LUISS

**DIPARTIMENTO DI GIURISPRUDENZA**
**CATTEDRA DI DIRITTO DEI MERCATI FINANZIARI**

# LE PIATTAFORME *FINTECH* ALLA PROVA DEL REGOLAMENTO MICAR: EVIDENZE DAL CASO FTX

Chiar.mo Prof. Salvatore Providenti
RELATORE

Chiar.mo Prof. Marino Perassi
CORRELATORE

**Francesco Silla**
(Matr. 155763)
CANDIDATO

Anno Accademico 2022/2023

# INDICE

# Introduzione

Il settore bancario rappresenta in modo esemplare la potenzialità dirompente della rivoluzione digitale.

Sebbene l'innovazione sia il *benchmark* del settore bancario, appare necessaria una riflessione specifica; ci si trova di fronte ad una rivoluzione epocale che non solo impatta sui modelli di *business* delle imprese del settore ma riveste particolare importanza considerato che dagli intermediari bancari dipende in misura cospicua lo sviluppo economico e la stabilità economica nel suo complesso.

In questo contesto, si assiste all'affermarsi di un nuovo sistema di servizi, più ampio, fluido e competitivo, nel quale accanto agli intermediari bancari tradizionali si affacciano nuovi attori e prestatori di servizi, capaci di intercettare con la loro offerta parte della clientela e guadagnando margini di intermediazione e di liquidità un tempo di esclusiva competenza delle banche.

Va subito detto che, su tale terreno, non è facile raggiungere un inquadramento unitario ed esaustivo poiché il settore è assai ampio e variegato ed include tutte quelle realtà che, attraverso le nuove tecnologie, rendono più efficienti i servizi finanziari esistenti o ne creano di nuovi, operando in numerosi segmenti di attività.

Il presente elaborato muove dalla considerazione che uno degli effetti più significativi della rivoluzione tecnologica è che nel mercato bancario la tradizionale catena del valore viene a frammentarsi in ragione dell'emergere di molteplici operatori che si focalizzano in modo esclusivo su specifici segmenti della filiera, che definiamo con il termine di *imprese FinTech*.

Sotto il profilo concorrenziale, l'impatto dell'attività delle imprese *FinTech* sul settore non può che determinare un giudizio di apprezzamento: l'operato dei nuovi *incumbents,* aumentando la concorrenza del mercato dei servizi finanziari ed erode i precedenti margini di profitto, fungendo da stimolo per gli operatori tradizionali e per lo sviluppo di nuovi importanti segmenti del settore finanziario.

Certamente, nello scenario che le banche hanno di fronte, l'innovazione digitale rappresenta una fondamentale occasione di sviluppo, ma può costituire anche una seria minaccia qualora esse non riescano a sfruttarne appieno le potenzialità, lasciando spazio ai nuovi concorrenti, in primo luogo ai giganti della tecnologia.

Le banche si trovano così oggi davanti a un bivio: o la disintermediazione favorita dall'innovazione digitale le spingerà progressivamente ai margini del nuovo mondo finanziario, oppure le stesse decideranno di adeguarsi e di competere, *in primis* percorrendo la strada che alcune grandi banche hanno già intrapreso, quella delle alleanze strategiche.

La domanda che viene da porsi è se in ragione del nuovo paradigma tecnologico sorgano rischi fino ad oggi non considerati. La risposta che scaturisce dal presente elaborato è negativa; gli interessi da tutelare restano infatti i medesimi (stabilità, buon funzionamento dei mercati, correttezza e tutela dei clienti, sicurezza dei sistemi di pagamento e di deposito etc.). In questo nuovo contesto, le questioni più delicate attengono certamente alle modalità di regolazione, cioè a come proteggere il sistema senza frenare l'innovazione e soprattutto a quale siano le scelte legislative più idonee ad un settore che presenta sì i rischi tradizionali ma con soggetti e strumenti completamente differenti.

Ci troviamo di fronte a una discontinuità così forte da poter essere annoverata tra i grandi passaggi della Storia che hanno mutato le regole del gioco e gli scenari economici-sociali in maniera irreversibile.

Non a caso tutte le analisi concordano nel sottolineare il carattere epocale della rivoluzione digitale, che viene definita appunto la quarta rivoluzione industriale.

Se di rivoluzione si tratta, occorre evidentemente mettere in discussione i paradigmi che hanno finora ispirato la disciplina dei diversi fenomeni finanziari, prendere atto che alcune categorie concettuali sono ormai superate e stabilire nuove regole e nuovi modelli.

Finanza e tecnologie rappresentano una continua evoluzione di potenzialità, di nuove opportunità che nascono in un mercato globale senza più confini fisici. Infinite sono diventate le potenzialità di scelta in tempo reale da parte di ciascun individuo, essendosi allargate enormemente le dimensioni di un mercato sempre più in espansione. Ma per essere davvero tale, un mercato non deve essere soltanto aperto; esso deve essere garantito, cioè inquadrato in norme e controlli che assicurino la certezza del diritto contro ogni possibilità di abuso o atto illecito che minerebbe alla base la sua stabilità. Mi torna in mente la teoria di Carl Schmitt a proposito del tentativo di neutralizzazione; l'autorevole giurista proprio nell'asserire la neutralità dell'economia e nel contrapporre l'universalità degli affari alla particolarità della politica, esprime, egli stesso, un fermo e rigido orientamento politico. L'economia

senza politica non è che una politica contrapposta ad un'altra. Questa consapevolezza spinge dunque a configurare il mercato come *locus artificialis*, che la legge costruisce e governa, orienta e controlla. Non c'è mercato al di fuori della decisione politica e della scelta legislativa. Si scopre in questo modo l'intrinseca "politicità" del mercato, che la legge può modellare e definire secondo principi diversi: ora privilegiando la riservatezza, ora l'assoluta e generale visibilità, ora esaltando l'autonomia e la responsabilità dei negozi giuridici, ora tutelando gli incauti. Questi, ed altri principi, determinano la fisionomia del mercato, sicché tanti sono i modelli o tipi di mercato quante le leggi regolatrici concepibili.

L'economia di mercato non è assenza di norme, ma serietà e rigore di norme, che componendosi nell'organicità degli statuti di mercato, garantiscono la libera competizione delle imprese, permettono calcoli sul futuro ed assicurano la stabilità dei negozi giuridici e del mercato stesso.

Sulla base di tali premesse, il Regolamento (UE) 2023/1114 - Markets in Crypto-Assets Regulation (*MiCAR)*, segna un cambiamento significativo nel mercato dei *crypto-asset,* introducendo per la prima volta, una legislazione armonizzata e vincolante, direttamente applicabile in tutti gli Stati membri dell'UE, per i partecipanti all'ecosistema delle cripto-attività.

Il MiCAR è diretto a ricondurre l'economia *crypto* in un sistema disciplinare che assicuri la tutela degli investitori, l'integrità dei mercati e le condizioni concorrenziali eque per i relativi operatori. In particolare, è auspicabile che il suddetto Regolamento riesca a definire un sistema di controllo (macro e microprudenziale) per gestire i rischi finanziari associati alle attività *crypto,* riducendo così il rischio di arbitraggio normativo tra attività economicamente simili, delineando invece un sistema preciso di obblighi e diritti a tutela del corretto funzionamento del mercato, il quale in un prossimo futuro potrebbe diventare interconnesso con i mercati finanziari tradizionali.

Il presente elaborato si pone come obiettivo quello di dimostrare l'attuale natura "*too big to ignore*" del settore *FinTech* e la sua esposizione ai medesimi rischi tradizionali, in linea con la *ratio* che sembra essere sottesa al Regolamento MiCA.

Infine, partendo da una disamina del suddetto Regolamento, della disciplina contro gli abusi di mercato e della regolamentazione Antiriciclaggio (AML) ed evidenziandone i limiti, si cerca in questa sede di dimostrare il superamento del principio di neutralità tecnologica di derivazione europea.

Il primo capitolo si focalizza innanzitutto sull'evoluzione del settore bancario tradizionale, in ragione del passaggio dal paradigma *open-banking* a quello *open-finance,* dando evidenza ad una trasformazione epocale per effetto della nascita di nuovi operatori, nuovi prodotti e nuovi servizi. Si procede poi all'illustrazione della nuova valuta bancaria che è costituita dai dati; è proprio grazie all'accesso dei dati, infatti, che possono essere sviluppate nuove funzioni di intermediazione indipendente e nuove fonti di guadagno per gli operatori del settore. Si sottolinea infine come la transizione in oggetto, si traduce in maggiore concorrenza ed efficienza, espresse in termini di maggiore varietà di servizi, minori costi ed ulteriori benefici per gli utenti.

Il secondo capitolo si concentra sull'analisi della struttura dei prestatori di servizi di cripto-attività, in particolar modo i c.d. *exchange*. Si passa poi all'esame di un caso di studio, il fallimento della piattaforma FTX; dall'analisi di questo caso di assoluto rilievo nel settore, si evince che le ragioni del fallimento sono da ritrovarsi nell'assenza di regolamentazione sia di tipo societario tradizionale che in funzione delle particolari attività svolte. Proprio l'assenza di regolamentazione ha portato un gigante *FinTech* ad un fallimento societario di tipo tradizionale, a prescindere dal settore in cui operava.

Si intende così dimostrare che il settore della finanza decentralizzata, seppur radicalmente differente da quello tradizionale, presenta rischi di natura societaria e finanziaria già presenti e attualmente noti, sottolineando la necessità impellente di attuare un approccio regolamentare transfrontaliero e globale, prima che si verifichino altri eventi negativi che possano minare la stabilità del sistema finanziario.

Il terzo capitolo procede, infine, alla disamina delle recenti discipline europee in materia di cripto-attività. In particolare, viene analizzata la disciplina del regolamento MiCA nei suoi punti salienti, la disciplina contro gli abusi di mercato e la disciplina antiriciclaggio (AML).

** la stesura del presente elaborato ha beneficiato della partecipazione ai convegni: "Il Regolamento MiCA nel contesto della disciplina bancaria e dei servizi di pagamento", organizzato da Banca d'Italia, tenutosi a Roma il 29 settembre 2023; "MiCAR and its coordination with existing EU financial market legislation", organizzato da Banca d'Italia e dall'Università Ca' Foscari di Venezia, tenutosi a Venezia il 14 novembre 2023.*

# Capitolo 1 – La digitalizzazione del sistema finanziario

SOMMARIO: 1. L'evoluzione del *FinTech*. – 2. Open Banking e Open Finance. – 2.1 *Open Banking*: la rivoluzione digitale del settore bancario. – 2.2 *Open Banking* e la nuova moneta: dati e informazioni. – 2.3 *Open Finance*: l'innovazione trasparente dei mercati finanziari. – 2.4 *Open Finance* e *Big Data*: verso un'offerta finanziaria su misura. – 2.5 *Open Finance* e digitalizzazione: rischi, asimmetria informativa e la sfida della tutela del consumatore. – 3. Dalla Concorrenza alla Cooperazione: Il Futuro FinTech. – 3.1 *FinTech* e banche: sinergie e sfide del futuro. – 4. Verso la PSD3. – 5. PSD2 e MiCAR.

## 1. L'evoluzione del *FinTech*

*FinTech* è il risultato dell'abbreviazione di "tecnologia finanziaria", consiste nel processo tecnologico innovativo avente diverse sfaccettature, molteplici significati ed implicazioni per il settore dei servizi finanziari, per i consumatori, per le imprese e per il sistema economico-finanziario nel suo complesso[1]. Il *FinTech* fa riferimento ad una pluralità di tipologie di imprese che svolgono attività finanziarie e che, generalmente, sono caratterizzate da una elevata specializzazione su specifiche parti della catena di valore delle attività bancarie. Si tratta di un fenomeno dirompente che, dapprima gradualmente, ed oggi con grande celerità, si è imposto sulla scena finanziaria recando una serie di promesse riguardo a benefici e opportunità di miglioramento del benessere finanziario[2] sia dei consumatori che delle imprese, offrendo soluzioni tecnologiche flessibili, *user-friendly* ed efficienti. Di conseguenza il *FinTech* ha assunto una duplice valenza potendo essere considerato sotto forma di *genus,* come l'ampio e complesso ecosistema con molteplici articolazioni (*i.e. RegTech, SupTech, InsurTech,* ecc.), oppure autonomamente, come fenomeno tecnologico o rivoluzionario, che si riflette, in particolare sulle modalità di prestazione dei servizi finanziari. La crescente

[1] M. T. PARACAMPO, *Fintech, introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, vol. II (G. Giappichelli Editore, 2019), 2.

[2] In tal senso anche il Parlamento europeo [cfr. *Competition issues in the Area of Financial Technology (FinTech)*, Study requested by the ECON Committee, July 2018, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/619027/IPOL_STU(2018)619027_EN.pdf, ove si legge: "*Fin Tech services offer significant potential benefits to European consumers, such as cost reduction, improvements in efficiency, greater transparency and a contribution to the goal of financial inclusion. FinTech has come to revolutionise the way in which traditional financial services providers work and interact with their customers. It is changing the dominant paradigms by which traditional financial services are provided, resulting in a significant disruption".*

diffusione di questo fenomeno ha innescato un processo innovativo il quale, facendo leva sulle nuove tecnologie, mira a creare nuovi prodotti, impostare nuovi servizi finanziari (*latu sensu* intesi e non sempre tipizzati), nuove modalità di prestazione dei servizi codificati e nuove modalità di comunicazione ed interazione con i clienti attuali e potenziali. A fronte dei numerosi benefici per i consumatori e delle opportunità per le imprese, il nuovo obiettivo degli operatori tradizionali è quello di una sostanziale riconsiderazione dei modelli di *business,* da ristrutturare, reinventare o implementare *ex novo,* attraverso un profondo *restyling* tecnologico, tale da farli competere con quelli dei nuovi *players,* entrati di recente nel mercato[3].

