello di occuparsi dell'inquadramento civilistico del fenomeno, quanto quello di intervenire in tema di antiriciclaggio e tutela del risparmio, dei consumatori e dei mercati finanziari in genera-

o di un diritto che possono essere trasferiti e archiviati elettronicamente, utilizzando la tecnologia di registro distribuito o tecnologia simile». Certamente resta da capire meglio il significato dell'espressione «rappresentazione digitale di un valore o di un diritto». Non è chiaro, infatti, se il termine «rappresentazione» debba intendersi come incorporazione, ovvero come obbligazione dell'emittente verso il portatore della cripto-attività e non come mera citazione di una posizione giuridica soggettiva altrui o ipotetica. Non è neppure chiaro cosa sia un «valore» giacché qualsiasi cosa può "rappresentare un valore", in senso soggettivo (valore affettivo) e oggettivo (valore di mercato). Nella definizione contenuta nella MiCAR, inoltre, non è chiaro neanche il significato di «tecnologia di registro distribuito o tecnologia simile». Quali sono i caratteri che distinguono un tale tecnologia. E in particolare, quali sono quelli rilevanti ai fini dell'applicazione della disciplina regolamentare. Il Regolamento MiCA prende presumibilmente spunto da due provvedimenti legislativi che hanno fatto molto discutere negli anni scorsi e che vale la pena menzionare per il contributo che hanno dato nella successiva elaborazione del concetto giuridico di token: il «Token and TT Service Provider Act» del Principato del Liechtenstein del 3 ottobre 2019 e la Legge federale svizzera «sull'adeguamento del diritto federale agli sviluppi della tecnologia di registro distribuito» del 25 settembre 2020 che ha modificato diverse disposizioni civilistiche. Nel nostro ordinamento, per esempio, la dicitura "all'ordine", o altra simile, comporta la trasmissibilità del diritto "rappresentato" secondo le girate del titolo (art. 2008 c.c.). Anche la CONSOB nel Documento per la discussione del 19 marzo 2019 (poi confermato nel Rapporto finale del 2 gennaio 2020) avente ad oggetto "Le offerte iniziali e gli scambi di cripto-attività", ha definito le cripto-attività come una «rappresentazione digitale di diritti connessi a investimenti in progetti imprenditoriali». La prima è una normativa incentrata non tanto sulla definizione di «token», ma innanzi tutto su quella di «Trustworthy Technology (TT)», ovvero la tecnologia grazie alla quale può essere garantita l'integrità dei token e il loro corretto trasferimento e disposizione. Si tratta, quindi, di una classe di tecnologie, non necessariamente DLT, idonee a rendere i token immodificabili (integrity) e trasferibili, ovvero univocamente attribuibili ad uno specifico soggetto. Il legislatore del Principato ha comunque fornito anche una definizione di «Token» quale: «a piece of information» trattata con una Trustworthy Technology, fornendo al contempo rilevanti chiarimenti in ordine alla sua natura giuridica, e cioè intendendolo come «a kind of "container" for representing a right». Torna, quindi, il concetto di "contenitore", ovvero di supporto virtuale che, a seconda del contenuto, si caratte-

le. Coerentemente con ciò, il Regolamento MiCA divide le cripto-attività in tre sottoinsiemi riservando a ciascuno di essi una disciplina ad hoc: i token collegati ad attività, i token di moneta elettronica e tutti gli altri token. L'assenza, tuttavia, di un approccio civilistico e "ontologico" del fenomeno, non consente sempre all'interprete di ricondurre un token alla corretta categoria, soprattutto quando si tratta di token ibridi. Consapevole di ciò, il Regolamento rinvia a successivi interventi di fonte secondaria dell'ESMA per emanare orientamenti, criteri interpretativi e norme tecniche in collaborazione con altre Autorità Europee di Vigilanza.

rizza in modo diverso. Si tratta di una prospettiva che si rivolge direttamente alla funzione del token; un inquadramento corretto e originale che non è stato accolto in termini altrettanto chiari dalle normative successive degli altri paesi europei né dal legislatore europeo. Venendo alla normativa elvetica, si rinviene la definizione di token come «diritto valore registrato», e in particolare come «un diritto che per accordo delle parti: 1. è iscritto in un registro di diritti valori; 2. può essere esercitato e trasferito soltanto per il tramite di detto registro» (Legge federale di complemento del Codice civile svizzero; Libro quinto: diritto delle obbligazioni – art. 973). Anche in questo caso, come per la legge del Liechtenstein, il perno pare essere la piattaforma informatica su cui i token sono generati e trasferiti (qui definita come «registro di diritti valori») piuttosto che il token in sé. Quest'ultimo, infatti, è rimesso all'indefinita nozione di "diritto-valore", locuzione ripresa nel Regolamento MiCA. A differenza del Regolamento MiCA, tuttavia, la legge svizzera non fa riferimento alla «rappresentazione», ma identifica un token come un diritto-valore in sé, a lasciar intendere che esso può incorporare un diritto, o può costituire di per sé un valore. Token come "contenitore" (di un "piece of information", legge del Liechtenstein) e token come "diritto-valore" (legge svizzera), sono i punti di partenza per il successivo passo verso una comprensione più profonda della natura giuridica del fenomeno token. Passo timidamente abbozzato dal regolamento europeo sul c.d. "pilot regime". Venendo invece alle leggi di "casa nostra" è bene ricordare che il 18 marzo 2023 è entrato in vigore il d.l. n. 25 del 17 marzo 2023 (il c.d. Decreto Fintech, poi convertito con modificazioni dalla legge 10 maggio 2023, n. 52) per l'attuazione del Regolamento (UE) 2022/858 «relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito» (anche noto come "DLT Pilot Regime" o "Regolamento DLT"). Il Decreto Fintech ha introdotto in Italia una disciplina comune sulle modalità di emissione, forme di registrazione e circolazione di «strumenti finanziari digitali», ovvero degli strumenti finanziari emessi su un «registro per la circolazione digitale» (un network DLT). In altri termini, si tratta di strumenti finanziari emessi in «formato tokenizzato» ovvero un nuovo formato che si affianca a quelli cartolare e dematerializzato già previsti dal Testo Unico della Finanza (d.lgs. n. 58/1998). Un formato che garantisce l'unicità (non duplicabilità) e immodificabilità. Il riferimento al termine «formato» è assai significativo giacché si discosta dalla generale nozione di «rappresentazione digitale di valore o diritti», a lasciar intendere che i token (ovvero gli strumenti finanziari digitali e le altre cripto-attività di cui al Regolamento MiCA) sono solo un particolare formato in cui un titolo può manifestarsi.

## 3. Acquisto e onboarding del cliente

Il primo passo per chi desidera sottoscrivere/acquistare un token è la scelta del tipo di token e l'identificazione delle piattaforme regolamentate dove questo

è disponibile. Come detto esistono, infatti, diversi tipi di token; gli utility token, i security token, gli stablecoin, ecc. Chi sottoscrive/acquista il token deve comprenderne bene le caratteristiche e le funzionalità, incluse le eventuali limitazioni di utilizzo e i rischi legati all'investimento. Le piattaforme regolamentate forniscono documenti come il white paper del progetto, che descrive i dettagli tecnici, economici e legali del token.

Per procedere con la sottoscrizione, è poi necessario aprire un account su una piattaforma di scambio o su una piattaforma blockchain. Qui l'utente dovrà fornire i dati di base per la registrazione, come nome, cognome, indirizzo e-mail e password. Tuttavia, la registrazione è solo il primo passo per poter accedere alla sottoscrizione del token; è, infatti, spesso richiesto di passare attraverso procedure più rigorose di verifica dell'identità richieste dalla normativa antiriciclaggio.

Tale verifica, chiamata anche Know Your Customer o KYC, è una misura di controllo, imposta sia dalle normative europee che da quelle nazionali, che le piattaforme devono applicare per garantire la trasparenza e la legittimità delle transazioni finanziarie.

Nel contesto della sottoscrizione di un token, la procedura KYC include:

- verifica dell'identità: all'utente viene richiesto di caricare documenti d'identità (es. carta d'identità, passaporto) per confermare la propria identità. Molte piattaforme utilizzano software avanzati di riconoscimento biometrico per accelerare il processo;
- prova di residenza: oltre all'identità, la residenza dell'utente viene normalmente verificata attraverso la presentazione di documenti che ne comprovano l'indirizzo, come bollette o estratti conto bancari recenti;
- raccolta di dati supplementari: a volte, le piattaforme richiedono ulteriori informazioni sull'origine dei fondi o sulle attività economiche dell'utente, per escludere profili sospetti;
- la procedura KYC permette alla piattaforma di tracciare in modo trasparente l'identità di ogni sottoscrittore, evitando così l'anonimato completo e consentendo un maggiore controllo delle transazioni.

La normativa antiriciclaggio impone poi alle piattaforme di attuare controlli rigorosi per impedire il riciclaggio di denaro.

Le misure AML fondamentali che una piattaforma adotta per monitorare e regolare la sottoscrizione dei token sono:

- monitoraggio delle transazioni: ogni transazione viene monitorata per individuare attività sospette o comportamenti che possono suggerire tentativi di riciclaggio. Algoritmi avanzati sono in grado di identificare modelli di comportamento irregolari, come trasferimenti di fondi tra più conti in rapida successione;
- controllo dei limiti di transazione: molti regolatori impongono limiti giornalieri o mensili alle transazioni finanziarie per evitare che grandi somme venga-

no trasferite rapidamente, consentendo alle piattaforme di analizzare i comportamenti degli utenti senza il rischio di flussi ingenti non giustificati;

• segnalazione di attività sospette: se la piattaforma rileva transazioni anomale o comportamenti che potrebbero indicare un'attività illecita, è obbligata a segnalare l'evento alle autorità competenti attraverso un rapporto di attività sospetta.

Una volta superate le verifiche previste dalla normativa antiriciclaggio, l'utente dovrà leggere e accettare i termini e le condizioni previste dalla piattaforma. Questo documento contrattuale descrive in dettaglio:

✓ Diritti e doveri dell'utente e della piattaforma.
✓ Regole di utilizzo dei token e responsabilità dell'utente.
✓ Rischi associati agli investimenti in token.
✓ Politiche sulla sicurezza per la gestione e la protezione dei token.
✓ Comprendere pienamente i termini consente all'utente di utilizzare in modo consapevole il token e aiuta a prevenire eventuali controversie future.

Dopo aver accettato i termini, l'utente può completare la sottoscrizione attraverso il pagamento. Le modalità di pagamento accettate possono prevedere sia l'utilizzo di criptovalute sia valute nazionali. La piattaforma trasferisce quindi il token all'utente al termine della transazione. Tuttavia, molte piattaforme prevedono ulteriori verifiche in caso di grandi trasferimenti, per assicurarsi che l'origine dei fondi sia legittima.

Una volta acquistati, i token vengono trasferiti al wallet (portafoglio digitale) dell'utente. È fondamentale che l'utente garantisca la sicurezza del proprio portafoglio.

Alcune delle misure di sicurezza più comuni includono:

1. uso di cold wallet: i cold wallet, dispositivi non connessi a Internet, sono ideali per la conservazione a lungo termine, in quanto offrono una protezione elevata contro attacchi informatici;
2. autenticazione a due fattori (2FA): attivare la 2FA aggiunge un livello di sicurezza per l'accesso al proprio portafoglio;
3. backup delle chiavi private: le chiavi private sono l'accesso diretto ai token e devono essere conservate in un luogo sicuro, poiché perderle significa perdere l'accesso al token stesso.

Anche dopo la sottoscrizione, la piattaforma può richiedere aggiornamenti periodici delle informazioni personali dell'utente per garantire che i dati siano sempre corretti e conformi. Alcune piattaforme conducono anche controlli di due diligence su base continuativa per gli utenti che movimentano grandi volumi di token o che hanno cambiato frequenza di transazione, come ulteriore misura contro il riciclaggio.

### 3.1. La possibile detenzione di token attraverso una fiduciaria

La gestione degli adempimenti fiscali connessi alla detenzione di token e cripto-attività in genere può essere affidata ad una società fiduciaria ovvero ad un soggetto che sulla base di una specifica autorizzazione rilasciata dal Ministro delle Imprese e del Made in Italy ai sensi della legge n. 39/1966. La sottoscrizione di un mandato fiduciario avente ad oggetto cripto-attività, acquistate/detenute da persone fisiche, attribuisce alla fiduciaria il ruolo di sostituto di imposta sugli eventuali capital gain derivanti dalla compravendita di criptovalute, esonerando il fiduciante dalla compilazione della dichiarazione dei redditi (quadro RT del Modello Redditi). Ciò è possibile per effetto delle integrazioni agli artt. 6 e 7 del d.lgs. n. 461/1997, operate dall'art. 1, comma 128 della legge n. 197/2022; per i redditi in esame sono espressamente ammesse le opzioni per i regimi del risparmio amministrato e del risparmio gestito.

Per quanto riguarda il risparmio amministrato, le particolarità da segnalare per le plusvalenze e gli altri proventi di cui all'art. 67, comma 1, lett. *c*-sexies del TUIR sono le seguenti:

- l'opzione può essere resa agli operatori non finanziari di cui all'art. 3, comma 5, lett. *i* e *i*-bis del d.lgs. n. 231/2007 (le società fiduciarie rientrano in tale categoria unita-mente alle banche e ai prestatori di servizi relativi all'utilizzo di valuta virtuale e ai prestatori di servizi di portafoglio digitale);
- non è ammessa la dichiarazione sostitutiva con cui i contribuenti attestano all'intermediario i dati e le informazioni necessarie per la liquidazione dell'imposta sostitutiva, ove l'intermediario non ne sia in possesso;
- così come per titoli, quote, certificati o rapporti, anche per le cripto-attività si considera cessione a titolo oneroso anche il trasferimento a rapporti di custodia o amministrazione intestati a soggetti diversi dagli intestatari del rapporto di provenienza, nonché ad un rapporto di gestione di cui all'art. 7 del d.lgs. n. 461/1997, salvo che il trasferimento non sia avvenuto per successione o donazione.

L'opzione per il regime del risparmio amministrato comporta l'applicazione dell'imposta sostitutiva al momento del realizzo da parte di un intermediario con cui il contribuente detiene uno stabile rapporto sulle plusvalenze e altri proventi derivanti da rimborsi, cessioni, permute o detenzione di cripto-attività. La sottoscrizione di un mandato fiduciario avente ad oggetto l'amministrazione, anche senza l'intestazione, di cripto-attività, consente di affidare alla fiduciaria il ruolo di sostituto d'imposta.

Al riguardo, la circ. Agenzia delle Entrate 30/2023 (par. 3.2.2) ha chiarito che lo stabile rapporto può essere costituito, a titolo esemplificativo, da un rapporto di custodia delle chiavi crittografiche e da un conto sul quale vengono addebitati/accreditati i flussi derivanti dalle cripto-attività.

Nel caso in cui le cripto-attività siano state affidate in custodia all'intermediario in un momento successivo alla acquisizione da parte del contribuente, il

conferimento delle stesse presso l'intermediario potrebbe comportare il trasferimento in un nuovo wallet aperto dall'intermediario che deterrà le chiavi crittografiche per conto del cliente. In tal caso il trasferimento delle cripto-attività dal wallet del contribuente al wallet dell'intermediario non costituisce una fattispecie fiscalmente rilevante.

Sul punto, la circ. 30/2023 chiarisce che, in assenza della compensazione dei risultati delle cripto-attività con quelli delle altre attività finanziarie, il deposito amministrato deve avere ad oggetto le sole cripto-attività.

La fiduciaria, all'atto del ricevimento del mandato, effettuerà tutte le ordinarie attività di adeguata verifica antiriciclaggio previste dalla vigente normativa (d.lgs. n. 231/2007) e provvederà altresì a comunicare all'anagrafe dei conti l'apertura del mandato (così come eventuali sue variazioni o cessazione) ai sensi dell'art. 7 del d.p.r. n. 605/1973. Il citato mandato fiduciario consentirà poi al cliente di gestire, nell'interesse anche dei propri eredi, il trasferimento delle criptovalute in caso di apertura di una successione. Ne consegue che in presenza di mandati fiduciari aventi ad oggetto l'amministrazione delle citate criptovalute, il fiduciante sarà esonerato (oltre che dalla compilazione del quadro RW con riferimento a tali asset, qualora gli stessi siano posseduti su piattaforme digitali estere, ai sensi dell'art. 4, comma 3 del d.l. n. 167/1990, e secondo quanto chiarito dall'Agenzia delle Entrate con la circ. 23 dicembre 2013 n. 38) anche dalla indicazione degli eventuali redditi in dichiarazione in quanto la società interpellante potrà e dovrà agire da sostituto di imposta, tutelando pertanto gli interessi dell'erario, oltre che quello dei propri clienti, obbligando questi ultimi alla compliance fiscale anche con riferimento a criptovalute gestite su piattaforme estere, non facilmente intercettabili dall'Amministrazione finanziaria, non trattandosi di circuiti bancari, e come tali, al momento, esclusi da qualsiasi forma di scambio di informazioni sulla base dei c.d. "CRS" (Common Reporting Standard). In particolare, la sostituzione di imposta sugli eventuali capital gain potrà avvenire nell'ambito del rapporto di risparmio amministrato regolato dall'art. 6 del d.lgs. n. 461/1997.

L'acquisto di token, e di cripto-attività in genere, deve avvenire nel rispetto di regole giuridiche, fiscali e antiriciclaggio alla cui osservanza sono tenuti i cripto asset service provider per effetto delle disposizioni stabilite a livello europee e poi recepite in Italia. Dall'inosservanza di tali norme possono derivare, per l'acquirente dei token, minori tutele sul piano giuridico e sanzioni sul piano fiscale mentre i cripto asset service provider potranno essere sanzionati dalle rispettive Autorità di Vigilanza. L'utilizzo di un sostituto d'imposta consente al detentore di cripto-attività di semplificare gli adempimenti posti a suo carico rendendo la gestione dei beni più semplice e più ordinata.

# Crisi bancarie e intelligenza artificiale tra prevenzione e nuove vulnerabilità

Allegra Canepa*

SOMMARIO: 1. La digitalizzazione del sistema bancario e l'evoluzione dei modelli di business: il caso delle banche digitali. – 1.1. Un modello di business all'insegna di specializzazione ed esternalizzazione. – 2. Digital intensity e nuovi fattori di rischio tra liquidità, depositi non assicurati e social media. – 3. Il ruolo dell'AI nell'attività delle Banche Centrali. – 4. Prospettive di sviluppo dell'IA tra banche e imprese: valutazione e cessione dei crediti deteriorati nel mercato secondario.

## 1. La digitalizzazione del sistema bancario e l'evoluzione dei modelli di business: il caso delle banche digitali

Una crisi bancaria è un processo articolato nella cui gestione assumono rilievo molteplici aspetti tra i quali la tempestività di azione e l'efficacia di intervento delle istituzioni coinvolte. Proprio la questione della tempestività di azione può essere influenzata dalla digitalizzazione e dallo sviluppo tecnologico sia nel determinare un'accelerazione delle crisi sia quale potenziale "strumento" di intervento ex-ante.

Infatti la trasformazione digitale impone di comprendere se anche nello sviluppo delle crisi vi possa essere un ruolo "positivo" della tecnologia nella gestione e nell'individuazione preventiva delle situazioni di rischio alla luce dell'affermazione degli algoritmi predittivi. Allo stesso tempo però è utile riflettere se vi sia anche un ruolo "negativo" quale fattore capace di favorire o accelerare il verificarsi di una crisi.

Come noto, l'impresa bancaria è un'organizzazione complessa e nello svolgimento delle sue attività è esposta a diversi fattori di rischio tra i quali quelli derivanti dal credito, dalla situazione di liquidità e dai tassi di interesse. Proprio per questo assume rilievo comprendere se la digitalizzazione possa essere consi-

* Il presente contributo è stato realizzato nell'ambito del Progetto Proportionating rules on bank crisis prevention and management to the case of retail banks: an analysis on the European and national legal framework (Pro. Re. Ba.), PNRR, Programma Nazionale di Ricerca e Progetti di Rilevante Interesse Nazionale (PRIN) – CUP N. H53D23002980006 – Codice Progetto 2022YXTHZF.

derata un elemento rilevante solo nell'erogazione dei servizi o se invece possa avere implicazioni anche sulla struttura organizzativa ed il modello di business con riflessi anche sui rischi appena richiamati.

Ciò significa esaminare questi aspetti in una duplice prospettiva e cioè quella di accelerazione di una crisi e contestualmente di possibile prevenzione o migliore gestione da parte delle autorità.

Per comprendere ed approfondire il primo aspetto può essere utile prendere in esame una particolare "tipologia" o meglio uno specifico modello e cioè quello delle c.d. banche digitali. Infatti queste banche possono consentire di valutare se lo sfruttamento della tecnologia abbia avuto effetti solo nell'erogazione dei servizi o ne abbia prodotti anche sul modello di business. Nello specifico appare di interesse soffermarsi sul rapporto tra riserve e liquidità nonché sulla composizione delle attività. La ripartizione e combinazione tra liquidità, credito e investimenti in titoli sul mercato merita attenzione in sé e per il ruolo che può rivestire nel verificarsi di una crisi come accaduto nel 2023 nella crisi delle banche digitali della Silicon Valley Bank.

Nelle banche digitali proprio la "*digital intensity*" sembra essere uno degli elementi capaci di consentire una loro crescente affermazione sul mercato come dimostrano gli Stati Uniti dove rappresentano già il 64% delle Less Significant Institution (LSI)[1]. Questa "*digital intensity*" si declina in primo luogo in un'ampia capacità di sfruttamento dei dati e dell'Intelligenza Artificiale per garantire un incremento della personalizzazione dei servizi[2] capace di attrarre il cliente e accompagnata anche da un'efficace assistenza clienti. In secondo luogo si evidenzia un ampio ricorso al credit scoring per garantire maggiore rapidità nell'accesso al credito ed anche un'offerta, di trading ed infine una gestione del portafoglio tramite app o piattaforma[3] con possibilità di comparazione in tempo reale. Il ricorso all'IA significa incremento di utilizzo dell'IA generativa e di modelli di linguaggio di grandi dimensioni applicati soprattutto al miglioramento delle operazioni interne anche se il rapido ritmo di integrazione rende complesso avere un quadro aggiornato di utilizzo.

Infine dal punto di vista delle attività si registra una maggiore propensione verso le criptoattività sulle quali il Comitato di Basilea nel dicembre 2022 aveva

---

[1] Si veda N. KOONT, T. SANTOS, L. ZINGALES, *Destabilizing digital "bank walks"*, New York Paper Series n. 328, maggio 2023, rep. papers.ssrn.com/sol3/papers.cfm?abstract_id=4443273. È utile ricordare come la classificazione di LSI americana sia basata su parametri differenti da quelli europei.

[2] Sul punto la Convenzione Interbancaria per l'Automazione (CIPA) e l'Associazione Bancaria Italiana nella Rilevazione sull'IT nel settore bancario italiano, paradigmi tecnologici innovativi 2023 evidenziano tra le principali criticità attese la cybersecurity, il rispetto della privacy e le tempistiche ed i costi di sviluppo (p. 12). Documento rep. https://www.cipa.it/rilevazioni/tecnologiche/2023/Rilevazione_tecnologica_2023.pdf.

[3] Sul punto si veda in particolare D. ARNAUDO, S. DEL PRETE, C. DEMMA, M. MANILE, A. ORAME, M. PAGNINI, C. ROSSI, P. ROSSI, G. SOGGIA, *The digital transformation in the Italian banking sector*, Quaderni di Economia e Finanza, Banca d'Italia, n. 682/2022, p. 5 e ss.

delineato anche un nuovo standard prudenziale specifico volto ad individuare i limiti dell'esposizione consentita alle banche alla luce dei potenziali rischi per la stabilità finanziaria, aspetto più volte richiamato anche dal Fondo Monetario Internazionale (FMI)[4].

### 1.1. Un modello di business all'insegna di specializzazione ed esternalizzazione

Agli aspetti appena richiamati vanno aggiunte altre due "tendenze" di queste banche e cioè una specializzazione nell'offerta ed un ampio ricorso alle esternalizzazioni. La prima va intesa come una vera e propria selezione dei servizi erogabili diretta ad individuare soltanto quelli potenzialmente più redditizi grazie alle commissioni come i sistemi di pagamento, la gestione patrimoniale ed il trading[5].

Il fatto che le banche digitali siano generalmente delle LSI fa riflettere anche sulla diminuzione di rilevanza della dimensione ai fini della capacità di accesso alla tecnologia nonché della possibile produzione di rischi sistemici. Si delinea pertanto una "controtendenza" rispetto a quanto avviene per le grandi piattaforme o per i prestatori di crypto-attività, dove per contro, si evidenzia una stretta correlazione tra incremento del rischio e maggiore dimensione con conseguente necessità di previsioni regolatorie specifiche e maggiormente stringenti proprio per i soggetti più rilevanti sul mercato[6].

La seconda questione alla quale porre attenzione riguarda la capacità di selezionare prodotti e servizi di terze parti integrabili nonché il ricorso a processi di esternalizzazione. Per questi ultimi la domanda continua a crescere e coinvolge terze parti[7], non sempre di natura finanziaria, conseguentemente più difficili da

---

[4] Il Comitato di Basilea ha distinto le criptoattività in due gruppi a seconda del livello di rischio. Si veda il Prudential Treatment of Cryptoasset exposures, del dicembre 2022 nonché il Basel III Monitoring Report, febbraio 2023 e il Consultative Document, Disclosure of Cryptoasset exposure, 17 ottobre 2023.

Per quanto concerne gli interventi del FMI si vedano da ultimi G20, Note on the macrofinancial implications of crypto assets, Febbraio 2023, p. 5 ss. rep. www.infm.org e FSB and IMF outline comprehensive approach to identify and respond to macroeconomic and financial stability risks associated with crypto-assets, settembre 2023, rep. https://www.fsb.org/2023/09/fsb-and-imf-outline-comprehensive-approach-to-identify-and-respond-to-macroeconomic-and-financial-stability-risks-associated-with-crypto-assets.

[5] Per maggiori dettagli sulla fisionomia ed evoluzione delle LSI si veda il Rapporto della Banca Centrale Europea, LSI Supervision Report 2022, www.bankingsupervision.europa.eu/ecb/pub/.

[6] Il riferimento è ai Regolamenti n. 2022/1925, Digital Markets Act (DMA) e n. 2023/1114 relativo ai mercati delle cripto-attività (MiCA)i che evidenziano i maggiori rischi e la necessità di regole più stringenti proprio per i soggetti che, per le loro caratteristiche dimensionali, sono in grado di avere effetti significativi sul mercato.

[7] Tale tendenza emerge anche dalla fotografia del contesto italiano effettuata da Convenzione Interbancaria per l'Automazione (CIPA) e Associazione Bancaria Italiana (ABI) nella Rilevazio-

vigilare (basti pensare ad es. ai servizi cloud) anche in presenza di un monitoraggio sugli accordi conclusi [8].

Proprio il rischio che da simili situazioni possano derivare nuove vulnerabilità sistemiche frutto del legame sempre più stretto tra sistemi di comunicazione e servizi finanziari era già stato evidenziato nel 2020. In un Rapporto del Comitato per il Rischio Sistemico (CESR) si sottolineava come "The high level of interconnectedness across financial institutions, financial markets and financial market infrastructures, and particularly the interdependencies of their IT systems, constitute a potential vulnerability" [9].

Inoltre la BCE aveva evidenziato, come in un quadro nel quale la spesa per esternalizzazioni, specialmente per il cloud [10], appare in crescita senza una contestuale garanzia sulla qualità dell'offerta, vista anche la concentrazione di questi mercati, comprese le attività critiche [11,] incrementa i rischi di vulnerabilità operative e sicurezza dei dati.

---

ne sull'IT nel settore bancario 2023, pubblicato nel luglio 2024 p.11 e ss. https://www.cipa.it/rilevazioni/economiche/2023/index.html.

[8] L'EBA nei suoi orientamenti dal 2019 prevede una raccolta centrale di dati relativi ai registri dell'outsurcing delle banche proprio per consentire alle autorità di vigilanza di avere una visione completa degli accordi di esternalizzazione anche al fine di valutarne criticità e concentrazione. Vedi EBA/GL/2019/02.

[9] Si veda CESR, Systemic cyber risk, febbraio 2020, p. 5, www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.da.pdf.

[10] È utile ricordare come al cloud possibili rischi possano derivare anche da hardware e dai Large Language Model (LLM) che possono avere costi molto elevati. Sul punto si veda in particolare FSB, The Financial stability implications of Artificial Intelligence, 14 novembre 2024, p. 6, https://www.fsb.org/2024/11/the-financial-stability-implications-of-artificial-intelligence/#:~:text=14%20November%202024%20FSB%20assesses, and%20regulatory%20frameworks%20and%20capabilities.

Sulla frammentazione della catena valore e l'outsourcing la Bank of England ha pubblicato un documento specifico nel febbraio 2023, Outsourcing and Third Party Risk Management Supervisory Statement: recognised payment system operators and specified service providers, 8 febbraio 2023, https://www.bankofengland.co.uk/paper/2023/ss/outsourcing-third-party-risk-management-ss-recognisedpayment-system-operators.

Sul tema in dottrina si vedano tra gli altri A. SACCO GINEVRI, *Esternalizzazione (*outsourcing*)*, in *Fintech: diritti, concorrenza, regole*, diretto da G. FINOCCHIARO, V. FALCE, Zanichelli, Bologna, 2019, 205 A. SCIARRONE ALIBRANDI, *Innovazione tecnologica, regolazione e supervisione dei mercati*, e M. SEPE, *Prestazione frazionata e regole di rapporto tra imprese*, entrambi in R. LENER, G. LUCHENA, C. ROBUSTELLA (a cura di), *Mercati regolati e nuove filiere del valore*, Giappichelli, Torino, 2021, rispettivamente p. 5 e p. 233 ss.; A. CANEPA, *Big Tech e mercati finanziari: "sbarco pacifico" o "invasione"? Analisi di un "approdo" con offerta "à la carte"*, in *Riv. trim. dir. econ*., 3/2021, p. 465 ss.; V. TROIANO, *Soggettività finanziaria e forme di aggregazione*, in *Riv. trim. dir. econ*., 1/2022, p. 92 ss.; F. CIRAOLO, *L'ecosistema digitale e l'evoluzione dei mercati*, in *Riv. trim. dir. econ*., 4/2022, p. 342 ss.; L. SPITALERI, *L'*outsourcing *nei servizi bancari e finanziari, profili di* governance *e prospettive di vigilanza*, in *Riv. trim. dir. econ.*, 2023, p. 136 ss. e L. AMMANNATI, *I nuovi paradigmi dell'impresa bancaria in epoca di transizione*, Quaderno di ricerca giuridica n. 99, Banca d'Italia, 2024.

[11] Si veda BCE, S*upervisory Review and Evaluation Process* (SREP) *Aggregated results of SREP 2023*, par. 5.5.2. Operational risk.

Anche per questo sul punto è intervenuto il regolamento n.2022/2554, Digital Operational Resilience Act c.d. DORA, con la predisposizione da parte delle entità finanziarie, di un quadro diretto alla gestione ed al controllo interno dei rischi informatici applicabile a tutti i fornitori terzi di servizi di Tecnologie dell'Informazione e della Comunicazione (TIC), compresi i servizi cloud. [12] In realtà il FSB proprio nel novembre 2024 ha avuto modo di sottolineare come potrebbe essere necessario un ulteriore lavoro volto a garantire quadri sufficientemente completi sugli sviluppi d'uso e le implicazioni per la stabilità finanziaria [13].

Nell'ambito del modello di business delle banche digitali schematicamente richiamato, l'aspetto più rilevante in questa sede è proprio quello delle attività e della liquidità ed il loro possibile ruolo nell'innescare una crisi caratterizzata anche una corsa digitale agli sportelli favorita dai media digitali. Tali dinamiche determinano la necessità di interventi estremamente tempestivi per non produrre possibili rischi sistemici ma non semplici da attuare.

Pertanto, a fianco di un esame dell'efficacia delle procedure esistenti alla luce dei cambiamenti in atto, appare di interesse anche valutare se e come la tecnologia possa avere un ruolo nella previsione e prevenzione di possibili crisi derivanti da crediti deteriorati o da problemi di liquidità frutto anche di fluttuazioni nei tassi. Ciò significa comprendere da un lato come l'IA possa essere utilizzata dalle banche nei modelli di risk assessment, per la previsione del deterioramento dei crediti e l'ottimizzazione dei requisiti di capitale [14] ed allo stesso tempo quale utilizzo possano farne le autorità di supervisione.

## 2. Digital intensity e nuovi fattori di rischio tra liquidità, depositi non assicurati e social media

Il caso della Silicon Valley Bank (SVB) [15] appare di interesse perché permette

[12] Il regolamento è stato poi seguito da due regolamenti delegati pubblicati in GUUE del 25 giugno 2024 rispettivamente n. 1772/2024 sui criteri per la classificazione degli incidenti connessi alle Tecnologie dell'IC e n. 2024/1774 sulla gestione dei rischi informatici.

Sul tema dei rischi informatici in ambito finanziario si veda anche il contributo di G. ZICCARDI in questo volume.

[13] Si veda FSB, *The financial stability implications of Artificial Intelligence*, cit., p. 6, e OECD – FSB, *Roundtable on Artificial Intelligence in Finance: Summary of key findings*, 30 settembre 2024, https://www.fsb.org/uploads/OECD-–-FSB-Roundtable-on-Artificial-Intelligence-AI-in-Finance.pdf.

[14] Sull'utilizzo in essere e gli sviluppi si veda in particolare il Report della consultazione EBA, *Machine learning for IRB models,* EBA/REP/2023/28, agosto 2023, https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2023/1061483/Follow-up%20report%20on%20machine%20learning%20for%20IRB%20models.pdf.

[15] È utile ricordare come le banche fallite in rapida successione in America siano state tre e cioè la SVN, la Signature e la Silvergate, quest'ultima in liquidazione volontaria.

di esaminare la crisi di una banca digitale e contestualmente una corsa agli sportelli peculiare perché generata proprio dall'intreccio con i social media e la loro capacità di diffusione pressoché istantanea di notizie comprese quelle rilevanti per i mercati finanziari.

Questo caso consente di riflettere anche su una struttura ed erogazione dei servizi all'insegna della "scomparsa" del tempo nella movimentazione dei depositi. Da questo punto di vista se è vero che il mobile e online banking sono disponibili da tempo è altrettanto vero che proprio negli ultimi anni si è registrato un utilizzo più ampio da parte dei depositanti. In questo quadro proprio l'IA potrebbe ulteriormente favorire la velocità di spostamento dei depositi aziendali grazie allo sfruttamento di informazioni quali feed di notizie o messaggi sui social media di immediata raggiungibilità e rapida consultabilità [16].

Proprio gli effetti dell'incremento di rapidità nella movimentazione di un deposito, associata ad un'immediatezza di circolazione di informazioni rilevanti attraverso i social media, sono osservabili nel caso della Silicon Valley Bank (SVB) e della Signature Bank che hanno generato uno stress bancario significativo in termini di sistema. Infatti, tra l'8 e l'11 marzo 2023 sono state chiuse e salvate tre banche con un patrimonio totale di circa 900 miliardi di dollari [17].

Per comprendere meglio lo sviluppo di questa corsa agli sportelli digitale è utile ricordare anche come le banche interessate fossero caratterizzate da una concentrazione dei depositi che sia per tipo di cliente che di settore visto che si trattava prevalentemente di società orientate al settore tecnologico [18]. Un ulteriore elemento da considerare è la situazione della banca dal punto di vista della liquidità e la maggiore sensibilità del mix di depositi alle variazioni dei tassi d'interesse [19].

Infatti, già prima della dichiarazione di insolvenza, sancita dalla Federal Deposit Insurance Corporation il 10 marzo 2023, vi era stato un notevole calo dei depositi, o per meglio dire uno spostamento verso "sedi" più redditizie dei fondi di private equity e venture capital [20], a seguito dell'aumento dei tassi deciso dalla Fed.

---

[16] Sul punto si veda in particolare FSB, *Depositor behaviour and interest rate and liquidity risks in the Financial System. Lessons from the march 2023 banking turmoi*, 23 ottobre 2024, p. 7, https://www.fsb.org/2024/10/depositor-behaviour-and-interest-rate-and-liquidity-risks-in-the-financial-system-lessons-from-the-march-2023-banking-turmoil/.p. 27.

[17] Sul punto si veda in particolare BIS, Report on the 2023 banking turmoil, ottobre 2023, rep. https://www.bis.org/bcbs/publ/d555.pdf.

[18] Una riflessione sul ruolo dei depositi non assicurati nel caso SVB è presente nel documento della Federal Deposit Insurance Corporation (FDIC), *Options for Deposit Insurance Reform*, 1 maggio 2023.

[19] Sul punto si veda in particolare FSB, *Depositor behaviour and interest rate* …, cit., p. 7.

[20] Come ricorda anche l'*Evaluation Report del Board of Governors of the Federal Reserve System*, la struttura di finanziamento risultava concentrata in società di private equity e venture capital e proprio per questo più soggetta a potenziale volatilità senza preavviso. Si veda il documento 2023 SR B 013, 25 settembre 2023, https://oig.federalreserve.gov/reports/board-material-loss-review-silicon-valley-bank-sep2023.pdf., p. 11.

Un tale deflusso di risorse aveva reso necessario un intervento finalizzato a limitare simili movimenti con una conseguente crescita degli interessi passivi da 0.1 a 1,2 miliardi di dollari in un anno. A questo elemento si era aggiunta, sul piano degli investimenti, la perdita derivante dai titoli a lunga scadenza venduti anticipatamente per coprire i prelievi di depositi [21].

In sostanza il problema di liquidità era stato affiancato da uno di solvibilità aggravata proprio dalla diffusione di informazioni rilevanti sul piano reputazionale e dalla velocità di azione dei depositanti [22] con conseguente produzione di problematiche di rilievo sistemico.

In particolare, la possibilità di diffondere informazioni in community di diretti interessati, nel caso in questione *venture capitalist*, la loro "intensità" di divulgazione [23] e la valutazione di attendibilità e affidabilità da parte degli interessati, nonostante provenissero da canali social, ha generato notevoli effetti sul mercato amplificati dall'alto numero di individui coinvolti anche grazie a *retweet* [24]. Del resto in un solo giorno, il 9 marzo 2023, è stata registrata una movimentazione addirittura di 42 bilioni di dollari con un deflusso pari al 24% e ad una velocità molto maggiore di quanto registrato in corse agli sportelli precedenti e "non digitali" come quella della Northern Rock [25]. Un simile deflusso è

[21] La banca aveva grandi esposizioni su portafogli a lunga scadenza. Sul punto si vedano i documenti UNITED STATES SENATE COMMITTEE ON BANKING, *Housing, and Urban Affairs, Recent Bank Failures and the Federal Regulatory Response*, 28 marzo 2023 e UNITED STATES, HOUSE OF REPRESENTATIVES FINANCIAL SERVICES COMMITTEE, *The Federal Regulators' Response to Recent Bank Failures*, 29 marzo 2023.

[22] È utile ricordare in tal senso che il deflusso dei depositi era già iniziato prima della corsa digitale agli sportelli dell'inizio del 2023. Secondo i dati riportati da N. KOONT, T. SANTOS, L. ZINGALES, cit., nel 2022 la SVB aveva già perso il 13% dei depositi.

[23] Per avere un'idea dell'intensità è utile ricordare come su Twitter, in un lasso temporale ristretto, il numero dei tweet con la parola "run" abbinata a SVB sia stato di 6.528 e quello sul contagio SVB di 9.662. Ancor più significativo è l'inizio della "conversazione" sullo stato di difficoltà della banca con il ticker sulla SVB e i tweet di invito al ritiro. Per un'analisi dei dati sui tweet nel caso SVB si veda in particolare J.A. COOKSON, C. FOX, J. GIL-BAZO, J.F. IMBET, C. SCHILLER, *Social media as a Bank Run Catalyst*, Université Paris-Dauphine Research Paper, n. 4422754, 2023, rep. www.wifpr.wharton.upenn.edu/wp-content/uploads/2023/09/Cookson-Fox-Gil-Bazo-Imbet-and-Schiller.pdf.

[24] Sul ruolo dei social media sui depositi retail si veda in particolare M. ACCORNERO, M. MOSCATELLI, *Listening to the buzz: social media sentiment and retail depositors' trust*, Working paper n. 1165, febbraio 2018, Banca d'Italia, e A. CANEPA, *L'efficacia della disciplina delle crisi bancarie e le proposte di riforma tra ripartizione di competenze, banche digitali e rischi di "fuga istantanea" dei depositi*, Quaderni di ricerca giuridica della Banca d'Italia n. 99, febbraio 2023, p. 349 ss.

[25] Proprio in riferimento al caso della corsa agli sportelli della Northern Rock avvenuta nel 2009, B. BORTOLOTTI e H.S. SHIN ricordavano come "Anche se i depositi possono essere prelevati su richiesta, fra i banchieri si sente spesso dire che è più facile divorziare che cambiare banca". Si veda IDD., *Da Mary Poppins a Northern Rock. Spunti sulle corse agli sportelli moderne*, in *Mercato Concorrenza Regole*, 2009, p. 81. Per una comparazione sulle corse agli sportelli verificatesi in passato si veda in particolare J. ROSE, *Understanding the speed and size of bunk runs in historical*

stato determinato anche della fisionomia dei depositanti coinvolti che erano principalmente di grandi dimensioni [26].

Tale aspetto fa riflettere sull'opportunità da parte delle autorità di introdurre forme di "monitoraggio" dei social media quale forma di "allerta precoce" rispetto a possibili criticità di una o più banche.

Proprio le dinamiche di questo caso inducono a soffermarsi anche sulla percentuale dei depositi non assicurati, molto elevanti nelle banche americane coinvolte, pari al 94% dei depositi nel 2022, [27] e che, alla luce di un incremento di sensibilità alla migrazione verso "sedi" più redditizie, potrebbero richiedere maggiore attenzione.

Infatti, proprio le variazioni dei tassi di interesse al rialzo, avvenute dopo un periodo di grande "stabilità" al ribasso dei tassi di interesse, anche a seguito del Covid e delle conseguenti incertezze economiche, hanno favorito una nuova attenzione degli utenti a questi aspetti e una maggiore propensione a cogliere i possibili vantaggi [28].

Tali dinamiche possono rappresentare un vantaggio per quelle banche capaci di risultare più attrattive [29] anche sul piano della liquidità, foriera però, anche di maggiori vulnerabilità e crisi di solvibilità per il possibile verificarsi di "esodi" rapidi e massicci.

In questi casi, come avvenuto nel caso delle banche americane, il fattore tempo assume rilevanza anche nella "risposta" da parte delle istituzioni per evitare costi più elevati per la gestione della crisi ed il contrasto di eventuali rischi sistemici. La necessità di un'accelerazione decisionale può però significare un maggiore ricorso a risorse pubbliche, come avvenuto nel caso americano con l'intervento della Federal Deposit Insurance Corporation, la FED ed il Tesoro, diretto a salvaguardare tutti i depositanti.

Sull'opportunità di una maggiore tempestività di azione da parte delle autori-

---

*comparison*, 26 maggio 2023, Federal Reserve Bank of St. Louis, https://www.stlouisfed.org/on-the-economy/2023/may/understanding-the-speed-and-size-of-bank-runs-in-historical-comparison.

[26] Per un approfondimento sul punto si veda in particolare M. CIPRIANI, T.M., EISENBACH, A. KOVNER, *Tracing bank run in real time*, Federal Reserve Bank of Nwe York, paper n. 1104 maggio 2024, rivisto nel dicembre 2024, https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr1104.pdf?sc_lang=en.

[27] Si veda l'*Evaluation Report del Board of Governors of the Federal Reserve System*, cit., p. 13.

[28] Per un'analisi delle implicazioni che ne possono derivare si veda in particolare il documento consultivo del COMITATO DI BASILEA, *Recalibration of shocks for interest rate risk in the banking book*, dicembre 2023, rep. https://www.bis.org/bcbs/publ/d561.pdf.

[29] È interessante in tal senso l'analisi anche sul processo di riorganizzazione delle banche alla luce della digitalizzazione e la loro riduzione della densità di filiali che inizialmente ha rappresentato un fattore di attrazione per la riduzione dei costi applicati ma successivamente è diventato anche un elemento di possibile diffidenza perché interpretabile anche come un peggioramento dello "stato di salute" della banca. Sul punto si veda in particolare E. BENMELECH, J. YANG, M. ZATOR, *Bank branch density and bank runs*, 2023, NBER Working Papers n. 31462, July 2023, rep. https://www.nber.org/papers/w31462.

tà è intervenuto anche il Financial Stability Board[30]. Nel contesto europeo l'obiettivo però non appare semplice da raggiungere vista l'esistenza di un complesso intreccio di competenze tra autorità, la necessità primariamente di una verifica dell'esistenza delle condizioni di applicabilità della risoluzione[31] e la possibilità di una gestione a livello nazionale, tutt'ora differenziata tra gli Stati, che potrebbe dare luogo ad un incremento delle eventuali risorse necessarie. Peraltro, la complessa ridefinizione di un sistema europeo di assicurazione dei depositi, tutt'ora in discussione[32] e la cui importanza è stata ribadita recentemente anche dalla BCE[33], come evidenziato anche dal caso SVB, esercita una notevole influenza sulle scelte e la fiducia dei depositanti con possibili ripercussioni in termini di liquidità, del verificarsi di una crisi e delle sue modalità di gestione[34]. Inoltre, è utile evidenziare come nel quadro delineato, emergano nuove dinamiche nel bilanciamento tra soddisfazione del cliente e redditività bancaria sulle quali nei prossimi anni l'IA potrebbe ulteriormente influire grazie alla sua utilizzabilità per comparare e indirizzare verso i depositi più in linea con le esigenze dei singoli. Ciò può significare possibili fluttuazioni di liquidità non sempre prevedibili, soprattutto dal punto di vista dei flussi, con produzione di difficoltà anche in banche apparentemente prive di criticità.

Inoltre, è opportuno tenere conto di come, proprio l'innovazione tecnologica, negli ultimi anni stia favorendo modalità sempre nuove, collegate ai pagamenti digitali, per offrire forme di detenzione del denaro capaci di diventare po-

---

[30] Il FSB alla luce della crisi delle banche americane ha evidenziato come vi sia la necessità che anche le autorità siano meglio preparate al verificarsi di corse agli sportelli realizzabili 24 h su 24, 7 giorni su 7 grazie a mobile banking ed al possibile influsso dei social media. Si veda FSB, *2023 Bank Failures: preliminay lessons learnt from resolution*, 10 ottobre 2023, p. 3.

[31] Per una ricostruzione delle decisioni e dei relativi interventi delle Corti europee si veda in particolare ECONOMIC GOVERNANCE AND EMU SCRUTINY UNIT (EGOV), *10 years of Banking Union's case-law: how did European Courts shape supervision and resolution practice in Banking Union?*, PE 755.729, September 2024, rep. https://www.europarl.europa.eu/RegData/etudes/STUD/2024/760271/IPOL_STU(2024)760271_EN.pdf.

[32] *Proposal for a directive of the european parliament and of the council amending Directive 2014/49/EU as regards the scope of deposit protection, use of deposit guarantee schemes funds, cross-border cooperation, and transparency*.

[33] Si veda nello specifico l'intervento di Claudia BUCH, chairwomen of Supervisory Board della BCE, 2 settembre 2024.

[34] Va ricordato come sul punto fosse presente una proposta nel pacchetto di modifica sulle crisi bancarie presentato nel 2023. Si tratta del documento COM (2023)228, di modifica della direttiva 2014/49/UE sul quale in data 14 giugno 2024 il Consiglio ha pubblicato il testo del mandato per la negoziazione col Parlamento europeo, 2023/0115. Mandate for negotiations with the European Parliament, 2023/115, 14 giugno 2024.

È utile ricordare che qualsiasi sistema di garanzia dei depositi sostenuto dagli Stati può indurre minore fiducia quando il sostegno è offerto da uno stato la cui situazione economica appare difficile come accaduto ad es. durante la crisi dei debiti sovrani quando si è assistito al trasferimento di molti depositi da paesi più a rischio in filiali di banche estere di paesi finanziariamente più solidi. Sul punto si veda in particolare D. BONFIM, J.A.C. SANTOS, *The importance of deposit insurance credibility*, *in Journal of Banking and Finance*, 2023, p. 1 ss.

tenzialmente concorrenti con i depositi e capaci di avere effetti nel quadro descritto.

Infine, è utile sottolineare come l'IA potrebbe rappresentare anche uno strumento capace di supportare le autorità nella previsione di fenomeni di corsa agli sportelli digitale grazie alla possibile individuazione e tipizzazione di segnali anticipatori comprensivi anche delle interazioni sui social media. Questi vantaggi vanno attentamente valutati anche alla luce dei possibili limiti dovuti all'individuazione di segnali di rischio tra loro differenziati alla luce delle "cause scatenanti" e dell'esistenza di fattori di accelerazione.

## 3. Il ruolo dell'AI nell'attività delle Banche Centrali

Nell'affrontare la struttura dei mercati finanziari il Rapporto del Financial Stability Oversight Council (FSOC) per il 2023 inseriva tra i rischi operativi e tecnologici anche l'utilizzo dell'intelligenza artificiale sottolineando proprio la sua duplice valenza quale strumento di incremento di efficienza e contestualmente anche di rischi [35]. Quest'ultimo aspetto è stato evidenziato nei paragrafi precedenti e proprio per questo si cercherà adesso di evidenziarne le potenzialità come strumento al di fuori del rapporto banca-cliente ed "al servizio" delle istituzioni. Il riferimento è in particolare al suo impiego nella supervisione vista la possibilità di ricorso all'AI nel rapporto tra soggetti vigilati e vigilanti [36], nel supporto all'identificazione di rischi combinati come quelli di liquidità e ritiro dei depositi [37] e nella velocizzazione degli interventi [38], nonché nell'ottimizzazione dei tempi delle relazioni di ispezione e nell'individuazione il più

[35] FINANCIAL STABILITY OVERSIGHT COUNCIL (FSOC), *Annual Report 2023*, p. 91 ss. rep. https://home.treasury.gov/system/files/261/FSOC2023AnnualReport.pdf.

[36] Sul punto si veda in particolare 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 Asrid, il Mulino, Bologna, 2022, p. 458.

[37] Le aree di possibile applicazione sono chiaramente più ampie e possono riguardare raccolta di informazioni al fine di costituzione di database, analisi macroeconomiche e dirette a sostenere la politica monetaria, vigilanza sui sistemi di pagamento, vigilanza e stabilità finanziaria. Sul punto si veda in particolare D. ARAUJO, S. DOERR, L. GAMBACORTA, B. TISSOT, *Artificial Intelligence in Central Banking,* in *Bis Bulletin*, n. 84 gennaio 2024, www.bis.org/publ/bisbull84.pdf.

Per favorire l'integrazione della tecnologia e dell'IA la BCE ha istituito fin dal 2019 il SupTech Lab. Sul piano nazionale si veda il piano strategico della Banca d'Italia 2023-2025 aggiornato a luglio 2024, rep. https://www.bancaditalia.it/media/notizie/2024/Piano-Strategico-2023-2025.pdf.

[38] Su questi aspetti compresa la possibilità di utilizzo nel procedimento di liquidazione coatta amministrativa si veda in particolare R. LENER, *Liquidazione coatta amministrativa e innovazione tecnologica*, in *Dialoghi di Diritto dell'Economia*, novembre 2023, p. 1 ss. Più in generale sul ruolo di velocizzazione della tecnologia nella gestione delle crisi si vedano G. LOIACONO, E. RULLI, *ResTech: innovative technologies for crisis resolution*, in *Journal of Bank Regulation*, 2022, p. 227 ss.

possibile anticipata del livello dei prestiti in sofferenza [39].

Su alcuni aspetti la sperimentazione di utilizzo è già in atto. Se consideriamo i crediti deteriorati ad esempio possiamo ricordare come, seppur non nel contesto europeo, da qualche anno [40] l'IA viene utilizzata con la finalità principale di supportare l'individuazione precoce di quei crediti, non individuati o non adeguatamente valutati, maggiormente soggetti a trasformarsi in deteriorati e capaci pertanto di generare perdite. Una simile anticipazione può consentire di richiedere preventivamente alle banche interessate di effettuare accantonamenti "di copertura" per ridurre il verificarsi di criticità [41]. In questo caso uno degli aspetti di maggiore utilità è ravvisabile proprio nella capacità di analisi ed elaborazione di un numero molto elevato di mutuatari in un giorno (pari a 3 milioni). Pur potendoci essere margini di errore, l'aspetto interessante è proprio quello della individuazione precoce delle situazioni da monitorare.

Se ci soffermiamo sul contesto europeo, la stessa Banca Centrale Europea sta approfondendo l'impiego dell'IA nelle attività di routine al fine di avere maggiore tempo da poter dedicare ai rischi più rilevanti. Allo stesso tempo, nella sua strategia per gli anni 2024-2028 sono stati previsti cospicui investimenti in applicazioni tecnologiche di supervisione volte a migliorare proprio l'analisi dei rischi ed il processo decisionale [42] in un quadro reso sempre più complesso dalla

---

[39] Su questo aspetto specifico si veda G. LEITNER, J. SINGH, A. VAN DER KRAAIJ, B. ZSÁMBOKI, *The rise of artificial intelligence: benefits and risks for financial stability*, maggio 2024, https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202405_02~58c3ce5246.en.html.

Più in generale per una panoramica dei modelli attualmente utilizzati si veda l'intervento di E. McCaul, From data to decisions: Ai and supervision, 26 febbraio 2024, www.bankingsupervision.europa.eu/press/interviews/date/2024/html/ssm.in240226~c6f7fc9251.en.html.

[40] Il riferimento è al Brasile dove il sistema ADAM, acronimo portoghese di Machine Learning Determined Sampling, applicato fin dal 2021 ha utilizzato un set di dati di formazione formato da più di 10000 analisi eseguite dagli ispettori negli anni e presenta un numero di falsi positivi molto basso. Per maggiori dettagli https://www.bcb.gov.br/en/publications/our_results_2021.

[41] Per un approfondimento sul sistema ADAM sperimentato dalla Banca centrale brasiliana e una oanoramica sull'attività delle altre banche centrali si vedano in particolare K. BEERMAN, J. PRENIO, R. ZAMIL, *Suptech tools for prudential supervision and their use during the pandemic, Financial Stability Institute n. 37*, dicembre 2021, www.bis.org/fsi/publ/insights37.pdf e D. ARAUJO, S. DOERR, L. GAMBACORTA, B. TISSOT, *Online annex for Artificial intelligence in Central Banking*, www.bis.org/publ/bisbull84_annex.pdf.

[42] Si vedano ECB, *Scaling up Suptech*, novembre 2022, www.bankingsupervision.europa.eu/press/publications/newsletter/2022/html/ssm.nl221117_4.en.html; G. CASCARINO, M. MOSCATELLI, F. PARLAPIANO, *Explainable Artificial Intelligence: interpreting default forecasting models based on Machine Learning*, Questioni di Economia e Finanza (Occasional Papers) n. 674, Banca d'Italia, 2022; C. BUCH, *Reforming the SREP: an important milestone towards more efficient and effective supervision in a new risk environment*, maggio 2024, www.bankingsupervision.europa.eu/press/blog/2024/html/ssm.blog240528~6f5a4f76c5.en.html, e ID., *The future of European banking supervision – connecting people and technology*, settembre 2024, bankingsupervision.europa.eu/press/speeches/date/2024/html/ssm.sp240918~522b3441ba.en.html e F. ELDERSON, *Embedding a strong data culture in supervision – another stepping stone towards effective supervision*, luglio

presenza ed interconnessione nel mercato finanziario di soggetti di natura finanziaria e non (basti pensare alle Big Tech).

Di particolare interesse appare uno degli strumenti realizzati, denominato Delphi, per evocare le capacità divinatorie dell'oracolo, diretto ad integrare indicatori basati sul rischio di mercato con informazioni ricavate da notizie, comprese quelle presenti sul web, al fine di generare alert funzionali a supportare le autorità di vigilanza nella valutazione del rischio di credito, nell'identificazione di rischi emergenti e nel loro sviluppo in tempo reale [43]. In particolare, gli alert sono il risultato della combinazione di sviluppi avversi, identificati mediante notizie su determinate società e loro esposizioni nei confronti delle banche. Un simile supporto può garantire un processo di valutazione più completo e soprattutto consentirebbe di intercettare preventivamente e, soprattutto, rapidamente possibili segnali derivanti dal mercato. Una simile azione è vantaggiosa dal punto di vista delle tempestività di azione perché consente di poter avere cognizione del possibile verificarsi del rischio. Allo stesso tempo apre però una riflessione sui rischi derivanti dall'utilizzo di informazioni, specialmente se presenti sul web, non sempre attendibili o non sempre valutabili in modo univoco e rispetto alle quali l'addestramento del sistema di AI, al fine di renderlo attendibile nelle valutazioni può risultare complesso.

Inoltre, i sensi regolamento europeo sull'Intelligenza artificiale [44] un'applicazione come Delphi potrebbe sembrare soggetta alle prescrizioni più stringenti derivanti dal grado di autonomia del sistema [45], comprese quelle sulla qualità dei dati di addestramento e convalida. Il considerando cinquantotto però precisa che "i sistemi di IA previsti dal diritto dell'Unione (…) a fini prudenziali per calcolare i requisiti patrimoniali degli enti creditizi e delle imprese assicurative non dovrebbero essere considerati ad alto rischio ai sensi del presente regolamento".

---

2024, www.bankingsupervision.europa.eu/press/speeches/date/2024/html/ssm.sp240705~b111343c50.en.html.

È utile ricordare come tra gli strumenti SupTech adottati a livello europeo vi siano Virtual Lab piattaforma per il SSM, Athena GPT piattaforma di analisi mediante IA, Agorà che raccoglie tutti i dati prudenziali, Navi piattaforma di analisi dati, Heimdall strumento di machine reading e analisie Gabi piattaforma per lo sviluppo di modelli di analisi dei dati.

[43] Un progetto simile denominato Ellipse è stato avviato da BIS Innovation Hub e la Monetary Authority di Singapore nel 2022. Per maggiori dettagli www.bis.org/publ/othp48.pdf.

[44] Regolamento UE 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale del 13 giugno 2024, in GUUE L del 17 luglio 2024.

[45] Si prevede anche il divieto assoluto in caso di applicazioni considerate lesive di diritti fondamentali (art. 5).

## 4. Prospettive di sviluppo dell'IA tra banche e imprese: valutazione e cessione dei crediti deteriorati nel mercato secondario

A conclusione di quest'analisi può essere utile sottolineare come nell'ambito delle crisi bancarie si possa pensare ad un utilizzo dell'intelligenza artificiale anche nel "rapporto tra banche e imprese" e nello specifico nella fase di valutazione dello stato dei crediti deteriorati [46] e nella eventuale decisione di optare per la cessione di questi crediti alle società specializzate (c.d. *credit servicer*). Più nel dettaglio potremmo dire che l'IA può offrire un supporto nell'identificazione precoce dei prestiti a rischio attraverso *alert* laddove, alla luce di modelli, si ravvisino segnali di un aumento del rischio di inadempienza e nella valutazione ai fini della possibile decisione di cessione e della tempistica migliore, sotto il profilo economico, per effettuarla.

Quest'ultimo punto merita particolare attenzione perché, come noto, anche alla luce della crisi del 2007-2008, le istituzioni europee hanno delineato una disciplina volta alla gestione dei crediti deteriorati ed in particolare a tenerne sotto controllo la crescita ed il valore. Secondo i dati di Banca d'Italia nel periodo tra il 2006 ed il 2022 su 199 miliardi di sofferenze gestite vi è stato un recupero di 65 miliardi attraverso gestione diretta e 48 tramite SVP [47]. In questo arco temporale si è inserita anche la direttiva 2021/2167 [48] volta a creare un mercato secondario dei crediti deteriorati che consentisse la loro cessione a società specializzate nella loro gestione ed iscritte in apposito albo come previsto dal d.lgs. n. 116 del 30 luglio

---

[46] Il regolamento (UE) n. 630/2019, che ha modificato il regolamento (UE) n. 575/2013 (Capital Requirements Regulation – CRR) fornisce una definizione di credito deteriorato. È utile ricordare come nelle statistiche italiane i crediti deteriorati siano suddivisi in tre classi: sofferenze e cioè le esposizioni verso soggetti in stato di insolvenza (anche non accertato giudizialmente) o situazioni equiparabili; inadempienze probabili e cioè le esposizioni per le quali la banca valuta improbabile che il debitore adempia integralmente alle sue obbligazioni contrattuali senza il ricorso ad azioni quali l'escussione delle garanzie, a prescindere dalla presenza di eventuali importi (o rate) scaduti e non pagati; esposizioni scadute o sconfinanti deteriorate cioè quelle scadute o eccedenti i limiti di affidamento da oltre 90 giorni. Sulla valutazione delle qualità del credito a fini di bilancio si ricorda anche la circolare n. 272 del 30 luglio 2008, Regole riguardanti specifiche tipologie di operazioni.

[47] Si veda Banca d'Italia, Note di stabilità e finanza, n.32/2022.

[48] Regolato dalla Direttiva (UE) 2021/2167 Secondary Market Directive (SMD) relativa ai gestori e agli acquirenti di crediti deteriorati recepita in Italia con il d.lgs. 30 luglio 2024, n. 116. Sul tema si veda in particolare F. SARTORI, *Sul "diritto della gestione degli attivi problematici (Non Performing Loans)": linee dell'evoluzione normativa*, in *Riv. dir. bancario*, 2018, p. 675 ss.; A. MALINCONICO, B. DI CERBO, *La cessione dei NPL: ostacoli e proposte per lo sviluppo del mercato europeo*, IPE Working paper n. 17, dicembre 2018, https://www.ipeistituto.it/master/images/file-pdf/WP/IPE_WP_17_2018_La-cessione-dei-NPL.pdf; F. CAPRIGLIONE, *Incidenza degli NPL sulla stabilità del sistema bancario. I possibili rimedi*, in *Riv. trim. dir. econ*., 2018, p. 217 ss. e ID., *La problematica dei crediti deteriorati*, in *Riv. trim. dir. econ*., 2019, p. 7. e V. LEMMA, *I fondi di NPL e UTP. Verso una gestione collettiva dei crediti deteriorati?, ivi*, p. 174 ss.; A. DOLMETTA, U. MALVAGNA, A.M. AROMOLO DE RINALDIS, *Gestori di NPL: ragioni di perplessità sullo schema di decreto legislativo di attuazione della direttiva 2021/2167*, in *Dialoghi di Diritto dell'Economia*, 2024, p. 1 ss.