Ad oggi manca una definizione univoca dell'istituto *de quo*; tale lacuna viene sopperita da descrizioni parziali, offerte da Autorità ed Istituzioni europee o da Organismi internazionali che hanno esaminato le varie potenzialità di sviluppo del fenomeno in corso, adottando un significato ampio che nella maggior parte dei casi ha riproposto la definizione generica e convenzionale offerta dal *Financial Stability Board*[4]: «*Technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services».*

Il *FinTech* è stata considerato dall'ESMA come una sottocategoria del più ampio processo di innovazione finanziaria, e definita come «*the act of creating and distributing new financial instruments, processes, business models and markets, including the new application of existing ideas in a different market context,* la seconda come *«a type of financial innovation that relies on Information Technology to function, e.g. internet, cloud etc. and that can result in new business models, applications, processes, products, or services with an associated effect on financial markets and institutions and the provisions of financial services*[5]*».*

Divenuto nel tempo sinonimo di "settore di servizi finanziari emergenti", è giunto ad indicare un'ampia gamma di servizi e prodotti (i.e. P2P, *crowdfunding platforms, robo advice, lending platforms,* valute virtuali, pagamenti *cashless*, ecc.) ed un ampio *range* di sviluppi sostenuti dalle nuove tecnologie come *DLT*, *blockchain*,

[3] PARACAMPO (n 1), 5 ss.
[4] Cfr. FSB, *Financial Stability Implications from Fintech. Supervisory and Regulatory Issues that Merit Authorities' Attention* del 27 giugno 2017, su *http://www.fsb.org/wp-content/ uploads/R270617.pdf.*
[5] Cfr. P. ARMSTRONG (Senior Risk Analysis Officer, Innovation and Products Team, ESMA), Financial Technology: *The Regulatory Tipping Points*, 27 September 2016, reperibile al *https://www.esma.europa.eu/sites/default/files/library/esma71-99-1051_speech_on_cryptoassets_-_pa.pdf*

analisi dei *BigData*, *cloud computing*, intelligenza artificiale ecc. con la finalità di rendere il sistema finanziario più efficiente. Alcune indicazioni funzionali sono state fornite successivamente dal Parlamento Europeo e dal *Financial Stability Board* i quali, partendo dalla premessa che le diverse articolazioni dell'ecosistema *FinTech* sono accomunate dal fatto di essere considerate come attività finanziarie che forniscono un valore aggiunto attraverso tecnologie digitali, hanno individuato i criteri base del servizio finanziario in materia di *FinTech.* Pertanto, quest'ultimo deve essere guidato dalla tecnologia, deve fornire una soluzione innovativa, che si sostanzi in un nuovo modello di *business* o un'alternativa a quanto già esistente nel settore finanziario ed infine offrire un significativo valore aggiunto ad ogni *stakeholder* coinvolto nella catena di valore (principalmente il consumatore)[6]. Uno dei principali parametri di riferimento della materia in oggetto, è l'incremento delle *performance* degli operatori del mercato bancario e finanziario, finalizzato alla riduzione dei costi transattivi nella prestazione ed erogazione dei servizi di investimento ed il miglioramento dei parametri della valutazione del rischio[7]. Per quanto riguarda il primo aspetto, l'utilizzo dei dati al fine di migliorare il *matching* tra i soggetti coinvolti nelle transazioni finanziarie, consente lo sfruttamento dei vantaggi connessi alle economie di scala nella gestione e condivisione di grandi quantità di informazioni; per quanto riguarda invece il miglioramento dei processi di valutazione del rischio i vantaggi si riflettono sul rapporto con l'investitore individuale, ed in ottica di valutazione sistemica dei prodotti di tipo aggregato, da parte degli investitori istituzionali. Di fronte a questo fenomeno evolutivo si assiste ad un progressivo cambiamento nella tassonomia soggettiva in ambito finanziario, conseguente all'irruzione sul mercato di nuovi *players,* che prestano servizi finanziari più efficienti e maggiormente rispondenti alle esigenze dei consumatori.

Il primo tentativo di mappatura dei principali soggetti sussumibili nel *genus* di *FinTech players* viene effettuato dall' *European Banking Authority*[8] la quale individua

[6] M. T. Paracampo, «*Fintech Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari»*., II, vol. I (G. Giappichelli Editore, 2021), 2–7, https://www.giappichelli.it/fintech-9788892129436.

[7] A. DAVOLA, «*Algoritmi decisionali e trasparenza bancaria»*, (Utet Giuridica, 2020).

[8] Cfr. EBA, «Report on the impact of FinTech on incumbent credit institutions' business».
models, cit.
L'Autorità risulta essere la prima ad aver tracciato i profili identificativi dei diversi players che si contendono il mercato con gli incumbents.
Le diverse species di *FinTech players* sono così identificate dall'EBA:
«Incumbent institutions: these are the incumbent credit institutions that provide the full range of banking services (e.g. retail and business lending payment services, wealth management)

le seguenti categorie: intermediari bancari e finanziari attivi nel campo dello sviluppo di servizi e soluzioni innovative (*incumbent istitutions*); nuovi soggetti emergenti, dotati di licenza bancaria e caratterizzati dalla prestazione di servizi finanziari digitali, focalizzate prevalentemente sulle mobile apps e senza filiali fisiche (*new digital-based institutions*); *startup* innovative che offrono soluzioni tecnologiche in ambito finanziario senza una licenza bancaria/*payment/e-money* (*other FinTech firms*); altre imprese che forniscono supporto tecnologico in termini di *software* o *hardware* nell'offerta dei servizi finanziari (*technology providers and ICT companies including BigTech firms*)[9].

via the network of established physical branch and online distribution channels. Incumbent institutions vary significantly in terms of their current level of digitalisation and application of Fin Tech solutions, as well as their governance capacity and financial capability to adopt innovative financial solutions.
New digital-based institutions: we define these as new entrant institutions, such as digital-only institutions/challenger banks with innovative business models, providing digital-based banking services that hold a credit institution or payment institution or e-money institution licence. These predominantly focus on the mobile application experience and have no physical branches.
Other FinTech firms: these are usually start-up firms, without a banking/payment/e-money licence, that offer technology-enabled financial innovation solutions that could result in new business models, applications or products.
Technology providers and ICT companies (including BigTech firms): typically, these companies provide technological support to institutions in terms of software applications and/or hard-ware. They primarily focus on the development and manufacturing of technology. BigTech firms are usually large and globally active with a relative advantage in terms of digital technology. They often have very large customer base and are engaged in providing various online-based services, for example retail customer-oriented e-commerce platforms, search engines and social networks, or business customer-oriented data storage or computing processing services».

[9] Cfr. V. BOSCIA, C. M. SCHENA, E V. STEFANELLI, a c. di, «*Digital banking e FinTech: l'intermediazione finanziaria tra cambiamenti tecnologici e sfide di mercato»*, Banca e mercati Saggi 142 (Roma: ABIServizi, Bancaria editrice, 2020), 45–47. cit. "la significativa crescita e rapida diffusione della digitalizzazione a livello mondiale ha portato all'emersione sul mercato di numerose *Big Tech* che, nell'ambito delle loro strategie di diversificazione rispetto all'originario *core business,* stanno sviluppando L'approccio della diversificazione strategica non costituisce certamente una novità, come testimoniato dalla pluralità di strutture conglomerali costituite nel tempo dai grandi gruppi industriali. Inoltre, al pari della generalità delle *FinTech*, le *Big Tech* offrono servizi finanziari innovativi, mediante applicativi o piattaforme digitali (*open API*, piattaforme elettroniche o *marketplace* digitali), che facilitano il contatto con la clientela e consentono un tempestivo soddisfacimento delle sue esigenze, al di là dei confini geografici che eventualmente separano l'operatore finanziario dal cliente.
Tuttavia, le *Big Tech* sono percepite come *digital disruptors* perché hanno un vantaggio competitivo che li rende operatori effettivamente temibili, anche da parte delle principali banche internazionali, in termini di conquista di quote di mercato in ambito finanziario. Le *Big Tech*, infatti, possono contare non solo su ingenti risorse finanziarie utili a fini di investimento in iniziative in ambito finanziario e su un sofisticato e particolarmente avanzato sviluppo tecnologico, ma anche e soprattutto su una mole significativa e diversificata di informazioni di natura sociodemografica e comportamentale (*big data*), acquisite nel tempo su un'ampia base di clientela.
Quest'ultimo costituisce uno degli aspetti di maggiore importanza sul piano competitivo. Le *Big Tech*, infatti, dispongono di una quantità significativa di dati e informazioni sulla propria clientela, che riguardano non solo il profilo delle scelte finanziarie (ad esempio le modalità di pagamento associate agli acquisti online) o taluni aspetti comportamentali, come è per le banche, ma anche abitudini e preferenze di spesa, comportamenti di consumo, orientamenti personali, relazioni sociali. Per le Big Tech diviene, dunque, possibile utilizzare queste informazioni adeguatamente rielaborate e interpretate per costruire offerte personalizzate rispetto al profilo della loro clientela e per orientarne le scelte anche in ambito finanziario."

Il lungo elenco dei provvedimenti adottati a livello comunitario[10] per regolare il mercato finanziario e bancario in questi ultimi anni fornisce una visione più chiara e precisa di come il settore sia stato - e continui ad essere - oggetto di attenzione da parte del legislatore europeo, di quelli nazionali e delle autorità regolamentari competenti[11].

Parte della dottrina[12] auspica che gli operatori già attivi sul mercato e i nuovi operatori possano beneficiare di pari condizioni operative, in modo da rendere possibile una più ampia diffusione sul mercato dei nuovi servizi *FinTech* anche al fine di garantire un elevato livello di protezione dei consumatori che si avvalgono di tali servizi. Lo stesso Parlamento europeo ha riconosciuto che «*la legislazione in materia di servizi finanziari dovrebbe essere rivista quando necessario e dovrebbe essere sufficientemente favorevole all'innovazione*» evidenziando come sia essenziale che «*i potenziali effetti della legislazione sull'innovazione siano sottoposti ad un'adeguata valutazione nell'ambito di una valutazione di impatto, affinchè questi sviluppi apportino nella maggior misura possibile benefici economici e sociali significativi*»[13] in conformità con il principio di innovazione.[14]

## 2. *Open Banking* e *Open Finance*

### *2.1* *Open Banking*: la rivoluzione digitale del settore bancario

In questi anni si è cominciato a parlare della banca del futuro come "banca digitale" o come *bank as platform o banking as a service*, in evidente analogia con le

[10] PSD2 (seconda Direttiva sui sistemi di pagamento); EMD2 (seconda Direttiva sulla moneta elettronica; PAD (Direttiva sui conti di pagamento); AMLD4 (quarta Direttiva sul contrasto al riciclaggio e la lotta al terrorismo); *regulatory technical standards* emanati dall'EBA (norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri); Regolamento SEPA; Regolamento sui pagamenti transfrontalieri; IFR (*Interchange Fees Regulation);* Direttiva sui diritti dei consumatori; GDPR (*General Data Protection Regulation*); Direttiva MIFID; Regolamento sui fondi di investimento denominati ELTIF; Regolamento MICA; Regolamento DORA.

[11] U. PIATTELLI, «*La regolamentazione del Fintech Dai nuovi sistemi di pagamento all'intelligenza artificiale. Aggiornato al D.L. 17 marzo 2023 c.d. «Decreto Fintech»*, seconda edizione (G. Giappichelli Editore, 2023), 8, https://www.giappichelli.it/la-regolamentazione-del-fintech-9788875245511.

[12] *Ibid.*

[13] Risoluzione 2016/2243 (INI).

[14] Cfr. SCHENA, TANDA, ARLOTTA, POTENZA (a cura di), *lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziari nell'era digitale*, in *quaderno FinTech* n.1 , marzo 2018.

modalità attraverso le quali si stanno sviluppando i nuovi operatori *FinTech*. La spinta combinata della globalizzazione, della digitalizzazione e della regolamentazione del settore, crea una trasformazione profonda di questi soggetti, che pone al centro della propria strategia i clienti. I soggetti bancari tradizionali dovrebbero sviluppare tecnologie adeguate a semplificare i processi interni e ridurre i costi operativi, sfruttando efficacemente i dati a loro disposizione e mostrarsi aperte alla collaborazione con altri operatori che possono creare servizi e tecnologie innovativi.

In questo scenario ha fortemente influito la diffusione *dell'open banking*, un nuovo paradigma che si fonda sulla condivisione di dati tra i diversi attori dell'ecosistema finanziario (banche tradizionali, banche digitali, *FinTech*, *Tech Providers*) per l'offerta di servizi di accesso ai conti autorizzata dai clienti stessi. Possiamo considerare l'*open banking* non come un fenomeno circoscritto ma come un *trend* in crescita a livello internazionale[15]. Questo fenomeno è figlio dell'entrata in vigore della Direttiva 2015/2366 sui servizi di pagamento (PSD2), la quale ha fatto da apripista, dando spazio ad un ecosistema aperto che consente lo scambio di informazioni e dati tra gli operatori coinvolti[16]. Secondo la definizione della *Bank of International Settlements* (BIS), con questo nuovo paradigma si intende una forma di «*condivisione e sfruttamento dei dati autorizzata dai clienti da parte delle banche con sviluppatori e aziende di terze parti per costruire nuovi servizi e applicazioni come quelli che offrono pagamenti in tempo reale, maggiori possibilità di trasparenza finanziaria per i titolari di conti e opportunità di marketing e cross-selling*»[17]. L'obiettivo dell'*open banking* è quello di innovare e rendere le transazioni bancarie più efficienti, meno costose, facili e più sicure, il tutto attraverso l'apertura di interfacce di programmazione (API)[18]. Queste, vengono utilizzate dalle banche, nei confronti delle aziende *FinTech* e laddove i clienti delle banche abbiano fornito il loro esplicito consenso, permette loro di accedere ai dati bancari e rende l'*online banking* più sicuro. Ciò avviene per effetto dell'obbligo di adottare sistemi di autenticazione a

[15] L. FRATINI PASSI, «*Open Banking: le sfide nel mercato globale*», *Bancaria Editrice* Bancaria n. 7-8/2022 (luglio - agosto 2022).
[16] L. FRATINI PASSI, «*Open Finance: tendenze e innovazione collaborativa*», *MINERVA BANCARIA* N.3/2023 (marzo 2023): 81-89.
[17] «BIS QUARTERLY REVIEW, MARCH 2023», *Report on Open Banking and application programming interfaces*. https://www.bis.org/publ/qtrpdf/r_qt2303.pdf.
[18] REPORT FSB, P. 5, nota 16, ove vengono così definite "*APIs are defined as a set of rules and specifications followed by software programmes to communicate with each other, and an interface between different software programmes that facilitates their interaction.",* disponibile su https://www.fsb.org/wp-content/uploads/P140219.pdf.

due fattori (*strong customer authentication*)[19] e il *dynamyc linking*[20]. Lo sviluppo tecnologico in questione ha portato alla nascita di una serie di servizi accessori, come ad esempio: i servizi di informazione sui conti, i quali forniscono all'utente di servizi di pagamento informazioni *online* aggregate su uno o più conti di pagamento, detenuti presso altri prestatori di servizi di pagamento a cui si ha accesso tramite interfacce *online;* o anche servizi di disposizione di ordini di pagamento che consentono al prestatore di servizi di disposizione di ordine di pagamento di assicurare al beneficiario che il pagamento è stato disposto. In termini più generali, è emblematico il cambiamento in atto nel settore bancario-finanziario, laddove al classico modello di banca che distribuisce i propri servizi mantenendo il controllo sull'intera filiera produttiva, si contrappone la sempre maggiore "disarticolazione" (*unbundling*) della catena di valore dell'intermediazione finanziaria in più segmenti, ciascuno dei quali è occupato da terze parti in grado di offrire specifici prodotti e servizi basati sulle nuove tecnologie digitali[21]. Questi servizi, prima dell'entrata in vigore della PSD2 non erano soggetti ad alcuna regolamentazione specifica e di conseguenza non erano sottoposti ad alcuna vigilanza. Merita peraltro sottolineare come, sposando gli orientamenti regolamentari maggioritari in materia di *FinTech*, anche le scelte normative della PSD2 si fondano sui principi di neutralità rispetto ai profili tecnologici[22]; le definizioni

[19] Art. 4 (30) della Direttiva (EU) 2015/2366, introduce il concetto di "autenticazione forte del cliente" (strong customer authentication, o SCA), definita come "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza(qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione".