2024 di recepimento della direttiva[49]. Nello specifico la direttiva fa riferimento a due categorie di operatori e cioè gli acquirenti dei crediti in sofferenza e i gestori di crediti in sofferenza di cui debbono necessariamente avvalersi gli acquirenti di crediti per lo svolgimento delle attività di gestione.

La ratio alla base dell'introduzione di misure finalizzate alla creazione e sviluppo di un mercato secondario è stata quella di generare benefici in termini di stabilità finanziaria e migliore funzionamento del mercato europeo dei capitali.

Tale opzione, vista la combinazione di regole contabili e di gestione in bilancio da rispettare per la gestione dei crediti deteriorati, ha favorito negli ultimi anni un ampio ricorso al mercato secondario da parte delle banche[50].

Infatti, il rischio di peggioramento/ulteriore svalutazione dei crediti interessati e le conseguenti implicazioni di bilancio hanno rappresentato per le banche un elemento di valutazione nonché un possibile incentivo alla cessione dei crediti deteriorati al fine di liberare capitale e migliorare i propri coefficienti patrimoniali[51].

In sostanza la banca, come ricordato da Lemma, attraverso la cessione "realizza un investimento rappresentato da strumenti finanziari e ponderato sulla base del valore che il gestore saprà estrarre dagli stessi"[52].

L'appetibilità di effettuare simili operazioni di cessione trova una conferma nei dati del rapporto 2023 di Banca d'Italia sui tassi di recupero delle sofferenze[53] dai quali emerge, negli ultimi anni, un costante incremento delle cessioni[54].

---

[49] In GU n. 189 del 13 agosto 2024. La previsione dell'Albo è indicata all'art. 114.5.

[50] Il riferimento è agli standard contabili basati sulle perdite attese nonché all'approccio di svalutazione progressiva dei NPL fino alla svalutazione integrale. Più in generale per un quadro ricostruttivo degli interventi di riforma del diritto bancario europeo e delle relative implicazioni si veda A. BROZZETTI, "*Ending of too big to fail" tra soft law e ordinamento bancario europeo. Dieci anni di riforme*, Cacucci, Bari, 2018.

[51] Per un approfondimento sul ricorso alla cartolarizzazione nel quadro di mercato attuale si vedano in particolare F. GONZALES, C. MORAR TRIANDAFIL, *The European significant risk transfer securitisation market*, ESRB Occasional paper 2023, https://www.esrb.europa.eu/pub/pdf/occasional/esrb.op23~07d5c3eef2.en.pdf#:~:text=The%20European%20significant%20risk%20transfer%20%28SRT%29%20securitisation%20market,of%20capital%2C%20flexibly%20and%20at%20a%20reasonable%20cost. e European Union, NPL Advisory Panel, Secondary Markets forn Non-Performing Loans: the role of securitisation, novembre 2023, https://finance.ec.europa.eu/document/download/4f537f03-1193-41b8-b06f-97ba84cb7f74_en?filename=2311-npl-advisory-panel-securitisation-paper_en.pdf.

[52] V. LEMMA, *op. cit*., p. 181. È utile ricordare come in questo processo le autorità valutino le transazioni facendo attenzione al grado di trasferimento di rischio dalle banche agli investitori.

[53] Nello specifico il rapporto segnala come nel 2022 siano state eliminate dai bilanci delle banche posizioni per circa 22 miliardi di euro e come l'incremento rispetto al 2021 sia ascrivibile principalmente alle cessioni passate da 14 a 18 milioni mentre l'ammontare delle posizioni chiuse in via ordinaria è rimasto sostanzialmente stabile. Si veda A. FISCHETTO, I. GUIDA, A. RENDINA, G. SANTINI, *Note di stabilità finanziaria e vigilanza n. 35*, Banca d'Italia, dicembre 2023, https://www.bancaditalia.it/pubblicazioni/note-stabilita/2023-0035/index.html?

[54] Si veda C. FRIGENI, *La governance bancaria come risk governance: evoluzione della regolazione internazionale e trasposizione nell'ordinamento italiano*, in M. MANCINI, A. PACIELLO, V. SANTORO, P. VALENSISE (a cura di), *Regole e Mercato*, Giappichelli, Torino, 2017, p. 45.

A fronte dei benefici per la banca, non più gravata dall'onere di mantenimento delle posizioni deteriorate, c'è da chiedersi se la società specializzata sia altrettanto capace di garantire strategie di continuità aziendale di un'impresa debitrice[55], laddove le condizioni lo consentano. Un simile dubbio appare giustificato sia dalla sostanziale mancanza di coordinamento tra le misure del codice della crisi e quelle inerenti il mercato dei crediti deteriorati, sia dalla differente logica, prevalentemente finanziaria, per non dire spesso liquidatoria[56], alla base dell'intervento del *credit servicer*. Del resto nel recupero crediti l'efficienza difficilmente va di pari passo con prospettive di lungo periodo.

Peraltro, un eventuale peggioramento delle prospettive di ripresa può avere riflessi anche per le banche qualora ad esempio, l'impresa interessata faccia parte di una filiera e la sua situazione possa influire anche sugli altri componenti della filiera magari anch'essi clienti della medesima banca. Inoltre, l'ampio ricorso alla cessione può determinare nel tempo un riassetto organizzativo delle banche stesse foriero però anche di una possibile riduzione complessiva delle competenze e capacità gestionali di tali crediti con possibili riflessi, nonostante disposizioni come quelle sulle Funzioni Operative Importanti (FOI)[57], nel caso in cui il *servicer* avesse difficoltà nella gestione dei portafogli. Peraltro, le performance degli operatori nel recupero hanno notevole rilevanza, come già evidenziato da Banca d'Italia nel 2020, in relazione al prezzo degli NPLs[58].

Il tema meriterebbe un approfondimento che non può essere oggetto del presente lavoro ma un punto in particolare merita attenzione ed è la questione della scelta di cessione della banca e delle implicazioni che ne possono derivare.

Due appaiono i punti di interesse. Il primo riguarda la scelta di cessione e la necessità avvertita dal legislatore di precisare, in sede di recepimento, che essa deve essere caratterizzata da un quadro informativo completo al fine di una valutazione del credito e della possibilità di recupero di valore. Si tratta di un aspetto

---

[55] È utile ricordare come in realtà la direttiva 2021/2167 preveda tra le attività di gestione del credito includa anche la rinegoziazione con il debitore dei termini e delle condizioni (art. 3, comma 9).

Su quest'aspetto anche in rapporto al nuovo codice della crisi si veda in particolare C. MOTTI, *L'evoluzione del ruolo delle banche nella crisi d'impresa*, in A. BROZZETTI (a cura di), *Banche, Europea e sviluppo economico*, Giuffrè, Milano, 2023, p. 83 ss.

[56] Sul punto si veda in particolare L. STANGHELLINI, N. USAI, *La gestione dei crediti deteriorati: strumenti giuridici, best practices e possibili evoluzioni, anche alla luce del codice della crisi*, in *Il dir. fall. e delle soc. comm.*, 2023, p. 978 ss. Per un quadro più generale sugli aspetti contabili e di bilancio M. MAGGIOLINO, *La disciplina giuridica della gestione dei crediti deteriorati nella prospettiva delle banche: profili critici*, Egea, Milano, 2020, pp. 112 e 152 ss.

[57] I FOI impongono che l'intermediario debba assicurare un presidio efficace in caso di rientro di queste attività ovvero di inefficienza del fornitore. Si veda in particolare la Segnalazione in materia di esternalizzazione di funzioni aziendali per gli intermediari vigilati, Provvedimento Banca d'Italia, delibera 166/2023; EBA/GL/2019/02; ESMA50-164-4285.

[58] Si veda Banca d'Italia, Diposizioni di vigilanza per la gestione dei crediti in sofferenza e la Nota illustrativa Approfondimento della Banca d'Italia sull'attività di gestione e recupero di crediti deteriorati del marzo 2020.

non solo funzionale all'intervento del *credit servicer* ed ai relativi effetti sugli accantonamenti [59] ma anche alla valutazione di mercato. Proprio a quest'aspetto si collega la seconda riflessione relativa ai prezzi sul mercato secondario che, come già evidenziato anche dai considerando della direttiva 2021/2167 [60], sono spesso bassi. Del resto, la situazione di mercato vede un'alta offerta proprio per la scelta delle banche di ricorrere sempre di più alle cessioni ed una domanda non altrettanto elevata visto anche il numero limitato di potenziali acquirenti.

Il tema dei prezzi assume una rilevanza specifica in relazione ai c.d. *Unlike To Pay* (UTP) perché si tratta di crediti per i quali la banca valuta improbabile l'adempimento da parte del debitore (siano essi ad es. finanziamenti, mutui o prestiti) anche senza che si sia ancora verificato il mancato rimborso di una rata [61]. Tale aspetto, nel quadro di una possibile cessione [62], appare di notevole interesse e può far decidere alla banca di procedere in una fase molto precoce per evitare i relativi accantonamenti. Apparentemente la ratio di una simile scelta appare vantaggiosa in quanto, non essendo l'interessato ancora inadempiente potrebbe esserci una migliore possibilità di recupero.

La valutazione però non è così lineare come potrebbe apparire visto che è basata su un certo grado di discrezionalità e non su parametri quantitativi fatta salva la primaria finalità di scegliere l'opzione capace di garantire maggiore recupero di valore.

Proprio per questo già diversi anni Capriglione sottolineava come fosse opportuno "non procedere a cessioni a prezzi significativamente inferiori ai valori di libro; ciò in quanto tali vendite possono produrre effetti indesiderati, erodendo la base patrimoniale degli enti creditizi che cedono gli NPL, con possibili ripercussioni sulla loro stabilità finanziaria" [63].

In tal senso dovrebbe essere valutato con attenzione anche il ricorso a ces-

---

[59] La previsione degli accantonamenti prudenziali con differenziazioni tra crediti garantiti e non era stata introdotta con il Reg. n. 630/2019.

[60] In particolare, il cons. 15 recita "La mancanza di pressione concorrenziale sul mercato per l'acquisto di crediti e per le attività di gestione dei crediti fa sì che le società di gestione dei crediti applichino agli acquirenti di crediti commissioni elevate per i loro servizi e ciò genera prezzi bassi sui mercati secondari del credito. Ciò riduce gli incentivi per gli enti creditizi a disfarsi dei loro stock di crediti deteriorati".

[61] La circolare di Banca d'Italia n. 272 del 30 luglio 2008 con il 10 aggiornamento del dicembre 2017aveva definito gli UTP facendo riferimento evidenziando come si tratti di inadempienze improbabili rispetto alle quali la banca valuta improbabile che, senza il ricorso ad azioni quali ad esempio l'escussione delle garanzie, il debitore possa adempiere integralmente alle sue obbligazioni creditizie. Tale valutazione deve essere operata in maniera indipendente dalla presenza di eventuali importi (o rate) scaduti e non pagati.

Come ricorda P. MESSINA, la valutazione può avvenire anche in presenza di elementi come una crisi del settore in cui opera il soggetto debitore che possano far ipotizzare un forte rischio di inadempimento. Si veda ID., *Unlike to pay,* in *Riv. trim. dir. econ.*, 2019, p. 201.

[62] È utile sottolineare come il D.Lgs. 114/2024 faccia esplicito riferimento alla sola cessione di crediti in sofferenza.

[63] F. CAPRIGLIONE, *Incidenza degli NPL sulla stabilità del sistema bancario …*, cit., p. 237.

sioni "in blocco" [64] che richiederebbero una valutazione "caso per caso" perché gli esiti, proprio sul piano dell'entità del recupero, potrebbero risultare differenti. A questo aspetto se ne intreccia anche un altro relativo alla possibilità di chi acquisisce, alla luce della sua natura, abbia una minore capacità di supportare una ristrutturazione capace di consentire un migliore recupero dal punto di vista dell'ammontare.

Si tratta di un punto che assume rilievo ancora maggiore alla luce di quanto previsto dal d.lgs. 30 luglio 2024, n. 116 laddove stabilisce che tra i compiti del gestore vi è anche "la rinegoziazione dei termini e delle condizioni contrattuali con il debitore" [65].

Il medesimo decreto aggiunge, come anticipato, che sul piano informativo le banche devono fornire "ai potenziali acquirenti di crediti in sofferenza le informazioni necessarie a questi ultimi per effettuare una valutazione del credito e della probabilità di recuperarne valore" e prescrive che le informazioni fornite debbono essere "corrette, chiare e non ingannevoli" [66]. Del resto, l'elemento informativo nel caso dei crediti in oggetto assume una duplice rilevanza: in una prima fase quando è funzionale a determinarne la concessione ed i termini e successivamente in presenza di un'eventuale cessione per la determinazione del prezzo. I due aspetti potrebbero anche essere correlati nel caso in cui il deterioramento sia frutto di un'analisi dei dati disponibili non corretta o errata con conseguente valutazione di affidabilità maggiore di quanto avrebbe dovuto essere. Su quest'ultimo punto, se si pensa al credit scoring, il ricorso all'intelligenza artificiale al fine di migliorare la stima è già ampiamente diffuso [67]. In questo

---

[64] Come noto, per i crediti deteriorati oltre al ricorso alla cessione in blocco le banche possono utilizzare le società veicolo ed alla cartolarizzazione delle sofferenze. Quest'ultima soluzione è stata adottata in particolare nel 2016 in coincidenza con l'adozione delle garanzie sulla cartolarizzazione delle sofferenze (GACS). Nel caso di cessioni in blocco uno degli aspetti più complessi potrebbe essere la differenziazione delle posizioni e l'inclusione anche di ipoteche su alcuni dei crediti ceduti con conseguente necessario rispetto delle formalità previste dall'art. 2843 c.c. Anche l'eventuale ricorso alla cessione in blocco ai sensi dell'art. 58 TUB e il conseguente assolvimento delle formalità previste potrebbe non esonerare dalla notifica individuale al singolo debitore della cessione. Si vedano in tal senso Cassazione n. 21281del 20 luglio 2023, Tribunale di Monza, sez. III, n. 1823/2023, Ordinanza del Tribunale di Brindisi 5 dicembre 2023, Cassazione, sez. III, n. 3405 del 6 febbraio 2024 e Corte d'Appello di Messina, n. 950 del 31 ottobre 2024. Per un commento dell'art. 58 si vedano in particolare V. TROIANO, *Art. 58 cessione di rapporti giuridici e banche*, in F. CAPRIGLIONE (a cura di), *Disciplina delle banche e degli intermediari finanziari. Commento al d.lgs. 385/1993*, Cedam, Padova, 1995, p. 170 ss.; P. MESSINA, *Requisiti di validità della cessione dei crediti 'in blocco'*, in *Foro it*., 2019, p. 3988 ss.

[65] Art. 114.1 co. 1.

[66] Si tratta rispettivamente dell'art. 114.8 lett. *a*, *b* e *d* che prescrivono correttezza, diligenza e trasparenza; informazioni corrette, chiari e non ingannevoli nonché in rapporto alle comunicazioni con i debitori la necessità di agire senza molestia, coercizione o indebito condizionamento. A tal proposito Dolmetta, Malvagna e Aromolo De Rinaldis sottolineano la peculiarità di una simile scelta di ribadire aspetti già previsti per la cessione di diritto comune. Si veda DOLMETTA, MALVAGNA, AROMOLO DE RINALDIS, *op. cit*., p. 3.

[67] Sullo sviluppo e i problemi nell'utilizzo del credit scoring si vedano in particolare. L. AMMANNATI, G. GRECO, *Piattaforme digitali, algoritmi e big data: il caso del credi scoring algoritmico,* in *Riv.*

quadro, visto che una delle principali difficoltà risiede nella valutazione del valore di questi crediti gli algoritmi predittivi potrebbero assumere un ruolo di supporto proprio per favorire stime differenziate in rapporto alle tempistiche di cessione alla luce della situazione del soggetto interessato e della tipologia di credito deteriorato [68].

Tale impiego potrebbe in parte rispondere anche ad alcune delle criticità delineate dal Rapporto annuale 2023 della BCE laddove si evidenziavano gravi debolezze nel processo di identificazione del deterioramento del credito sia in rapporto ad aumenti significativi del rischio di credito che degli UTP e delle perdite di credito attese [69].

Peraltro, un possibile utilizzo dell'IA in tutta la filiera del credito dalla valutazione del merito creditizio [70] dalla concessione fino alla gestione degli UTP e dei crediti deteriorati potrebbe avere riflessi non solo sulle singole posizioni ma di sistema. Infatti, è utile ricordare che, anche se il dato dei NPLs risulta in calo da alcuni anni [71], l'inflazione e le variazioni del tasso di interesse potrebbero influire su questo andamento nel medio periodo.

---

*trim. dir. econ*., 2/2021, p. 290 ss. e ID., *Il credit scoring "intelligente": esperienze, rischi e nuove regole,* in L. AMMANNATI, A. CANEPA, *La finanza nell'età degli algoritmi*, Giappichelli, Torino, 2023, p. 1 ss.

[68] In tal senso, ad esempio è utile ricordare come ad esempio per i mutui, sia già in corso di sperimentazione l'utilizzo dell'IA da parte delle società specializzate per stimare in anticipo il possibile valore di mercato ed i tempi di vendita di un immobile.

[69] Si veda ECB, *Annual Report on Supervisory Activities*, 2023, p.1.3.3.1, https://www.bankingsupervision.europa.eu/press/other-publications/annual-report/html/ssm.ar2023~2def923d71.en.html.

[70] Il credit scoring algoritmico si presenta ancora principalmente basato su fonti interne e banche dati creditizie anche se nel credito al consumo in particolare le piattaforme di BNPL si basano su algoritmi che utilizzando anche altri dati come quelli di "fedeltà" e affidabilità dedotta dalla storia creditizia con la piattaforma. Sul primo aspetto si vedano in particolare L. AMMANNATI, G. GRECO, *Il credit scoring "intelligente": esperienze rischi e nuove regole*, in *Riv. dir. bancario*, 2023, p. 461 ss. e M. RABITTI, *Credit scoring via machine learning e prestito responsabile*, in E. GINEVRA, R. LATTANZI, U. MALVAGNA, U. MINNECI, G. MUCCIARRONE, A. SCIARRONE ALIBRANDI (a cura di), *L'orizzonte è una linea che non c'è. Liber Amicorum per A. Dolmetta*, Pacini, Pisa, 2023, p. 333 ss.; L. GAMBACORTA, H. YIPING, Q. HAN, W. JINGYI, *How do machine learning and non-traditional data affect credit scoring New evidence from a Chinese fintech firm*, in *Journal of Financial Stability*, 2024.

Sulla tipologia di dati utilizzati dalle piattaforme di BNPL si consenta il rinvio a A. CANEPA, *Super Apps, pagamenti mobile e nuove forme di credito digitale al consumo: il Buy Now Pay Later*, in L. AMMANNATI, A. CANEPA, *La finanza nell'età degli algoritmi*, Giappichelli, Torino, 2023, p. 95 ss. e IDD., *"Alla ricerca del tempo perduto" nei mercati finanziari: l'accelerazione digitale nei pagamenti, nell'accesso al credito e nella movimentazione dei depositi*, in *Riv. trim. dir. econ*., 2024, p. 524 ss.

[71] Il rapporto della Banca Centrale Europea aggiornato al 2024 indicava una percentuale del 2,6 di crediti classificati come deteriorati a livello europeo pari ad un volume di 347 bilioni. Si veda https://www.ecb.europa.eu/press/pr/date/2025/html/ecb.pr250207~cb9caa3836.it.html

# Dalla giustizia civile alla giustizia alternativa nell'era digitale

Chiara Reali*

SOMMARIO: 1. Introduzione. – 2. Lo scenario giuridico di riferimento. La "Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziali e negli ambiti connessi". – 3. (*Segue*) Il percorso europeo verso la regolamentazione della materia. – 4. (*Segue*) Il quadro normativo attuale. – 5. Opportunità e rischi dell'impiego dell'intelligenza artificiale nel settore della giustizia civile. – 6. L'intelligenza artificiale nei sistemi di risoluzione stragiudiziale delle controversie. – 7. Riflessioni conclusive.

## 1. Introduzione

Negli ultimi anni è cresciuto l'interesse per l'innovazione tecnologica e per i connessi risvolti applicativi nell'ambito giudiziario. In particolare, i sistemi di intelligenza artificiale sono oggetto di studio e di dibattito per incrementare l'efficienza della giustizia: come si dirà meglio nel prosieguo, se, da un lato, ne sono riconosciuti i vantaggi in termini di certezza del diritto e celerità delle decisioni, dall'altro, è emersa fin da subito la necessità di introdurre cautele per uno sviluppo di queste tecnologie sicuro, affidabile e rispettoso dei diritti fondamentali.

Sono state date più definizioni di "Intelligenza Artificiale" ("IA" o, con l'acronimo inglese di *Artificial Intelligence*, "AI"): si è parlato di sistemi computazionali in grado di eseguire diverse attività che altrimenti richiederebbero l'impiego dell'intelligenza umana[1]; di una locuzione che descrive "*la possibilità che le macchine, in una certa misura, «pensino», o piuttosto imitino il pensiero umano, basato sull'apprendimento e sull'utilizzazione di generalizzazioni, che le perso-*

* Le opinioni espresse sono personali e non impegnano in alcun modo l'Istituto di appartenenza.

[1] Il termine "intelligenza artificiale" è stato coniato dal matematico e informatico statunitense John McCarthy nel 1955. McCarthy è stato uno dei pionieri nel campo dell'intelligenza artificiale e ha ricoperto un ruolo significativo nello sviluppo delle prime idee e dei primi concetti fondamentali in materia (cfr. J. MCCARTHY, M.L. MINSKY, N. ROCHESTER, C.E. SHANNON, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, August 31, 1955, in *AI Magazine*, 27, 2006, 12-14).

*ne usano per prendere le decisioni quotidiane*" [2]. O ancora, di "*abilità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività*" [3].

Nel regolamento dell'UE sull'intelligenza artificiale – primo atto legislativo al mondo a disciplinare la materia – il sistema di IA viene definito 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*" [4].

Esistono in particolare due tipologie di IA: l'intelligenza artificiale debole, che si riferisce ai sistemi progettati per compiti specifici, sfruttando qualità come l'apprendimento automatico da parte della macchina, opportunamente allenata da set di dati pertinenti, e l'intelligenza artificiale forte, che mira a realizzare una vera e propria intelligenza comparabile a quella umana, trattandosi di sistemi in grado di simulare a pieno titolo il comportamento dell'uomo, in quanto agiscono in maniera del tutto autonoma, a prescindere dal contesto di riferimento e dai possibili compiti loro assegnati.

In ambito giuridico le tecnologie più utilizzate dai modelli di IA sono: il *Machine Learning*, che consiste nell'applicazione di metodi di apprendimento automatico, basati, cioè, sull'immagazzinamento, sull'incrocio e sulla correlazione coordinata di una gran quantità di dati in entrata, nonché sulla deduzione di un modello e sulla successiva applicazione di tale modello ai nuovi casi (in "autoapprendimento") [5]; il *Natural Language Processing* [6], che si riferisce al trattamento informatico del linguaggio umano, con lo scopo di sviluppare algoritmi in grado di analizzare, rappresentare e quindi "comprendere" il linguaggio naturale, scritto o parlato, in maniera similare o addirittura più performante rispetto agli esseri umani.

In tutti i casi ciò che contraddistingue questi modelli è la capacità di analizzare una moltitudine di dati, potendo essere utilizzati per supportare l'organo giudicante a vari livelli, dalla fase di valutazione delle prove fino a quella decisoria.

---

[2] Così J. NIEVA FENOLL, *Intelligenza artificiale e processo*, Giappichelli, Torino, 2019.

[3] È quanto si legge sul sito del Parlamento europeo.

[4] Art. 3, n. 1 del Regolamento (UE) 2024/1689 del 13 giugno 2024, sul quale si rinvia al par. 4.

[5] Si distinguono in particolare 3 modelli: i) l'apprendimento supervisionato (da un essere umano), in cui al sistema viene sottoposto un insieme di dati di addestramento etichettati (il c.d. *training set*), a partire dai quali classificare i casi nuovi; ii) l'apprendimento "per rinforzo", in cui viene "insegnato" al sistema come identificare successi e fallimenti a partire da proprie o altrui azioni, in base all'incidenza di queste ultime sul raggiungimento dell'utilità perseguita; iii) l'apprendimento non supervisionato, caratterizzato dall'assenza di indicazioni esterne (dati non strutturati).

[6] Si tratta di un'applicazione di *Deep Learning* (apprendimento profondo), che consiste di un insieme di tecniche basate su reti neurali artificiali somiglianti al cervello umano, che consentono ai computer di apprendere dai dati senza la supervisione e l'intervento umano. Inoltre, questi metodi possono adattarsi ai cambiamenti degli ambienti e fornire un miglioramento continuo alle capacità apprese.

Il dibattito fin qui sviluppatosi si è concentrato sull'applicazione dell'intelligenza artificiale alle decisioni giudiziarie: qui si intende ripercorrere il quadro giuridico di riferimento e le considerazioni maturate con riferimento alla giustizia civile, per vedere successivamente come il primo incide sui sistemi di risoluzione alternativa delle controversie (*Alternative Dispute Resolution* – ADR) e quante delle seconde siano replicabili per tali sistemi.

## 2. Lo scenario giuridico di riferimento. La "Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziali e negli ambiti connessi"

Il primo testo europeo che stabilisce principi etici per l'utilizzo dell'IA in ambito giudiziario è la "*Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziali e negli ambiti connessi*", adottata nel dicembre 2018 dalla Commissione europea per l'efficienza della giustizia (CEPEJ), che costituisce una ramificazione del Consiglio d'Europa. Il documento, di carattere non vincolante, costituisce il primo tentativo di sistematizzazione del trattamento automatizzato – basato su tecniche di IA – delle decisioni e dei dati giudiziari, fornendo risposte concrete alle preoccupazioni che i sistemi algoritmici, applicati alla giustizia, sollevano in relazione al rispetto dei diritti individuali e alla protezione dei dati personali.

La carta individua cinque principi sostanziali e metodologici, applicabili sia agli attori privati (come le *start-up* attive sul mercato delle nuove tecnologie applicate ai servizi giuridici – le *legaltech*), sia alle autorità pubbliche: il principio del rispetto dei diritti fondamentali; il principio di non discriminazione; il principio di qualità e sicurezza; il principio di trasparenza, imparzialità ed equità; infine, il principio del "*controllo da parte dell'utilizzatore*".

Con il principio del rispetto dei diritti fondamentali, si prescrive che l'elaborazione e l'impiego dei sistemi di IA siano compatibili con tali diritti, come sanciti nella Carta EDU e nella Convenzione n. 108 del Consiglio d'Europa. "*Quando gli strumenti di intelligenza artificiale sono utilizzati per dirimere una controversia, per fornire supporto nel processo decisionale giudiziario, o per orientare il pubblico, è essenziale assicurare che essi non minino le garanzie del diritto di accesso a un giudice e del diritto a un equo processo (parità delle armi e rispetto del contraddittorio)*". La Carta sottolinea quindi l'opportunità di "*approcci* etico-fin dall'elaborazione *o* diritti-umani-fin-dall'elaborazione*"*.

Il principio di non discriminazione è volto a "*prevenire specificamente lo sviluppo o l'intensificazione di qualsiasi discriminazione tra persone o gruppi di persone*" e a incoraggiare "*l'utilizzo dell'apprendimento automatico e delle analisi scientifiche multidisciplinari, al fine di contrastare tali discriminazioni*".

Il principio di qualità e sicurezza si riferisce al "*trattamento di decisioni e dati giudiziari*", stabilendo a tale fine di *"utilizzare fonti certificate e dati intangibili con modelli elaborati multidisciplinarmente, in un ambiente tecnologico sicuro*". L'elaborazione dei dati dovrebbe quindi avvenire mediante l'apprendimento au-

tomatico basato su certificati originali, dovendosi altresì garantire l'integrità di questi dati in tutte le fasi dell'elaborazione. Inoltre, si raccomanda la creazione di gruppi di lavoro multidisciplinari, integrati da giudici e ricercatori di scienze sociali e informatiche, sia per la fase di elaborazione, sia per la successiva applicazione delle soluzioni proposte.

Il principio di trasparenza, imparzialità ed equità è volto a "*rendere le metodologie di trattamento dei dati accessibili e comprensibili, autorizzare verifiche esterne*", sancendo che "*[d]eve essere raggiunto un equilibrio tra la proprietà intellettuale di alcune metodologie di trattamento e l'esigenza di trasparenza (accesso al processo creativo), imparzialità (assenza di pregiudizi), equità e integrità intellettuale (privilegiare gli interessi della giustizia), quando si utilizzano strumenti che possono avere conseguenze giuridiche, o che possono incidere significativamente sulla vita delle persone*".

Infine, il principio del "*controllo da parte dell'utilizzatore*" impone di "*precludere un approccio prescrittivo e assicurare che gli utilizzatori siano attori informati e abbiano il controllo delle loro scelte*". Si sottolinea così che i "*professionisti della giustizia dovrebbero essere in grado, in qualsiasi momento, di rivedere le decisioni giudiziarie e i dati utilizzati per produrre un risultato e continuare ad avere la possibilità di non essere necessariamente vincolati a esso alla luce delle caratteristiche specifiche di tale caso concreto*". Inoltre, si deve informare ciascun utente, con un linguaggio chiaro e comprensibile, in merito alla natura vincolante o meno delle soluzioni proposte dagli strumenti di IA, nonché con riguardo al suo diritto alla tutela legale e al ricorso innanzi all'Autorità giudiziaria.

La Carta si compone poi di alcune Appendici dove la CEPEJ si sofferma sulle applicazioni possibili e formula raccomandazioni specifiche, individuando vantaggi e rischi.

In particolare, nella Carta si evidenzia come l'utilizzo dell'IA nei sistemi giudiziari possa contribuire al miglioramento dell'efficienza della giustizia: "*la previsione delle decisioni dei giudici in materia civile, commerciale e amministrativa sembra essere un vantaggio potenzialmente auspicabile, benché talvolta per motivi molto diversi, sia per i responsabili della politica giudiziaria pubblica che per i professionisti privati del diritto. Qualunque sia la tradizione giuridica del Paese, l'incertezza giuridica, ovvero il rischio di vedere la propria pretesa giuridica accolta o rigettata, suscita il desiderio di essere in grado di quantificare tali fattori grazie all'ausilio di tali nuove applicazioni tecnologiche*"[7]. Vengono così analizzati gli strumenti di IA di "giustizia predittiva", ovvero i modelli utilizzati per il trattamento e l'analisi della giurisprudenza con lo scopo di prevedere l'esito di un giudizio[8], precisandosi che sarebbe più consono parlare di "previsione" e non di "predizione". Infatti, "*[l]a*

[7] Cfr. par. 6 del documento.

[8] Per "giustizia predittiva" si intende la possibilità di prevedere l'esito di un giudizio tramite determinati calcoli: la probabile sentenza relativa a uno specifico caso, attraverso l'ausilio di algoritmi. I sistemi di giustizia predittiva sono capaci di raccogliere tutta la giurisprudenza su una determinata fattispecie e stimare le probabilità che i procedimenti giudiziali ad incardinarsi si risolvano in un senso o in un altro. Cfr. sul tema L. VIOLA, *Giustizia predittiva*, in *Enc. giur*., Roma, 2018.

*predizione è l'atto di annunciare anticipatamente* (prae*, prima* – dictare*, dire) gli avvenimenti futuri (per ispirazione sovrannaturale, chiaroveggenza o premonizione). La previsione, d'altra parte, è il risultato dell'osservazione* (visere*, vedere) di un insieme di dati al fine di prevedere una situazione futura*" [9].

La CEPEJ conclude che dovrebbero essere incoraggiati gli utilizzi dell'IA per valorizzare il patrimonio giurisprudenziale, per facilitare l'accesso al diritto (senza sostituire l'intervento umano) e per implementare nuovi strumenti strategici, "*permettendo, per esempio, di svolgere valutazioni quantitative e qualitative e di effettuare proiezioni (per esempio in relazione alle future risorse umane e di bilancio)*" [10].

Nella Carta sono infine indicati come utilizzi possibili, ma con "*notevoli precauzioni metodologiche*" [11], gli strumenti di IA volti a fornire supporto per la redazione di tabelle relative ad alcune controversie di carattere civile (come in tema di risarcimento del danno), per le misure di risoluzione alternativa delle controversie in materia civile, alle quali gli utenti siano indirizzati se le possibilità di successo delle vie giudiziarie appaiono scarse, nonché per la risoluzione delle controversie *on line*, rispetto alle quali si raccomanda che le parti siano informate in modo chiaro e comprensibile del fatto che il trattamento della loro controversia è svolto in modo interamente automatico o con la partecipazione di un mediatore o di un arbitro.

Per contro, viene riportato come utilizzo "*da esaminare al termine di supplementari studi scientifici*" il modello di IA destinato ad anticipare le decisioni dei tribunali, in quanto "*il solo trattamento statistico di dati lessicali rivela la frequenza dell'utilizzo di alcuni gruppi di parole ma non individua i motivi reali di una decisione e non svolge un'analisi giuridica*"; d'altra parte, i "*sistemi ibridi, basati sulla costruzione di modelli matematici che si suppone rappresentino una gamma diversificata del ragionamento dei giudici, non sono più efficienti perché rimangono limitati dagli errori del campione di dati che hanno trattato o se vi è stato un ribaltamento della giurisprudenza*" [12].

## 3. (*Segue*) Il percorso europeo verso la regolamentazione della materia

L'attenzione dell'Unione Europea allo sviluppo dell'intelligenza artificiale – e alla relativa applicazione, tra l'altro, ai sistemi giudiziari – è testimoniata dal percorso che, attraverso una serie di atti non vincolanti, ha portato all'adozione in

[9] Cfr. par. 3 della Carta. Si legge nel prosieguo che "*L'espressione giustizia predittiva dovrebbe essere abbandonata in quanto è ambigua e ingannevole. Tali strumenti sono basati su metodi di analisi della giurisprudenza che utilizzano metodi statistici che non riproducono in alcun modo il ragionamento giuridico, ma possono cercare di descriverlo*".

[10] Cfr. Appendice II.

[11] *Ibidem.*

[12] *Ibidem.*

data 13 giugno 2024 del Regolamento (UE) 2024/1689, che stabilisce regole armonizzate sulla materia.

La prima iniziativa europea nel settore può essere individuata nella risoluzione del Parlamento europeo del 16 febbraio 2017 "*recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*" [13]: già con tale risoluzione emerge lo scopo europeo di individuare un equilibrio che sostenga l'innovazione tecnologica mantenendo al contempo un'elevata sicurezza e tutela dei diritti dei cittadini.

Con la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni del 25 aprile 2018, recante *"Intelligenza Artificiale per l'Europa"* [14], sono stati delineati gli obiettivi di: *i*) implementare gli investimenti nella ricerca e nell'innovazione; *ii*) preparare i cittadini europei ai mutamenti socioeconomici apportati dall'intelligenza artificiale; *iii*) predisporre e assicurare un quadro etico e giuridico adeguato.

Con la successiva Comunicazione del 7 dicembre 2018 la Commissione europea ha diffuso il "*Piano coordinato sull'intelligenza artificiale*" [15], volto a promuovere gli investimenti e la cooperazione con gli Stati membri nello sviluppo dell'intelligenza artificiale, per assicurare la competitività dell'Unione nel suo complesso.

Poco dopo la conclusione dei lavori della CEPEJ [16], il Parlamento europeo è tornato in argomento con la risoluzione del 12 febbraio 2019, recante "*Una politica industriale europea globale in materia di robotica e intelligenza artificiale*" [17], ove ha sottolineato la necessità di promuovere lo sviluppo di una "*società sostenuta dall'intelligenza artificiale e dalla robotica*", come fattore indispensabile per migliorare la produttività delle imprese, la crescita economica e il benessere sociale, pur a fronte dei possibili usi illeciti dei sistemi IA, che possono determinare gravi pericoli per la tutela dei diritti individuali e della sicurezza nazionale, nonché per la tenuta stessa della democrazia.

L'approccio antropocentrico all'IA, volto a garantire che i valori umani rivestano un ruolo centrale nelle modalità di implementazione, distribuzione e utilizzo delle nuove tecnologie, è testimoniato dagli "*Orientamenti etici per un'intelligenza artificiale affidabile*" [18], rilasciati in data 8 aprile 2019 da un Gruppo

---

[13] Reperibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017IP0051&from=DE.

[14] Reperibile su: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52018DC0237.

[15] Reperibile al seguente link: https://eur-lex.europa.eu/resource.html?uri=cellar:22ee84bb-fa04-11e8-a96d-01aa75ed71a1.0004.02/DOC_1&format=PDF.

[16] Ci si riferisce alla "*Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziali e negli ambiti connessi*", su cui cfr. par. 2.

[17] Reperibile su: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019IP0081.

[18] Reperibile su: https://digital-strategy.ec.europa.eu/it/library/ethics-guidelines-trustworthy-ai.

(indipendente) di esperti ad alto livello sull'intelligenza artificiale, istituito dalla Commissione europea nel giugno 2018.

Il documento rivolge a tutti i portatori di interessi (che progettano, sviluppano, distribuiscono, utilizzano l'IA o ne sono interessati) principi etici e indicazioni sulle modalità di attuazione pratica di detti principi, al fine di promuovere un'IA affidabile. In particolare viene indicato che, per essere tale, l'intelligenza artificiale deve basarsi, durante l'intero ciclo di vita del sistema, su tre componenti: legalità, eticità e robustezza. Il documento specifica di non affrontare esplicitamente la prima componente, ma offre orientamenti per promuovere e garantire l'eticità e la robustezza dell'IA (la seconda e la terza componente): "*[e]ssi mirano a fare dell'etica un pilastro fondamentale per sviluppare un approccio unico all'IA volto a favorire, rendere possibile e salvaguardare la prosperità umana a livello individuale e il bene comune a livello sociale*" [19].

Gli orientamenti si compongono di tre parti: il capitolo I, che individua i principi etici e i valori correlati che devono essere rispettati dagli sviluppatori e operatori dei sistemi di IA; il capitolo II, che delinea i requisiti che tali sistemi dovrebbero soddisfare; il capitolo III, che fornisce una lista di controllo per la valutazione in concreto dell'affidabilità dell'IA, volta a rendere operativi i requisiti enunciati nel capitolo II.

Partendo dal presupposto che i sistemi di IA devono migliorare il benessere individuale e collettivo, sono indicati – con evidenti sovrapposizioni con i principi enunciati dalla "*Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziali e negli ambiti connessi*" – quattro principi etici, fondati sui diritti fondamentali sanciti dai trattati UE, dalla Carta dei diritti fondamentali dell'Unione europea e dal diritto internazionale in materia di diritti umani: *i*) il principio del rispetto dell'autonomia umana, in base al quale gli esseri umani che interagiscono con i sistemi di IA devono poter mantenere la propria piena ed effettiva autodeterminazione; *ii*) il principio della prevenzione dei danni, in forza del quale i sistemi di IA e gli ambienti in cui operano devono essere sicuri e protetti, al fine di tutelare la dignità umana nonché l'integrità fisica e psichica degli esseri umani; *iii*) il principio di equità, inteso sia in senso sostanziale, come impegno ad assicurare una distribuzione giusta ed equa di costi e di benefici nonché a garantire che gli individui e i gruppi siano liberi da distorsioni inique, discriminazioni e stigmatizzazioni, sia in senso procedurale, quale facoltà di presentare un ricorso efficace contro le decisioni elaborate dai sistemi di IA; *iv*) il principio dell'esplicabilità, che deve permeare i processi, lo scopo e, per quanto possibile, le decisioni dei sistemi di IA rispetto a coloro che ne sono anche indirettamente interessati.

Ai fini dell'implementazione e della realizzazione di un'IA affidabile, i principi etici sono declinati in sette requisiti concreti, rivolti ai diversi portatori di interessi che partecipano al ciclo di vita delle nuove applicazioni tecnologiche, dagli sviluppatori e distributori (che possono includere anche organizzazioni

[19] Cfr. "Introduzione", p. 6.

pubbliche) fino agli utenti finali e alla società in generale, che devono esserne informati e avere la facoltà di domandarne il rispetto.

Il primo requisito – intervento e sorveglianza umani – è connesso al principio del rispetto dell'autonomia privata e prevede che i sistemi di IA dovrebbero responsabilizzare gli esseri umani, consentendo loro di prendere decisioni informate e promuovendo i loro diritti fondamentali; al tempo stesso, devono essere garantiti adeguati meccanismi di sorveglianza, che possono essere conseguiti mediante approcci "*human-in-the-loop*", "*human-on-the-loop*" e "*human-in-command*".

Il secondo e il terzo requisito – robustezza tecnica e sicurezza, riservatezza e *governance* dei dati – sono collegati al principio di prevenzione dei danni: in base al secondo requisito, i sistemi di IA devono essere resilienti e sicuri, nonché accurati, affidabili e riproducibili; in forza del terzo requisito, devono essere provvisti di adeguati meccanismi di *governance* al fine di assicurare la qualità e l'integrità dei dati utilizzati, l'accesso soltanto al personale qualificato e la trattazione nel rispetto della riservatezza durante l'intero ciclo di vita del sistema.

Il quarto requisito traduce il principio dell'esplicabilità e comprende la trasparenza dei dati, del sistema e dei modelli di *business* dell'IA. In concreto, il requisito di trasparenza implica la tracciabilità dei dati e dei processi che determinano la decisione del sistema di IA, la spiegabilità dei processi tecnici e decisionali, con modalità adeguate ai portatori di interessi coinvolti, nonché l'informativa su capacità e limiti del modello, garantendo agli utenti la conoscenza e la consapevolezza di interagire con un'applicazione di IA.

Strettamente connesso al principio di equità è il quinto requisito – diversità, non discriminazione ed equità –, volto a garantire la parità di trattamento e la parità di accesso, con una progettazione incentrata sull'utente e inclusiva. Da un lato, quindi, si intende evitare distorsioni inique, in quanto potrebbero avere molteplici implicazioni negative, dall'emarginazione dei gruppi vulnerabili all'inasprimento dei pregiudizi e delle discriminazioni; dall'altro lato, si raccomanda di promuovere la diversità, in modo da rendere i sistemi di IA accessibili a tutti e coinvolgere i portatori di interessi pertinenti durante l'intero ciclo di vita.

Il sesto requisito – benessere sociale e ambientale – si pone in linea con i principi di equità e di prevenzione dei danni, prescrivendo l'utilizzo dell'IA a beneficio di tutti gli esseri umani, comprese le generazioni future. I processi di sviluppo, distribuzione e impiego delle applicazioni di IA dovrebbero perciò essere sostenibili e rispettosi dell'ambiente e il loro impatto sociale dovrebbe essere preso attentamente in considerazione.

Il settimo e ultimo requisito – responsabilità – è legato al principio di equità e prevede l'adozione di meccanismi che garantiscano l'*accountability* dei sistemi di IA e dei loro risultati. Ciò implica la verificabilità dei dati e dei processi di progettazione, la possibilità di riferire in merito ad azioni o decisioni che contribuiscono a un determinato risultato del sistema e la garanzia di strumenti accessibili e adeguati di ricorso in caso di effetti negativi.

Gli orientamenti si concludono con una lista di controllo per la valutazione dell'affidabilità dell'IA, destinata a sviluppatori e distributori delle nuove tecno-

logie ed elaborata sulla base dei requisiti sopra indicati, nonché, similmente alla "*Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziali e negli ambiti connessi*", con una esemplificazione di modelli di IA che dovrebbero essere incoraggiati e di altri che, invece, si pongono in contrasto con i valori fondamentali dell'Europa (diritti fondamentali, democrazia e Stato di diritto), quali i sistemi di IA nascosti.

I requisiti individuati negli "*Orientamenti etici per un'intelligenza artificiale affidabile*" sono stati fatti propri dalla Commissione europea con la comunicazione "*Creare fiducia nell'intelligenza artificiale antropocentrica*", coeva alla pubblicazione degli orientamenti medesimi. In tale occasione, viene ribadito che la strategia europea in materia mira ad assicurare che l'innovazione tecnologica sia posta al servizio delle persone e destinata a migliorare il benessere economico e sociale. Si evidenzia poi che, sebbene gli orientamenti elaborati dal gruppo di esperti ad alto livello sull'IA non siano vincolanti, "*numerose disposizioni vigenti del diritto dell'Unione (spesso settoriali o specifiche per un determinato uso) già comprendono uno o più di questi requisiti fondamentali, ad esempio la sicurezza, la protezione dei dati personali, la tutela della riservatezza o le norme per la salvaguardia dell'ambiente*" [20].

La successiva, significativa tappa del percorso europeo, che ha gettato le basi per l'emanazione della proposta di regolamento in materia, è il Libro Bianco sull'intelligenza artificiale (intitolato "*Un approccio europeo all'eccellenza e alla fiducia*" [21]), pubblicato il 19 febbraio 2020, ove nuovamente si riconoscono i benefici del progresso tecnologico, ma se ne evidenziano anche i pericoli di pregiudizio per i valori su cui si fonda l'Unione europea e di violazione dei diritti fondamentali, ivi compresi, per quanto qui di interesse, la protezione dei dati personali, il diritto a un ricorso giurisdizionale effettivo e a un giudice imparziale, nonché la tutela dei consumatori. Si segnala inoltre che le caratteristiche specifiche di molte applicazioni di IA, tra cui l'opacità (c.d. effetto "scatola nera" [22]), possono rendere difficile il controllo del rispetto delle normative dell'Unione volte a proteggere i diritti fondamentali e ostacolarne l'applicazione effettiva.

Viene quindi messo in luce che, se da un lato la legislazione dell'UE rimane in linea di principio pienamente operativa, dall'altro lato, il quadro normativo (comune, come hanno rilevato gli Stati membri) può essere migliorato per affrontare le peculiari criticità legate alle nuove tecnologie, quali appunto la concreta applicazione del diritto interno ed europeo (ad esempio in materia di sicu-

---

[20] Cfr. par. 2.1.

Il testo della comunicazione è reperibile qui: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A52019DC0168.

[21] Reperibile qui: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020DC0065.

Sui temi affrontati nel documento si veda G. PROIETTI, *Il Libro Bianco sull'intelligenza artificiale. L'approccio europeo tra diritto ed etica*, in *Giustiziacivile.com*, giugno 2020.

[22] Si parla di "scatola nera", o "*black box*", quando il modello di IA è caratterizzato da opacità nel suo funzionamento: essendo noti solo *input* e *output*, e non anche il comportamento interno dell'applicazione, è difficile comprendere come viene assunta la decisione finale.

rezza dei prodotti) e l'esigenza di un'adeguata regolamentazione rispetto ai nuovi rischi cui l'uso dell'IA nei prodotti e nei servizi può dare luogo – come i rischi di opacità degli algoritmi, quelli collegati alle minacce informatiche, o derivanti dall'inserimento di dati errati in fase di progettazione, o ancora nuovi rischi per la sicurezza che possono presentarsi con l'aggiornamento dei sistemi.

La Commissione europea ha quindi concluso che, "*oltre agli eventuali adeguamenti della legislazione esistente, potrebbe essere necessaria una nuova normativa specifica sull'IA al fine di adeguare il quadro giuridico dell'UE agli sviluppi tecnologici e commerciali attuali e futuri*" [23], adottando una "*definizione di IA abbastanza flessibile da accogliere il progresso tecnico, ma anche sufficientemente precisa da garantire la necessaria certezza del diritto*" [24].

Il nuovo quadro normativo per l'IA dovrebbe, secondo quanto si legge nel Libro Bianco, seguire un approccio basato sul rischio (*risk-based approach*), dovendo però essere definiti criteri chiari e comprensibili per distinguere le diverse applicazioni di IA e per stabilire se tali applicazioni siano o meno "ad alto rischio". In proposito, occorre "*valutare gli interessi in gioco e considerare se il settore interessato e l'uso previsto per tale applicazione implichino rischi significativi, in particolare per quanto concerne la protezione della sicurezza, dei diritti dei consumatori e dei diritti fondamentali*" [25]. In questa prospettiva, dovrebbe essere considerata ad alto rischio un'applicazione di IA al ricorrere di due criteri cumulativi: che sia utilizzata in settori, da indicarsi in maniera specifica ed esaustiva (con elenco da aggiornare periodicamente), "*in cui, date le caratteristiche delle attività abitualmente svolte, si possono prevedere rischi significativi*" [26]; che sia impiegata "*in modo tale da poter generare rischi significativi*" [27], tenuto conto dell'impatto per i soggetti interessati.

Le prescrizioni per i sistemi di IA ad alto rischio dovrebbero riguardare: i dati di addestramento, affinché siano adottate le misure necessarie per garantire il rispetto dei valori e delle norme dell'UE, in particolare per quanto riguarda la sicurezza e la tutela dei diritti fondamentali; la tenuta dei dati e dei registri, anche al fine di garantire la protezione delle informazioni riservate; gli obblighi di informazione, al fine di promuovere un uso responsabile dell'IA e la consapevolezza degli utenti; la robustezza e la precisione, per presidiare l'affidabilità dei modelli; la sorveglianza umana, volta ad assicurare che il sistema di IA non comprometta l'autonomia umana né provochi altri effetti negativi.

Nell'ambito del nuovo quadro giuridico per l'IA, per le applicazioni che non sono considerate ad alto rischio la Commissione europea ha suggerito l'istituzione di un "*sistema di etichettatura*" su base volontaria: "*gli operatori economici interessati non soggetti alle prescrizioni obbligatorie potrebbero decidere, su base volontaria, di conformarsi a tali prescrizioni o di impegnarsi al rispetto di una serie*

---

[23] Cfr. par. B, ultimo cpv. del cap. 5 del Libro Bianco.

[24] Cfr. par. C, 3° cpv. del cap. 5 del Libro Bianco.

[25] *Ibidem,* 9° cpv.

[26] *Ibidem*, 10° cpv.

[27] *Ibidem*, 11° cpv.

*specifica di prescrizioni analoghe, stabilite appositamente ai fini del sistema volontario. Agli operatori economici interessati sarebbe allora assegnato un marchio di qualità per le loro applicazioni di IA*", che consentirebbe agli utenti di riconoscerne l'affidabilità in quanto conformi a determinati parametri di riferimento, obiettivi e standardizzati a livello europeo, oltre agli obblighi giuridici normalmente applicabili. "*Ciò contribuirebbe a rafforzare la fiducia degli utenti nei sistemi di IA e a promuovere l'adozione generale della tecnologia*" [28].

Lo strumento normativo in tema di IA che il Libro Bianco ha proposto è dunque basato su un "*approccio antropocentrico, etico, sostenibile e rispettoso dei valori e dei diritti fondamentali*", volto "*a promuovere la capacità di innovazione dell'Europa nel settore dell'IA, sostenendo nel contempo lo sviluppo e la diffusione di un'IA etica e affidabile in tutta l'economia dell'UE*" [29].

Le ultime sollecitazioni alla Commissione per un intervento legislativo nella materia sono pervenute dal Parlamento europeo e dal Consiglio europeo. Quest'ultimo, con il documento pubblicato il 2 ottobre 2020 [30], ha ribadito la necessità di promuovere gli investimenti nella ricerca, nello sviluppo e nella diffusione dell'intelligenza artificiale, assicurando la cooperazione tra i centri di ricerca europei e fornendo – nell'ambito di un quadro legislativo – una definizione chiara e oggettiva dei sistemi di IA da considerare ad alto rischio. In un secondo documento, di poco successivo (21 ottobre 2020), "*The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change*" [31], il Consiglio europeo ha fatto propria l'indicazione della Commissione, contenuta nel Libro Bianco sull'IA, di verificare l'adeguatezza della legislazione UE rispetto ai rischi e alle opportunità delle nuove tecnologie, procedendo agli interventi normativi necessari ad assicurarne l'applicazione effettiva, nonché la protezione dei principi e dei valori dell'Unione. Viene infatti posta l'attenzione sulle problematiche derivanti dalla complessità e, in taluni casi, dall'opacità dei sistemi di IA, che potrebbero pregiudicare la tutela dei diritti fondamentali, e viene evidenziata "*the importance of creating awareness*" [32] sulle capacità e sull'utilizzo delle applicazioni di IA, tra gli altri, nelle istituzioni governative e nella magistratura.

Il Parlamento europeo, invece, è intervenuto con la risoluzione del 20 ottobre 2020, recante raccomandazioni alla Commissione concernenti "*il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate*" [33], ove viene condiviso l'approccio basato sul rischio – già indicato dalla Commissione nel Libro Bianco – per la regolamentazione dell'IA, con l'ela-

---

[28] Cfr. par. G, 3° cpv. del cap. 5 del Libro Bianco.

[29] Cfr. 3° cpv. del cap. 6 del Libro Bianco.

[30] Reperibile al seguente link: https://www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf.

[31] Reperibile al seguente link: https://www.consilium.europa.eu/media/46496/st11481-en20.pdf.

[32] Cfr. cpv. 13 del documento.

[33] Reperibile al seguente link: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_IT.html.

borazione di un elenco esaustivo di settori ad alto rischio e di usi o scopi ad alto rischio, da sottoporre a revisione periodica. In pari data, con la Risoluzione recante raccomandazioni alla Commissione "*su un regime di responsabilità civile per l'intelligenza artificiale*" [34], il Parlamento europeo ha affermato la necessità di una legislazione uniforme per assicurare lo sviluppo dell'IA nel rispetto dei valori europei e dei diritti dei cittadini, con "*adeguamenti specifici e coordinati dei regimi di responsabilità per evitare una situazione in cui le persone che subiscono pregiudizi o danni al patrimonio non ottengano un risarcimento*" [35].

## 4. (*Segue*) Il quadro normativo attuale

Si approda così, in data 21 aprile 2021, alla proposta di regolamento europeo sull'intelligenza artificiale [36], sussunta nell'ambito applicativo dell'art. 114 del TFUE, che prevede l'adozione di misure destinate ad assicurare l'instaurazione e il funzionamento del mercato interno: la proposta costituisce infatti "*una parte fondamentale della strategia dell'Unione per il mercato unico digitale*" [37].

La bozza di provvedimento è successivamente oggetto di trattative tra le istituzioni comunitarie e di un lungo processo di negoziazione fra gli Stati membri conclusosi con un accordo politico nel dicembre 2023 [38], che ha condotto all'ap-

---

[34] Reperibile al seguente link: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_IT.html.

[35] Cfr. cpv. 6 del documento.

[36] Reperibile al seguente link: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0006.02/DOC_1&format=PDF.

[37] È quanto si legge nella relazione accompagnatoria, a proposito della base giuridica (cfr. par. 2 del documento, reperibile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206).

[38] Cfr. Comunicato stampa del Consiglio dell'Unione europea del 9 dicembre 2023, reperibile su: https://www.consilium.europa.eu/it/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/.

Per commenti sulla proposta di regolamento cfr. A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?*, Il Mulino, Bologna, 2022; C. SCHEPISI, *Diritti fondamentali, principi democratici, e rule of law: quale ruolo e quale responsabilità per gli Stati nella regolazione dell'intelligenza artificiale*, in *Studi sull'integrazione europea*, n. 1/2022; G. FINOCCHIARO, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in C. CAMARDI (a cura di), *La via europea per l'Intelligenza artificiale. Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche, Ca' Foscari Venezia, 25-26 novembre 2021*, Wolters Kluwer, Milano, 2022; M. FASAN, *L'intelligenza artificiale nel settore della giustizia. Prime riflessioni alla luce della proposta di Regolamento (UE) in materia di AI*, in *Queste Istituzioni*, n. 4/2022.

Sugli emendamenti apportati alla proposta di regolamento della Commissione cfr. A. ALAIMO, *Il Regolamento sull'Intelligenza Artificiale: dalla proposta della Commissione al testo approvato dal Parlamento. Ha ancora senso il pensiero pessimistico?*, in *federalismi.it*, n. 25/2023.

provazione del testo finale del Regolamento (UE) 2024/1689 del 13 giugno 2024 (c.d. *AI Act*) [39].

Lo scopo del regolamento è di fissare un quadro giuridico uniforme per lo sviluppo e la diffusione di un'IA antropocentrica, sicura, affidabile e soprattutto etica, nonché per la creazione di un mercato digitale unico [40].

I destinatari delle norme sono i fornitori di sistemi di intelligenza artificiale che immettono sul mercato UE tali sistemi, nonché gli operatori, anche se situati fuori dall'UE, qualora l'*output* prodotto dall'applicazione di IA venga utilizzato nel territorio dell'Unione.

L'impianto normativo segue un approccio orizzontale e, come indicato dalla Commissione europea nel Libro Bianco sull'IA, basato sul rischio, distinguendo quattro livelli di rischio secondo una "piramide" fondata sulla proporzionalità delle regole rispetto alla tipologia e alla gravità dei potenziali danni dei sistemi di IA sulla sicurezza e sui diritti fondamentali dei cittadini. Così, alla cuspide della piramide si collocano le applicazioni di IA vietate, in quanto contravvengono ai valori e ai principi dell'Unione Europea: si tratta dei sistemi a rischio inaccettabile per la sicurezza e i diritti fondamentali delle persone, in cui rientrano i modelli c.d. di "*social scoring*" o "punteggio sociale" per finalità pubbliche o private [41].

---

[39] Per i primi commenti sull'*AI Act* si vedano: F. FERRI (a cura di), *L'Unione europea e la nuova disciplina sull'intelligenza artificiale: questioni e prospettive*, in *Quaderni AISDUE* – Fascicolo speciale n. 2/2024; F.M. MANCIOPPI, *La regolamentazione dell'intelligenza artificiale come opzione per la salvaguardia dei valori fondamentali dell'UE*, in *federalismi.it*, n. 7/2024; I. DE FEO, A. AFFERNI, *AI Act: il Regolamento sull'Intelligenza Artificiale adottato dal Parlamento UE*, su *dirittobancario.it*, 14 marzo 2024; M. CARTA, *Il Regolamento UE sull'Intelligenza artificiale: alcune questioni aperte*, in *EJ*, n. 3/2024; G. CRIALESI, *Verso un'intelligenza artificiale UE antropocentrica e affidabile che garantirà la sicurezza e i diritti di imprese e cittadini*, in *Pratica fiscale e professionale,* n. 14/2024; D. MENDOLA, *Il Regolamento Europeo sull'Intelligenza Artificiale per un uso "sostenibile" della tecnologia*, in *Diritto e Giustizia*, 8 agosto 2024.

[40] Pubblicato in Gazzetta Ufficiale dell'Unione europea il 12 luglio 2024, l'*AI Act* è entrato in vigore il successivo 2 agosto e sarà pienamente applicabile a distanza di due anni, con alcune eccezioni: i divieti entreranno in vigore dopo sei mesi, le norme di *governance* e gli obblighi per i modelli di IA per uso generale diventeranno applicabili dopo 12 mesi e le norme per i sistemi di IA – integrati in prodotti regolamentati – si applicheranno dopo 36 mesi.

[41] Tali sistemi assegnano un punteggio a ciascun individuo in base al suo comportamento, influenzando in questo modo l'accesso ai servizi, all'occupazione, o ad altre opportunità.

In conformità a quanto stabilito dall'art. 96 dell'*AI Act*, in data 4 febbraio 2025 la Commissione europea ha pubblicato gli orientamenti sulle pratiche vietate in materia di intelligenza artificiale, fornendo spiegazioni ed esemplificazioni sull'attuazione pratica delle previsioni di cui all'art. 5 del regolamento, entrate in vigore il 2 febbraio 2025 (cfr. nota 40). L'obiettivo è esplicitato nella comunicazione accompagnatoria: "[t]*he Draft Guidelines annexed to this Communication aim to increase legal clarity and to provide insights into the Commission's interpretation of the prohibitions in Article 5 AI Act with a view to ensuring their consistent, effective and uniform application*".

Le linee guida non sono al momento state adottate formalmente, non essendo ancora disponibili le traduzioni in tutte le lingue dell'Unione. Saranno pertanto applicabili dalla data della relativa adozione formale, senza comunque essere vincolanti: la Commissione ha ricordato anzi come "*[a]ny authoritative interpretation of the AI Act may ultimately only be given by the Court of Justice of the European Union ('CJEU')*" (cfr. cap. 1 della bozza di linee guida).

I testi della comunicazione e della bozza di orientamenti sono reperibili al seguente link: https://

Le applicazioni ammesse sono invece suddivise in sistemi ad alto rischio, a rischio limitato e a rischio minimo.

Alla base della piramide si trovano i sistemi di IA a rischio minimo, ovvero con impatto minimo o nullo sui diritti o sulla sicurezza delle persone, essendo perciò esenti da obblighi; le imprese possono comunque impegnarsi a titolo volontario ad adottare codici di condotta aggiuntivi.

Nel mezzo sono allocati i sistemi di IA a rischio limitato e quelli ad alto rischio.

I sistemi di IA a rischio limitato presentano solo un rischio limitato per i diritti e le libertà degli individui: in quanto tali, sono soggetti a semplici obblighi di trasparenza, tra i quali in particolare l'obbligo di informare l'utente che sta interagendo con un'applicazione di intelligenza artificiale o del fatto che un particolare contenuto è stato creato attraverso l'intelligenza artificiale (ad esempio, i contenuti "*deep fake*"), al fine di consentire all'utente medesimo di utilizzare la tecnologia in modo informato e consapevole.

Sono considerati ad alto rischio i modelli di IA che provocano un rischio significativo per la sicurezza, la salute, l'ambiente o i diritti fondamentali degli individui. A causa dell'alta potenzialità di danno, prima di essere introdotti o utilizzati nell'UE sono soggetti a rigorosi requisiti e obblighi, che riguardano l'adozione di sistemi di attenuazione dei rischi, la qualità dei set di dati utilizzati (che deve essere elevata), la conservazione delle registrazioni, la trasparenza e l'informativa agli utenti, oltre all'adozione di adeguati livelli di accuratezza, robustezza e cybersicurezza.

L'*AI Act* richiede, inoltre, che gli operatori di sistemi di IA ad alto rischio effettuino una valutazione dell'impatto sui diritti fondamentali prima che tali sistemi siano immessi sul mercato.

Le decisioni elaborate dalle applicazioni di IA ad alto rischio devono, infine, essere sufficientemente trasparenti, spiegabili e documentate [42].