[20] Oltre alla SCA, la PSD2 ha introdotto una ulteriore fattore di sicurezza volto a proteggere il buyer tramite il c.d. Collegamento Dinamico (*Dynamic Linking*). Le transazioni di pagamento elettronico da remoto, infatti, sono soggette a un maggiore rischio di fronte rispetto agli strumenti di pagamento tradizionali. Pertanto, si è reso necessario introdurre dei requisiti aggiuntivi per la transazione, al fine di assicurare che gli elementi colleghino in modo dinamico l'operazione all'importo e al beneficiario specificati dal pagatore al momento di disporre l'operazione. Il collegamento dinamico è possibile attraverso la generazione di codici di autenticazione soggetti a una serie di rigorosi requisiti di sicurezza. Tali codici dovrebbero essere basati su soluzioni quali la generazione e la convalida di password monouso, firme elettroniche o altre conferme della validità basate sulla crittografia che utilizzano chiavi o materiale crittografico.
Tramite il Collegamento Dinamico, per effettuare la transazione sarà dunque necessaria l'autenticazione della singola operazione di pagamento tramite un codice univoco associato specificamente a quella transazione e alle sue caratteristiche, quali l'importo ed il beneficiario. Regolamento Delegato (UE) 2018/389 del 27 novembre 2017 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri, considerando (4) e (5).

[21] *SPEECH GIVEN BY MARK CARNEY, GOVERNOR OF THE BANK OF ENGLAND CHAIR OF THE FINANCIAL STABILITY BOARD, «The Promise of FinTech – Something New Under the Sun?*» (Deutsche Bundesbank G20 conference on "Digitising finance, financial inclusion and financial literacy", Wiesbaden: BANK OF ENGLAND, 2017), 14, https://www.bis.org/review/r170126b.pdf.

[22] Intendendosi per neutralità tecnologica, l'approccio "neutrale" delle autorità di regolamentazione rispetto alle tecnologie e non imporre né favorire in via discriminatoria l'uso di un particolare tipo di

contenute nella direttiva non fanno infatti riferimento a specifiche soluzioni tecniche, potendo quindi ricomprendere anche eventuali nuove fattispecie[23].

## *2.2 Open Banking*, la nuova moneta: dati e informazioni

Emerge così l'ampio ventaglio di problematiche giuridiche che interessano la materia in esame, sul piano della tutela dei consumatori e in materia di sicurezza, responsabilità e concorrenza, nonché della sicurezza dei dati[24]. I nuovi servizi di pagamento, infatti, presuppongono l'accessibilità, sia diretta che indiretta dei fornitori al conto del pagatore. Ciò implica che un prestatore di servizi di pagamento di radicamento del conto (ASPSP)[25] (come una banca), che offre un meccanismo per l'accesso indiretto, dovrebbe permettere l'accesso diretto ai fornitori che gestiscono gli ordini di pagamento. È importante sottolineare come gli *smartphones* siano diventati una piattaforma per consentire agli sviluppatori terzi di proporre nuovi prodotti agli utenti. Attraverso l'impiego delle *application program interface* (API)[26], ovvero di sistemi che consentono a diversi applicativi software di comunicare tra loro, anche senza l'intervento di operatori umani, questi dispositivi si sono trasformati in abilitatori di pagamenti, permettendo così l'acquisizione di nuovi clienti. Ciò assume rilievo per le cd. *BigTech* che possono operare nel settore dei servizi *FinTech*.

Come precedentemente accennato, in Europa l'adozione nel 2018 della *Payment Service Directive 2* (PSD2)[27] ha posto le basi per la diffusione dell'*open banking,* abbassando le barriere all'ingresso nel mercato dei fornitori di terze parti,

---

tecnologia, ma garantire che uno stesso servizio sia soggetto a norme equivalenti, a prescindere dal modo in cui è prestato); EUR-LEX, *«Verso Un Nuovo Quadro per l'infrastruttura Delle Comunicazioni Elettroniche.*», https://eur-lex.europa.eu/IT/legal-content/summary/a-new-framework-for-electronic-communications-services.html.

[23] F. CIRAOLO*, «Open Banking, Open Problems. Aspetti controversi del nuovo modello dei "sistemi bancari aperti"*», Rivista di Diritto Bancario anno 2020, fascicolo IV, sezione I.

[24] L. JENG, *Open Banking* (New York: Oxford Academic, 2022), https://doi.org/10.1093/oso/9780197582879.001.0001.

[25] "Prestatore di servizi di pagamento di radicamento del conto" ("ASPSP"): un prestatore di servizi di pagamento che fornisce e amministra un conto di pagamento per un pagatore. EDPB, «Linee guida 06/2020 sull'interazione tra la seconda direttiva sui servizi di pagamento e il GDPR Versione 2.0», 15 dicembre 2020, https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202006_psd2_afterpublicconsultation_it.pdf.

[26] "Un'API ossia un'interfaccia di programmazione di una applicazione, è un insieme di comandi formalizzati che consentono alle applicazioni software di comunicare tra loro in modo uniforme e di sfruttare i servizi di base per crearne altri incentrati sul cliente." N. ELLENA, «*API: cosa sono e perché sono importanti per il Fintech*», Money.it, 18 gennaio 2023, https://www.money.it/API-fintech-cosa-sono-e-perche-sono-importanti.

[27] Direttiva UE 2015/2366 del 25 novembre 2015, recepita in Italia con d. lgs. n. 218/2017 (in vigore dal 13 gennaio 2018).

permettendo di stimolare ulteriormente la concorrenza e la cooperazione nei servizi finanziari.

Il paradigma dell'*open banking* si basa infatti sulla cooperazione tra diversi attori: banche tradizionali, banche digitali, *FinTech* e *Tech Providers*, i quali sono tutti coinvolti nell'ecosistema, anche se con ruoli e obiettivi differenti. Quello che la normativa richiede è che le banche mettano a fattor comune un bene finora custodito molto gelosamente: le informazioni sui propri clienti. Pertanto, un soggetto terzo (*third party provider, TPPs*), può interporsi nel rapporto tra banca e cliente, mutandone le modalità di interazione e di gestione, con un grado di trasparenza mai sperimentato prima[28]. Considerato, infatti, che le banche non hanno alcun interesse a condividere i dati dei propri clienti con altre imprese in grado di offrire ulteriori servizi a valore aggiunto, l'introduzione di un obbligo di accesso ai conti a favore di terze parti comporta maggiore concorrenza nel mercato dei servizi di pagamento e stimola l'innovazione[29].

È innegabile come oggi l'informazione abbia assunto il ruolo di risorsa strategica essenziale, nonché fulcro della produzione di valore dei mercati. La Direttiva citata non fissa un generico principio di accesso non oneroso a tutti i dati detenuti dagli istituti bancari, ma solamente a quelli strumentali per consentire lo sviluppo dei servizi essenziali e imprescindibili in ogni soluzione innovativa nel campo dei pagamenti. Questo accesso "gratuito *ex lege*"[30] è circoscritto sia nell'ambito di applicazione (poiché è previsto solo per i conti di pagamento), sia nelle finalità, che sono limitati alla disposizione di un ordine di pagamento per il PISP (*Payment Initiation Service Providers)*[31], e all'offerta di servizi informativi per consentire all'utente di avere un panorama completo della propria situazione finanziaria in un dato momento per l'AISP

[28] S. AMBROSINI, «Rivista di Diritto Bancario, dottrina e giurisprudenza commentata», *Open Banking, Open Problems. Aspetti controversi del nuovo modello dei "sistemi bancari aperti"*, 2020.
[29] S. VEZZOSO, «*Fintech, Access to Data, and the Role of Competition Policy*», SSRN Scholarly Paper (Rochester, NY, 22 gennaio 2018), 35, https://doi.org/10.2139/ssrn.3106594.
[30] La c.d. *access to account rule*, in gergo *XS2A rule*.
[31] Più in dettaglio, i servizi del primo tipo consentono al prestatore (PISP) di disporre un pagamento, per conto dell'utente, a valere su un conto intrattenuto da quest'ultimo presso un altro intermediario (il prestatore di servizi di pagamento di radicamento del conto, o *Account Servicing Payment Service Provider*, ASPSP), assicurando contestualmente al beneficiario del pagamento che lo stesso è stato disposto. In termini tecnici, se si legge il considerando 27 della PSD2, essi consentono di effettuare bonifici *online* attraverso «*un software che fa da ponte tra il sito web del commerciante e la piattaforma di online banking della banca del pagatore*», ponendosi, dunque, come una valida e più economica alternativa ai tradizionali pagamenti con carta (per effettuare transazioni su *Internet*, infatti, l'utente deve solo possedere un conto corrente con accesso remoto, mentre il commerciante non è obbligato ad aderire ad un card scheme e a sopportare i relativi costi).

(*Account Information Service Providers)*[32]. Queste restrizioni sembrano finalizzate a bilanciare l'abbattimento delle barriere all'ingresso nei servizi di pagamento, con l'intento di stimolare la concorrenza, proteggendo contemporaneamente gli investimenti che l'istituto - presso cui è aperto il conto -deve fare per preservare i valori depositati, le infrastrutture tecnologiche impiegate e, più in generale, la sicurezza di tutte le informazioni raccolte[33]. È pertanto plausibile prevedere che gli intermediari finanziari, in un futuro prossimo, siano in grado di esercitare tre funzioni principali: (i) l'aggregazione della domanda, in un contesto in cui la banca mantiene la relazione con la clientela, delegando la produzione dei servizi a terzi; (ii) la produzione di servizi finanziari specifici, in cui la banca si specializza, lasciando la loro distribuzione a piattaforme di aggregazione e perdendo così la relazione diretta con la clientela[34]; (iii) la produzione di dati e analisi in cui la banca si pone come intermediario tra produzione e distribuzione di servizi, facilitando la connessione delle parti attraverso l'uso di *big data* per collegare e valutare consumatori e fornitori di servizi, offrendo servizi di *credit scoring*, *know your customer* e *data security*. Tuttavia, ciò che sembra ormai chiaro, a seguito dell'entrata in vigore della PSD2, è che il modo di gestire l'asset più importante del credito e della finanza, ovvero le informazioni sulla base delle quali ogni operatore del settore deve condurre le proprie analisi e fare le proprie scelte per offrire servizi e prodotti ai clienti, cambierà completamente. La rilevanza di queste informazioni è stata probabilmente sottovalutata fino ad ora, con la conseguenza che anche il tipo di relazione con la clientela è destinato a cambiare, spostandosi dallo sportello bancario allo *smartphone.*

[32] Gli *Account Information Services* emergono con l'intento di fornire all'utente un quadro consolidato delle informazioni riguardanti i conti che detiene presso diversi intermediari (cioè, uno o più fornitori di servizi di pagamento che detengono il conto), permettendogli di avere una visione completa della propria situazione finanziaria e dei propri comportamenti di spesa. In pratica, attraverso l'accesso al servizio via una specifica piattaforma online, l'utente ha la possibilità di ottenere un resoconto dettagliato e strutturato di tutti i propri conti di pagamento e di prenderne, quindi, decisioni informate riguardo la gestione efficace delle proprie risorse.

[33] C. MUROLO, «Open Banking: così le banche possono conservare il rapporto diretto con il cliente», *Agenda Digitale*, 5 ottobre 2017, https://www.agendadigitale.eu/cittadinanza-digitale/open-banking-cosi-le-banche-possono-conservare-il-rapporto-diretto-con-il-cliente/.

[34] Al riguardo, è stato sottolineato che l'effetto più significativo delle nuove disposizioni normative consiste nel venir meno del «monopolio degli istituti di credito sui dati bancari dei clienti, frutto di investimenti, relazioni con la clientela e regole molto stringenti», come anche della stessa «esclusività del rapporto con la clientela», con ciò determinandosi una significativa trasformazione dell'operatività bancaria. A. ARGENTATI, «*Banks and new Competitive Scenario: FinTech*, *the Open Banking Paradigm and the Threat of Big Tech Companies*», Mercato Concorrenza Regole, fasc. 3 (3 dicembre 2018): 441–466.

## *2.3* *Open Finance*: l'innovazione trasparente dei mercati finanziari

Oggi si parla molto di *open finance*, la quale viene considerata come lo *step* successivo dell'*open banking* verso un ecosistema completamente "*open"*. È un paradigma che consente ai *player* che operano nel settore finanziario di condividere tra loro, dati finanziari, non più solo relativi ai pagamenti[35], sempre previo il consenso dei clienti. Ciò estende significativamente il panorama precedente, consentendo ai *provider* terzi autorizzati, di accedere ad una più ampia gamma di dati finanziari dei consumatori, riguardanti prodotti, prezzi, contratti di risparmio, conti, pensioni, mutui, assicurazioni, investimenti, azioni ed altro ancora. Questi dati sono preziosi anche per la creazione di prodotti e servizi finanziari personalizzati, progettati per rispondere alle necessità ed aspettative dei clienti. Come emerge dalle nuove iniziative del mercato, le API possono consentire agli operatori *Open Banking & Finance* di collaborare tra loro. Le *Application Programming Interface* consentono, infatti, alle banche, di integrare i servizi di terze parti nei propri canali *web* in modo semplice, riducendo così i costi di integrazione e il *time to market*. Ad oggi questo modello è ampiamente adottato dalle banche digitali che sviluppano soluzioni migliori per fornire i risultati attesi dai clienti.

Questo modello inoltre, consente alle banche di arricchire la propria offerta di servizi bancari non forniti direttamente, integrandola con servizi non bancari. Implementando l'*open finance* le banche potranno generare nuove entrate attraverso la vendita incrociata e incrementale di nuovi servizi, prodotti e offerte su misura, in modo da attirare clienti e allo stesso tempo ridurre i costi di sviluppo per le nuove offerte[36]. La Commissione Europea sta ampliando le novità introdotte dalla Direttiva PSD2 nel settore dell'*open banking*, lanciando nuove iniziative, tra cui il *Digital*

[35] DIRECTORATE-GENERAL FOR FINANCIAL STABILITY, FINANCIAL SERVICES AND CAPITAL MARKETS UNION, «*Report on Open Finance*», 24 ottobre 2022, https://finance.ec.europa.eu/publications/report-open-finance_en#:~:text=Description,perspective%20of%20the%20Expert%20Group.

[36] CBI IN COLLABORAZIONE CON PwC, «*THE GLOBAL OPEN FINANCE REPORT*», marzo 2023, https://www.cbi-org.eu/Media-Events/Next-Appointments/The-Global-Open-Finance-Report.

*Finance Package*[37], l'*Open Finance Consultation*[38] e l'*European Data Act*[39]*,* mirando a promuovere interventi normativi più adeguati ed efficaci, necessari per facilitare lo sviluppo di servizi e prodotti *disruptive*[40], riducendo contestualmente la presenza dei potenziali rischi associati a tali nuove attività; tutto ciò nell'ottica di aumentare la stabilità e l'efficienza del settore finanziario. Appare dunque evidente che l'*Open Finance* rappresenti l'evoluzione dell'*Open Banking*.

Questo nuovo *trend* offre quindi un modello di condivisione delle informazioni che consente agli utenti di condividere i propri dati finanziari (bancari e non) con terze parti, contribuendo alla creazione di servizi finanziari innovativi e modelli di *business* inediti, sfruttando fonti di dati precedentemente inesplorate. L*'Open Finance* potrebbe anche aiutare il settore finanziario e bancario nel promuovere un contesto normativo più favorevole[41]. Questa evoluzione potrebbe fornire a clienti, imprese e banche maggiore trasparenza, controllo e sicurezza, contribuendo alla creazione di un efficace sistema antifrode e aumentando la sicurezza informatica nel sistema bancario e finanziario. Tale sistema aperto, richiede tuttavia una strategica considerazione dell'ampiezza dei dati condivisi e del grado di standardizzazione dei medesimi da parte dei vari attori del mercato.