Il regolamento contiene in allegato l'elenco dei sistemi di IA considerati ad alto rischio, oggetto di revisione periodica da parte della Commissione: tra questi figurano le applicazioni nel settore dell'amministrazione della giustizia, ivi compresi gli strumenti di risoluzione alternativa delle controversie (*Alternative Dispute Resolution* – ADR). In particolare, il punto 8, lett. *a*, dell'Allegato III dell'*AI Act* si riferisce ai "*sistemi di IA destinati a essere usati da un'autorità giudiziaria o per suo conto per assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti, o a essere uti-*

---

digital-strategy.ec.europa.eu/it/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act.

[42] Secondo A. CORRERA, "*Le disposizioni, se calate nella specifica dimensione giudiziaria, dovrebbero comportare che gli operatori giudiziari/utilizzatori di beni o servizi fondati su applicazioni di IA siano costantemente informati ed aggiornati circa la possibilità che essi possano condurre, ad esempio, a decisioni discriminatorie, a valutazioni deterministiche oppure ad errate cristallizzazioni della giurisprudenza, e suggerire, all'occorrenza, gli opportuni rimedi e/o correttivi*" (cfr. *Il ruolo dell'Intelligenza artificiale nel paradigma europeo dell'E-justice. Prime riflessioni alla luce dell'AI Act*, pag. 21, in F. FERRI (a cura di), *L'Unione europea e la nuova disciplina sull'intelligenza artificiale: questioni e prospettive*, cit.).

*lizzati in modo analogo nella risoluzione alternativa delle controversie*".

Nel considerando (61) dell'*AI Act* si precisa ancora che i modelli di IA destinati a essere utilizzati dagli organismi ADR nelle attività di ricerca e interpretazione dei fatti e del diritto, o nell'applicazione della legge ai casi concreti, "*dovrebbero essere considerati ad alto rischio quando gli esiti dei procedimenti di risoluzione alternativa delle controversie producono effetti giuridici per le parti*".

Nello stesso considerando si fa però una distinzione per i "*sistemi di IA destinati ad attività amministrative puramente accessorie, che non incidono sull'effettiva amministrazione della giustizia nei singoli casi, quali l'anonimizzazione o la pseudonimizzazione di decisioni, documenti o dati giudiziari, la comunicazione tra il personale, i compiti amministrativi*": a queste applicazioni non è "*opportuno*" (i.e. proporzionale rispetto ai rischi da tutelare) estendere la classificazione dei sistemi ad alto rischio.

L'indicata distinzione è declinata nell'art. 6, par. 3 del regolamento, ove si prevede, per quanto qui di interesse, che un sistema di IA nel settore della giustizia (anche alternativa) non è considerato ad alto rischio "*se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale*". Ciò si verifica, secondo la predetta norma, "*quando è soddisfatta almeno una qualsiasi delle condizioni seguenti: a) il sistema di IA è destinato a eseguire un compito procedurale limitato; b) il sistema di IA è destinato a migliorare il risultato di un'attività umana precedentemente completata; c) il sistema di IA è destinato a rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non è finalizzato a sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana; o d) il sistema di IA è destinato a eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi d'uso elencati nell'allegato III*".

Il (solo) considerando (61) esplicita l'approccio antropocentrico escludendo l'ammissibilità del giudice-robot; si evidenzia infatti che "*[l]'utilizzo di strumenti di IA può fornire sostegno al potere decisionale dei giudici o all'indipendenza del potere giudiziario, ma non dovrebbe sostituirlo: il processo decisionale finale deve rimanere un'attività a guida umana*". Non si rinvengono, tuttavia, norme in questo senso.

Il principio generale del divieto delle decisioni completamente automatizzate è contenuto nel Regolamento europeo sulla protezione dei dati personali n. 2016/679 (*General Data Protection Regulation* – GDPR): l'art. 22 del GDPR – con una norma che, riguardando le decisioni automatizzate, può applicarsi anche al processo e ai sistemi di risoluzione stragiudiziale delle controversie – dispone che "*L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*".

Il divieto generale soffre però delle eccezioni [43]: qui rilevano, in particolare, il

[43] Cfr. par. 2 dell'art. 22 citato.

consenso dell'interessato o il caso in cui il trattamento sia espressamente previsto dal diritto dell'Unione o degli Stati membri. Ma anche quando, con il consenso dell'interessato, si superi la necessità dell'intervento umano nell'assunzione della decisione, è previsto che "il *titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione*" [44]. E il considerando (71) del GDPR, che illustra tale norma, specifica che le "*garanzie adeguate… dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione*".

Medesimo approccio è seguito dai lavori di revisione della Direttiva 2013/11/UE, sulla risoluzione alternativa delle controversie dei consumatori (Direttiva ADR), che si pongono come obiettivo, tra gli altri, quello di adeguare il quadro dei sistemi stragiudiziali delle liti al mercato digitale. In particolare, nella proposta della Commissione europea si prevede che gli Stati membri debbano garantire il diritto delle parti di chiedere che l'esito della procedura ADR sia riesaminato da una persona fisica quando la procedura è stata espletata con mezzi automatizzati [45]. La bozza di norma risulta anzi più severa rispetto alle previsioni dell'*AI Act*, non essendo al momento richiamata l'eccezione – prevista nel regolamento sull'intelligenza artificiale – per le attività amministrative puramente accessorie, che non incidono sull'effettiva amministrazione della giustizia alternativa.

## 5. Opportunità e rischi dell'impiego dell'intelligenza artificiale nel settore della giustizia civile

L'interesse crescente per l'impiego dell'IA in ambito giuridico si lega al concetto di giustizia "efficiente", che assicuri adeguata (e celere) protezione alle istanze delle parti e così favorisca la migliore allocazione delle risorse, portando al benessere economico [46].

---

[44] *Ibidem*, par. 3.

[45] La proposta di revisione della Direttiva ADR è stata adottata dalla Commissione il 17 ottobre 2023; è reperibile al seguente link: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52023PC0649.

Nel testo sono riportate – per quanto di interesse – le modifiche prospettate all'art. 5 della citata direttiva.

[46] Sul dibattito in tema di utilizzo dell'IA nel settore della giustizia si segnalano, *ex multis*: G. STAGLIANÒ, *Giustizia civile, intelligenza artificiale e protezione dei dati personali*, in *Rivista elettronica di Diritto, Economia, Management*, n. 1/2024; V. VITKOV, *L'intelligenza artificiale e la giustizia civile. Luci e ombre*, *ivi*; G. FINOCCHIARO, *L'intelligenza artificiale nell'ambito giudiziario*, in *Rivista Trimestrale di Diritto e Procedura Civile*, n. 2/2024; A. CORRERA, *Il ruolo dell'Intelligenza artificiale nel paradigma europeo dell'E-justice. Prime riflessioni alla luce dell'AI Act*, cit.; A. SAN-

Nella "*Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi*" si fa strada l'idea che la giustizia, per essere efficiente, deve essere prevedibile[47]. In questa prospettiva, l'utilizzo dell'IA favorisce il consolidamento e la certezza del diritto: le nuove tecnologie applicate a *smart data* giuridici sono in grado di soddisfare bisogni informativi che difficilmente potrebbero essere garantiti con i tradizionali motori di ricerca. Queste applicazioni potrebbero quindi rappresentare uno strumento di lavoro efficace sia per il giudice, favorendo la coerenza delle decisioni giudiziarie e la loro previsione, sia per l'avvocato, consentendogli di conoscere, seppure in termini probabilistici, l'esito di un giudizio e quindi di orientare la propria linea difensiva, con effetti anche deflattivi sui carichi di lavoro dei tribunali.

Gli strumenti di IA si prestano in particolare a essere impiegati nel vaglio del contenzioso con carattere di serialità: gli algoritmi, all'occorrenza utilizzati anche per i profili quantitativi della decisione da assumere, semplificherebbero l'attività del giudice, che potrebbe così dedicarsi all'esame delle controversie più complesse, e indirizzerebbero l'attività dell'avvocato verso la conclusione di accordi e l'attenuazione dei conflitti.

Oltre alla coerenza, anche la qualità delle decisioni giudiziarie ne trarrebbe giovamento, potendo basarsi su una ricerca molto più accurata e approfondita.

Negli *input* forniti alle applicazioni occorre peraltro che siano inclusi, oltre alla massima dei provvedimenti giudiziari, anche gli elementi caratterizzanti delle fattispecie esaminate, in modo che gli *output* siano accurati e affidabili: gli operatori del settore dovrebbero quindi controllare che i dati del caso alla loro

---

TUOSSO, G. SARTOR, *La giustizia predittiva: una visione realistica*, in *Giurisprudenza italiana*, n. 7/2022; G. MELIOTA, *Intelligenza artificiale e giustizia predittiva*, in *Rivista di diritto del risparmio*, n. 2/2022; G. ZACCARIA, *Mutazioni del diritto: innovazione tecnologica e applicazioni predittive*, in *Ars interpretandi*, n. 1/2021; E. BATTELLI, *Giustizia predittiva, decisione robotica e ruolo del giudice*, in *Giustizia civile*, n. 2/2020; F. DONATI, *Intelligenza artificiale e giustizia*, in *Rivista AIC*, n. 1/2020; C. CASONATO, *Intelligenza artificiale e giustizia: potenzialità e rischi*, in *DPCE online*, n. 3/2020; ID., *Per una intelligenza artificiale costituzionalmente orientata*, in AA.VV., *Blog per i 70 anni di Roberto Toniatti. "Pluralismo nel diritto costituzionale comparato"*, 2020; J. CASTELLANOS-CLARAMUNT, *Garanzie giuridiche contro l'intelligenza artificiale*, in *i-lex. Scienze Giuridiche, Scienze Cognitive e Intelligenza Artificiale*, numero speciale *AI and Justice*, dicembre 2020; A. CARLEO (a cura di), *Decisione robotica*, Il Mulino, Bologna, 2019; R. MATTERA, *Decisione negoziale e giudiziale: quale spazio per la robotica?*, in *La nuova giurisprudenza civile commentata*, n. 1/2019; J. NIEVA FENOLL, *Intelligenza artificiale e processo*, cit.; C. CASTELLI, D. PIANA, *Giustizia predittiva. La qualità della giustizia in due tempi*, in *Questione Giustizia*, n. 4/2018.

La rilevanza nel nostro Paese dell'intelligenza artificiale applicata al diritto è testimoniata, da ultimo, dall'istituzione (con D.M. del 10 luglio 2024) presso il Ministero della giustizia di un *Osservatorio permanente per l'uso dell'intelligenza artificiale nell'attività giurisdizionale*: operativo dal 23 ottobre 2024, l'Osservatorio si pone l'obiettivo di approfondire gli ambiti di interazione tra i sistemi di IA e la giurisdizione, con particolare riguardo ai profili della qualità e della sicurezza delle banche dati e agli strumenti di supporto dell'attività giurisdizionale e delle professioni giuridiche.

[47] Cfr. *supra*, par. 2.

Peraltro già M. WEBER in, *Economia e società*, ed. 1974, sosteneva che il diritto è basato su regole scritte e la certezza del diritto altro non è se non la prevedibilità dell'esito giudiziale.

attenzione, immessi nel sistema di IA, siano completi e corretti, al fine poi di analizzare e utilizzare gli esiti elaborati dall'applicazione.

Se quelli sopra illustrati costituiscono i principali vantaggi dell'utilizzo dell'IA nel settore della giustizia civile, ne sono stati evidenziati anche i rischi e gli svantaggi.

È stato osservato che l'attività di ricerca della normativa applicabile e dei precedenti giudiziari rilevanti può essere utilmente condotta attraverso i sistemi di IA, ma l'attività di interpretazione, che caratterizza e qualifica l'attività di un giurista, non può essere affidata – quanto meno non in via esclusiva – a queste applicazioni. Infatti, i modelli di IA imparano dalle informazioni fornite come *input*, ovvero dal passato, mentre la sussunzione della fattispecie concreta in quella astratta, la valutazione dei fatti rilevanti e l'individuazione delle norme applicabili al caso concreto richiedono un'attività creativa di interpretazione che non può essere rimessa alle macchine. Senza quest'attività, si prospetterebbe il rischio di standardizzazione delle decisioni e di staticità degli orientamenti giurisprudenziali, determinando un effetto c.d. performativo: l'operatore del diritto – e in particolare il giudice – si appiattirebbe sugli esiti dell'algoritmo e non ci sarebbe più spazio per l'interpretazione evolutiva. Si potrebbe delineare anche un rischio per l'imparzialità e l'indipendenza del giudice, nella misura in cui questi non sia libero di assumere decisioni divergenti rispetto agli *output* della macchina [48].

I sistemi di giustizia predittiva potrebbero poi compromettere il diritto alla tutela giurisdizionale effettiva: la probabilità di sconfitta indicata dall'algoritmo, infatti, potrebbe far desistere l'avvocato dall'adire le vie giudiziali, dando luogo a nuovi spazi di vulnerabilità. E l'auspicato effetto deflattivo di tali sistemi si potrebbe realizzare, in realtà, soltanto nella misura in cui il giudice sia vincolato agli esiti della macchina e non possa discostarsene.

Un ulteriore aspetto attiene alla qualità e all'affidabilità dei dati di addestramento della macchina: chi governa il sistema di IA, in uno con i dati con i quali viene alimentato, potrebbe nei fatti controllare anche le sue decisioni selezionando in modo arbitrario gli *input* da fornire alla macchina. Se poi vengono introdotti dati che sono frutto di pregiudizi per l'addestramento dell'algoritmo, questi si replicano e moltiplicano con il rischio di consolidamento dei *bias*, portando a decisioni ingiuste o discriminatorie.

A ciò si potrebbero aggiungere difficoltà dei modelli di IA nell'elaborazione dei dati di *input*, dovute al contenuto più o meno standardizzato dei dati stessi. Il sistema Claudette [49], addestrato – mediante metodi di apprendimento automati-

---

[48] Osserva G. ARIOLLI sul punto che "*Vincolare il robot alla giurisprudenza pregressa impedisce l'evoluzione degli indirizzi giurisprudenziali e preclude al diritto di esercitare la sua funzione primaria, ossia fornire risposte a bisogni umani regolandone i rapporti in modo corrispondente alle esigenze sociali del particolare momento storico. Un simile vincolo, poi, si pone in contrasto con l'art. 101 della Costituzione, subordinando il giudice non solo alla legge, ma alla giurisprudenza predittiva.*" (cfr. *Nomofilachia, giustizia predittiva e intelligenza artificiale*, in *giustiziainsieme.it*, 3 novembre 2023).

[49] Claudette – "automated CLAUse DETectEr" è un progetto di ricerca interdisciplinare portato

co supervisionato[50] – per la valutazione sia della vessatorietà delle clausole di contratti di fornitura di beni e servizi *on line*, sia delle informative sulla tutela della *privacy*, ha restituito risultati più precisi nella classificazione delle prime, in quanto i contratti hanno per l'appunto contenuti maggiormente standardizzati. Similmente all'informativa sul trattamento dei dati personali, invece, l'individuazione degli elementi caratterizzanti dei provvedimenti giudiziari, da utilizzare come dati di addestramento, potrebbe rivelarsi piuttosto complessa: i diversi stili redazionali dei giudici potrebbero infatti ostacolare la sistematizzazione delle decisioni.

Oltre ai dati, anche le modalità di funzionamento dell'algoritmo potrebbero sfuggire al controllo di chi poi dovrebbe comunque assumersi la responsabilità della decisione. E, quando si tratta del giudice, anche sotto questo profilo si prospetta un rischio per la sua imparzialità e indipendenza.

I problemi di scarsa trasparenza od opacità del processo decisionale, riconducibili al fenomeno della *black box*[51], potrebbero nei fatti non consentire di comprendere i passaggi logici attraverso i quali l'IA sia pervenuta a una data previsione o decisione. L'impossibilità di accedere alle informazioni necessarie su cui si basano i modelli decisionali fondati sull'IA può quindi dare luogo a un contesto di asimmetria informativa incompatibile con il rispetto del diritto di difesa e della parità delle armi, indispensabile per garantire un equo processo. Potrebbe perfino tradursi in un vizio di motivazione della decisione, che finirebbe per perdere la funzione essenziale di verifica dell'*iter* logico-argomentativo seguito dal giudice.

Invero, un sistema di IA, per quanto addestrato sulle fonti normative e sulla relativa gerarchia, sui precedenti giudiziari e sulla diversa rilevanza degli stessi (in base all'organo giudicante), nonché sugli orientamenti della dottrina, difficilmente potrebbe riprodurre il ragionamento umano, mentre l'obbligo di motivazione dei provvedimenti giurisdizionali è sancito dalla Costituzione – all'art. 111, comma 6 – a garanzia della trasparenza, dell'imparzialità e della correttezza dell'azione giudiziaria.

I rischi insiti nell'utilizzo dei sistemi di IA sembrano dunque portare ad assumere la prevedibilità del giudizio – quale precipitato della certezza del diritto – non come un valore da realizzare senza eccezioni, ma come un'opportunità: in questa prospettiva, l'IA potrebbe svolgere un ruolo di supporto nel condurre una molteplicità di attività connesse all'amministrazione della giustizia, prima fra tutte quella di ricerca, senza sostituirsi al giudice né agli altri operatori del diritto.

---

avanti da alcuni ricercatori dell'Istituto Universitario Europeo di Fiesole, guidato dai professori Giovanni Sartor e Hans-W. Micklitz, in collaborazione con gli ingegneri dell'università di Bologna e dell'Università di Modena e Reggio Emilia. Sul tema cfr.: F. LAGIOIA, G. SARTOR, *L'intelligenza artificiale per i diritti dei cittadini: il progetto Claudette*, in *Rivisteweb*, n. 1/2020; IDD., *Intelligenza artificiale per I diritti dei consumatori e tutela privacy: il Sistema Claudette*, in *agendadigitale.eu*, 29 gennaio 2021; M. FEDERICO, *L'intelligenza artificiale alla prova. I diritti dei consumatori e il programma Claudette*, in *La via europea per l'Intelligenza Artificiale. Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche Ca' Foscari Venezia, 25-26 novembre 2021*, cit.

[50] Cfr. nota 5.

[51] Cfr. nota 22.

Resta poi sullo sfondo l'avvicinamento dei sistemi di *civil law* a quelli di *common law*, che può essere determinato dall'innovazione tecnologica: nei sistemi di *civil law* il giudice applica la legge ai casi particolari, mentre con l'impiego dell'IA dovrebbe verificare se il caso da esaminare è identico o assimilabile a quelli restituiti dalla macchina, con un approccio che evoca lo *stare decisis* tipico del modello di *common law*[52].

## 6. L'intelligenza artificiale nei sistemi di risoluzione stragiudiziale delle controversie

La trattazione del tema relativo all'utilizzo dell'IA nei sistemi di risoluzione stragiudiziale delle controversie (anche noti con l'acronimo ADR, da *Alternative Dispute Resolution*)[53] richiede una breve premessa sulla differente impostazione

---

[52] Si veda sul punto E. BATTELLI, *Giustizia predittiva, decisione robotica e ruolo del giudice*, cit., ove si osserva che "*la riforma del 2016 … ha sostanzialmente trasformato il giudizio civile di legittimità, stabilendo che i precedenti che costituiscono la giurisprudenza della Corte di Cassazione, ai sensi dell'art. 360-bis c.p.c., hanno natura vincolante per legge. E la stessa Suprema Corte, sez. VI civile, nella sentenza n. 7155 del 2017 ha restituito autonoma rilevanza alla inammissibilità prevista dal 360-bis rispetto ai casi di manifesta fondatezza e infondatezza del 375, n. 5, c.p.c., tale per cui può ben dirsi che lo* stare decisis *abbia trovato accoglimento anche in Italia. E ciò, non sembri inutile dirlo, favorisce proprio il possibile impiego della robotica applicata alla giustizia*".

Richiama l'importanza del precedente – che, "*se pur non vincolante, non si limiti a essere persuasivo, ma riesca a divenire influente*" – anche la Prima Presidente della Cassazione, M. Cassano, in occasione dell'inaugurazione dell'anno giudiziario 2025, tenuto conto, nel moderno ruolo della Suprema Corte, del dinamismo della nostra società, cui si accompagna un crescente bisogno di prevedibilità della giustizia. Tuttavia ne sottolinea la differenza rispetto al modello di *common law*: "[i]*l precedente giudiziale non ha valore vincolante nei termini propri dei sistemi anglosassoni, ma solo persuasivo e tale valenza assume una particolare consistenza allorché la precedente decisione provenga dalla Corte di cassazione, investita per legge della funzione di assicurare l'esatta osservanza e l'uniforme interpretazione della legge. L'osservanza del precedente in ragione della sua particolare efficacia persuasiva piuttosto che di un vincolo di legge, costituisce espressione, allo stesso tempo, del principio costituzionale di esclusiva soggezione del giudice alla legge e di un atteggiamento culturale che, senza in alcun modo compromettere l'indipendenza interna, funzionale del giudice, garantisce l'esercizio della funzione giurisdizionale in modo coerente con il principio costituzionale di eguaglianza, assicurando che fattispecie uguali abbiano un identico trattamento in sede giudiziale, nonché con il diritto fondamentale alla certezza e alla prevedibilità del diritto affermato più volte dalla Corte europea dei diritti dell'uomo*" (cfr. cap. 2, par. 2, della *Relazione sull'amministrazione della giustizia nell'anno 2024*).

[53] Per un contributo (raro e) specifico sulla materia si veda C. PILIA, *L'intelligenza artificiale e la mediazione nei sistemi ADR/ODR*, in R. GIORDANO, A. PANZAROLA, A. POLICE, S. PREZIOSI, M. PROTO (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Giuffrè, Milano, 2022.

A livello internazionale si ricordano invece, per le professioni legali, le *Guidelines on the Use of Artificial Intelligence in Mediation*, adottate il 1° gennaio 2025 dalla *International Bar Association* (IBA): si legge ivi che "[t]*he growing use of AI presents an unprecedented opportunity to facilitate mediation by improving efficiency, reducing costs, and broadening access to justice, provided that AI is*

di tali sistemi rispetto allo strumento tradizionale di tutela del diritto, ovvero il processo.

La tutela giudiziale, in quanto somministrata dallo Stato per assicurare il rispetto e l'attuazione della legge, è soggetta a un minuzioso statuto pubblicistico nazionale[54], attraverso il quale viene fornita una risposta autoritativa alle situazioni patologiche dei rapporti giuridici. I metodi di risoluzione alternativa delle controversie, invece, si caratterizzano per dare spazio all'autonomia negoziale delle parti, che, attraverso procedure snelle, informali e rapide, possono adottare un approccio consensuale e costruttivo alla soluzione della lite, in una prospettiva di giustizia partecipativa anziché autoritativa[55].

L'autonomia privata che connota i meccanismi di ADR – parlandosi al riguardo anche di degiurisdizionalizzazione degli strumenti di tutela dei diritti (che rientrano nella disponibilità delle parti) – li rende in via di principio più permeabili al progresso tecnologico rispetto al sistema giurisdizionale. Occorre tuttavia avere presente che il nostro ordinamento prevede delle cautele procedurali per la mediazione delle controversie civili e commerciali, sia essa obbligatoria o facoltativa alla luce delle previsioni del d.lgs. n. 28/2010, come aggiornate dalla riforma Cartabia[56], in relazione agli effetti annessi al relativo svolgimento (di cui si dirà nel prosieguo).

Intesa quale strumento deflattivo del processo civile, la mediazione è stata imposta dal legislatore, configurandola come condizione di procedibilità della domanda giudiziale, nelle materie specificamente indicate all'art. 5, comma 1, del citato d.lgs. n. 28/2010[57], tra cui si annoverano i contratti assicurativi, bancari e finanziari. L'obbligatorietà della mediazione, sempre in termini di condizione di procedibilità (*rectius* proseguibilità) dell'azione, può derivare anche

---

*integrated into mediations with appropriate safeguards*". Il testo integrale delle linee guida è reperibile al seguente link: https://iba-aim.com/.

[54] Così lo definisce C. PILIA, *L'intelligenza artificiale e la mediazione nei sistemi ADR/ODR*, cit.

[55] Sulla differenza tra "cultura del conflitto" e "cultura della conciliazione" cfr.: F. DANOVI, *ADR: giustizia non più solo alternativa ma complementare*, in F. DANOVI, F. FERRARIS (a cura di), *ADR. Una giustizia complementare*, Giuffrè, Milano, 2018; M. MARINARO, *"Il Paese dove tutto finisce in tribunale". Riflessioni sparse sulle prospettive di riforma della giustizia civile*, in judicium.it, 2018; Id., *La mediazione dei conflitti tra personalismo e solidarismo costituzionali*, in *Materiali di ricerca per la mediazione conciliativa*, Vol. II, Aracne, Roma, 2014.

[56] Si fa riferimento al d.lgs. n. 149/2022, che ha novellato il d.lgs. n. 28/2010, a suo tempo emanato per dare attuazione alla Direttiva 2008/52/CE, "*relativa a determinati aspetti della mediazione in materia civile e commerciale*", ove si consentiva agli Stati membri di rendere il ricorso alla mediazione "*obbligatorio oppure soggetto a incentivi o sanzioni, sia prima che dopo l'inizio del procedimento giudiziario*", senza però impedire il diritto di accesso al sistema giudiziario (cfr. art. 5, par. 2 della direttiva).

[57] L'art. 5, comma 1 così dispone: "*Chi intende esercitare in giudizio un'azione relativa a una controversia in materia di condominio, diritti reali, divisione, successioni ereditarie, patti di famiglia, locazione, comodato, affitto di aziende, risarcimento del danno derivante da responsabilità medica e sanitaria e da diffamazione con il mezzo della stampa o con altro mezzo di pubblicità, contratti assicurativi, bancari e finanziari, associazione in partecipazione, consorzio, franchising, opera, rete, somministrazione, società di persone e subfornitura, è tenuto preliminarmente a esperire il procedimento di mediazione ai sensi del presente capo*".

dall'ordine del giudice (mediazione c.d. demandata), il quale ha facoltà di disporre in questo senso fino alla fase di appello e per tutte le controversie civili e commerciali vertenti su diritti disponibili. Diversamente, con la medesima estensione applicativa della mediazione demandata dal giudice le parti possono ricorrere alla mediazione volontaria.

Differendo soltanto nelle modalità di attivazione, per ogni tipologia di mediazione ivi regolata [58] il d.lgs. n. 28/2010 contiene norme procedurali identiche, secondo il modello della mediazione c.d. amministrata, di tipo facilitativo e, in via gradata, valutativo. Si prevede in particolare che la domanda di mediazione esplichi sulla prescrizione gli stessi effetti dell'atto introduttivo del giudizio, impedendo invece una sola volta la decadenza (al fine di evitare il rischio di possibili abusi dell'istituto); si contemplano poi agevolazioni di carattere fiscale e la possibilità che l'accordo di conciliazione sia dotato di efficacia esecutiva.

In questa cornice normativa, quando le parti sono libere di scegliere la mediazione come strumento di risoluzione delle controversie, il consenso può essere utilmente prestato anche per la procedura automatizzata, come previsto dall'art. 22 del GDPR: gli strumenti di IA potrebbero qui essere impiegati per facilitare il vaglio delle pretese delle parti, o finanche per sostituire l'attività del mediatore. Potrebbe tuttavia dubitarsi che la mediazione volontaria condotta da un robot si collochi ancora nel perimetro di operatività del d.lgs. n. 28/2010, stante la nozione di mediatore, che presuppone la presenza di una persona fisica, contenuta nell'art. 1, lett. *b* del predetto decreto [59]; sul piano delle implicazioni giuridiche, ciò comporterebbe che la domanda di mediazione non avrebbe effetti su prescrizione e decadenza, le parti non potrebbero beneficiare delle agevolazioni fiscali, né l'eventuale accordo raggiunto sarebbe suscettibile di acquisire forza esecutiva, rimanendo assoggettato alla disciplina contrattuale.

D'altra parte, ove la controversia, non rientrante nell'ambito di operatività della mediazione obbligatoria, presenti le caratteristiche oggettive e soggettive tali da giustificare l'applicazione del d.lgs. n. 130/2015, che disciplina la risoluzione alternativa delle liti dei consumatori in attuazione della Direttiva 2013/11/UE (c.d. Direttiva ADR) [60], sicuramente la mediazione non potrebbe essere condotta da un agente virtuale, poiché già la legislazione europea fa riferimento alle "persone fisiche" incari-

[58] Oltre alla mediazione obbligatoria (*ex lege* o *iussu iudicis*) e facoltativa, già richiamate sopra, si tratta della mediazione c.d. concordata, ovvero pattuita dalle parti in via preventiva rispetto al sorgere della lite.

[59] Secondo l'art. 1, lett. *b*, si intende per "*mediatore*" "*la persona o le persone fisiche che, individualmente o collegialmente, svolgono la mediazione rimanendo prive, in ogni caso, del potere di rendere giudizi o decisioni vincolanti per i destinatari del servizio medesimo*".

[60] Si tratta in specifico delle controversie relative a obbligazioni derivanti da contratti di vendita o di servizi stipulati tra professionista e consumatore, disciplinate dal Titolo II-*bis* del Codice del consumo, introdotto dal d.lgs. n. 130/2015, in recepimento della Direttiva ADR.

Tale normativa riguarda sia gli ADR di tipo conciliativo che gli ADR decisori, ma rispetto a questi ultimi sono esclusi dall'ambito applicativo i metodi di risoluzione alternativa che prevedono la possibilità di imporre la soluzione della controversia alle parti.

cate di tale funzione [61] nell'indicare gli standard di armonizzazione comuni.

In ogni caso, prescindendo dalla questione della normativa applicabile, anche per il mediatore-robot potrebbero presentarsi i problemi, sopra evidenziati per la giustizia civile [62], sulla qualità e affidabilità dei dati di addestramento, con evidenti maggiori rischi se non viene osservato il principio del "*controllo da parte dell'utilizzatore*" indicato nella "*Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziali e negli ambiti connessi*" [63]. A ciò si aggiunga che l'attività di mediazione ha una connotazione fortemente personale, richiedendo, oltre a competenze interdisciplinari, empatia, capacità di comunicare e interagire, ascolto e comprensione: si tratta di qualità umane che difficilmente un algoritmo può replicare, indispensabili per indagare interessi e bisogni delle parti al fine di elaborare la possibile soluzione della controversia o agevolare le parti stesse in tale direzione.

Alla luce delle superiori considerazioni sembra quindi preferibile che le applicazioni di IA siano destinate piuttosto per funzionalità di supporto al mediatore, quali la generazione di domande da rivolgere alle parti, la valutazione delle rispettive esigenze, la ricostruzione del quadro informativo che le parti possono utilizzare come base di partenza per la negoziazione o la formulazione della proposta di accordo che abbia maggiori probabilità di accettazione. Le nuove tecnologie potrebbero poi essere di ausilio all'istante nella scelta dell'organismo di mediazione cui rivolgersi e ad entrambe le parti per definire la propria strategia negoziale e difensiva; inoltre, benefici potrebbero essere tratti dagli organismi di mediazione in termini organizzativi, ad esempio per l'individuazione del o dei mediatori cui affidare la controversia, per la raccolta e classificazione delle domande ricevute o per il monitoraggio sulla qualità dei servizi offerti.