Guardando al futuro, si prevede che l'*Open Finance* continuerà a crescere, spinto principalmente da due fattori: l'offerta di servizi finanziari personalizzati e l'introduzione dell'Euro Digitale[42]. La PSD2 ha avviato una *disruption* nei sistemi di pagamento che sta gradualmente estendendo i suoi effetti a tutti i servizi finanziari, incoraggiando *partnership* e collaborazioni tra *FinTech* e industria bancaria. Ciò porta ad un arricchimento dell'offerta, tanto più in quanto risponde alle esigenze specifiche del cliente e non è limitata ai servizi bancari tradizionali.

---

[37] il *Digital Finance package* rappresenta un insieme di misure legislative che definiscono in che modo l'UE può sostenere la trasformazione digitale e l'innovazione del settore finanziario, includendo azioni significative nei settori della *Digital Identity,* dell'*open finance,* dei *crypto-assets* della *digital resilience* e della *blockchain.*

[38] L'*Open Finance Consultation* è una consultazione pubblica mirata, lanciata dalla Commissione per raccogliere i *feedback* del mercato sull'applicazione e l'impatto della PSD2 e dei pareri sull'*Open Finance.*

[39] L'*European Data Act* è una proposta di regolamentazione di un quadro armonizzato per la condivisione dei dati nell'Unione Europea. Questa legge aumenterà la quantità di dati disponibili per l'uso e stabilirà linee guida per l'accesso, la gestione e le finalità in tutti i settori economici dell'UE.

[40] «*L'innovazione tecnologica è definita disruptive, o dirompente, quando determina un cambiamento in un ecosistema economico*». In J. BOWER, C. CHRISTENSEN, «*Disruptive Technologies: Catching the Wave», Harvard Business Review*, (1995) 73 , 43-53.

[41] S. MACCARONE, intervista in "*THE GLOBAL OPEN FINANCE REPORT*", marzo 2023, https://www.cbi-org.eu/Media-Events/Next-Appointments/The-Global-Open-Finance-Report.

[42] Cfr. S. L. FURNARI, D. SCHETTINI, *Euro digitale: primi commenti alla Proposta di Regolamento. Tra innovazione tecnologia e adozione di massa* in Dirittobancario.it, 2023.

## *2.4 Open Finance* e *Big Data*: verso un'offerta finanziaria su misura

Le nuove tecnologie consentono di affidare a sofisticati strumenti automatizzati gran parte della vicenda negoziale, comprendendo non solo la fase finale relativa alla conclusione, ma anche quelle precedenti, quali l'attività di predisposizione degli assetti negoziali, di individuazione dell'oggetto, di selezione della controparte con cui negoziare. Tutte queste attività sono in grado di modificare le modalità tradizionali di produzione e distribuzione dei beni e di strumenti, creando valore attraverso l'automazione di processi riguardanti l'utilizzo delle informazioni che permettono di conoscere meglio il mercato e di comprenderne i bisogni in tempi rapidi e diretti.

Attraverso l'aggregazione di enormi quantità di dati e di informazioni, reperiti dalla *digital experience* e dalle vicende *off-line*, si riesce a profilare analiticamente la clientela ed a progettare e creare nuovi prodotti e servizi per investitori, capaci di intercettarne esigenze e bisogni[43]. Si raggiungono in questo modo elevati livelli di personalizzazione delle offerte che presentano numerosi vantaggi per tutti i soggetti coinvolti e per il sistema nel suo complesso. I maggiori benefici prodotti da tali tecnologie consistono, pertanto, nell'acquisizione di una profonda conoscenza della clientela e di una sua più accurata segmentazione per categorie omogenee[44].

La profilazione[45], comprende anche il trattamento[46] dei dati raccolti, che può considerarsi personalizzata rispetto al singolo soggetto ovvero rivolta ad un "*group-targeting*". Vengono utilizzati dati personali di particolare rilievo per il settore finanziario, la profilazione è sottoposta al sistema di garanzie dettato dalla normativa europea del regolamento GDPR, il quale stabilisce che l'intermediario finanziario, in

---

[43] R. LENER, G. LUCHENA, C. ROBUSTELLA, "*Mercati regolati e nuove filiere di valore"*, I, Diritto dell'economia, G. Giappichelli editore, 2021.

[44] Cfr. R. LENER, «*Tecnologie e attività finanziaria*», in Rivista trimestrale di diritto dell'economia 3/2019, 267 ss.

[45] Secondo la definizione accolta dall'art. 4, comma 1, n. 4 del regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, Regolamento Generale sulla Protezione dei dati (GDPR), per "profilazione" si intende *"qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica"*.

46 Secondo la definizione accolta dall'art. 4, comma 1, n. 2 del richiamato Regolamento per "Trattamenti" si intende «operazione o insieme di operazioni, compiute con o senza ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».

caso di trattamento di dati personali utilizzati nell'ambito di un processo decisionale automatizzato, dovrà informare i clienti sull'uso la cui raccolta è finalizzata, incluso l'eventuale individuazione del mercato di riferimento, richiedendo un'espressa autorizzazione qualora procedano a un intreccio dei relativi dati sfruttando fonti diverse[47]. L'utilizzo dei dati nel paradigma *open finance* trova riconoscimento giuridico, in campo finanziario, all'interno delle disposizioni dettate in tema di *product governance.* La disciplina individua nel controllo della filiera produttiva lo strumento principale di *governance* del prodotto, in modo da garantire l'innovazione ed al contempo contenere i rischi connessi alla distribuzione presso la clientela *retail*. Prevista nell'impianto generale adottato dalla MIFID II, direttiva 2014/65/UE[48], e dal connesso regolamento MiFIR, n. 600/2014[49], nonché della direttiva delegata 2017/593/UE[50] e dalle linee guida adottate dall'ESMA[51], la cui attuazione ha comportato l'inserimento dei commi 2-*bis* e 2-*ter* dell'art. 21 TUF e del titolo VIII del Regolamento Intermediari adottato dalla Consob.

La disciplina in dettaglio, sancisce l'obbligo di implementare l'attività degli intermediari con specifici protocolli per definire un mercato di riferimento, denominato "*target market*", considerato adatto per un dato strumento finanziario e al quale tale strumento sarà in seguito indirizzato. La responsabilità di definire un *target market* chiaro spetta sia al produttore, ossia il "*manufacturer*", che è colui che progetta, realizza, rilascia e/o pianifica strumenti finanziari o che assiste gli emittenti

[47] Va richiamato in particolare l'art 22 del regolamento GDPR relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE regolamento generale sulla protezione dei dati, che prevede che il cliente può vantare un vero e proprio diritto a non essere sottoposto a un procedimento automatizzato, che potrebbe avere effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Tale divieto non si applica nel caso in cui la decisione sia necessaria per la stessa conclusione o per l'esecuzione del contratto tra l'interessato e il soggetto che procede al trattamento dei dati o qualora si basi sul consenso esplicitamente espresso dall'interessato ovvero, infine, qualora la decisione sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato. La profilazione deve essere condotta dal titolare del trattamento in modo da garantire 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.

[48] *Markets in Financial Instruments Directive* del Parlamento Europeo e del Consiglio del 15 maggio 2014 relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE e la direttiva 2011/61/UE.

[49] *Markets in Financial Instruments Regulation* (UE) n. 600/2014 del Parlamento Europeo e del Consiglio, del 15 maggio 2014, sui mercati degli strumenti finanziari e che modifica il regolamento (UE) n. 648/2012.

[50] Direttiva Delegata della commissione del 7 aprile 2016 che integra la direttiva 2014/65/UE del Parlamento europeo e del Consiglio per quanto riguarda la salvaguardia degli strumenti finanziari e dei fondi dei clienti, gli obblighi di governance dei prodotti e le regole applicabili.

[51] *ESMA, Guidelines on Mifid II product governance requirements*, del 5 febbraio 2018.

nell'esecuzione di tali operazioni, sia all'ente distributivo, il "*distributor*", ossia chi propone e suggerisce tali strumenti alla clientela, all'interno di un sistema che enfatizza i principi di "*know your customer*" e "*know your product*"[52].

In particolare, per quanto rileva nel presente elaborato, preme sottolineare l'importanza dell'attuazione del primo principio, che evidenzia la necessità di comprendere e categorizzare la clientela sin dalla fase di generazione e diffusione dell'asset finanziario. In tal modo la profilazione del cliente diviene un processo articolato in più fasi diverse e con un sempre maggiore approfondimento in ordine al tipo di informazioni raccolte[53]. Entrambi i soggetti sono inoltre chiamati a identificare il mercato di riferimento negativo, delineando i segmenti di clienti per i quali il prodotto concepito non risponde alle loro necessità, peculiarità e obiettivi. L'utilizzo dei *bigdata* nel *framework open finance* ha come obiettivo principale oltre alla creazione di valore, quello di rafforzare la protezione del cliente mediante l'applicazione della suddetta disciplina, riducendo i fenomeni di *misselling*, ovvero di collocamento di strumenti inadeguati perché non conformi alla propensione al rischio o agli obiettivi di investimento del cliente che li ha acquistati.

Fra gli aspetti di maggiore rilevanza nella personalizzazione dell'offerta, spicca la crescente attenzione dedicata al cliente, a cui è attribuita una rinnovata centralità nelle trattative con gli intermediari, conosciuta come "*customer centricity*", e più ampiamente, lungo l'intera filiera del prodotto.

Attraverso la conoscenza sempre più analitica e approfondita, consentita dall'analisi dei *bigdata,* vengono valorizzati i bisogni e le esigenze del singolo investitore, offrendo soluzioni finanziarie su misura.[54] In tal modo le contrattazioni personalizzate sostituiranno le più tradizionali offerte standardizzate, portando con sé l'esigenza della protezione dei dati, ponendo in evidenza le individualità dei clienti e favorendo rapporti cd. *tailor made*. Ciò comporta un cambiamento profondo dei processi di produzione e offerta dei beni, coerentemente con la tendenza generale che vede le aziende concentrarsi sulla personalizzazione dei loro prodotti.

---

[52] Cfr. A. PERRONE, *"Servizi d'investimento e tutela dell'investitore",* in Banca borsa e titoli di credito, 2019; (I): 1-16 [https://hdl.handle.net/10807/133055].

[53] F. MATTASSOGLIO, «*La profilazione dell'investitore nell'era dei big data. I rischi dell'estremizzazione della regola del "know your customer" (The Customer's profiling in the Era of Big Data.The Risks related to the radicalization of the "know your customer's role)*» n. 4 (1 gennaio 2016): 233–254.

[54] V. RICCIUTO, *«La tutela dell'investitore finanziario. Prime riflessioni su contratto, vigilanza* e *regolazione del mercato nella c.d. MiFID 2*», gennaio 2016, 10.

Le avanzate tecnologie permettono alle imprese di accedere a informazioni dettagliate rapidamente, con precisione e a costi contenuti, senza basarsi su *feedback* diretti ma attraverso l'elaborazione e analisi dei dati, permettendo di interpretare le dinamiche economiche e personali dei clienti, comprendere le loro aspettative e guidarli verso il conseguimento dei loro scopi. A questo si riferisce il termine "*customer intimacy*"[55].

In tal modo le imprese, possono formulare strategie più competitive e proposte altamente innovative, potenziando sia la loro efficienza che quella del sistema. L'automazione di tali flussi, chiaramente, porta vantaggi economici, minimizzando i costi associati all'indagine, alla negoziazione e di *enforcement*, grazie all'intervento delle soluzioni tecnologiche che riducono l'errore umano e i margini di incertezza, ottimizzando le transazioni finanziarie per prevenire incoerenze e ambiguità.

## *2.5* ***Open Finance*** **e digitalizzazione: rischi, asimmetria informativa e la sfida della tutela del consumatore**

Accanto agli innegabili benefici di cui si è trattato in precedenza, emergono alcune preoccupazioni riguardo ai suddetti meccanismi[56], in particolare per rischi che riguardano i possibili pregiudizi per i consumatori e la stabilità del sistema finanziario nel suo complesso. Al di là dei profili connessi ad applicazioni distorte o illecite che possono influenzare illegittimamente la posizione dei clienti, la questione fondamentale è la mancanza di neutralità e la sostanziale opacità nella percezione degli algoritmi come "*black boxes*", opache nel loro funzionamento e inesplicabili negli esiti. La grande quantità di dati raccolti e analizzati si presenta spesso come poco trasparente, e va oltre la capacità degli individui e delle autorità di comprendere i

[55] EBA, R. BAIRROS, 2016. *«Discussion Paper - on innovative uses of consumer data by financial institutions*», European Asylum Support Office. Malta. cit, ha ritenuto che se vengono mitigati i rischi, gli usi innovativi dei dati possono comportare benefici per i consumatori migliorando la qualità dei prodotti e offrendo loro servizi più personalizzati adattati alle loro esigenze e una migliore comprensione della loro situazione finanziaria. Potrebbero anche portare a risparmi sui costi per i consumatori, sebbene non necessariamente attraverso risparmi sui costi delle campagne di marketing realizzate dagli istituti finanziari sui consumatori, anche attraverso l'offerta di sconti mirati con specifici partner commerciali. A loro volta, gli istituti finanziari possono anche beneficiare di una maggiore efficienza in termini di costi / ricavi, migliore gestione dei rischi e compliance normativa.

[56] F. *MATTASSOGLIO, (2017). «Big data: impatto sui servizi finanziari e sulla tutela dei dati personali». In M.T. Paracampo (a cura di), «Fintech: introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*» (pp. 65-80). Giappichelli.

motivi e gli scopi di tali attività. In questo contesto, si sottolinea che l'integrità dei dati e la trasparenza degli algoritmi, spesso carenti di validazione, possono portare a correlazioni errate e sottostima delle implicazioni legali, sociali ed economiche, aumentando il rischio di utilizzo dei dati in modo inappropriato e fraudolento, con conseguenti vizi nelle procedure decisionali per i singoli e per la collettività[57].

Riguardo al rapporto contrattuale, emergono due principali rischi per i clienti: uno di natura finanziaria dell'accordo e all'oggetto specifico dell'operazione, ed un secondo, nuovo, correlato all'adozione di tecnologie digitali nel fornire il servizio e nell'identificazione del prodotto offerto. L'impiego della tecnologia, infatti, tende a rendere il contratto finanziario poco trasparente, accentuando il divario già esistente tra le parti e amplificando l'asimmetria informativa, un aspetto già intrinseco in tali operazioni. Il cliente, infatti, è destinatario di una offerta che si presenta complessa e di difficile comprensione in ordine ai motivi e ai criteri che ne hanno determinato l'oggetto, le condizioni e il prezzo.

Inoltre, il cliente, che aderisce ad un contratto predisposto unilateralmente, sembra subire ulteriori limitazioni legate alla selezione di un prodotto o servizio, condizionati da elementi estrinseci rispetto al contratto stesso. Le scelte sono fortemente guidate dal profilo del consumatore, che si è delineato dopo aver raccolto ed elaborato le informazioni su di lui. Il rischio consiste nella potenziale riduzione della capacità di compiere scelte autonome da parte del consumatore e nella crescente inclinazione a posizioni "passive" rispetto a prodotti o servizi proposti come ottimali, convenienti e in linea con il profilo delineato. Quanto più il fenomeno di *open finance* sarà efficiente, tanto più passiva risulterà la posizione degli utenti, la cui libertà di scelta sarà sempre più circoscritta all'interno di mercati ristretti e segmentati.