Ove si verta sulla mediazione obbligatoria, l'impiego dell'IA, sebbene non incontri i vincoli derivanti dal principio costituzionale del giudice naturale precostituito [64], va comunque coniugato con il rispetto dei diritti fondamentali, essendo in particolare necessario garantire, come indicato nella "*Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziali e negli ambiti connessi*", il diritto di accesso al giudice [65].

---

[61] Cfr. art. 6 della Direttiva ADR e art. 141-*bis*, commi 4 e 5 del Codice del consumo.

Si rammenta che l'art. 141, comma 6, del Codice del consumo fa salve, in linea con quanto consentito dall'art. 1 della Direttiva ADR, le norme che prevedono l'obbligatorietà delle procedure di risoluzione stragiudiziale delle controversie, prima fra tutte quella contemplata dal d.lgs. n. 28/2010. Sul rapporto – invero problematico – tra la disciplina sulla mediazione obbligatoria e quella relativa agli ADR di consumo si veda la sentenza della Corte di giustizia dell'Unione europea del 14 giugno 2017 (causa C-75/16).

[62] Cfr. *supra*, par. 5.

[63] Cfr. *supra*, par. 2.

[64] Art. 25, comma 1 della Costituzione.

[65] Negli "*Orientamenti etici per un'intelligenza artificiale affidabile*" si fa riferimento al principio di equità in senso procedurale (cfr. *supra*, par. 3).

Questo tema è stato affrontato anche dalla Corte di giustizia dell'Unione europea, che ha ritenuto il tentativo obbligatorio di mediazione, stabilito dal d.lgs. n. 28/2010, compatibile con la tu-

Sembra poi che qui non possa porsi la questione del mediatore artificiale, alla luce della già richiamata definizione di mediatore di cui all'art. 1, lett. *b* del d.lgs. n. 28/2010: ora, se per la mediazione volontaria tale nozione potrebbe essere superata – con le riserve espresse sopra, anche sul conseguente regime normativo – con il consenso delle parti, le caratteristiche della mediazione obbligatoria inducono sicuramente a una lettura restrittiva, sebbene a livello di normativa europea non consti un divieto netto in questo senso. Invero, come detto sopra [66], quanto indicato nel considerando (61) dell'*AI Act* – ovvero che "[*l]'utilizzo di strumenti di IA può fornire sostegno al potere decisionale dei giudici o all'indipendenza del potere giudiziario, ma non dovrebbe sostituirlo: il processo decisionale finale deve rimanere un'attività a guida umana*" – non è confluito in un precetto nemmeno con riferimento alla giustizia togata; l'art. 22 del GDPR ammette la decisione automatizzata dietro consenso dell'interessato, oltre all'eccezione costituita dalla specifica previsione euro-unitaria o nazionale. E anche la proposta di revisione della Direttiva ADR sembra consentire la decisione automatizzata, purché sia fatto salvo il diritto dell'interessato al riesame a cura di una persona fisica. Il divieto del mediatore-robot sembra dunque, allo stato, potersi evincere sicuramente dal solo diritto interno quando si tratta della mediazione quale condizione di procedibilità della domanda giudiziale.

Sulla base del quadro legislativo attuale, pertanto, nella mediazione obbligatoria l'IA può essere impiegata, oltre che per attività amministrative od organizzative quali la catalogazione delle istanze, per l'implementazione di motori avanzati di ricerca della normativa e della giurisprudenza con le stesse finalità indicate per la mediazione facoltativa. Quando si tratta di attività meramente accessorie all'amministrazione della giustizia alternativa, i sistemi di IA non saranno considerati ad alto rischio, secondo la deroga accordata dall'*AI Act*.

Lo sviluppo dei motori di ricerca presenta, come detto sopra, le stesse criticità già viste per la giustizia civile, legate al contenuto più o meno standardizzato dei dati di *input*, alla gerarchia delle fonti normative e alla diversa rilevanza dell'organo giudicante. Potrebbe poi rivelarsi più complesso per gli ADR di tipo decisorio rispetto a quelli conciliativi, poiché per i primi i dati di addestramento dovrebbero includere anche le decisioni dello stesso sistema stragiudiziale, salvo fondarsi solo su tali decisioni.

Gli esiti dei sistemi di IA, opportunamente verificati sulla base del principio del rispetto dell'autonomia, indicato dagli "*Orientamenti etici per un'intelligenza artificiale affidabile*" [67], possono rappresentare un utile strumento di supporto sia negli ADR di tipo conciliativo, per la definizione da parte del mediatore della proposta di soluzione bonaria della controversia, o – nel caso si tratti di mediazione solo facilitativa – per orientarlo nell'assistenza alle parti nella ricerca

tela giurisdizionale effettiva proprio purché non sia impedito alle parti di rivolgersi al giudice (cfr. sentenza del 14 giugno 2017, causa C-75/16).

[66] Cfr. par. 4.

[67] Cfr. *supra*, par. 3.

dell'accordo, sia negli ADR di tipo decisorio, agevolando la valutazione delle posizioni contrapposte.

L'eventuale staticità degli orientamenti giurisprudenziali, che potrebbe derivare dall'utilizzo acritico delle decisioni elaborate dalle applicazioni di IA, si ripercuoterebbe anche sui sistemi ADR che siano aditi per espletare la condizione di procedibilità prevista dal d.lgs. n. 28/2010: l'interpretazione evolutiva del diritto sarebbe infatti scoraggiata dal diverso – e immutabile – esito giudiziario previsto dall'algoritmo.

Occorre ancora considerare che il tema della trasparenza delle modalità di funzionamento dei modelli di IA potrebbe porsi anche nella mediazione, come per la giustizia civile, sebbene in termini non del tutto sovrapponibili all'ambito giudiziario, per le ragioni indicate sopra sulla differente natura della tutela giudiziale e stragiudiziale dei diritti. Invero, se in linea generale si può sostenere che il fenomeno della *black box*[68] è comunque compensato dalla circostanza che l'*output* non è vincolante, la disciplina sul procedimento di mediazione di cui al d.lgs. n. 28/2010, applicabile – come detto sopra – a tutte le tipologie di mediazione contemplate dal decreto, prevede delle sanzioni processuali per il rifiuto della proposta di conciliazione, che il mediatore può formulare sia in caso mancato raggiungimento dell'accordo tra le parti, sia in qualsiasi fase della procedura a fronte di una concorde richiesta delle stesse. In particolare, l'art. 13 del decreto incide sul regime delle spese del successivo giudizio, disponendo che, ove il provvedimento di natura giurisdizionale coincida integralmente o in parte con la proposta di conciliazione, il giudice rispettivamente debba o, "*se ricorrono gravi ed eccezionali ragioni*" (da indicare nella decisione), possa escludere la ripetizione delle spese sostenute dalla parte vittoriosa che abbia rifiutato la soluzione risolutiva formulata dal mediatore[69]. Poiché dunque il rifiuto della proposta di conciliazione è idoneo – almeno potenzialmente[70] – a esplicare effetti sul processo avviato dalla parte che, al suggerito accordo, abbia preferito rivolgersi al giudice, la spiegabilità degli algoritmi appare acquisire rilevanza ai fini della determinazione della stessa di accettare o meno la soluzione di composizione della vertenza ipotizzata dal mediatore.

---

[68] Cfr. nota 22.

[69] La sanzione ha un diverso peso nelle due ipotesi: in caso di totale coincidenza tra provvedimento del giudice e proposta del mediatore (peraltro inverosimile, considerato che la proposta del mediatore tiene conto non solo delle posizioni delle parti, come potrebbero essere rappresentate innanzi al giudice, ma anche dei loro interessi e bisogni al fine di individuare la soluzione per la composizione della lite), sono previste l'esclusione *ex lege* della ripetizione delle spese sostenute dalla parte vincitrice che ha rifiutato la proposta, riferibili al periodo successivo alla formulazione della stessa, ivi compresa l'indennità corrisposta al mediatore, e la condanna al rimborso delle spese sostenute dalla parte soccombente relative allo stesso periodo, nonché la corresponsione a favore dell'erario di un'ulteriore somma pari al contributo unificato dovuto per il giudizio; in caso di parziale coincidenza, il giudice può escludere la ripetizione, a carico della parte vittoriosa nel merito, delle sole spese per l'indennità del mediatore.

[70] Le previsioni dell'art. 13, sostanzialmente analoghe a quelle introdotte fin dall'origine dal d.lgs. n. 28/2010, sono di difficile applicazione per la diversità strutturale tra mediazione e giudizio.

L'opacità dei meccanismi automatizzati funzionali alla soluzione delle liti potrebbe atteggiarsi anche a "giustificato motivo" della mancata partecipazione al primo incontro di mediazione, alla quale, similmente al rifiuto della proposta di conciliazione, il d.lgs. n. 28/2010 annette conseguenze processuali nell'eventuale successivo giudizio[71].

Anche ove si tratti di applicare la disciplina sui metodi ADR in materia di consumo, si pone ugualmente la questione della spiegabilità delle eventuali applicazioni di IA utilizzate, in ragione del principio di trasparenza che deve permeare tali sistemi: in particolare, *ex* art. 141-*quater* del Codice del consumo, gli organismi *de quibus* sono tenuti a pubblicare sui rispettivi siti *web*, in modo chiaro e facilmente comprensibile, le norme che regolano la procedura.

Qualche considerazione a sé stante va riservata ai sistemi ADR – di tipo decisorio – previsti nei settori bancario (Arbitro Bancario Finanziario – ABF), finanziario (Arbitro per le controversie finanziarie – ACF) e assicurativo (Arbitro Assicurativo – AAS, ad oggi costituendo), che il legislatore ha equiparato al tentativo obbligatorio di mediazione ai fini dell'assolvimento dell'indicata condizione di procedibilità[72].

In proposito, potrebbe innanzitutto sorgere il dubbio se le regole armonizzate sulle applicazioni di IA ad alto rischio valgano anche per gli algoritmi impiegati nell'ambito di tali sistemi, posto che il considerando (61) dell'*AI Act* fa riferimento ai procedimenti di risoluzione alternativa delle controversie i cui esiti "*producono effetti giuridici per le parti*".

Le decisioni dell'ABF e dell'ACF non sono vincolanti per le parti, né possono

---

[71] Si fa riferimento all'art. 12-*bis*, introdotto dalla riforma Cartabia per disporre un apparato sanzionatorio più incisivo per la mancata partecipazione, senza giustificato motivo, alla mediazione. È infatti previsto che: i) il giudice ne possa desumere argomenti di prova ai sensi dell'art. 116, secondo comma, c.p.c.; ii) quando la mediazione costituisce condizione di procedibilità, la parte costituita sia condannata al versamento a favore dell'erario di una somma pari al doppio del contributo unificato dovuto per il giudizio e, ove soccombente, possa essere altresì condannata al pagamento in favore della controparte di una somma equitativamente determinata entro il limite delle spese del giudizio maturate dopo la conclusione del procedimento di mediazione; iii) in tale ultima evenienza, il giudice trasmetta copia del provvedimento al pubblico ministero presso la sezione giurisdizionale della Corte dei conti, se la parte soccombente è una delle amministrazioni pubbliche di cui al d.lgs. n. 165/2001, ovvero alla competente Autorità di Vigilanza se si tratta un soggetto dalla stessa vigilato.

[72] Cfr. art. 5, comma 3, del d.lgs. n. 28/2010.

Sull'istituzione dell'Arbitro Assicurativo si rammenta che è stato di recente pubblicato in Gazzetta Ufficiale (G.U. n. 6 del 9 gennaio 2025) il decreto n. 215 del 6 novembre 2024, adottato dal Ministero delle imprese e del Made in Italy di concerto con il Ministero della giustizia, sulla "*determinazione dei criteri di svolgimento delle procedure di risoluzione stragiudiziale delle controversie con la clientela relative alle prestazioni e ai servizi assicurativi derivanti dai contratti di assicurazione, nonché dei criteri di composizione dell'organo decidente e della natura delle controversie*". Il regolamento ministeriale demanda all'Ivass l'adozione delle disposizioni attuative e di dettaglio entro il termine di quattro mesi dalla data di entrata in vigore del decreto medesimo, avvenuta il 24 gennaio 2025. L'operatività del nuovo Arbitro sarà poi dichiarata dall'IVASS con proprio provvedimento, da pubblicarsi sul sito internet dell'Autorità di Vigilanza entro e non oltre il termine di cinque mesi dalla pubblicazione delle disposizioni tecniche e attuative.

acquisire efficacia di titolo esecutivo come gli accordi di conciliazione[73]. Tuttavia, il mancato ottemperamento da parte degli intermediari alle pronunce favorevoli alla clientela dà luogo alla sanzione reputazionale, costituita dalla pubblicazione dell'inadempimento sia sul sito *web* dell'ADR, sia sulla *homepage* del sito dell'istituto inadempiente (e, per l'ACF, anche su due quotidiani a diffusione nazionale)[74]. Sotto questo profilo, dunque, si può sostenere che gli esiti dei procedimenti ABF e ACF producono effetti giuridici per le parti, non senza sottolineare che il *caveat* del considerando non ha trovato spazio nelle previsioni del regolamento.

Oltre alla richiamata sanzione reputazionale, su cui si fonda l'efficacia dei due sistemi ADR, un'altra peculiarità dell'ABF e dell'ACF – e verosimilmente anche del futuro AAS[75] – risiede nella funzione conformativa della condotta degli intermediari: al di là della composizione della lite, le decisioni di tali sistemi individuano e promuovono le migliori pratiche di mercato, al fine di favorirne l'adozione[76]. E infatti in entrambi i casi è previsto che gli intermediari gestiscano i re-

---

[73] Cfr. art. 12 del d.lgs. n. 28/2010.

[74] Cfr., per l'ABF, Sez. VI, par. 4 delle Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari (reperibili qui: https://www.arbitrobancariofinanziario.it/abf/normativa/index.html) e, per l'ACF, l'art. 16 del Regolamento concernente l'Arbitro per le Controversie Finanziarie (ACF) (reperibile qui: https://www.acf.consob.it/web/guest/normativa/normativa-acf).

Per l'Arbitro Assicurativo è previsto un analogo meccanismo di *shame culture* (cfr. art. 12 del D.M. 215/2024).

[75] Si veda sul punto S. DE POLIS, Segretario Generale dell'Ivass: "*Che fisionomia avrà l'Arbitro Assicurativo. È chiaro che il nuovo organismo si ispira alla struttura degli altri due arbitri del settore finanziario, nel solco dei criteri qualitativi della direttiva 2013/11 sui sistemi ADR, recepiti nel Codice del consumo. L'ABF e l'ACF hanno d'altronde dato prova di grande efficienza nell'offrire una tutela rapida, economica ed efficace ed anche per questo rappresentano un esempio e una guida autorevole per l'Arbitro Assicurativo*" (*L'Arbitro Assicurativo*, in *Riforma della giustizia civile e tutela stragiudiziale: quali opportunità per cittadini e imprese? Atti del convegno ACF – ANSPC – Sapienza Università di Roma*, *24 ottobre 2022*, *Quaderno giuridico Consob* n. 27/2023).

Le parole del Segretario Generale dell'Ivass trovano conferma nel regolamento ministeriale istitutivo dell'Arbitro Assicurativo, di recente emanato (cfr. nota 72): il modello organizzativo è strutturato in linea con gli altri due sistemi stragiudiziali già operativi presso Banca d'Italia e Consob, ciò che lascia intendere che anche il nuovo strumento di risoluzione alternativa delle controversie svolgerà, con riferimento al settore assicurativo, la medesima funzione dell'ABF e dell'ACF rispetto ai comportamenti degli operatori.

Si segnala peraltro – per mera completezza – una novità dal punto di vista procedurale: il regolamento prevede che il carattere documentale del procedimento possa essere derogato, e dunque l'Arbitro Assicurativo avrà la facoltà di sentire le parti, nei casi di cui all'art. 11, comma 4 del decreto, ovvero quando l'Arbitro, una volta accertato il diritto al risarcimento del danno, ne disponga la liquidazione in via equitativa "*sulla base degli elementi a tal fine forniti dalle parti*".

Per i primi commenti al D.M. 215/2024 si segnalano: V. MIRRA, *In dirittura d'arrivo l'Arbitro per le controversie assicurative*, in dirittobancario.it, 31/01/2025; M. MARINARO, *Adr e arbitro assicurativo: approvate le regole sui criteri di svolgimento della procedura,* nella *Guida al Diritto – Il Sole 24 Ore* n. 4/2025.

[76] P. SIRENA ha osservato che *"nel settore bancario e finanziario, dove la concorrenza non è abbastanza efficiente da indirizzare i comportamenti degli intermediari e da evitare i rischi di fallimen-*

clami ricevuti tenendo in considerazione gli orientamenti espressi dagli ADR[77].

La descritta funzione conformativa presuppone, per esplicarsi, l'uniformità di orientamenti: per il sistema ACF, appare più agevole da perseguire trattandosi di un solo Collegio, che deve assicurare omogeneità di trattazione ai casi analoghi; nel sistema ABF, invece, l'organo decidente si compone di sette Collegi, con un Collegio di coordinamento deputato – come una sorta di sezioni unite dell'ABF – a comporre le posizioni difformi dei consessi territoriali, ovvero a prevenirle[78].

In questo scenario, applicazioni di IA destinate alla ricerca dei precedenti dell'ABF e dell'ACF potrebbero contribuire all'omogeneizzazione e quindi alla prevedibilità delle decisioni, rafforzando l'effetto conformativo e di indirizzo dei comportamenti degli operatori sotteso agli orientamenti di tali sistemi ADR[79].

Inoltre, la capacità conformativa delle decisioni ABF e ACF richiede che le stesse siano pubblicate: in particolare, ciò avviene sui siti dei due ADR, previa anonimizzazione del testo delle pronunce rispetto alle parti della controversia[80]. L'anzidetta attività, che implica un controllo su qualsiasi dato che possa disvelare

---

*to del mercato causati dalla selezione avversa e dall'azzardo morale, lo scopo ultimo dei sistemi di ADR è quello di indurli ad aderire alle best practices e agli standards più elevati di correttezza nei confronti dei loro clienti e di trasparenza dei loro contratti. Per molte ragioni, i sistemi di ADR possono essere maggiormente efficaci nel modificare i comportamenti degli intermediari rispetto alla giurisdizione dello Stato, il cui esercizio ha un impatto spesso trascurabile sul livello di compliance degli intermediari e sulla effettività della regolazione del mercato.* […] *I sistemi di ADR svolgono così una funzione quasi-regolatoria più che quasi-giudiziaria, conferendo alla voce dei consumatori l'idoneità a incidere sulle pratiche commerciali diffuse sul mercato"* (*I sistemi di ADR nel settore bancario e finanziario*, in *La nuova giurisprudenza civile commentata* n. 9/2018).

[77] Cfr. Sez. VI, par. 1 delle Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari e l'art. 3, comma 4 del Regolamento concernente l'Arbitro per le Controversie Finanziarie (ACF).

[78] Cfr. Sez. III, par. 5 delle Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari.

Oltre al Collegio di coordinamento, le Disposizioni sul funzionamento dell'ABF (alla Sez. VI, par. 6) contemplano la Conferenza dei Collegi quale sede di confronto fra i poli decisori al fine di accrescere la funzionalità del sistema.

Quanto all'Arbitro Assicurativo, il D.M. 215/2024 rimette all'Ivass la fissazione del numero di Collegi, "*tenuto conto del numero dei ricorsi ricevuti e della tipologia di controversie*" e "*in modo da garantire efficienza e tempestività nella definizione dei ricorsi e nel rispetto di quanto previsto dall'articolo 141*-bis *del codice del consumo*" (cfr. art. 4, comma 1).

[79] Invero la Banca d'Italia sta implementando un sistema di IA denominato *AbefTech*, destinato alla ricerca di decisioni su casi analoghi (cfr. al riguardo la *Relazione annuale sull'attività dell'Arbitro Bancario Finanziario*, anno 2023, cap. 1).

[80] P. SIRENA ha avuto modo di evidenziare al riguardo che *"[m]entre la riservatezza è un caposaldo irrinunciabile dei lodi arbitrali, essa non è opportuna riguardo alle decisioni prese dai sistemi di ADR nel settore bancario e neppure riguardo agli accordi transattivi conclusi tra le parti. Al contrario, tali decisioni e accordi, omettendo i nomi delle parti e altri dati personali, dovrebbero essere resi facilmente disponibili da parte degli intermediari e dei loro clienti, al fine di promuovere le migliori pratiche di mercato e di favorirne l'adozione. In tal modo, sarebbe data agli intermediari la possibilità di migliorare ulteriormente il proprio grado di compliance e ai clienti di minimizzare il rischio di selezione avversa nelle loro scelte di mercato"* (*I sistemi di ADR nel settore bancario e finanziario* cit.).

l'identità delle parti (quali i dati catastali, o le denominazioni dei prodotti bancari e finanziari) ben si presta a essere svolta con l'intelligenza artificiale, essendo proprio uno degli esempi riportati nel considerando (61) dell'*AI Act* di "*attività amministrative puramente accessorie, che non incidono sull'effettiva amministrazione della giustizia nei singoli casi*". I sistemi di IA sviluppati per questa finalità sono dunque da considerarsi non ad alto rischio, pur operando nel campo della giustizia (alternativa), secondo quanto stabilito dal regolamento europeo.

L'IA potrebbe poi essere impiegata per l'individuazione dei casi di manifesta inammissibilità del ricorso all'ABF, ovvero delle cause di irricevibilità o inammissibilità del ricorso all'ACF, tenuto conto che per entrambi gli ADR sono previsti limiti di competenza temporale, per materia e per valore; un simile utilizzo potrebbe prospettarsi anche per l'Arbitro Assicurativo, profilandosi regole analoghe sul relativo ambito di operatività [81]. Più problematico appare invece l'utilizzo dell'IA per la redazione di tabelle di calcolo, ad esempio per la quantificazione del danno riconosciuto alla parte ricorrente: in questi casi, infatti, oltre alla particolare attenzione alla qualità dei dati di addestramento degli algoritmi, sarebbe pregnante il rispetto del principio del "*controllo da parte dell'utilizzatore*", raccomandato dalla "*Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziali e negli ambiti connessi*" [82].

In tutti gli ambiti prospettati di possibile utilizzo dell'IA nelle tutele stragiudiziali deve trattarsi di applicazioni trasparenti e verificabili, ossia progettate e sviluppate in modo da consentire il controllo sull'accuratezza dei dati inseriti e la spiegabilità delle modalità di funzionamento: le parti devono essere informate e pienamente consapevoli, nonché prestare il proprio consenso all'impiego delle nuove tecnologie – da rendere noto, quindi, in sede di regolamento di procedura [83] – per la composizione della loro vertenza, dovendo altresì essere poste nella condizione di riscontrare la correttezza del relativo processo decisionale. Ciò vale a maggior ragione per gli ADR in ambito bancario, finanziario e (in futuro) assicurativo, tenuto conto che tali sistemi non assolvono soltanto a una funzione deflattiva del contenzioso giudiziario, ma costituiscono pure meccanismi di risoluzione delle controversie complementari alla giustizia civile, trovando ivi accesso le c.d. *small claim*, che, per l'esiguità degli importi in contestazione, non sono portate nelle aule dei tribunali.

---

[81] Si vedano rispettivamente: per l'ABF, la Sez. I, par. 4 delle *Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari*; per l'ACF, l'art. 4 del *Regolamento concernente l'Arbitro per le Controversie Finanziarie (ACF);* per l'AAS, l'art. 9 del D.M. 215/2024.

[82] La Carta raccomanda altresì per tale utilizzo "*notevoli precauzioni metodologiche*" (cfr. *supra*, par. 2).

[83] Si rammenta che tale regolamento deve essere sottoposto, ai fini dell'accreditamento quale organismo di mediazione *ex* art. 16 del d.lgs. n. 28/2010, od organismo di ADR per i consumatori *ex* art. 141-*decies* del Codice del consumo, rispettivamente al Ministero della giustizia o all'Autorità competente di cui all'art. 141-*octies* del Codice del consumo in sede di domanda di iscrizione al relativo elenco.

## 7. Riflessioni conclusive

L'intelligenza artificiale può contribuire all'efficacia e alla qualità dei sistemi ADR, rispondendo a esigenze di semplificazione e di razionalizzazione dell'organizzazione e delle modalità di funzionamento di tali sistemi.

Occorre peraltro promuoverne un utilizzo responsabile, trasparente e socialmente utile. Sotto quest'ultimo profilo, è importante assicurare alla società civile l'accesso ai sistemi di IA: in prospettiva, servizi automatizzati di consulenza legale, che offrano anche una rappresentazione delle possibili modalità di risoluzione della controversia, potrebbero contribuire all'emersione e alla tutela di ulteriori situazioni giuridicamente rilevanti [84].

Il percorso sin qui tracciato si incentra, sebbene in modo non sempre univoco, su un'intelligenza artificiale complementare – piuttosto che sostitutiva – dell'intelligenza umana: l'indipendenza e l'autonomia di giudizio di chi amministra la giustizia, anche alternativa, devono rimanere salde al fine di consentire all'ordinamento giuridico di progredire, evolversi e mutare in ragione del mutamento del contesto di riferimento.

L'innovazione tecnologica è destinata ad avere un impatto rilevante sull'esercizio della funzione giurisdizionale, intesa in senso lato come comprensiva anche delle forme di giustizia alternativa, e costringe a ripensare il tradizionale quadro dei diritti e delle corrispondenti tutele, ma non vanno messi in discussione i valori e i principi su cui si fonda la predetta funzione, che deve restare, nel suo nucleo essenziale, una prerogativa umana.

---

[84] Secondo F. LAGIOIA e G. SARTOR, "*Come osservava il celebre economista Ken Galbraith, per assicurare un'adeguata protezione ai cittadini, non sono sufficienti gli strumenti normativi e la loro attuazione da parte di organi pubblici, ma sono altresì necessari i contropoteri o poteri compensativi (countervailing power) della società civile. I cittadini e le loro organizzazioni possono individuare abusi, informare il pubblico, promuovere l'applicazione delle norme, ed esercitare forme di pressione collettiva. Per essere efficace, tuttavia, un contropotere deve disporre di mezzi adeguati a quelli a diposizione del potere cui si oppone. Nell'era dell'intelligenza artificiale l'esercizio di un contropotere da parte società civile presuppone che anche la società civile sia in grado di avvalersi dell'intelligenza artificiale. Solo se i cittadini e le loro organizzazioni saranno in grado di utilizzare l'intelligenza artificiale a loro vantaggio potranno resistere e rispondere alle imprese e ai governi il cui potere è sostenuto dall'intelligenza artificiale*" (*Intelligenza artificiale per I diritti dei consumatori e tutela privacy: il Sistema Claudette*, cit.).

# Rilevazione e mitigazione dei *bias* negli algoritmi di classificazione con il metodo BRIO: il caso del *credit scoring*

Alessandro Giuseppe Buda, Greta Coraglia, Francesco Genco, Chiara Manganini, Giuseppe Primiero



## 1. Intelligenza artificiale e pregiudizi

Negli ultimi anni, il crescente uso dell'intelligenza artificiale (IA) in diversi settori ha portato enormi cambiamenti sociali, culturali, e tecnologici, specialmente laddove integrata all'interno di processi decisionali. In particolare il *credit scoring*, ovvero la stima dell'affidabilità creditizia, risulta essere uno degli ambiti in cui l'applicazione della IA suscita maggiore interesse, necessitando al tempo stesso di un attento controllo.

All'interno della vasta gamma di tecnologie che vanno sotto il nome di "intelligenza artificiale", in ambito creditizio vengono utilizzati algoritmi di *classificazione*, ovvero metodi per etichettare o categorizzare automaticamente oggetti o individui, basandosi su informazioni già conosciute. In pratica, un algoritmo di classificazione impara da esempi precedenti per poter prevedere a quale *classe* appartenga un nuovo oggetto o individuo.

Le informazioni su cui si basa l'algoritmo di classificazione, tecnicamente quelle con cui *si allena*, influenzano fortemente il suo comportamento. Supponiamo per esempio di costruire un algoritmo che voglia prevedere la probabilità che una data automobile faccia un incidente nei successivi 12 mesi e di allenarlo su dei dati del passato rispetto ai quali *tutte* le automobili che hanno fatto incidenti sono gialle, mentre quelle blu non sono *mai* state coinvolte in alcun sinistro. Se queste sono tutte e sole le informazioni che diamo all'algoritmo, è verosimile aspettarsi che questo preveda una più alta probabilità di

incidente nel caso di un'automobile gialla, rispetto a un'automobile blu [1].

Fenomeni come questo sono ben noti nell'ambito dell'IA, e vengono generalmente catalogati con il nome di *bias*: si tratta di distorsioni, spesso dovute a dati incompleti o non rappresentativi, che portano le macchine a prendere decisioni ingiuste o non corrette. In quale senso questa scorrettezza sia da intendersi, lo vedremo fra poco. In altre parole, proprio per loro natura, gli algoritmi di classificazione tendono a perpetuare, e talvolta ad amplificare pregiudizi, disuguaglianze e polarizzazioni, ed è pertanto opportuno che chi li utilizza per prendere decisioni sensibili, come quelle in ambito finanziario, ne sia consapevole ed eventualmente predisponga adeguati meccanismi di allerta e correzione.

Anche se fosse possibile accertare la qualità dei dati con cui un algoritmo è allenato, il che non è sempre banale nel caso di programmi proprietari o soggetti a segreto industriale, la loro grande quantità e la complessità dell'architettura tramite la quale vengono processati rendono gli algoritmi di IA intrinsecamente opachi e di difficile comprensione anche ai loro stessi sviluppatori.

L'AI Act è il primo regolamento dell'Unione Europea con l'obiettivo di istituire un quadro normativo e giuridico [2] per lo sviluppo e l'uso dell'intelligenza artificiale, puntando inoltre a stabilire quale sia un comportamento desiderabile per tali sistemi [3]. Per esempio, l'Autorità Bancaria Europea (EBA) scrive che un sistema di IA "deve garantire la protezione dei gruppi contro la discriminazione (diretta o indiretta)" [4], tenendo in considerazione che esistono diversi criteri secondo i quali un gruppo possa dirsi discriminato, e diverse misure di mitigazione di eventuali discriminazioni. D'altra parte, un algoritmo che si comporta in maniera perfettamente *indiscriminata*, al pari del lancio di una moneta, può assolvere a ben poche funzioni.

Conciliare tutte queste necessità richiede perciò una gran cura, non solo tecnica, ma anche etica e legale, nonché l'implementazione di meccanismi che pos-

---

[1] Sulla correlazione fra incidenti e colore delle auto, si veda https://www.ncbi.nlm.nih.gov/pmc/articles/PMC300804/.

[2] JTC 21 (CEN-CENELEC Joint Technical Committee 21 'Artificial Intelligence') ha pubblicato una lista di "AI Harmonized Standards" che sono stati adottati ufficialmente dalla Commissione Europea. Tra questi si trova lo standard CEN/CLC ISO/IEC TR 24027:2023, pubblicato nel dicembre 2023, che riguarda precisamente tecniche di misurazione e metodi per stimare il bias relativo all'IA.https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:77588&cs=117D63AEABBD08BA3E8BB52AB13F068A7.