La letteratura economica ha sottolineato anche il pericolo "*aftermarket"* per il consumatore, di restare intrappolato in un contesto dove la sua prima decisione di acquisto determina le successive, in un ambiente controllato da chi possiede e gestisce i suoi dati. L'utente, in questo modo, rischierebbe di trovarsi in una dinamica totalmente automatizzata, con una partecipazione non sufficientemente libera e attiva[58].

Il rischio di una crescente asimmetria informativa dell'utente pone il problema per garantire un equilibrio contrattuale attraverso un flusso informativo che permetta

[57] M.T. PARACAMPO, «*FinTech tra algoritmi, trasparenza e algo-governance*», *Diritto della Banca e del Mercato Finanziario*, fasc. 2 (gennaio 2019).
[58] M. DELMASTRO E A. NICITA, «*Big data. Come stanno cambiando il nostro mondo*», 2019, Il Mulino.

scelte finanziarie consapevoli e autonome. Questa consapevolezza, sia a livello europeo che nazionale, ha spesso a che fare con il principio di trasparenza. Sulla base di tale principio sono stati imposti agli intermediari obblighi di divulgazione sempre più dettagliati, visti come essenziali, per rendere l'utente consapevole delle implicazioni del contratto, delle sue condizioni legali ed economiche, e delle caratteristiche dello strumento finanziario e del soggetto che lo ha emesso o offerto.

Da una prospettiva orientata alla scelta informata, che costituisce una componente fondamentale dell'intero sistema protettivo, tra le molteplici informazioni di natura finanziaria che l'intermediario deve trasmettere al cliente durante la fornitura di un servizio, dovrebbero essere incluse anche quelle che illustrano i meccanismi che hanno portato alla determinazione dell'offerta con quelle condizioni e modalità, a quei prezzi. In questo contesto, è essenziale assoggettare ad obblighi informativi e di trasparenza anche gli elementi centrali che hanno dato origine a quell'offerta, ovvero i dati e gli algoritmi che li elaborano. Il cliente dovrebbe essere messo al corrente delle metodologie adottate, dei dati impiegati e degli esiti conseguiti. Queste informazioni dovrebbero, quindi, essere considerate alla stregua di ogni altra informazione che la legge richiede venga fornita al cliente per garantire una piena comprensione degli aspetti salienti del contratto[59].

Nel settore bancario, si potrebbe ritenere che tali dettagli rientrino tra le "*informazioni essenziali del rapporto contrattuale*" che, secondo le normative sulla trasparenza contrattuale, «*la banca deve rendere noti ai clienti*" in modo "*corretto, chiaro ed esauriente nonché adeguato alla forma di comunicazione utilizzata e alle caratteristiche dei servizi e della clientela*», affinché il cliente possa comprendere esattamente il servizio o il contratto offerto[60]. Nel settore mobiliare, queste informazioni potrebbero essere incluse tra i doveri informativi previsti dall'art. 21 TUF[61], da considerarsi quali specificazione dei principi generali dettati dal primo comma lett. *a),* il quale prevede: Obblighi di comportamento informati ai criteri di diligenza, correttezza e trasparenza per servire al meglio l'interesse dei clienti e per l'integrità dei mercati ovvero degli obblighi previsti dalla successiva lettera *b)* della medesima disposizione che impone agli intermediari di operare in modo che i clienti

[59] F. CAPRIGLIONE, «*Manuale di Diritto bancario e finanziario*», 505 ss. II (Cedam, 2019),
[60] Cfr. BANCA D'ITALIA, «Trasparenza delle operazioni e dei servizi bancari e finanziari Correttezza delle relazioni tra intermediari e clienti», marzo 2009, https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2009/resoconto-consultazione-pubblica/trasparenza_documento_consultazione.pdf.
[61] Cfr. G. CAVALLARO, «*Commentario al Testo Unico della Finanza*» (Pacini Editore, 2021).

siano sempre adeguatamente informati. Obblighi, le cui modalità operative vengono previste dagli artt. 36 ss. del Regolamento Intermediari[62], secondo i quali gli intermediari "*forniscono in tempo utile ai clienti o potenziali clienti, in una forma comprensibile, informazioni appropriate affinché essi possano ragionevolmente comprendere la natura del servizio di investimento e del tipo specifico di strumenti finanziari che sono loro proposti, nonché i rischi a essi connessi e, di conseguenza, possano prendere le decisioni in materia di investimento con cognizione di causa*". Tali informazioni devono essere rese in modo "*chiaro, corretto e non fuorviante*", con l'obiettivo di migliorare la consapevolezza del cliente e permettergli una valutazione ponderata degli impegni derivanti dall'eventuale stipula di un contratto.

Le soluzioni prospettate avrebbero il merito di garantire al cliente le stesse protezioni previste nei casi in cui l'intermediario non rispetti i suoi obblighi comportamentali e informativi. Tuttavia, tali proposte sarebbero tuttora ancorate a un approccio tradizionale che offre una protezione *ex post* al cliente, intervenendo nella fase conclusiva del rapporto con l'intermediario. Nonostante le numerose critiche mosse a tale sistema, ritenuto inadeguato per assicurare un effettivo equilibrio informativo nel contratto, e stante la difficile realizzazione di una piena consapevolezza da parte del cliente, le sfide emergenti sono legate sia all'identificazione precisa dell'oggetto dell'informazione sia alla sua comprensione da parte del cliente[63].

Alcuni ritengono che, appare oltremodo difficile riuscire a fornire informazioni che siano "*chiare e corrette*" e "*complete*", dato che un compito del genere, necessita di competenze particolarmente avanzate e specialistiche, raramente presenti sia tra i destinatari sia tra coloro incaricati di impartire tali informazioni. Un aumento nella trasparenza, in realtà, potrebbe rivelarsi superfluo o, quantomeno, inappropriato, poiché i consumatori spesso non riescono a comprendere tali informazioni a causa del *gap* strutturale di conoscenze tecnologiche che li distanzia dalle imprese. La nozione di asimmetria informativa nel *framework open finance,* presenta caratteri nuovi, non solo per la fonte di provenienza, derivante dall'uso delle tecnologie, ma anche perché il cliente ricopre una "duplice" posizione, quella di destinatario delle informazioni e

62 Regolamento intermediari, Adottato con delibera n. 20307 del 15.2.2018

63 A. Antonucci, «I contratti di mercato finanziario» - II (Pacini Editore, 2022), cit., 44, definisce la figura del "risparmiatore adeguatamente informato" alla stregua di un fantasioso soggetto. Gli obblighi di trasparenza presuppongono, infatti, l'esistenza di un soggetto perfettamente razionale, capace di elaborare e utilizzare tutte le informazioni a tutela dei propri interessi e della propria posizione.

quella di produttore delle stesse, successivamente utilizzate per la costruzione del nuovo bene ritenuto a lui conforme[64].

In un contesto che progredisce verso l'istituzione di un mercato unico digitale, all'interno del quale viene garantita la libera circolazione dei dati, personali e non, è necessaria una revisione dell'approccio regolatorio e interpretativo tradizionale. Tale revisione dovrebbe focalizzarsi sulle fasi di produzione e circolazione degli strumenti finanziari, ancor prima della loro allocazione definitiva presso gli utenti finali. Considerando che i dati sono diventati una componente cruciale dell'attività economica, poiché generano ricchezza ed incrementano il valore della stessa, è essenziale definire meccanismi che offrano piena contezza e adeguata percezione delle modalità di cessione a chi intende introdurli nel sistema. Tale spostamento *ex ante* della disciplina, in aggiunta al quadro regolatorio *ex post* basato sulla trasparenza, potrebbe arricchire efficacemente il sistema di tutela del cliente.

In una visione certamente limitata, vista l'evoluzione rapida del panorama, si potrebbero identificare soluzioni mirate a superare le emergenti asimmetrie informative nel contesto finanziario. L'obiettivo potrebbe essere quello di riorientare il sistema valorizzando la centralità rinnovata del cliente, facendone un soggetto dinamico del mercato, capace di esercitare un ruolo attivo nella scelta e nell'acquisizione dei beni e servizi, mediante strumenti legislativi e regolatori che possano aumentarne la capacità di discernimento ed il senso critico[65].

Il GDPR emerge come un punto di partenza rilevante, poiché basa le proprie disposizioni sul principio per cui gli individui debbano avere "*il controllo dei dati personali che li riguardano*"[66] per poter limitare l'utilizzo da parte di terzi, anche mediante informazioni significative sulla «*esistenza di un processo decisionale automatizzato, compresa la profilazione, nonché informazioni significative sulla logica utilizzata e sull'importanza e le conseguenze previste di tale trattamento per l'interessato*»[67].

La strada che potrebbe essere percorsa dovrebbe, in altri termini, attuare il principio secondo il quale sarebbe opportuno riuscire ad utilizzare i dati e non solamente essere utilizzati. Fornire strumenti che consentano una comprensione chiara

[64] L. AMMANNATI, «*La circolazione dei dati: dal consumo alla produzione*», *Astrid rassegna*, 1° gennaio 2020.
[65] L. AMMANNATI, *«Il paradigma del consumatore nell'era digitale: consumatore digitale o digitalizzazione del consumatore?»* Fondazione G. Capriglione (2019).
[66] GDPR, *considerando* n.7
[67] GDPR, Artt. 13 e 15

dei dati, del loro utilizzo e del loro valore, potrebbe rivoluzionare l'interazione con gli intermediari, in linea con le tendenze regolatorie recenti.

La crescente rilevanza degli algoritmi, che possono potenzialmente sostituire le basi contrattuali, sottolinea l'importanza della piena consapevolezza da parte dei clienti. Ciò potrebbe portare al superamento dell'approccio tradizionale basato su doveri informativi, bilanciando meglio il sistema attraverso il riconoscimento di poteri, facoltà e responsabilità in capo ai titolari dei dati.

Tale assunto potrebbe costituire una base per future iniziative, benché richieda competenze specifiche non sempre presenti tra i clienti al dettaglio. È imperativo sottolineare che, guardando al futuro, diventa indispensabile possedere una conoscenza, almeno di base, delle tecnologie per avere una partecipazione attiva in una società sempre più digitalizzata.

Questo rappresenta una sfida per legislatori, regolatori e istituzioni chiamate a cercare soluzioni normative capaci sia di guidare l'evoluzione tecnologica che di minimizzare i rischi, garantendo certezza giuridica e equilibrio tra progresso tecnologico, tutela dei clienti e stabilità del sistema. Inoltre, le banche dovranno rispondere alle esigenze di una clientela sempre più esigente consolidando la collaborazione con le *FinTech*, sfruttando la fiducia che il mondo bancario ha da parte della clientela e la capacità di innovazione che caratterizza le *FinTech*. Allo stesso tempo, ci si aspetta che un forte impulso all'innovazione e *all'Open Finance* provenga dall'introduzione dell'euro digitale[68].

## *3.* Dalla concorrenza alla cooperazione: il futuro *FinTech*

L'*Open Banking* è un elemento chiave nell'evoluzione del *FinTech*, l'ecosistema in cui l'innovazione tecnologica si fonde con la finanza, generando cambiamenti significativi nella modalità di erogazione dei servizi finanziari[69]. Questo paradigma, che emerge nel contesto di un'accelerata transizione digitale nel settore bancario, introduce un modello di gestione dell'informazione finanziaria radicalmente diverso.

[68] V. SORGE , intervista in "*THE GLOBAL OPEN FINANCE REPORT*", marzo 2023, https://www.cbi-org.eu/Media-Events/Next-Appointments/The-Global-Open-Finance-Report.
[69] D. A. ZETZSCHE, R.P. BUCKLEY, D. W. ARNER, J. N. BARBERIS, "*From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance"*, SSRN Scholarly Paper (Rochester, NY, 28 aprile 2017), https://doi.org/10.2139/ssrn.2959925.

Mentre da un lato questo modello sembrerebbe minare le strutture tradizionali, dall'altro propone un livello inaudito di efficienza, personalizzazione e trasparenza.

Questo scambio di informazioni, se gestito correttamente, ha il potenziale di portare benefici considerevoli a tutte le parti coinvolte. Da un lato, gli utenti possono avere accesso a servizi finanziari su misura e possono confrontare in maniera più efficace le diverse offerte presenti sul mercato. Dall'altro lato, le banche e i fornitori di servizi finanziari terzi possono trarre vantaggio da queste nuove informazioni per affinare la loro offerta, creando prodotti e servizi estremamente mirati alle esigenze specifiche del cliente. Un altro aspetto importante, e al tempo stesso critico nel nuovo contesto, continua ad essere la conoscenza e l'interpretazione dei bisogni e di ciò che è valore per i clienti. Sono infatti i clienti ad essere responsabili delle transazioni e sono ancora i clienti a decidere cosa abbia valore. I nuovi *competitors* hanno colto appieno tale necessità e sapientemente la traducono in opportunità strategiche. Con la conseguenza che la conoscenza del cliente diventa un bene prezioso; essa inoltre accresce di importanza quanto più si amplia l'ambito di azione del singolo e la sua operatività[70]. Ne consegue che anche la relazione banca-cliente deve evolvere orientandosi, sempre di più, in una prospettiva di bisogni da soddisfare e non più di prodotti da proporre.

Premesso che l'impatto del digitale è pervasivo nel campo bancario e ogni cliente da tempo è diventato un cliente digitale[71], va ricordato che parlare di *retail banking*, oggi, significa fare riferimento a tantissime tecnologie diverse e convergenti. Per quanto riguarda le *FinTech*, si può parlare di "*digital-only banking";* esse, infatti, ricercano e sviluppano proposizioni di valore nuove, con riferimento a bisogni talora tradizionali e tali da soddisfare esigenze di una domanda, che sperimenta in molti casi difficoltà nella relazione con il servizio bancario tradizionale. Queste, offrono valore al cliente garantendo esperienze "*banking seemless*", per quanto riguarda la funzione economica, ma caratterizzate da minori attriti sul fronte della *user experience*.

Sebbene, come si è detto, l'espansione del *FinTech* si sia caratterizzata per l'applicazione di tecnologie connesse alla rivoluzione digitale nel settore dei mercati finanziari, i mutamenti che hanno investito la società contemporanea, con particolare riferimento ai fenomeni di *datification*, hanno determinato il progressivo avvicinamento

[70] A. OMARINI, «*Banks and Fintechs: How to Develop a Digital Open Banking Approach for the Bank's Future*», *International Business Research* 11 (10 agosto 2018): 23, https://doi.org/10.5539/ibr.v11n9p23.
[71] ACCENTURE, «*Banking Customer 2020, Report*», 2015.

al settore finanziario da parte di imprese operanti in settori differenti (*e-commerce*, telecomunicazioni, piattaforme di *social media*, ecc.). L'ingresso delle *big data companies* è stato reso possibile dalla capacità di predisporre e offrire prodotti e servizi finanziari basati sullo sfruttamento dei *know-how*, delle infrastrutture e soprattutto dei dati acquisiti nel proprio ambito di operatività tradizionale. Inoltre, come si è accennato precedentemente l'introduzione di nuovi modelli di business nel settore dei mercati finanziari, incide sugli equilibri economici del settore nonché sulla relazione con i consumatori, i quali diventano investitori *retail*[72]. Nel far ciò i nuovi *incumbent*[73] operano un'integrazione funzionale dei propri servizi nelle diverse aree, eliminando le tradizionali architetture consolidate della catena di valore nei mercati finanziari e offrendo nuove piattaforme di negoziazione.

In questo quadro se c'è un dato che viene costantemente messo in luce da tutte le analisi di settore, attiene al ritardo dei *player* esistenti che "in molti casi non stanno ancora al passo con questa ondata di investimenti in innovazione, a causa di retaggi tecnologici e della scarsa rapidità con cui le banche sono in grado di far proprie le nuove tecnologie"[74].

Si sta però via via prendendo consapevolezza che le *startup FinTech* possono diventare degli importanti alleati, anche duraturi, degli operatori tradizionali. Il mercato testimonia che la via più promettente è probabilmente quella della transizione dalla competizione, alla proficua cooperazione tra banche e *FinTech* grazie alla quale gli intermediari tradizionali potrebbero colmare il *gap* tecnologico che oggi ne rallenta la capacità di reazione, mentre le imprese *FinTech* potrebbero avere accesso alla vasta platea dei clienti bancari cui offrire i propri servizi aggiuntivi[75].

Emerge secondo molti, la necessità di superare i modelli di regolamentazione "per soggetti"[76] che hanno caratterizzato l'evolversi della normativa bancaria e finanziaria,

---

[72] D. GERADIN, «*What Should EU Competition Policy Do to Address the Concerns Raised by the Digital Platforms' Market Power?*», SSRN Scholarly Paper (Rochester, NY, 30 settembre 2018), https://doi.org/10.2139/ssrn.3257967.

[73] Per "*incumbent*" si intende un'Impresa, solitamente di grandi dimensioni, che controlla una quota elevata di uno specifico mercato.

[74] C. BARBAGALLO, «*Il sistema bancario italiano: situazione e prospettive*», (Bologna, 24 marzo 2018).

[75] A. ARGENTATI «*banche e big tech: criticità e strumenti per governare la nuova relazione competitiva. prime riflessioni*», in *Mercati regolati e nuove filiere di valore* (G. Giappichelli Editore, 2021), 188 ss.

[76] Il modello si richiama propriamente alle "istituzioni", e l'assetto regolamentare che sottende può riferirsi ai soggetti ovvero ai mercati finanziari e ai nuovi incumbents. "Il vantaggio di tale modello consiste nella circostanza che ogni intermediario fa capo ad un'unica autorità di vigilanza, altamente specializzata nel proprio settore di competenza, così da evitare duplicazione nei controlli. Per contro, tale tipologia di vigilanza presenta problemi e necessita di correttivi quando trova applicazione a soggetti diversi abilitati a svolgere le stesse attività, comportando l'applicazione di disposizioni

nonché l'operato delle *authorities* competenti, passando ad una regolamentazione "per attività"[77]; ciò consentirebbe di valorizzare e responsabilizzare il ruolo di ciascun attore nell'ecosistema finanziario, a prescindere dalla riconducibilità del relativo *nomen* all'interno di una categoria nota della disciplina di settore. Oltre alle questioni relative alla sicurezza, l'*Open Banking* richiede la definizione di un quadro normativo che regoli le relazioni tra i vari attori coinvolti. Tale quadro deve delineare i diritti e gli obblighi di banche, fornitori di servizi finanziari terzi e utenti, stabilendo norme chiare per l'accesso e l'utilizzo dei dati.

Sono le stesse Istituzioni europee che, avendo ben presente il rischio di una pericolosa frammentazione normativa derivante dal *FinTech,* si mostrano favorevoli alla creazione di un *level playing field* caratterizzato da regole certe e da una omogenea applicazione delle stesse agli intermediari tradizionali e ai nuovi *incumbent.*

Il *level playing field* è un principio basato sull'idea di parità tra gli Stati membri europei e tra i consumatori che operano nel mercato comune europeo. Un mercato con queste caratteristiche comporta specifici obblighi e diritti in capo agli operatori del mercato, sugli Stati membri e sui consumatori.

Creare un campo di operatività equo nel sistema di pagamento è un progetto complesso, poiché richiede di imporre obblighi rigorosi agli operatori del settore e di creare un sistema di pagamento coerente, consistente e funzionale a beneficio dei consumatori e degli operatori del mercato. Per realizzare questo obiettivo, sarebbe necessario affrontare le questioni di frammentazione normativa, creazione di opportuni standard di parità e definizione degli standard antitrust e della concorrenza.

Sembra emergere in tal senso un approccio integrato tra *hard law* e *soft law*, essendo accertata l'utilità della *soft law* in materia di regolamentazione finanziaria a livello internazionale. In merito a questi rapporti che sono estranei ai tradizionali meccanismi di intermediazione si pone, infatti, la questione che i nuovi operatori possano operare in modalità anticoncorrenziale, essendo di fatto non soggetti alle articolate e vincolanti discipline vigenti[78].

---

differente per operazioni della stessa natura solo in quanto eseguite da soggetti "istituzionalmente" diversi. in B. RAGANELLI, «Frontiere di Diritto Pubblico dell'economia», 147, 2019.

[77] La "vigilanza per attività", prevede una forma di controllo specifica per ogni attività di intermediazione, cosicchè ciascun servizio finanziario è sottoposto alla supervisione di una determinata autorità, indipendentemente dall'operatore che lo offre." _Ibidem.

[78] In Italia è previsto che se l'istituto di moneta elettronica svolge anche altre attività imprenditoriali diverse dall'emissione di moneta elettronica e dalla prestazione dei servizi di pagamento autorizzati, deve costituire un patrimonio destinato unico per l'emissione di moneta elettronica, la prestazione dei servizi di pagamento e per le relative attività accessorie e strumentali (art. 114-quinquies TUB). Si noti che per l'autorizzazione a svolgere attività come istituto di moneta elettronica, non è prescritto un

## *3.1* *FinTech* e banche: sinergie e sfide del Futuro

Come si ha avuto modo di evidenziare, le banche e le compagnie assicurative e molte altre realtà stanno attraversando un periodo di trasformazione significativo con sfide e opportunità dettate dalle nuove tecnologie. Nel concreto l'innovazione introdotta dal *FinTech* si concretizza in diversi fenomeni che continuamente modificano le dinamiche del sistema finanziario. Le opportunità per il settore tradizionale sono molteplici, a partire dalla *disruption* digitale che porta ad una evoluzione dei modelli e degli algoritmi sottostanti le decisioni di business delle banche, come l'utilizzo dell'intelligenza artificiale per valutazioni creditizie e antifrode, il tutto facilitato dalla nascita dei *framework open banking* e *open finance,* che consentono lo scambio di informazioni non solo finanziarie, facilitandone la circolazione in un ecosistema aperto. Altri importanti opportunità nascono dalla crescente trasformazione della domanda, nata da un profondo cambio di aspettative dei clienti i quali, sperimentando le potenzialità dei nuovi settori come quello delle cripto-attività, si aspettano processi sempre più digitali, intuitivi ed efficienti. La qualità del servizio offerto e della *customer experience* sono elementi cruciali in questo nuovo assetto operativo, caratterizzato da una elevata competizione con *focus* su margini e ricavi e tensioni tra le banche tradizionali e nuovi operatori del settore[79].

In risposta a queste nuove necessità si osservano sempre più di frequente collaborazioni e integrazioni tra banche tradizionali e attori *FinTech* specializzati, giustificate dai vertici delle banche in ragione di interessi riguardanti: l'aumento dei ricavi, riduzione del *time-to-market*, miglioramento della *customer loyalty* e lo sviluppo di nuovi prodotti e servizi per migliorare la *customer experience*[80].

---

oggetto sociale esclusivo. In quanto autorizzati, gli istituti di moneta elettronica possono "trasformare" immediatamente in moneta elettronica i fondi ricevuti dal richiedente e "prestare servizi di pagamento e le relative attività accessorie". Per quanto riguarda l'operatività in Italia di un soggetto che ha ricevuto l'autorizzazione ad operare come istituto di moneta elettronica in un altro stato comunitario, sempre l'art. 114-quinquies TUB, al comma 7 prevede che «gli istituti di moneta elettronica con sede legale in un altro stato comunitario possono operare nel territorio della Repubblica anche senza stabilirvi succursali dopo che la Banca d'Italia sia stata informata dall'autorità competente dello stato di origine». Cfr. F. FIMMANÒ E G. FALCONE, FinTech (Edizioni Scientifiche Italiane, 2019).

[79] L. FRATINI PASSI, «*Open Finance: tendenze e innovazione collaborativa*», Minerva Bancaria 03/2023, 91 ss.

[80] K. POWELL, «*If You Can't Beat 'em, Join 'em: 77% of Banks Feel Pressure to Collaborate With Fintechs That They View as a Threat to Their Existence*», Business Wire, 12 gennaio 2023,

Come già precedentemente accennato, il modello della *partnership* presenta una opportunità strategica *win-win*. Per quanto riguarda l'attore *FinTech* le banche dispongono di risorse quali una ampia base di clienti, prossimità fisica e ampia fiducia, licenze e dati proprietari ma soprattutto il *know-how* normativo in un ambiente estremamente regolato. Allo stesso modo gli attori tradizionali possono trarre beneficio dalla collaborazione, avendo accesso alle più moderne tecnologie, potendo diversificare la base dei clienti e facendo leva su una struttura organizzativa meno burocratizzata e invece concentrata sulla massima efficienza dei processi interni; inoltre, le realtà *FinTech* hanno una maggiore propensione al rischio e requisiti di capitale minori rispetto a un istituto tradizionale. Le suddette opportunità pongono però sfide su diversi fronti. Banca d'Italia evidenzia come il 30% degli intermediari incontra difficoltà a causa dei fattori tecnologici, primo fra tutti la mancanza di interoperabilità tra nuovi e vecchi sistemi[81].

Una seconda sfida legata alle tecnologie attiene al controllo dei rischi per la sicurezza informatica; infatti, si riscontra una asimmetria tra gli istituti tradizionali che, in ossequio alla disciplina vigente, operano con controlli di sicurezza estremamente elaborati e invece gli attori *FinTech* non sono regolati in modo altrettanto rigoroso sui processi di sicurezza ed autenticazione[82].

In ottica di collaborazione, non può essere trascurato tale elemento, anche se appare poco probabile che le *FinTech* adottino nei loro sistemi le stesse misure di sicurezza che sono parte integrante delle strutture tradizionali. L'alternativa più realistica sembrerebbe un metodo di lavoro collaborativo e organizzato, basato sull'analisi meticolosa dei rischi, modellato *ad-hoc* sulla specifica realtà *FinTech*.

Partendo dall'analisi dai sistemi *FinTech*, le parti coinvolte potrebbero avere un approccio collaborativo, assicurando il mantenimento degli *standard* di qualità tradizionali, pur interfacciandosi con le nuove piattaforme.

Ma il contesto normativo presenta complicazioni non soltanto in relazione alla *cybersicurezza*.

Il coinvolgimento di collaborazioni con soggetti esterni, potrebbe innescare problemi legali a causa dell'inadeguata regolamentazione contrattuale tra le parti coinvolte. In una visione più ampia, una sinergia di questo tipo modificherebbe il

[81] BANCA D'ITALIA, «*Indagine FinTech nel sistema finanziario italiano*», 2021, https://www.bancaditalia.it/pubblicazioni/indagine-fintech/2021/2021-FINTECH-INDAGINE.pdf.
[82] M. BONUOMO, A. BO, P. BOSSI, «*Prove di collaborazione tra FinTech e banche: quali sfide e come superarle?*», Minerva Bancaria 03/2023.

profilo di rischio dell'ente bancario, introducendo potenzialmente rischi operativi, di liquidità, di mercato, creditizio e reputazionali. La selezione del *partner FinTech* dovrebbe essere una scelta ben ponderata, e l'iter decisionale dovrebbe integrare una solida fase di *due diligence*, per ridurre le probabilità di rischi e potenziali perdite, sia finanziarie che di reputazione. In fase di *due diligence*, la banca dovrebbe accertarsi che la controparte sia effettivamente in grado di adempiere alle proprie obbligazioni contrattuali, valutando le misure di *risk management* da implementare. Inoltre, per ottemperare agli stringenti obblighi di *disclosure* e *reporting,* eventuali rischi evidenziati durante la fase di *due diligence* dovrebbero essere formalizzati, elaborando *contingency plan* documentati. Entrambi i soggetti dovrebbero consultare ed approvare questi piani prima di formalizzare la collaborazione.

Un *focus* necessario ulteriore in termini di integrazione tra banche e *FinTech* concerne le basi economico-finanziarie di una *FinTech* rispetto a un intermediario tradizionale. La struttura finanziaria delle *FinTech* è intrinsecamente più fragile, e ciò pone sfide su come la banca possa sostenere la gestione del capitale circolante della *FinTech* in sede di *partnership*. Questo aspetto è particolarmente sensibile in termini di tempistica dei pagamenti, per prevenire complicazioni di carattere finanziario per la *FinTech*. Un altro aspetto cruciale riguarda la gestione dei flussi di cassa: mentre i nuovi *incumbents* ambiscono a flussi costanti e stabili, spesso su modelli *pay-per-use*, la banca tende a preferire investimenti iniziali per poi ottimizzare i costi nel lungo termine[83]. Per assicurare che tali interessi siano considerati, potrebbe essere opportuno creare divisioni interne agli operatori tradizionali che si occupino esclusivamente delle collaborazioni in oggetto al fine di renderle sin dalla sottoscrizione, operative in un'ottica stabile e duratura anche per quanto riguarda gli aspetti remunerativi.

Come si è avuto modo di indicare in questo breve approfondimento, il settore *FinTech* comprende operatori con caratteristiche e operatività differenti e ciò giustifica l'esigenza che l'approccio di collaborazione debba essere personalizzato in base alle caratteristiche specifiche degli stessi. Le banche qualora scelgano di iniziare collaborazioni con i nuovi *incumbents*, dovranno comunicarlo al mercato, accertandosi che gli interessi dei clienti siano allineati con la natura della collaborazione stessa.

L'attuale contesto di mercato rappresenta un'opportunità unica per gli istituti tradizionali. I rialzi dei tassi di interesse e il contesto macroeconomico incerto

[83] A. M. AL SHANTI, A. JORDAN, D. MCMILLAN, «*The Impact of Digital Transformation towards Blockchain Technology Application in Banks to Improve Accounting Information Quality and Corporate Governance Effectiveness*» in Cogent economics&finance (2023).

potrebbero rappresentare una minaccia per le *FinTech*, a causa delle loro caratteristiche intrinseche. Di conseguenza le banche sono ora ben posizionate per ottenere il meglio dai modelli di *partnership* con i nuovi operatori del settore. È fondamentale che il mondo bancario tradizionale allarghi il proprio interesse strategico per includere nuove frontiere della tecnologia applicata a pagamenti e altri servizi bancari, integrando il proprio *know-how* regolamentare e di *risk management*.

## 4. Verso la PSD3

Il 28 giugno 2023, la Commissione europea ha presentato un pacchetto di misure con l'obiettivo di rinnovare i servizi di pagamento e stabilire linee guida per l'accesso ai dati finanziari[84]. Queste iniziative includono l'aggiornamento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (PSD2) e l'istituzione di un *framework* in materia di *open finance*, come annunciato nella Strategia sui pagamenti al dettaglio[85] e per la finanza digitale[86] proposte dalla Commissione nell'ambito del *Digital Finance Package* nel 2020.