[3] JTC 21 (CEN-CENELEC Joint Technical Committee 21 'Artificial Intelligence') ha pubblicato una lista di "AI Harmonized Standards" che sono stati adottati ufficialmente dalla Commissione Europea. Tra questi si trova lo standard CEN/CLC ISO/IEC TR 24027:2023, pubblicato nel dicembre 2023, che riguarda precisamente tecniche di misurazione e metodi per stimare il bias relativo all'IA. https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT:77588&cs=117D63AEABBD08BA3E8BB52AB13F068A7.

[4] EBA report on big data and advanced analytics, gennaio 2020 https://www.eba.europa.eu/sites/default/files/document_library/Final%20Report%20on%20Big%20Data%20and%20Advanced%20Analytics.pdf.

sano rendere l'uso di algoritmi di classificazione più giusto e, possibilmente, più efficiente.

## 2. Algoritmi per l'affidabilità creditizia

L'affidabilità creditizia di un individuo viene calcolata sulla base di un punteggio derivato da vari fattori quali la storia creditizia, il reddito e il livello di indebitamento, determinando quindi la probabilità che il richiedente possa estinguere un debito. Il *credit scoring* ha il potenziale di offrire una maggiore accuratezza ed efficienza, tempi più brevi di risposta e motivazioni eque ed oggettive. Allo stesso tempo, considerate le osservazioni precedenti, e vista la grande sensibilità del tema, richiede una ancora maggiore attenzione.

Garantire un trattamento equo – in gergo tecnico, *fair* – è fondamentale perché possa essere mantenuta fiducia nei sistemi di IA, oltre che ovviamente nella loro capacità di preservare principi fondamentali di giustizia sociale e non discriminazione. I *bias* presenti nei dati con cui sono allenati gli algoritmi, il design di questi ultimi, e il modo in cui sono integrati nei processi decisionali possono produrre esiti iniqui, e cercare di rettificarli può portare a una riduzione della capacità predittiva, che nel caso della concessione del credito può avere conseguenze economiche rilevanti non solo per l'ente creditore. La sfida attuale è dunque quella di trovare, per i processi decisionali basati sugli algoritmi di IA, un punto di equilibrio tra la sostenibilità economica, dettata da esigenze di mercato, e i requisiti di equità imposti invece dal regolatore europeo e dall'etica.

Proprio per l'importanza della sfida, diversi sono gli algoritmi in uso e le metriche proposte per cercare di misurare eventuali comportamenti indesiderati. Un passo fondamentale che contraddistingue la definizione di tali metodi è la selezione delle *caratteristiche di riferimento* rispetto alle quali si vuole garantire un comportamento equo: nel caso delle automobili della sezione precedente, potrebbe essere desiderabile che il programma si comporti imparzialmente rispetto al colore (e cioè che un colore non sia penalizzato più di un altro) o all'età del conducente (perché non siano discriminate le persone molto giovani, o molto vecchie, ad esempio; questo ovviamente a discapito del fatto che possa essere *effettivamente* più probabile per una persona anziana causare un incidente). Individuare le caratteristiche che definiscono classi da salvaguardare, in gergo tecnico chiamate *sensitive* o *protected features*, rimane una scelta del controllore, che sia il legislatore o l'analista che supervisiona l'algoritmo (chiamato anche modello), e non è in alcun modo determinata da quest'ultimo.

Alcuni studi[5] hanno esaminato importanti standard del settore come la FICO

[5] Si veda per esempio M. HARDT, E. PRICE, N. SREBRO, *Equality of opportunity in supervised learning*, in D. LEE, M. SUGIYAMA, U. LUXBURG, I. GUYON, R. GARNETT (eds.), *Advances in neural information processing systems*, 2016, vol. 29, pp. 1-9.

(Fair Isaac Corporation)[6] prendendo in considerazione etnia e solvibilità come attributi sensibili e analizzandoli sotto la lente di due tra i più discussi principi di equità in relazione al tema dell'IA, cioè quello di *parità statistica* e di *pari opportunità*. Un modello soddisfa la *parità statistica*[7] (detta anche *parità demografica*) quando i diversi gruppi sensibili di interesse (ad esempio, il gruppo degli uomini e quello delle donne) ottengono tassi uguali di decisioni positive. Se un modello, per esempio, concede in proporzione più prestiti ai richiedenti che presentano una determinata caratteristica sensibile (ad esempio, agli uomini) rispetto che a un'altra (ad esempio, alle donne), allora non rispetta la parità statistica, perché sta adottando un trattamento disuguale, e quindi potenzialmente ingiusto.

Il principio di *pari opportunità*,[8] invece, consiste nell'idea che un algoritmo per dirsi equo debba trattare in modo simile gli individui che hanno caratteristiche simili, garantendo loro le stesse possibilità di successo se essi sono qualificati allo stesso modo. Ad esempio, un modello per l'assegnazione di un prestito finanziario dovrebbe garantire a tutti gli individui che presentano un profilo finanziario simile la stessa probabilità di ottenere una decisione positiva, indipendentemente dal loro genere o etnia. In altre parole, se l'algoritmo discrimina tra persone con lo stesso livello di merito sulla base della loro appartenenza ad un gruppo sensibile, esso non sta rispettando il principio di pari opportunità.

È cruciale notare come i due principi appena descritti spesso non possono essere soddisfatti contemporaneamente da uno stesso sistema decisionale. Per esempio, il principio di parità statistica prevede che il tasso di successo dei richiedenti uomini (numero di richiedenti uomini che ottengono il prestito, sul totale dei richiedenti uomini) sia uguale a quello delle richiedenti donne. Il problema è che potrebbe succedere che le richiedenti donne abbiano in media un profilo finanziario meno affidabile di quello degli uomini. In questo caso, soddisfare il principio di parità statistica finirebbe per creare dei casi in cui a una richiedente donna venga accordato il prestito mentre ad alcuni uomini ugualmente meritevoli no, violando così il principio di pari opportunità.

Una considerevole quantità di studi, inoltre, si è concentrata sul proporre meccanismi di mitigazione per correggere comportamenti indesiderati, una volta scoperti. Alcuni di questi propongono tecniche che consistono in interventi sui dati di allenamento del modello;[9] altri, tecniche che riguardano il modo in

[6] https://community.fico.com/s/explainable-machine-learning-challenge.

[7] S. Barocas, M. Hardt, A. Narayanan, *Fairness and Machine Learning*, in *fairmlbook.org*, 2019.

[8] C. Dwork, M. Hardt, T. Pitassi, O. Reingold, R. Zemel, *Fairness through awareness*, in *Proceedings of the 3rd innovations in theoretical computer science conference*, 2012, pp. 214-226.

[9] M. Feldman, S.A. Friedler, J. Moeller, C. Scheidegger, S. Venkatasubramanian, *Certifying and removing disparate impact*, in *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2015, pp. 259-268.

cui il modello è allenato [10]; altri ancora, tecniche basate sui principi della teoria dei giochi cooperativi [11].

## 3. Metodi simbolici e l'approccio di BRIO

Sebbene nella letteratura scientifica ormai abbondino metodi e strumenti di analisi dell'equità e di mitigazione dei pregiudizi causati dall'IA, è ancora raro trovare metodologie e soluzioni pronte all'uso, che concretamente diano la possibilità al *decision-maker* di condurre, tramite queste, un'analisi complessiva del rischio di violazione dell'equità relativo a tutte le caratteristiche sensibili di interesse.

In secondo luogo, molti di questi metodi si basano sul presupposto che per analizzare un modello sia necessario conoscerne l'architettura e su che dati esso sia stato allenato. Nella pratica, però, questo è raramente possibile: dal punto di vista di un organo di controllo, può essere difficile ottenere, da chi è esaminato, dettagli precisi su come siano costruiti i modelli da analizzare. Da un lato, è molto frequente che le aziende affidino lo sviluppo di tecnologie di IA a soggetti esterni e che quindi non conoscano a loro volta i dettagli tecnici dell'algoritmo che impiegano nei propri processi decisionali. D'altro canto, persino un modello allenato da zero può raggiungere livelli di complessità talmente elevati da rendere praticamente impossibile stabilire effettivamente come funzioni e quali siano i suoi parametri e iper-parametri più rilevanti.

Per rispondere ad entrambe le difficoltà è possibile utilizzare un approccio *simbolico*, che consiste nel rappresentare la conoscenza e il ragionamento tramite regole e simboli chiari, simili a quelli che usiamo nel linguaggio ordinario, e dal significato preciso, come avviene per quelli del linguaggio logico formale. Impiegando questo approccio, il problema del controllo dell'IA può essere risolto con una strategia *post-hoc:* dato un modello possibilmente opaco di IA da analizzare, e costruito un modello simbolico trasparente di conoscenza, usiamo il secondo come metro di controllo del primo. In particolare, verifichiamo quanto il comportamento dell'IA sia distante da quanto determinato dal modello simbolico. In pratica, questo significa controllare l'algoritmo tramite regole definite da esseri umani, come se stessimo definendo un criterio o un insieme di

---

[10] M. Donini, L. Oneto, S. Ben-David, J.S. Shawe-Taylor, M. Pontil, *Empirical risk minimization under fairness constraints*, in *Advances in neural information processing systems*, vol. 32, 2018, pp. 2796-2806.

M.B. Zafar, I. Valera, M.G. Rogriguez, K.P. Gummadi, *Fairness constraints: Mechanisms for fair classification*, in *Artificial intelligence and statistics*, pp. 962-970. Proceedings of Machine Learning Research, 2017.

[11] G. Babaei, P. Giudici, *How fair is machine learning in credit lending?*, in *Quality and Reliability Engineering International*, 40(6), 2024 , pp. 3452-3464. https://doi.org/10.1002/qre.3579.

istruzioni che vorremmo l'IA seguisse nello svolgimento del suo compito. Nel caso specifico in esame, si introduce [12] un calcolo probabilistico e lo si utilizza per implementare uno strumento di rilevazione del *bias* e di analisi del rischio chiamato BRIO [13] (Bias, RIsk and Opacity in AI). La sua natura simbolica permette al programma di funzionare anche nel caso in cui non si sappia nulla del modello, e restituisce un'analisi dettagliata del rischio di comportamenti iniqui rispetto a tutte le caratteristiche sensibili selezionate.

Sviluppato all'interno dello spin-off universitario MIRAI (http://mirai.systems), il software BRIO dispone di un modulo dedicato alla rilevazione di possibili violazioni del principio di parità statistica discusso sopra. Più nel dettaglio, BRIO prende in esame le predizioni di un modello di classificazione, sotto forma di un insieme di dati con le loro relative caratteristiche, e un insieme di parametri inclusa la designazione di una o più caratteristiche sensibili di interesse, restituendo una valutazione del rischio che il modello in esame sia ingiusto rispetto a quelle caratteristiche sensibili. Il sistema guida l'utente nel processo di impostazione dei parametri ed è personalizzabile rispetto ai dettagli matematici dell'analisi: le scelte lasciate all'utente sono quelle che effettivamente fanno la differenza concettuale nell'esito dell'analisi, e di ciascuna vengono spiegate le implicazioni lungo il percorso.

In particolare, BRIO permette di condurre diverse analisi:

1. permette di comparare il comportamento del modello rispetto a un modello desiderabile dato: per esempio potremmo voler concedere il credito ad esattamente (o almeno) il 30% delle persone giovani che lo chiedono, o che il 30% di tutti i beneficiari fossero giovani;
2. permette di comparare il comportamento del modello rispetto a diversi

---

[12] Fabio Aurelio D'ASARO, Giuseppe PRIMIERO, *Probabilistic typed natural deduction for trustworthy computations*, *Proceedings of the 22nd International Workshop on Trust in Agent Societies (TRUST 2021) Co-located with the 20th International Conferences on Autonomous Agents and Multiagent Systems (AAMAS 2021), London, UK, May 3-7, 2021. CEUR Workshop Proceedings 3022, CEUR-WS.org 2021.*

Giuseppe PRIMIERO, Fabio Aurelio D'ASARO, *Proof-checking bias in labeling methods*, in 1st Workshop on Bias, Ethical AI, Explainability and the Role of Logic and Logic Programming, BEWARE 2022; Udine; Italy; 2 December 2022, CEUR Workshop Proceedings, Volume 3319, 2022, Pages 9-19.

Francesco A. GENCO, Giuseppe PRIMIERO, *A typed lambda-calculus for establishing trust in probabilistic programs*, *CoRR abs/2302.00958,* 2023.

Fabio Aurelio D'ASARO, Francesco GENCO, Giuseppe PRIMIERO, *Checking trustworthiness of probabilistic computations in a typed natural deduction system*, *Journal of Logic and Computation*, exaf003, https://doi.org/10.1093/logcom/exaf003, 2025.2024.

[13] Greta CORAGLIA, Fabio Aurelio D'ASARO, Francesco Antonio GENCO, Davide GIANNUZZI, Davide POSILLIPO, Giuseppe PRIMIERO, Christian QUAGGIO, *BrioxAlkemy: a bias detecting tool*, Proceedings of the 2nd Workshop on Bias, Ethical AI, Explainability and the role of Logic and Logic Programming co-located with the 22nd International Conference of the Italian Association for Artificial Intelligence (AI*IA 2023), pp. 44-60, 2024.

gruppi relativi alla stessa caratteristica sensibile, per esempio misurando il diverso trattamento rispetto al genere o all'età.

Se l'analisi segnala un possibile comportamento distorto, è possibile effettuare un successivo controllo su alcune o tutte le sottoclassi delle classi sensibili considerate. Questa seconda verifica mira a stabilire se i pregiudizi riscontrati a livello delle classi possano essere spiegati da caratteristiche non sensibili degli individui il cui utilizzo nel prendere decisioni sia moralmente accettabile. Per esempio è possibile che una persona giovane abbia generalmente una minore liquidità, e che quindi sia esclusa dal credito in virtù di questo fatto, piuttosto che per la sua età [14].

I risultati dei due test possono essere in seguito aggregati in un'unica misura di rischio che tiene conto di diversi fattori: quanti individui sono potenziali vittime dell'iniquità del sistema; quanto questa è marcata; quanto è severo il controllo effettuato. Questi ultimi due criteri, in particolare, dipendono dalla scelta del *margine di errore* che si decide di dare a BRIO perché valuti se una differenza di comportamento sia sufficientemente piccola da essere considerata trascurabile. La scelta del margine di errore è essa stessa parte del processo di personalizzazione del programma, e prevede una certa libertà di giudizio: mettendo un margine di errore basso, BRIO sarà estremamente attento e tollererà poche trasgressioni (questo è preferibile in contesti nei quali è più grave che il modello di IA dia un giudizio positivo a chi non lo merita piuttosto che un giudizio negativo a chi ne merita uno positivo), mentre un margine alto è più permissivo (ed è quindi più adatto quando, nel dubbio, è preferibile che un individuo riceva un giudizio positivo). Questo esplicito accento sulla personalizzazione del comportamento dello strumento di analisi è un ulteriore riferimento alla necessità di stilare criteri guida, se non una vera e propria legislazione, che armonizzi le scelte dei diversi settori industriali in funzione del loro impatto sociale e della loro diffusione.

## 4. Prospettive future: mitigazione, analisi dei ricavi

Uno strumento come BRIO, basato su una combinazione di metodologia simbolica e statistica, può essere ulteriormente utilizzato per analizzare l'interazione fra la generazione di ricavi e la gestione del rischio di comportamenti iniqui. È possibile condurre uno studio quantitativo degli effetti che le scelte legate alla gestione di questo tipo di rischio possono avere sulle entrate e, in parti-

[14] Se questo comportamento sia poi a sua volta indesiderabile è, di nuovo, una scelta dell'utilizzo del programma. BRIO si limita a segnalare il diverso comportamento condizionatamente alle caratteristiche disponibili. Nel caso un utente volesse inserire anche la liquidità fra gli attributi rispetto ai quali non è lecito fare valutazioni, è sufficiente marcarla a sua volta fra le caratteristiche "protette".

colare, cercare di capire come la scelta di un certo valore di soglia nella misura dell'affidabilità creditizia – spesso convenzionalmente fissata a 580 punti [15] – influenzi i ricavi e la misura complessiva di rischio.

Supponiamo, realisticamente, che un modello per il calcolo dell'affidabilità finanziaria classifichi come buoni pagatori tutti coloro che possiedono un punteggio superiore a 580. Chiamiamolo CF-580. Con strumenti in forze all'industria del credito possiamo calcolare quale sia il guadagno atteso nel concedere un prestito a tutti gli individui considerati buoni pagatori (secondo la definizione di cui sopra), e al negarlo a quelli che si prevede essere cattivi pagatori, per esempio utilizzando dati come gli accantonamenti e il tasso di insolvenza. Possiamo poi calcolare la misura generale di rischio rispetto ad alcune caratteristiche che determinano le classi che desideriamo proteggere, e registrare anche questo valore.

Scegliendo una soglia differente, e decidendo di indicare come buoni pagatori tutti gli individui con un punteggio superiore a 550, otterremo un algoritmo di classificazione diverso, supponiamo di chiamarlo CF-550. Anche se è evidente che fra CF-550 e CF-580 ci sia un legame stretto, possiamo ripetere le misure di profitto atteso e di rischio, e confrontarle fra loro: osserviamo [16] che l'uso di un algoritmo più equo non implica necessariamente un calo dei profitti, e che un algoritmo più permissivo non è necessariamente più equo. Entrambe queste affermazioni sono ragionevoli, anche se possono risultare poco intuitive. Si pensi, per esempio, a un algoritmo molto "cauto", CF-700, che concede prestiti solamente a individui molto affidabili dal punto di vista del credito. È chiaro che un istituto di credito abbia poco da guadagnare a utilizzare CF-700, sia per i tassi bassi che per l'esiguo numero di individui che effettivamente rispettano i criteri di CF-700. Allo stesso modo, il guadagno dell'istituto di credito sarebbe scarso se questo concedesse prestiti a tutti coloro che ne fanno domanda. Similmente al profitto, la misura di rischio può essere *non monotona*, nel senso che essa assume valori altalenanti al variare del valore di soglia impiegato per discriminare i debitori affidabili da quelli non affidabili. È perciò possibile pensare di ottenere pari o maggiore profitto, e contemporaneamente una maggiore equità.

Le analisi di questo tipo ci indicano che è possibile controllare e valutare gli strumenti automatici di decisione, anche in contesti cruciali come il *credit scoring*, affinché il loro comportamento sia equo rispetto a quelle che consideriamo caratteristiche sensibili degli individui. Inoltre, risulta evidente dall'applicazione del sistema di controllo BRIO che è possibile indirizzare le scelte dell'industria verso l'impiego di strumenti automatici di valutazione e previsione più equi e

[15] https://www.experian.com/blogs/ask-experian/credit-education/score-basics/550-credit-score/.

[16] Greta CORAGLIA, Francesco A. GENCO, Pellegrino PIANTADOSI, Enrico BAGLI, Pietro GIUFFRIDA, Davide POSILLIPO, Giuseppe PRIMIERO, *Evaluating AI fairness in credit scoring with the BRIO tool*, *CoRR abs/2406.03292 (2024).*

socialmente giusti senza che questo precluda necessariamente una parte dei profitti potenziali.

## 5. Conclusione

Abbiamo presentato il problema dei bias generati da algoritmi di Intelligenza Artificiale nel contesto della valutazione del credito e illustrato brevemente l'uso dello strumento BRIO per la rilevazione delle violazioni di equità e per la misurazione del rischio associato a tali violazioni. Lo strumento BRIO consente di confrontare il trattamento di classi sensibili da parte del modello. Questa analisi evidenzia l'importanza di integrare considerazioni di equità nei modelli (non solo di valutazione del credito) e mettono in risalto il potenziale di metriche innovative per fornire una valutazione integrata della loro equità. Il lavoro di sviluppo di MIRAI ha come obiettivo quello di estendere questo approccio, perfezionando ulteriormente gli strumenti e i metodi utilizzati per garantire equità nei sistemi basati sull'intelligenza artificiale.

# La Compliance nell'era dell'intelligenza artificiale: un approccio probabilistico

Daniela Bragante, Francesco Pallavicino



## 1. Introduzione

L'intelligenza artificiale (IA) rappresenta una delle più promettenti tecnologie per ottimizzare le attività della Funzione Compliance, specialmente nel contesto di un panorama normativo in rapida evoluzione. Oggi i presupposti ci sono tutti, l'IA è una realtà che trasversalmente abbraccia potenzialmente tutti i settori.

In questo contributo cercheremo di illustrare alcune potenziali opportunità per la Funzione Compliance negli ambiti nei quali l'attività si esplica, e specificatamente: l'individuazione ed il monitoraggio della normativa esterna, l'analisi di impatto e la valutazione di nuovi progetti e iniziative, il processo di *compliance risk assessment*, l'apertura e la gestione delle azioni correttive, il reporting di compliance e le altre attività della Funzione Compliance.

La Funzione Compliance svolge numerose attività critiche per la gestione del rischio di non conformità, fornendo inoltre assistenza e consulenza alle unità organizzative e agli Organi Sociali della Società. In ciascuna delle attività in capo alla Funzione Compliance l'IA può fornire un supporto rilevante, migliorando l'efficienza, riducendo il rischio di errori e garantendo una maggiore tempestività nelle risposte.

L'introduzione di sistemi di Intelligenza Artificiale nei processi di compliance consente inoltre di modificare tali processi secondo criteri di maggiore flessibilità, efficienza e opportunità, adottando un approccio di tipo probabilistico alla compliance. Tale approccio si basa sull'utilizzo dell'IA per fornire valutazioni di conformità in termini di probabilità, anziché attraverso giudizi binari (conforme/non conforme). Questo metodo consente di esprimere, per ogni proces-

so, prodotto, servizio o documento esaminato, una percentuale che indica la probabilità che essi siano effettivamente conformi alle normative vigenti. Tale approccio fornisce una guida quantitativa utile all'operatore umano, che può quindi intervenire laddove il rischio di non conformità sia più elevato, ottimizzando così il processo decisionale.

In pratica, l'IA analizza le normative e i dati, assegnando una probabilità di conformità che permette di identificare con maggiore precisione le aree a rischio. Questo aiuta a migliorare l'efficienza della Funzione Compliance, poiché consente di concentrare gli sforzi solo sulle questioni più critiche. L'operatore, invece di eseguire un controllo completo e dettagliato su tutti gli elementi, può focalizzarsi su quelle aree in cui l'IA ha segnalato una probabilità inferiore di conformità, riducendo così il tempo di intervento e aumentando la precisione delle valutazioni.

L'approccio probabilistico favorisce quindi una gestione più dinamica e proattiva del rischio di non conformità, combinando l'automazione offerta dall'IA con l'intervento umano, laddove necessario. In questo modo, la Funzione Compliance può migliorare la propria capacità di monitorare e adeguarsi ai cambiamenti normativi, massimizzando l'efficienza operativa e riducendo al minimo il rischio di sanzioni o violazioni.

Tuttavia, come ogni medaglia ha il suo rovescio. Il mercato è ancora giovane ed in evoluzione e per certi versi sembra peccare, talvolta, di eccessivo entusiasmo. Nonostante le numerose sfide, tra le quali anche quelle di natura etica, le opportunità sono però numerose, soprattutto per coloro che sanno e sapranno cogliere l'importanza dell'innovazione e della sperimentazione. Evoluzione che consentirà alla Funzione Compliance di continuare quel percorso che l'ha portata ad essere un fondamentale elemento strategico di promozione di una cultura etica e sostenibile a supporto delle iniziative di business.

## 2. Individuazione e monitoraggio della normativa esterna

La tempestiva individuazione delle nuove normative e il monitoraggio nel continuo degli aggiornamenti normativi costituiscono un'attività cruciale della Funzione Compliance.

L'intelligenza artificiale, in particolare attraverso tecniche di *Text Mining* e *Natural Language Processing* (NLP), consente di analizzare rapidamente grandi quantità di dati normativi provenienti da fonti istituzionali, come le Autorità di Vigilanza, le associazioni di categoria, gli organismi di regolamentazione e le rassegne stampa finanziarie.

Secondo uno studio di Arner, Barberis e Buckley (2017) [1], l'automazione dei processi di individuazione normativa permette di ridurre i tempi di reazione e di

[1] D.W. Arner, J.N. Barberis, R.P. Buckley, *FinTech, RegTech, and the Reconceptualization*

aumentare l'accuratezza nel riconoscimento dei cambiamenti regolamentari. Questo approccio può risultare particolarmente efficace in contesti in cui le normative cambiano frequentemente e devono essere costantemente verificate.

L'IA può essere programmata per monitorare questi siti, analizzando in tempo reale nuove pubblicazioni e identificando le normative rilevanti attraverso algoritmi di *Machine Learning* (ML) che apprendono le priorità normative aziendali (Zavolokina et al. 2020)[2]. Algoritmi di machine learning possono essere utilizzati per estrarre automaticamente i paragrafi delle normative che impattano maggiormente i processi aziendali, evitando la necessità di una lettura manuale completa dei documenti normativi.

La valutazione dell'impatto operativo delle nuove normative è una fase fondamentale del processo di compliance. Tradizionalmente, questo processo comporta un'analisi manuale delle disposizioni normative e un confronto con le politiche aziendali esistenti. Tuttavia, l'IA può facilitare questo compito, sfruttando strumenti di analisi predittiva per simulare gli impatti potenziali delle nuove normative sugli asset aziendali. Uno studio condotto da Veale e Binns (2017)[3] ha evidenziato come gli algoritmi predittivi possano ridurre gli errori interpretativi e migliorare la precisione delle valutazioni di impatto normativo.

Nel contesto specifico dell'analisi normativa, l'IA può confrontare automaticamente le nuove disposizioni con le procedure esistenti, evidenziando eventuali disallineamenti. I modelli basati su ML permettono inoltre di prevedere le aree più vulnerabili alle modifiche legislative e suggeriscono misure di adeguamento personalizzate. Secondo la Financial Stability Board (FSB)[4], l'adozione di strumenti predittivi migliora la capacità di un'organizzazione di rispondere in modo proattivo ai cambiamenti normativi, minimizzando l'impatto sui processi aziendali.

Adottando un approccio probabilistico, l'IA potrebbe confrontare i nuovi requisiti normativi con i processi interni esistenti, esprimendo una probabilità che questi siano effettivamente conformi. Ad esempio, se una nuova regolamentazione riguarda le procedure di antiriciclaggio, l'IA potrebbe valutare che le procedure esistenti siano conformi con una probabilità del 95%, ma potrebbe segnalare una vulnerabilità con una probabilità del 5%. Questo permette all'operatore umano di comprendere dove intervenire per colmare i potenziali rischi e aumentare la probabilità di conformità. Tale sistema probabilistico consente inol-

---

*of Financial Regulation*, in *Northwestern Journal of International Law & Business*, 37(3), 2017, pp. 371-413.

[2] L. ZAVOLOKINA, M. DOLATA, G. SCHWABE, *RegTech – The Nucleus of Innovation in the Digital Transformation of Regulatory Processes*, in *Electronic Markets*, 30(1), 2020, pp. 1-13.

[3] M. VEALE, R. BINNS, *Fairer Machine Learning in the Real World: Mitigating Discrimination without Collecting Sensitive Data*, in *Big Data & Society*, 4(2), 2017, pp. 1-17.

[4] FINANCIAL STABILITY BOARD, *Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications*, 2020. Disponibile su: https://www.fsb.org.

tre di evidenziare le aree grigie in cui un controllo umano è necessario per perfezionare l'analisi e prendere decisioni finali (Zavolokina et al. 2020)[2].

La comunicazione tempestiva dei risultati delle analisi normative alle unità organizzative impattate costituisce un aspetto critico nella gestione della conformità. L'uso dell'intelligenza artificiale in questo contesto può semplificare la redazione e la distribuzione di alert informativi e normativi, consentendo una comunicazione chiara e standardizzata attraverso l'uso di modelli di linguaggio generativo. Inoltre, l'AI può essere utilizzata per supportare la *gap analysis*, identificando automaticamente le discrepanze tra le nuove normative e le politiche aziendali.

Secondo la European Banking Authority (EBA 2020)[5], l'adozione di soluzioni di intelligenza artificiale nella comunicazione normativa consente di ridurre i rischi di incomprensioni e di migliorare la tracciabilità delle azioni di adeguamento. Inoltre, attraverso l'analisi automatizzata delle normative, le organizzazioni possono ottenere una mappatura accurata delle lacune rispetto agli standard legali, facilitando la creazione di un Piano delle Azioni di Adeguamento efficace e puntuale.

Un ulteriore ambito in cui l'IA può apportare benefici è nella gestione e nel monitoraggio delle azioni di adeguamento. L'adozione di strumenti di machine learning consente un monitoraggio continuo e proattivo del rispetto delle tempistiche previste per l'implementazione delle misure di adeguamento, nonché un'analisi dell'efficacia degli interventi posti in essere. In uno studio condotto da Hildebrandt (2019)[6], si evidenzia come l'uso di algoritmi di apprendimento automatico possa migliorare il follow-up delle azioni di adeguamento, riducendo i rischi legati a una scarsa implementazione delle nuove normative.

L'adozione di sistemi di reporting avanzati, basati sull'intelligenza artificiale, può fornire un'analisi dettagliata dello stato di avanzamento delle azioni di adeguamento. Secondo la Banca d'Italia (2021)[7], tali strumenti offrono una visione complessiva del livello di conformità aziendale e facilitano la gestione delle eventuali azioni di adeguamento necessarie per allinearsi alle nuove disposizioni legislative.

In sintesi, l'adozione dell'intelligenza artificiale nella Funzione Compliance rappresenta una soluzione innovativa ed efficace per rispondere alle crescenti esigenze normative. Le sue applicazioni permettono di ottimizzare processi chiave come l'individuazione e il monitoraggio normativo, l'analisi dell'impatto delle nuove disposizioni, la comunicazione interna e il monitoraggio delle relative azioni di adeguamento. Gli studi accademici e i documenti istituzionali citati eviden-

---

[5] European Banking Authority, *EBA Report on Big Data and Advanced Analytics*, 2020. Disponibile su: https://www.eba.europa.eu.

[6] M. Hildebrandt, *Law for Computer Scientists and Other Folk*, Oxford University Press, Oxford, 2019.

[7] Banca d'Italia, *Relazione Annuale: L'Innovazione Tecnologica e l'Intelligenza Artificiale nel Sistema Finanziario Italiano*, 2021. Disponibile su: https://www.bancaditalia.it.

ziano come l'IA possa migliorare l'efficienza operativa e ridurre i rischi di non conformità, promuovendo un approccio proattivo e tempestivo alla gestione delle normative.

## 3. Analisi di impatto e valutazione di nuovi progetti e iniziative

È oramai approccio consolidato coinvolgere la Funzione Compliance, fin dalla fase iniziale, nella valutazione dei nuovi prodotti, servizi o modifiche a quelli esistenti. Questa attività include la valutazione del rischio di conformità, che può beneficiare notevolmente dell'adozione dell'intelligenza artificiale. Gli strumenti di analisi predittiva possono simulare scenari normativi basati su dati storici e sulle regolamentazioni esistenti, fornendo previsioni accurate su come un nuovo progetto potrebbe violare determinate normative o richiedere adeguamenti specifici.

L'approccio probabilistico consente all'IA di valutare il rischio con precisione, attribuendo percentuali di conformità per ogni area normativa. Ad esempio, per un nuovo prodotto finanziario digitale, l'IA potrebbe valutare una probabilità del 90% che le procedure di protezione dei dati personali siano conformi alle normative GDPR, ma solo il 70% di probabilità che le procedure antiriciclaggio siano adeguate, suggerendo all'operatore di concentrarsi su quest'ultima area. Grazie a queste valutazioni probabilistiche, l'operatore umano può decidere se accettare i suggerimenti dell'IA o condurre ulteriori analisi per aumentare la probabilità di conformità e ridurre il rischio di violazioni.