In merito alla revisione della PSD2, le iniziative della Commissione si articolano in due documenti: (i) una proposta di regolamento relativa ai servizi di pagamento nell'UE (PSR); (ii) una proposta di direttiva sui servizi di pagamento e sulla moneta elettronica (PSD3). Quest'ultima si concentra sulle procedure di autorizzazione e supervisione degli istituti di pagamento, cercando di superare le criticità emerse dall'applicazione della PSD2, tenendo conto anche delle consultazioni svolte nel 2022 con istituzioni e parti interessate.

La proposta legislativa relativa all'*open finance*, contenuta in un regolamento, prendendo spunto dall'esperienza dell'*open banking* mira a definire un *framework* unitario per la condivisione da parte dei soggetti regolati dei dati finanziari con *third party providers*. L'obiettivo è favorire lo sviluppo di prodotti e servizi finanziari più innovativi per gli utenti e accrescere la concorrenza nel settore finanziario.

---

[84] I testi delle proposte legislative sono consultabili al seguente indirizzo: https://finance.ec.europa.eu/publications/ financial-data-access-and-payments-package_en.

[85] «*Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa a una strategia in materia di pagamenti al dettaglio per l'UE*», (COM(2020)592), (2020), https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020DC0592.

[86] *«comunicazione della commissione al parlamento europeo, al consiglio, al comitato economico e sociale europeo e al comitato delle regioni relativa a una strategia in materia di finanza digitale per l'UE*», (COM(2020)591), (2020), https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52020DC0591.

Queste proposte, insieme alle iniziative riguardanti l'euro digitale rilasciate dalla Commissione lo stesso giorno[87], contribuiscono a delineare la nuova architettura dei pagamenti dell'UE, e saranno ora esaminate dal Parlamento europeo e dal Consiglio.

Prima di analizzare le principali modifiche apportate alla PSD2, è importante notare che molte di queste sono incluse nel PSR. La scelta della Commissione di optare per un regolamento, risponde chiaramente all'esigenza di rafforzare e armonizzare al livello europeo la disciplina dei servizi di pagamento, prevedendo regole uniformi e direttamente applicabili in tutta l'UE.

Con la proposta di regolamento, la Commissione mira a: (i) prevedere nuove misure per combattere e mitigare le frodi nei pagamenti, come quella di consentire ai prestatori di servizi di pagamento di condividere tra loro le informazioni relative alle frodi tramite piattaforme informatiche dedicate; (ii) rafforzare le regole in materia di *strong customer authentication*; (iii) rendere obbligatorio per tutti i bonifici un sistema di verifica della corrispondenza tra il numero IBAN inserito e il nome del beneficiario del pagamento[88], e rafforzare i diritti di rimborso dei consumatori vittime di frodi; (iv) migliorare i presidi a tutela dei consumatori, ad esempio accelerando il pagamento dei fondi bloccati non utilizzati su carte di pagamento e prevedendo che l'importo bloccato sia proporzionato all'importo finale previsto; e fornendo informazioni più trasparenti sulle spese relative alle operazioni all'ATM; (vi) garantire un *level playing field* tra prestatori di servizi di pagamento bancari e non bancari, ad esempio con riferimento all'accesso ai sistemi di pagamento dell'UE; (vii) migliorare il funzionamento dell'*open banking*; (viii) migliorare la disponibilità di contante anche in zone periferiche, consentendo ai rivenditori di beni e servizi di permettere il prelievo di contante ai clienti senza richiedere un acquisto.

Per quanto riguarda la PSD3, essa mira a unificare il quadro stabilito dalla PSD2 con quello della direttiva sulla moneta elettronica (direttiva 2009/110/CE, EMD2) al fine di superare le difficoltà pratiche riscontrate dalle autorità nel delineare chiaramente

[87] In dettaglio, la Commissione ha presentato: (i) una proposta di regolamento volta a definire il quadro giuridico e gli elementi essenziali dell'euro digitale, che, una volta adottato dal Parlamento europeo e dal Consiglio, consentirebbe alla Banca centrale europea di introdurre un euro digitale ampiamente utilizzabile e disponibile, fermo restando che spetterà in ultima analisi a quest'ultima decidere se e quando emettere l'euro digitale; e (ii) una proposta legislativa sul corso legale del contante in euro per salvaguardare il ruolo del contante, garantire che sia ampiamente accettato come mezzo di pagamento e rimanga facilmente accessibile per i cittadini e le imprese in tutta l'area dell'euro. I testi delle proposte legislative sono disponibili al seguente indirizzo: https://finance.ec.europa.eu/publications/digital-euro-package_en.

[88] Tale misura prevista nella proposta di regolamento sui pagamenti istantanei, viene sostanzialmente estesa a tutti i bonifici nell'UE.

i due regimi e nel distinguere i servizi di moneta elettronica da quelli di pagamento offerti dagli istituti di pagamento. Questa nuova direttiva propone un singolo regime di autorizzazione per gli istituti di pagamento, che potranno quindi svolgere servizi di pagamento o di moneta elettronica ed elimina sostanzialmente la figura dell'istituto della moneta elettronica. Le procedure per la richiesta dell'autorizzazione restano per lo più invariate rispetto alla PSD2. Pressoché invariate risultano altresì le disposizioni relative agli agenti, alle filiali e all'*outsourcing*, nonché quelle sulla prestazione transfrontaliera di servizi da parte degli istituti di pagamento e sulla vigilanza di tali servizi. La PSD3 prevede un regime di *grandfathering* per le autorizzazioni di istituti di pagamento già esistenti e istituti di moneta elettronica a condizione che la domanda di autorizzazione ai sensi della presente direttiva sia presentata entro 24 mesi dalla sua entrata in vigore.

In merito *all'open finance*, la proposta di regolamento richiede ai soggetti regolati di condividere un *set* più ampio di dati finanziari rispetto all'*open banking,* e sottopone tale condivisione ad una regolamentazione parzialmente diversa innovativa rispetto a quella della PSD2 per i dati bancari. In particolare, i dati che dovranno essere condivisi, su richiesta del cliente, comprendono: i dati relativi a contratti di credito ipotecario, prestiti e conti, ad eccezione dei conti di pagamento, che rimangono soggetti alle regole in materia di *open banking*; investimenti in strumenti finanziari, prodotti di investimento assicurativi, *crypto-asset*, beni immobili e altre attività finanziarie; i dati raccolti ai fini dell'esecuzione della valutazione di appropriatezza e adeguatezza ai sensi dell'articolo 25 di MiFID; prodotti pensionistici; assicurazioni non vita, ad eccezione di alcune tipologie particolarmente sensibili per il loro legame con la salute del cliente.[89]

Data la natura ed estensione di tali dati, i soggetti cui si applicherà il regolamento, in quanto titolari dei dati, sono banche, istituti di pagamento, istituti di moneta elettronica, imprese di investimento, fornitori di servizi di crypto-asset, emittenti di *token* collegati ad attività, gestori di FIA, gestori di OICVM, imprese di assicurazione, intermediari assicurativi, istituti di previdenza professionale, agenzie di *rating* del credito, fornitori di servizi di *crowdfunding* e fornitori di PEPP[90].

La condivisione sarà permessa solo a favore di soggetti appartenenti a queste categorie, cui si aggiunge una nuova tipologia di soggetto regolato, il cd. "*financial*

[89] Cfr. CHIOMENTI, «*Servizi di pagamento e Open finance: le proposte dalla Commissione europea*», giugno 2023.
[90] *Ibidem.*

*information service provider* (FISP)[91]" per il quale è previsto un regime autorizzatorio *ad hoc*.

Per la condivisione dei dati dei clienti, per la quale la proposta di regolamento prevede lo sviluppo di *standard* comuni e la creazione di interfacce tecniche, i titolari dei dati avranno diritto a un compenso ragionevole da parte degli utilizzatori, in linea con i principi generali della condivisione dei dati tra imprese (B2B) stabiliti nella proposta europea di Legge sui dati[92]. Nel caso in cui l'utilizzatore dei dati sia una PMI (ad esempio una piccola impresa FinTech), l'eventuale compenso non dovrà superare i costi direttamente sostenuti per l'accesso ai dati.

Come è stato evidenziato precedentemente, i progressi tecnologici aggiungono valore ai prodotti e servizi di pagamento, ma ne aumentano anche il rischio. Tale rischiosità nasce da nuovi tipi di asimmetrie nei pagamenti digitalizzati. Il termine "asimmetria" può descrivere vari rischi di sicurezza legati all'ascesa delle tecnologie *disruptive* nei pagamenti, così come ambiguità concettuali o lacune normative correlate.

La legislazione dovrebbe identificare tali nuove asimmetrie e fornire soluzioni appropriate. La PSD2 affronta asimmetrie derivanti dall'uso crescente di terze parti nell'esecuzione dei pagamenti.

Infatti, la direttiva ha contribuito a creare condizioni di parità per i fornitori di servizi di pagamento nell'era digitale e ha promosso la sicurezza dei pagamenti digitali prevenendo l'abuso dei dati dei consumatori. Tuttavia, il mercato e la tecnologia hanno continuato a svilupparsi parallelamente all'implementazione della PSD2 e sono emerse nuove asimmetrie.

## 5. PSD2 e MiCAR

Un tema cruciale è l'ascesa dei *crypto-asset*, che sono supportati dalla crittografia e dalle tecnologie di registro distribuito, non emessi o garantiti da un'autorità pubblica e sfruttabili in varie funzioni economiche. Nell'UE, i *crypto-asset* sono principalmente regolamentati dal MiCAR.

[91] Cfr. S. HANSEN, «*How Will Open Finance and the Financial Data Access Regulation Impact the Financial Sector?*», 3 agosto 2023. https://www.ey.com/en_be/financial-services/how-will-open-finance-and-financial-data-access-regulation-impact-financial-sector.

[92] «*Proposta di regolamento del parlamento europeo e del consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati)*», (COM/2022/68), (2022), https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=COM%3A2022%3A68%3AFIN.

La PSD2 e il MiCAR promuovono obiettivi simili, in quanto entrambi mirano a stabilire una base legale ad hoc per i nuovi attori del mercato[93], adottare un approccio pro-competitivo[94] ed aumentare la fiducia dei consumatori e l'integrità del mercato[95]. Tuttavia, PSD2 e MiCAR si sovrappongono marginalmente, quando si considerano i "*funds*" e quando si affronta il trattamento legislativo dei nuovi attori del mercato, in particolare dei fornitori di servizi di *crypto-asset* (CASP). In relazione al primo punto, è opportuno notare che l'EBA ha messo in guardia su nuovi formati di *crypto-asset* che corrispondono ampiamente alla definizione di e-money fornita dalla Seconda Direttiva sulla moneta Elettronica (EMD2)[96].

Se una società eseguisse "servizi di pagamento" con un *crypto-asset* che si qualifica come *e-money* utilizzando la tecnologia dei registri distribuiti, tale attività rientrerebbe nell'ambito della PSD2 in virtù del fatto di essere "*funds*". Una tale situazione porterebbe a una definizione incoerente dei *crypto-asset* come "*funds*"[97], il che risulterebbe problematico soprattutto per quanto riguarda gli *asset reference token* (ART) e gli *e-money token* (EMT). L'attrattiva dei pagamenti degli ART e degli EMT dipenderà dai meccanismi di stabilizzazione[98], ma sarebbe auspicabile un migliore coordinamento tra PSD2 e MiCAR nella definizione di "*funds*" Inoltre, passando all'analisi delle asimmetrie derivanti dal trattamento legislativo dei CASP, se quest'ultimo stipula un contratto con un beneficiario per accettare *crypto-asset* (diversi dagli EMT), dovrebbe rispettare le stesse regole sulla protezione dei consumatori previste dalla PSD2 per i fornitori di servizi di pagamento. Tuttavia, le disposizioni della PSD2 e del MiCAR sulla protezione dei consumatori non sono sovrapponibili. Pertanto, sarebbe necessario autorizzare il CASP secondo il regime PSD2, o designare un fornitore di servizi di pagamento autorizzato PSD2. Inoltre, sarebbe necessaria anche una maggiore chiarezza riguardo alla natura dell'attività dei CASP[99]. Alla luce di quanto

[93] PSD2, Recitals, p. 6; MiCAR, Recitals, p. 1
[94] PSD2, Recitals, p. 67; MiCAR, Recitals, p. 5.
[95] PSD2, Recitals, pp. 4-6; MiCAR, Recitals, p. 5.
[96] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L 267.
[97] T. VAN DER LINDEN E T. SHIRAZI, «*Markets in Crypto-Assets Regulation: Does It Provide Legal Certainty and Increase Adoption of Crypto-Assets?*», *Financial Innovation* 9, fasc. 1 (10 gennaio 2023): 22.
[98] G. GIMIGLIANO, «*Payment Tokens and the Path Towards MiCA*», (2022) 8(1) The Italian Journal 367.
[99] EUROPEAN COMMISSION. DIRECTORATE GENERAL FOR FINANCIAL STABILITY, FINANCIAL SERVICES AND CAPITAL MARKETS UNION., VVA., E CEPS., «*A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2* ». (LU: Publications Office, 2023).

sopra, è auspicabile un intervento che migliori il coordinamento tra la direttiva PSD2 ed il regolamento MiCAR.