Il processo di consulenza può essere ulteriormente sviluppato realizzando uno strumento di Virtual Assistant che, identificando la tipologia di riferimento normativo e le fonti dati a cui attingere, analizza la domanda e incrocia la richiesta con il patrimonio informativo aziendale e le fonti esterne, fornendo una risposta ai quesiti formulati da indirizzare in funzione del livello di confidenza. Il processo così definito, attraverso strumenti di IA anche generativa, consente, inoltre, di efficientare le modalità di risposta facendo tesoro di pareri già validati dalla Funzione Compliance, riproducendoli autonomamente in funzione del livello di confidenza. Può fornire, inoltre, ausilio all'operatore umano nella predisposizione di pareri predisponendo una prima versione del documento con una evidente riduzione dei tempi di elaborazione dello stesso e conseguenti importanti efficientamenti.

Un'altra attività centrale della Funzione Compliance riguarda la valutazione dei reclami, in particolare quelli rivolti all'Arbitro Bancario Finanziario (ABF) o alla Banca d'Italia. L'IA può essere di grande aiuto nell'automatizzare la classificazione e l'analisi dei reclami ricevuti. Attraverso tecnologie di machine learning, i sistemi possono analizzare il contenuto dei reclami, identificare pattern ricorrenti e assegnare una probabilità che un reclamo possa rappresentare una potenziale violazione normativa.

Per esempio, se un reclamo riguarda presunte pratiche scorrette nella vendita di un prodotto finanziario, l'IA potrebbe calcolare una probabilità dell'85% che tale reclamo rappresenti una violazione delle normative sulla trasparenza finanziaria. Un reclamo riguardante un problema tecnico, invece, potrebbe presentare solo una probabilità del 30% di essere associato a una violazione normativa. Grazie a queste valutazioni probabilistiche, l'operatore umano può dare priorità ai reclami con un rischio più elevato di violazione, risolvendo i casi più urgenti con maggiore efficienza (Banca d'Italia 2021) [8].

La Funzione Compliance è inoltre responsabile dell'analisi della contrattualistica sia attiva che passiva per garantire che essa sia conforme alle normative vigenti. L'IA, attraverso tecnologie di NLP, può analizzare automaticamente i contratti e fornire una valutazione probabilistica delle clausole, indicando con quale probabilità ciascuna di esse rispetti i requisiti normativi.

Un esempio concreto potrebbe essere l'analisi di una clausola riguardante la privacy dei dati, che l'IA potrebbe valutare come conforme con una probabilità del 95%, mentre una clausola relativa alla trasparenza finanziaria potrebbe risultare conforme solo con una probabilità del 70%. Tali probabilità forniscono all'operatore una chiara indicazione delle aree che richiedono un intervento umano. Questo approccio non solo accelera la revisione contrattuale, ma consente anche di concentrarsi sui punti più critici, garantendo che eventuali lacune normative vengano identificate e risolte prima della finalizzazione del contratto. La possibilità di visualizzare le valutazioni in termini probabilistici rende il processo più trasparente e permette di mitigare i rischi in modo più accurato (European Banking Authority 2020) [9].

L'IA può supportare la Funzione Compliance anche nella validazione delle comunicazioni aziendali, assicurando che i contenuti siano conformi alle normative. Questo è particolarmente rilevante nel contesto delle comunicazioni promozionali o informative rivolte alla clientela, dove le violazioni possono portare a sanzioni significative. Un sistema di IA potrebbe associare a ciascuna comunicazione una probabilità di conformità. Anche in questo caso l'operatore umano può così decidere di approfondire solo le aree dove la probabilità di conformità è più bassa, rendendo il processo di validazione più efficiente e preciso.

L'integrazione dell'intelligenza artificiale nelle attività della Funzione Compliance, con un approccio probabilistico, fornisce una visione più sfumata e quantitativa della conformità normativa. L'IA esprime le proprie valutazioni in termini di probabilità, permettendo agli operatori di intervenire in modo mirato, ottimizzando le risorse e garantendo una maggiore accuratezza nelle decisioni. Questo approccio consente alla Funzione Compliance di prendere decisioni pro-

[8] BANCA D'ITALIA, *Relazione Annuale: L'Innovazione Tecnologica e l'Intelligenza Artificiale nel Sistema Finanziario Italiano*, 2021. Disponibile su: https://www.bancaditalia.it.

[9] EUROPEAN BANKING AUTHORITY, *EBA Report on Big Data and Advanced Analytics*, 2020. Disponibile su: https://www.eba.europa.eu.

attive e basate sui dati, riducendo i tempi operativi e minimizzando i rischi complessivi di non conformità.

## 4. Compliance Risk Assessment

La Funzione Compliance si occupa di valutare il rischio inerente e residuo di non conformità a livello di area normativa, con una metodologia che integra sia aspetti quantitativi che qualitativi.

L'integrazione dell'IA in queste attività può migliorare notevolmente l'efficienza e la precisione di tali attività, soprattutto attraverso l'adozione di un approccio probabilistico. L'IA può infatti analizzare in modo automatico grandi volumi di dati e assegnare probabilità specifiche agli eventi di rischio, offrendo una stima accurata del rischio di non conformità e del suo impatto reputazionale.

In questa sede, analizzeremo le principali aree di applicazione dell'IA nella Funzione Compliance descritta, con particolare attenzione ai benefici offerti dall'approccio probabilistico.

*Misurazione del rischio inerente di non conformità*

La misurazione del rischio inerente, da intendersi quale massima esposizione al rischio di non conformità, attuale e prospettico, in assenza di presidi di controllo, è fondamentale per valutare la probabilità che si verifichi una violazione normativa. La misurazione del rischio inerente è quantificata considerando il risultato del calcolo della probabilità dell'evento di rischio e dell'impatto sanzionatorio e reputazionale connesso al mancato rispetto degli specifici precetti normativi.

In particolare, la probabilità di accadimento del rischio è determinata in funzione di diversi fattori, tra i quali la tipologia di clientela, il canale di distribuzione, i volumi delle transazioni, il tasso annuo di crescita dei prodotti o servizi, le risultanze di verifiche condotte da altre Funzioni o Autorità. L'IA, attraverso algoritmi di machine learning e modelli statistici, può automatizzare il processo di analisi di questi *driver*, assegnando probabilità di accadimento.

Ad esempio, l'IA potrebbe stimare che un prodotto destinato al mercato estero, con un alto tasso di crescita e un numero elevato di transazioni processate, abbia una probabilità del 70% di incorrere in una violazione della normativa sulla trasparenza finanziaria. Allo stesso tempo, potrebbe segnalare un rischio del 90% per quanto riguarda la violazione delle norme antiriciclaggio, offrendo una guida quantitativa su dove concentrare gli sforzi di monitoraggio.

Questo approccio non solo permette alla Funzione Compliance di identificare con maggiore precisione i potenziali rischi, ma consente anche di allocare in modo più efficiente le risorse, concentrandosi sulle aree a più alto rischio. Inoltre, la capacità dell'IA di aggiornare le proprie previsioni in tempo reale, in base

a nuovi dati e contesti, garantisce un monitoraggio continuo e dinamico del rischio (Zavolokina et al. 2020) [10].

Anche con riferimento all'impatto sanzionatorio e reputazionale del rischio l'IA può svolgere un ruolo chiave. Utilizzando dati storici relativi a sanzioni precedenti e analisi del *sentiment online*, l'IA può stimare l'impatto che una violazione normativa avrebbe sulla reputazione dell'azienda nonché prevedere la potenziale sanzione.

Ad esempio, un sistema di IA potrebbe valutare che una violazione della normativa sul trattamento dei dati personali comporti una probabilità del 75% di subire sanzioni superiori a €500.000, e al contempo calcolare un impatto reputazionale con un rischio dell'80%, a causa della possibile esposizione mediatica e delle ripercussioni sulle relazioni con i principali stakeholder aziendali. Questo tipo di analisi probabilistica consente alla Funzione Compliance di prendere decisioni più informate e di stabilire azioni correttive adeguate.

Inoltre, l'IA può integrare fonti esterne di informazioni, come report istituzionali o sanzioni comminate da Autorità di Vigilanza ad altre aziende del settore, migliorando così la capacità di prevedere il rischio di impatto reputazionale e rafforzando il sistema di compliance (Financial Stability Board 2020) [11].

*Maturità del sistema di compliance e la valutazione del rischio residuo*

La misurazione della maturità del sistema di compliance e la valutazione del rischio residuo rappresentano altri ambiti critici per la Funzione Compliance. L'IA può supportare queste attività attraverso tecniche di campionamento avanzato e analisi predittiva. Ad esempio, utilizzando un campionamento sistematico o casuale, l'IA può selezionare i dati da verificare con maggiore accuratezza rispetto ai metodi tradizionali, ottimizzando il tempo necessario per l'esecuzione dei test di impianto e di funzionamento.

Per quanto riguarda la valutazione del rischio residuo, l'IA può fornire un approccio probabilistico che combina la probabilità di non conformità con la maturità dei presidi di compliance esistenti. Questo permette alla Funzione Compliance di avere una visione più completa e dinamica del rischio. Ad esempio, se il sistema di compliance è considerato molto maturo, l'IA potrebbe calcolare che il rischio residuo è basso (con una probabilità del 20%), nonostante il rischio inerente sia alto. In questo modo, la funzione può decidere se implementare ulteriori azioni correttive o mantenere il livello di monitoraggio attuale, basandosi su una valutazione oggettiva e probabilistica dei rischi.

Inoltre, l'IA può automatizzare la redazione di questi report, analizzando i

---

[10] L. ZAVOLOKINA, M. DOLATA, G. SCHWABE, *RegTech – The Nucleus of Innovation in the Digital Transformation of Regulatory Processes*, in *Electronic Markets*, 30(1), 2020, pp. 1-13.

[11] FINANCIAL STABILITY BOARD, *Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications*, 2020. Disponibile su: https://www.fsb.org.

dati raccolti nell'ambito dell'attività di misurazione e di verifica per singola area normativa.

## 5. Azioni Correttive

Fase cruciale del processo di compliance riguarda la gestione delle azioni correttive.

Le diverse fasi di apertura, monitoraggio e chiusura delle Azioni Correttive, nonché il loro processo di escalation, devono essere gestite secondo un processo rigoroso, finalizzato a garantire un presidio adeguato del rischio di non conformità. In questo contesto, l'IA può svolgere un ruolo chiave, migliorando l'accuratezza delle valutazioni e velocizzando le decisioni.

L'IA può intervenire già nelle prime fasi dell'identificazione delle debolezze e della valutazione del rischio, fornendo una stima probabilistica della gravità di ciascuna debolezza identificata. Ad esempio, nel contesto delle azioni correttive che derivano da novità normative o da attività di *compliance risk assessment*, l'IA potrebbe calcolare la probabilità di successo delle azioni proposte basandosi su dati storici e best practice di settore. Un sistema di IA potrebbe assegnare, ad esempio, una probabilità dell'80% che una specifica azione correttiva risolva il rischio di non conformità legato a un cambiamento normativo riguardante la privacy dei dati, mentre per altre azioni potrebbe segnalare una probabilità inferiore, suggerendo così la necessità di ulteriori interventi correttivi.

Il monitoraggio continuo delle azioni correttive è un processo formale strutturato, che implica la richiesta di documentazione idealmente effettuata con periodicità trimestrale o, per azioni di particolare rilevanza, con aggiornamenti mensili. In questo ambito, l'IA può supportare la Funzione Compliance automatizzando il monitoraggio e il follow-up delle azioni correttive. Sistemi di IA potrebbero monitorare lo stato di avanzamento di ciascuna azione e inviare *alert* automatici all'*owner* di compliance qualora si rilevi un ritardo o un'incongruenza nelle attività programmate. Questo approccio non solo riduce il carico di lavoro manuale ma migliora anche la capacità di rilevare tempestivamente eventuali problematiche che richiedono un intervento correttivo urgente.

Inoltre, un sistema di machine learning potrebbe analizzare i dati storici relativi alle azioni correttive precedenti e prevedere quali azioni abbiano una probabilità più alta di essere completate con successo entro le scadenze prefissate. Questo approccio probabilistico permetterebbe alla Funzione Compliance di concentrarsi sulle azioni più critiche, ottimizzando le risorse a disposizione.

Il processo di escalation, che riveste un ruolo chiave nella gestione del rischio di non conformità, viene attivato quando le Azioni Correttive sono prossime o superano una definita soglia di attenzione.

In questa fase, l'IA può giocare un ruolo determinante nell'identificare au-

tomaticamente le azioni che stanno superando tali soglie e che richiedono un intervento urgente. Attraverso l'analisi dei dati raccolti nel sistema di gestione delle azioni correttive, un algoritmo di machine learning potrebbe segnalare in tempo reale quando un'azione correttiva è prossima al superamento della soglia, suggerendo quali azioni hanno priorità più alta e quali possono essere posticipate senza rischi significativi.

Ad esempio, se una specifica azione correttiva legata alla normativa antiriciclaggio ha una probabilità elevata (90%) di superare la soglia di attenzione a causa di ritardi nel processo di revisione, l'IA potrebbe inviare un *alert* automatico al responsabile della direzione, suggerendo una revisione urgente o una ridefinizione delle scadenze. Questo tipo di intervento proattivo consente alla Funzione Compliance di prevenire situazioni critiche, migliorando la gestione delle priorità e riducendo i rischi operativi e reputazionali.

L'adozione dell'intelligenza artificiale può trasformare profondamente il modo in cui vengono gestite le azioni correttive e il rischio di non conformità. L'IA, anche in questo ambito consente di migliorare l'efficienza e la precisione del monitoraggio, automatizzando processi critici come il follow-up delle azioni correttive. Inoltre, l'IA offre strumenti avanzati per identificare le priorità nelle attività di escalation, fornendo una guida proattiva per la gestione del rischio in modo tempestivo e accurato.

## 6. Reporting di Compliance

La redazione di reportistica, interna ed esterna, è un'attività importante, per motivi istituzionali oltre che operativi, e si presta tipicamente all'automazione informata una volta definiti rigorosamente finalità, metodo e fonti a seconda del contesto e del destinatario finale.

Il Compliance Plan rappresenta uno degli strumenti fondamentali della Funzione Compliance per la gestione del rischio di non conformità. Esso si articola in diverse fasi, tra cui pianificazione, monitoraggio e aggiornamento, con l'obiettivo di coprire l'intero perimetro normativo in un arco temporale definito, basato sui rischi identificati. L'IA, attraverso tecniche di machine learning e analisi predittiva, può supportare la Funzione Compliance nella valutazione dei rischi legati ai processi normativi e operativi.

L'IA può facilitare la pianificazione delle risorse tramite un sistema di *capacity planning*, utilizzando modelli predittivi per stimare l'assorbimento delle risorse necessarie per ciascuna attività e ottimizzare la distribuzione del carico di lavoro. In questo modo, la Funzione Compliance può pianificare in modo più efficace, tenendo conto della disponibilità e delle competenze del personale, riducendo il rischio di sovraccarico.

Anche la redazione del *Compliance Plan* può beneficiare dell'IA. L'IA può

automatizzare la raccolta e l'analisi dei dati relativi allo stato di avanzamento delle attività, inviando aggiornamenti in tempo reale ai responsabili della Funzione Compliance e segnalando eventuali ritardi o anomalie. Ad esempio, un sistema di machine learning potrebbe analizzare le azioni pianificate e stimare la probabilità che una determinata attività venga completata nei tempi stabiliti, con una previsione basata su dati storici.

Un altro ambito in cui l'IA può fornire un contributo essenziale è nella fase di aggiornamento del *Compliance Plan*, specialmente quando emergono nuovi rischi o cambiano le priorità normative. L'IA potrebbe analizzare i nuovi dati relativi a modifiche normative, eventi imprevisti o esiti di audit, aggiornando automaticamente il piano in base alla probabilità che questi eventi impattino sui processi aziendali. Ad esempio, se un nuovo regolamento sui pagamenti digitali viene introdotto, l'IA può calcolare una probabilità del 70% che i processi relativi dell'azienda non siano conformi, suggerendo immediatamente le modifiche necessarie al Compliance Plan.

Lo stesso dicasi per il *Compliance Periodical Reporting* e la *Compliance Dashboard*, strumenti chiave per monitorare l'efficacia delle azioni intraprese e garantire la trasparenza verso le Direzioni, gli Organi di Vertice e le Autorità di Vigilanza. L'IA può migliorare la qualità del reporting attraverso la raccolta automatica di dati e la generazione di report in tempo reale.

Anche la predisposizione della Relazione Annuale della Funzione Compliance, che include l'analisi delle attività svolte e la valutazione complessiva del sistema di controllo interno, può essere supportata dall'IA per migliorare l'efficacia e la tempestività della redazione del documento. Sistemi di intelligenza artificiale possono raccogliere automaticamente i dati dalle attività di compliance svolte durante l'anno, integrando i risultati delle verifiche e dei test di funzionamento. Inoltre, l'IA può generare stime probabilistiche sugli scenari futuri, suggerendo le aree in cui il rischio di non conformità rimane elevato e necessitano di ulteriori interventi.

Fondamentale sarà guidare l'IA attraverso un preventivo e rigoroso percorso di definizione della struttura delle diverse tipologie di *Reporting* e delle relative fonti alimentanti.

## 7. Le altre attività della Funzione Compliance

Esistono altri ambiti in cui questa è coinvolta nella gestione dei processi aziendali. Queste possono includere: la gestione della *Compliance Culture*, i conflitti di interesse, il *whistleblowing* e l'anticorruzione. Trattasi di attività il cui impatto sulla conformità normativa e sulla reputazione aziendale rimane di primaria importanza. L'intelligenza artificiale può fornire un contributo significativo nelle diverse aree descritte, migliorando l'efficienza e l'efficacia delle attività di monitoraggio, gestione e reporting.

Di seguito, esploreremo come l'IA può supportare ciascuna di queste attività.

*Compliance Culture*

La Compliance Culture rappresenta un elemento cruciale nella promozione di comportamenti aziendali allineati con i requisiti normativi e i valori etici.

Idealmente, la Funzione Compliance collabora con le funzioni di Sviluppo Organizzativo e Formazione per identificare le esigenze formative e assicurarsi che i corsi siano in linea con le normative vigenti. L'IA può fornire un supporto fondamentale in questa attività attraverso strumenti di analisi predittiva e tecnologie di apprendimento automatico (machine learning).

L'IA può essere utilizzata per identificare i fabbisogni formativi in modo più preciso, analizzando i dati relativi ai dipendenti, alle loro performance e ai feedback formativi passati. Ad esempio, un sistema di IA può analizzare i risultati dei test di conformità per individuare le aree in cui il personale mostra necessità di rafforzamento, suggerendo percorsi formativi mirati. Inoltre, l'IA può monitorare in tempo reale l'efficacia dei corsi di formazione erogati, misurando il miglioramento delle competenze e suggerendo eventuali aggiustamenti nei contenuti dei corsi in base alle esigenze emergenti, anche in tempo reale (Zavolokina et al. 2020) [12].

Un ulteriore contributo dell'IA può riguardare la personalizzazione dei percorsi formativi. Grazie all'utilizzo di algoritmi di Natural Language Processing (NLP), l'IA può analizzare il profilo dei singoli dipendenti, le aree di rischio a cui sono esposti e il contesto normativo applicabile, fornendo percorsi di formazione personalizzati. Questo approccio migliora l'efficacia della formazione e assicura che la *Compliance Culture* sia diffusa in modo capillare all'interno dell'organizzazione.

*Conflitti di interesse*

L'IA può svolgere un ruolo essenziale in queste attività automatizzando la raccolta e l'analisi dei dati relativi ai potenziali conflitti di interesse.

Attraverso l'analisi predittiva, l'IA può identificare potenziali conflitti di interesse prima che si verifichino. Ad esempio, un sistema di IA potrebbe monitorare in modo continuo le transazioni aziendali, i ruoli e le responsabilità dei dipendenti, segnalando automaticamente situazioni che potrebbero configurare un conflitto di interessi. Un modello di machine learning può attribuire una probabilità di rischio a ciascun conflitto identificato, permettendo alla Funzione Compliance di agire proattivamente e prevenire situazioni critiche.

Inoltre, l'IA può migliorare la gestione del Registro dei Conflitti di Interesse, automatizzando la classificazione dei casi e generando *alert* automatici quando i presidi di controllo non sono stati adeguatamente implementati. Questo approccio aumenta l'efficacia del monitoraggio e riduce i tempi di intervento.

---

[12] L. ZAVOLOKINA, M. DOLATA, G. SCHWABE, *RegTech – The Nucleus of Innovation in the Digital Transformation of Regulatory Processes*, in *Electronic Markets*, 30(1), 2020, pp. 1-13.

*Whistleblowing*

La gestione del whistleblowing è un'altra area in cui l'IA può apportare un notevole contributo. L'IA può supportare questa attività automatizzando la raccolta e l'analisi delle segnalazioni. Attraverso l'uso di NLP, i sistemi di IA possono analizzare le segnalazioni di whistleblowing e identificare automaticamente i pattern più critici, valutando la gravità di ciascun caso. Un sistema di machine learning può assegnare una probabilità di validità alle segnalazioni ricevute, consentendo alla Funzione Compliance di dare priorità a quelle più rilevanti. Questo approccio probabilistico non solo migliora l'efficienza del processo di gestione delle segnalazioni, ma riduce anche il rischio di trascurare situazioni potenzialmente gravi.

Un ulteriore contributo dell'IA consiste nell'analisi dei dati storici relativi alle segnalazioni, consentendo di identificare aree ad alto rischio e suggerendo azioni preventive per mitigare il rischio di futuri incidenti.

*Anticorruzione*

L'IA può fornire un supporto rilevante anche nella gestione delle politiche di anticorruzione. La Funzione Compliance deve infatti garantire che i principi contenuti nella policy anticorruzione siano rispettati e come debba gestire le richieste di informazioni provenienti da interlocutori esterni. L'IA può automatizzare il monitoraggio delle transazioni aziendali per individuare eventuali anomalie che potrebbero indicare pratiche corruttive.

Ad esempio, un sistema di IA può analizzare in tempo reale le transazioni finanziarie e assegnare una probabilità che una determinata transazione sia associata a pratiche di corruzione, basandosi su indicatori come l'importo, la frequenza delle transazioni o la presenza di intermediari non regolamentati. Questo consente alla Funzione Compliance di intervenire rapidamente per verificare e, se necessario, bloccare le transazioni sospette (Financial Stability Board 2020) [13].

Inoltre, l'IA può gestire in modo efficiente i questionari anticorruzione inviati dai clienti o dagli stakeholder, compilando automaticamente i campi richiesti e assicurando che le risposte siano conformi alle normative e alle politiche aziendali. Questo approccio riduce significativamente il tempo dedicato alla gestione di queste richieste e migliora la precisione delle risposte fornite.

L'integrazione dell'intelligenza artificiale nelle diverse attività offre notevoli opportunità per migliorare l'efficienza operativa e ridurre il rischio di non conformità. L'IA consente di monitorare in modo più efficace i rischi, intervenire proattivamente e migliorare la qualità dei processi decisionali. Un approccio probabilistico, in particolare, consente di ottimizzare l'allocazione delle risorse, focalizzandosi sulle aree a maggiore rischio.

---

[13] FINANCIAL STABILITY BOARD, *Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications*, 2020. Disponibile su: https://www.fsb.org.

## 8. Considerazioni conclusive

L'introduzione dell'intelligenza artificiale nella Funzione Compliance rappresenta una delle innovazioni più significative per migliorare la gestione del rischio di non conformità, l'efficienza operativa e la capacità di adattarsi a un contesto normativo in continua evoluzione.

Nel corso dell'analisi delle attività descritte e della letteratura esaminata, è emerso come l'IA possa supportare efficacemente la Funzione Compliance in diversi ambiti, dall'automazione dei processi di monitoraggio del rischio di non conformità nelle sue diverse fasi, al reporting e gestione documentale.

L'intelligenza artificiale offre diversi vantaggi chiave per la Funzione Compliance. In primo luogo, essa consente di automatizzare le attività più ripetitive e operative, come la gestione della documentazione e la rendicontazione periodica. Questo permette un significativo miglioramento dell'efficienza operativa, consentendo ai professionisti della compliance di concentrarsi su attività più strategiche, che richiedono maggiore attenzione e capacità decisionali. Inoltre, l'automazione riduce notevolmente il margine di errore umano, migliorando l'affidabilità dei processi di monitoraggio e rendicontazione.

Un altro contributo rilevante dell'IA è la sua capacità di fornire previsioni accurate attraverso l'analisi predittiva. L'IA, utilizzando algoritmi di *machine learning*, è in grado di analizzare grandi quantità di dati e identificare con maggiore precisione le aree a rischio di non conformità. Questa caratteristica consente di approcciare il ruolo della compliance secondo modalità innovative basate sul concetto di probabilità, inapplicabile fino ad ora nella gestione di processi quasi esclusivamente manuali o basati su capacità valutative unicamente di tipo umano. Questo approccio probabilistico offre alla Funzione Compliance la possibilità di gestire in modo più efficiente le risorse, concentrandosi sui rischi più elevati e adottando una postura proattiva nella gestione delle criticità.

La capacità dell'IA di monitorare continuamente l'aderenza ai requisiti normativi, combinata con la possibilità di adattarsi dinamicamente ai cambiamenti normativi, rappresenta un ulteriore punto di forza. L'IA permette di aggiornare automaticamente i sistemi di controllo e monitoraggio in base alle nuove normative o alle modifiche regolamentari, garantendo una conformità costante e riducendo il rischio di sanzioni. Questo processo dinamico offre una flessibilità operativa che le metodologie tradizionali difficilmente possono raggiungere.

Infine, un ulteriore vantaggio è rappresentato dal contributo dell'IA alla formazione e alla diffusione della cultura della conformità all'interno dell'organizzazione. Attraverso strumenti di personalizzazione dei percorsi formativi, l'IA può migliorare l'efficacia dei programmi di formazione, assicurando sia erogata una formazione mirata e in linea con le loro specifiche esigenze e responsabilità. Questo processo favorisce la diffusione di una solida cultura aziendale basata sui principi di conformità, riducendo il rischio di violazioni dovute alla scarsa conoscenza o consapevolezza delle normative applicabili.

Guardando ulteriormente al futuro, l'adozione dell'IA nell'ambito della gestione del rischio di non conformità continuerà a evolversi e ad ampliarsi. Alcuni degli sviluppi più probabili includono:

– l'Intelligenza Artificiale Generativa per la Redazione e Revisione dei Contratti: In futuro, strumenti di IA avanzati saranno in grado non solo di analizzare e segnalare clausole potenzialmente non conformi nei contratti, ma anche di suggerire revisioni e modifiche, redigendo automaticamente contratti che rispettino pienamente i requisiti normativi e riducendo il rischio di non conformità legata alla documentazione contrattuale;

– i sistemi di IA Cognitiva e Decision Making Autonomo: in prospettiva, le tecnologie di IA cognitiva potrebbero essere utilizzate per adottare decisioni autonome in determinate circostanze. L'IA potrebbe prendere decisioni su questioni minori o procedurali, lasciando ai responsabili umani solo i casi più complessi o strategici, con un notevole risparmio di tempo;

– il miglioramento della trasparenza e della compliance Integrata con i Processi di Business: l'IA potrebbe evolversi ulteriormente per integrarsi con tutti i principali processi di business, rendendo la compliance una parte integrante delle attività quotidiane piuttosto che una funzione separata. Ciò permetterebbe una conformità costante e monitorata in tempo reale su tutte le operazioni aziendali, minimizzando le discrepanze e riducendo la necessità di interventi correttivi.

In sintesi, l'introduzione dell'intelligenza artificiale nella Funzione Compliance rappresenta una svolta cruciale per le organizzazioni che operano in settori regolamentati. I vantaggi in termini di automazione, accuratezza nelle previsioni e miglioramento dell'efficienza operativa sono, in alcuni casi, già evidenti, ma le potenzialità di questa tecnologia non sono ancora del tutto esplorate.

L'IA non solo potrà migliorare le operazioni della Funzione Compliance, ma anche trasformare radicalmente il modo in cui le aziende gestiscono il rischio di non conformità, permettendo decisioni più rapide, strategiche e basate su dati oggettivi.

In futuro, si prevede che l'IA diventi uno strumento ancora più integrato e autonomo, riducendo progressivamente la dipendenza da interventi manuali e aumentando la resilienza delle organizzazioni ai cambiamenti normativi e ai rischi emergenti.

Nella consapevolezza, allo stesso tempo, che l'automazione non potrà e non dovrà sostituire l'apporto esperienziale e ricostruttivo che la mente dell'uomo, al contrario, potrà e dovrà conferire e che si trovino soluzioni adeguate alle importanti sfide etiche che questa rivoluzione si porta con sé.

Finito di stampare nel mese di marzo 2025
nella LegoDigit s.r.l. – Via Galileo Galilei, 15/1 – 38015 Lavis (TN)

UNIVERSITÀ DEGLI STUDI DI MILANO
DIPARTIMENTO DI STUDI INTERNAZIONALI
GIURIDICI E STORICO-POLITICI

---

COLLANA DI STUDI SCIENTIFICI

***Per i tipi Giuffrè***

1. S. Dossi, E. Giunchi, F. Montessoro (a cura di), *L'Asia tra passato e futuro. Scritti in ricordo di Enrica Collotti Pischel*, Milano, 2014.
2. M.N. Bugetti, *La risoluzione extragiudiziale del conflitto coniugale*, Milano, 2015.
3. G. Marchetti, *La delegazione legislativa tra Parlamento e Governo: studio sulle recenti trasformazioni del modello costituzionale*, Milano, 2016.

***Per i tipi Giappichelli***

4. M. Valenti, *La questione del Sahara occidentale alla luce del principio di autodeterminazione dei popoli*, Torino, 2017.
5. L. Ammannati, R. Cafari Panico (a cura di), *I servizi pubblici: vecchi problemi e nuove regole*, Torino, 2018.
6. E. Giunchi, C. Ponti (a cura di), *Le armi nel mondo contemporaneo. Temi scelti su proliferazione, regimi di controllo e disarmo*, Torino, 2019.
7. L. Marotti, *Il doppio grado di giudizio nel processo internazionale*, Torino, 2019.
8. S. Dominelli, G.L. Greco (a cura di), *I mercati dei servizi fra regolazione e* governance, Torino, 2019.
9. S. Lanni (a cura di), *Sostenibilità globale e culture giuridiche comparate, Atti del Convegno SIRD, Milano, 22 aprile 2022*, Torino, 2022.
10. L. Ammannati, A. Canepa (a cura di), *La finanza nell'età degli algoritmi*, Torino, 2023.
11. J. Benarafa, *Il* takaful *oltre il legal transplant. L'etica islamica di fronte al rischio assicurativo*, Torino, 2024.
12. G. Marchetti, *Il "principio fondamentale ambientalista" nella prospettiva multilivello e il suo impatto sull'assetto costituzionale*, Torino, 2024.
13. L. Ammannati, A. Canepa, G.L. Greco, U. Minneci (a cura di), *Mercati finanziari e transizione digitale. Una tassonomia*, Torino, 2025.