Prima dell'approvazione della PSD3 ci sono ancora degli ostacoli da superare. La mancanza di piena armonizzazione e completa applicazione delle norme tra gli Stati membri, rappresenta un tassello fondamentale per completare l'evoluzione normativa, infatti, l'ambito dei servizi di pagamento deve ancora essere pienamente allineato con altre politiche e legislazioni dell'UE. In particolare, al Regolamento Generale sulla Protezione dei Dati (GDPR), alla Direttiva sulla moneta Elettronica (EMD2) e il Regolamento MiCA. Inoltre, il ruolo dei nuovi *incumbents* (incluse le *BigTech* e i prestatori di servizi in materia di *crypto-asset*) nel settore dei pagamenti deve essere ancora chiarito. Appare importante sottolineare che a causa delle infrastrutture tecnologiche sottostanti, non è possibile prospettare una regolamentazione futura con la stessa mentalità che ha guidato il legislatore in passato. Come sottolineato dal Vicedirettore generale della Banca d'Italia Piero Cipollone: «*Penso che dovremmo prima di tutto comprendere le profonde implicazioni del nuovo ambiente tecnologico; per me, la caratteristica più sorprendente è che la catena di approvvigionamento di un servizio di pagamento viene sempre più frammentata tra attori specializzati e interdipendenti coinvolti nella struttura creata dalla tecnologia, anche in assenza di qualsiasi rapporto contrattuale. Per rendere chiaro ciò che sto cercando di dire, ricordiamoci che prima che la PSD2 entrasse in vigore, i principali attori nel campo dei servizi di pagamento erano PSP tradizionali (banche, istituzioni di denaro elettronico e istituzioni di pagamento) e le regolamentazioni erano incentrate su queste entità. La PSD2 ha contribuito a mettere fine all'esclusività del rapporto banca-cliente; permette a nuovi player come i Terzi Fornitori di Servizi (TPP) di offrire nuovi servizi ai loro clienti, ovvero i servizi di open banking, senza avere alcun rapporto contrattuale con i fornitori di servizi di pagamento sui cui questi clienti detengono i loro risparmi. è la "legge dell'API" che regola i rapporti tra parti che non si conoscono tra loro e che possono fidarsi l'uno dell'altro solo grazie alla garanzia digitale offerta dagli standard tecnologici: questa è anche la strada che porterà l'open banking verso l'open finance. Queste interdipendenze tecnologiche saranno altrettanto valide per le soluzioni di pagamento e i servizi finanziari sviluppati grazie all'utilizzo della tecnologia DLT. In questo contesto, il ruolo degli intermediari è destinato a diminuire, se non a scomparire del tutto, a beneficio di relazioni completamente automatizzate tra parti sconosciute ma comunque interconnesse. Inoltre, questo implica anche che dobbiamo riconsiderare il*

*nostro approccio regolamentare e superare la domanda su cosa dovremmo regolamentare. Infatti, sarà sempre più difficile, se non impossibile, identificare chi fa cosa; le soluzioni di pagamento e i servizi finanziari saranno forniti da una moltitudine di attori specializzati che, uniti dalla tecnologia, parteciperanno all'offerta di un singolo servizio. Inoltre, dato che questi attori non saranno necessariamente connessi da rapporti contrattuali, diventerà impossibile identificare chi ha la responsabilità ultima del servizio fornito al cliente finale. In questo contesto, sarà impossibile continuare a regolamentare come abbiamo fatto finora. Ma come dovremmo procedere? Penso che la strada da percorrere sia quella di concentrarsi sulla regolamentazione delle attività piuttosto che delle entità. Questo è l'approccio che l'UE ha adottato per i cripto-asset e che ha portato all'adozione del MiCAR; in questo contesto, il legislatore dell'UE ha deciso di non considerare le differenze tra chi fa cosa ma piuttosto di concentrarsi sulle attività svolte. Quindi, la mia risposta è: dovremmo regolamentare le attività.*»[100].

Appare quindi fondamentale riflettere sul nuovo paradigma tecnologico che si auspica nella PSD3; il tradizionale approccio di vigilanza e supervisione, che postula responsabilità chiaramente riconducibili a specifiche entità, sembrerebbe non più adatto a rispondere alle sfide poste dal nuovo ecosistema frammentato di attori.

Questo approccio è in linea con il nuovo quadro di riferimento dell'Eurosistema per la sorveglianza degli strumenti, schemi e dispositivi di pagamento elettronici (PISA)[101], applicabile dal novembre 2022, che è fondamentale perché introduce due novità significative. Innanzitutto, supera la nozione tradizionale di "trasferimento di fondi", abbracciando invece quella di "trasferimento di valore", estendendo così l'ambito di sorveglianza ai *token* di pagamento digitali. Altrettanto fondamentale risulta quindi rivedere la nozione di neutralità tecnologica, applicandola ai nuovi eterogenei servizi e attori del mercato.

In conclusione, il settore dei pagamenti al dettaglio è un incubatore di innovazione. Le banche centrali e le autorità di vigilanza possono svolgere un ruolo chiave nel garantire che le esternalità positive dell'innovazione vadano a beneficio sia dei consumatori che delle imprese[102].

---

[100] P. CIPOLLONE, «*Towards PSD3: The Dynamics of Digitalized Payment Systems*», aprile 2023.
[101] EUROPEAN CENTRAL BANK, «*Eurosystem Oversight Framework for Electronic Payment Instruments, Schemes and Arrangements*», novembre 2021, https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf.
[102] DIRITTO BANCARIO, «Verso la PSD3: la posizione di Banca d'Italia», *DB*, 17 aprile 2023, https://www.dirittobancario.it/art/verso-la-psd3-la-posizione-di-banca-ditalia/.

# Capitolo 2 – Il caso FTX e il fenomeno del nuovo *shadowbanking*

SOMMARIO: 1. Cripto-attività, sistemi di custodia. – 1.1 Introduzione ai fondamenti della DLT. – 1.2 Inquadramento tecnico giuridico degli *smart-contracts*. – 1.3 Aspetti tecnici e giuridici dei *token* alla base delle cripto-attività. – 1.4 Analisi delle definizioni delle autorità nel contesto delle cripto-attività. – 1.5 Disamina delle categorie di cripto-attività: dall'impatto giuridico alle considerazioni normative. – 1.6 Sistemi di custodia. – 2. CEX e DEX. – 2.1 Differenze operative tra *Centralized Exchange* (CEX) e *Decentralized Exchange* (DEX) nel contesto *FinTech.* – 2.2 Nozione di "*exchange*" nel quadro normativo UE. – 3. Il caso FTX: dalle origini al declino - analisi delle fasi cruciali. – 3.1 FTX e Alameda Research: la nascita di un gigante delle criptovalute. – 3.2 Il Tracollo di FTX, le vicende che hanno portato al fallimento. – 3.3 FTX: un esame dettagliato delle cause del collasso e punti di contatto con le esternalità tipiche della finanza tradizionale. – 4. sfide regolamentari nel settore delle cripto-attività: analisi empirica sui rischi sistemici e il fenomeno dello *shadow banking.* – 4.1 Interconnessioni finanziarie: analisi dei rischi e lezioni dal "*crypto-winter*". – 4.2 Rischi sistemici nelle cripto-attività: uno sguardo dettagliato alle sfide regolamentari nell'ecosistema *FinTech.* – 4.3 *FinTech*, l'illusione della decentralizzazione. – 4.4 *Governance* e trasparenza: prospettive della regolamentazione finanziaria per un mercato *crypto* affidabile.

## 1. Crypto-attività, sistemi di custodia

### 1.1 Introduzione ai fondamenti della DLT

Le innovazioni tecnologiche rivolte al mondo finanziario sono state nel precedente capitolo identificate come *Fintech*. Il settore dei servizi finanziari ha mostrato un'ampia predisposizione verso le emergenti tecnologie; in effetti, sono rari i servizi che non hanno subito una "trasformazione" dal punto di vista tecnologico. Nel dominio *Fintech*, l'innovazione tecnologica introduce nuovi schemi organizzativi dei

servizi d'investimento, dove il rapporto tra intermediari e investitori si caratterizza per una crescente sostituzione dell'intervento umano nei processi di scelta mediante l'impiego di algoritmi. Come si è visto, le soluzioni informatiche, sia *hardware* che *software*, possono rendere automatici i processi decisionali, delegando all'apparato non solo l'esecuzione, ma, anche il decidere di intraprendere un'azione, attraverso l'elaborazione dei dati.

Questo, però, non significa che il contributo decisionale umano sia assente; la capacità di programmazione, innata in ogni tecnologia basata su algoritmi, implica che l'individuo (dietro la macchina) stabilisca un insieme di direttive che definiscono preventivamente le risposte del dispositivo alla percezione di un dato *input*.

Mediante queste direttive, il software interviene emettendo comandi quando si verificano le condizioni predefinite. Pertanto, esiste indiscutibilmente un intervento decisionale umano, che serve da "orientamento" e "direzione" per le funzioni e le azioni che saranno poi effettivamente eseguite dal *software*.

Anche con le nuove soluzioni, la finanza convenzionale è ancora strutturata sul ruolo predominante dell'essere umano.

Nel settore finanziario, alcune soluzioni tecnologiche hanno conosciuto un'evoluzione sorprendentemente veloce in breve tempo; un chiaro esempio di ciò è rinvenibile nella proliferazione di piattaforme nel campo della finanza decentralizzata.

Nel contesto della Finanza Decentralizzata, l'interazione umana è, per così dire, ulteriormente minimizzata: l'individuo non eroga più direttamente il servizio, seppur supportato dalla tecnologia, ma si limita a codificare il *software* che fornisce il servizio.

Prima di analizzare cosa sia un *crypto-asset* è necessario effettuare una breve disamina dei tre elementi su cui si basa l'esistenza di una cripto-attività. L'infrastruttura su cui si basano è denominata "*distribuited ledger technology"* (DLT), secondo quanto stabilito nell'art. 8-ter del d.l. del 14 dicembre 2018, n. 135[103], che è stato successivamente convertito nella legge n. 12/2019 (il c.d. "Decreto

[103] art. 8-ter, l. n. 12/2019: «1. Si definiscono «tecnologie basate su registri distribuiti» le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili. 2. Si definisce "*smart contract*" un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli *smart contract* soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto.

semplificazioni"), il termine "tecnologie basate su registri distribuiti" si riferisce alle *«piattaforme e ai sistemi digitali tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili».* Questa definizione evidenzia le peculiarità di una DLT, pur non chiarendo il suo ruolo con riferimento alla nozione di criptovaluta. In realtà, la DLT rappresenta la base tecnica che rende possibile l'esistenza di una cripto-attività e, di conseguenza, anche la sua diffusione, vendita e scambio.

Sul piano tecnico, le Distributed Ledger Technologies (DLT) si identificano come architetture informatiche di natura distribuita. Si caratterizzano per essere composte da una rete di nodi di elaborazione, che interagiscono al fine di mantenere un registro condiviso. Quest'ultimo viene aggiornato attraverso specifici algoritmi di consenso che definiscono le regole per l'aggiornamento stesso. Le *blockchain* rappresentano una specifica categoria all'interno delle DLT, distinte per la loro struttura di registro in blocchi di transazioni (che sono le unità base di aggiornamento del registro), e per il modo in cui questi blocchi sono collegati. Questi collegamenti sono realizzati tramite funzioni crittografiche che consentono l'aggiunta di nuovi dati al registro, ma impediscono la modifica dei blocchi preesistenti.

La definizione di DLT come formulata dal regolamento europeo 2022/858 (DLT Pilot regime), è di una tecnologia che facilita l'operatività e l'utilizzo di registri distribuiti, dove un registro distribuito è inteso come un archivio di informazioni condivise tra diversi nodi di rete DLT. Questi nodi lavorano in sincronia attraverso un meccanismo di consenso.

Le DLT vengono classificate in base ai loro profili di accesso, sia per la lettura che per la scrittura. Le DLT pubbliche permettono l'accesso a chiunque per la consultazione delle informazioni nel registro, mentre quelle private limitano questo accesso solo a nodi autorizzati. Per quanto riguarda la scrittura, le DLT si differenziano in *permissionless* e *permissioned*[104], a seconda delle restrizioni imposte sulla

[104] la struttura di governo delle DLT *permissioned* è basata su processi di coordinamento esplicito tra i gestori, in linea con quanto avviene ad esempio nelle tradizionali strutture societarie. Più complessa è invece l'analisi della struttura di governo delle DLT *permissionless*, in cui alcuni processi possono

partecipazione al meccanismo di consenso, che è fondamentale per l'aggiornamento dello stato del registro[105]. Una DLT è essenzialmente l'infrastruttura tecnologica che permette la registrazione, lo scambio e l'offerta di *token*, oltre a facilitare l'implementazione degli *smart contract*. Il suo ruolo principale è quello di agire come un registro che detiene tutte le caratteristiche legate ad una specifica cripto-attività, inclusi, ad esempio, la quantità e la natura della stessa, gli individui che le hanno acquisite e ogni successivo trasferimento o transazione riguardante una determinata cripto-attività.

Dal punto di vista operativo, una DLT consente *«la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia, verificabili da ciascun partecipante, non alterabili e non modificabili»*.

Di norma, le informazioni racchiuse in una DLT sono visibili pubblicamente; la trasparenza è appunto un'altra qualità essenziale di un sistema DLT[106]. Questa trasparenza rende possibile a chiunque visionare la cronologia di tutte le informazioni salvate nel corso del tempo e analizzare ogni registrazione, favorendo l'accessibilità del registro e il controllo diffuso da parte di tutti gli interessati. Funzione questa che, se utilizzata per un sistema di criptovalute, consente di ricostruire tutte le transazioni effettuate nel tempo. L'apertura e la stabilità fanno della DLT una tecnologia estremamente solida, il che la rende idonea anche per transazioni economicamente rilevanti, grazie alla fiducia che gli utenti ripongono in essa, anche in assenza di un "ente centrale" che supervisioni le operazioni di registrazione o ne assicuri la corretta esecuzione[107].

---

essere regolati, a vario livello, dalla governance algoritmica, detta anche "*on-chain*". La governance *on-chain* si distingue da quella "*off-chain*" in quanto automatizza le funzioni di governo.

[105] BANCA D'ITALIA, «*La governance delle blockchain e di sistemi basati sulla tecnologia dei registri distribuiti*», n 773, giugno 2023.

[106] Sul punto è necessario chiarire che la trasparenza garantita da una rete DLT può essere assoluta o relativa a seconda che la partecipazione al sistema sia aperta a chiunque o solo ad alcuni soggetti determinati. Nel primo caso si parlerà di DLT *permissionless*, in quanto non è necessario un preventivo permesso per aderire al sistema. Nel secondo, invece, avremo una DLT *permissioned*, ovvero un sistema DLT in cui tutti i partecipanti sono stati preventivamente accettati e la cui partecipazione è, dunque, ristretta a un numero specifico di soggetti. Ai concetti di DLT *permissionless* e *permissioned* devono poi essere affiancati quelli di DLT pubbliche e private. Nonostante l'esistenza di parziali sovrapposizioni fra le caratteristiche di queste reti, è comunque possibile definire come private le DLT appartenenti a un ente o una organizzazione ben precisa; le DLT pubbliche, di converso, non avranno alcun soggetto di "appartenenza". Per maggiori approfondi- menti sull'argomento e sulle differenze fra queste quattro categorie, in R. BATTAGLINI, M. T. GIORDANO, *«Blockchain e Smart Contract»,* Milano, 2019, p. 51 e ss.

[107] R. LENER, G. CARRARO et al., *«FINTECH: DIRITTO, TECNOLOGIA E FINANZA»* (Minerva Bancaria, 2018.

Gli elementi tecnici che rendono un'infrastruttura digitale sia stabile che aperta sono la decentralizzazione e la crittografia. Nelle DLT maggiormente diffuse, la crittografia interviene in due fasi fondamentali. La prima fase si verifica quando un individuo realizza una transazione, cioè movimenta le proprie cripto-attività. Attraverso specifici programmi, ogni operazione di trasferimento è "autenticata" usando un sistema di chiavi crittografiche asimmetriche, permettendo di associare un'azione al soggetto che l'ha eseguita[108]. La seconda fase riguarda la convalida delle transazioni suddette.

## 1.2 Inquadramento tecnico-giuridico degli *Smart Contract*

Il secondo elemento alla base delle cripto-attività è la nozione di *smart contract*[109].

L'emergere di nuove *blockchain*, ha ampliato le capacità che una DLT può offrire, beneficiando dell'immensa capacità di calcolo condivisa. Di conseguenza, sono state introdotte DLT capaci di svolgere compiti ancor più sofisticati rispetto alla semplice registrazione di informazioni, mediante l'opportunità di utilizzare la potenza di calcolo dei *computer* partecipanti alla rete per processare specifici *software* chiamati appunto *smart contract*[110].

Sebbene generalmente si tenda a definire questo strumento come una semplice trasposizione in codice informatico di un contratto, questi non dovrebbero essere riduttivamente etichettati come "contratti intelligenti". In realtà, uno *smart contract* è uno strumento tecnologico che facilita l'attuazione automatizzata di processi

[108] L'identificazione avviene seguendo il criterio secondo il quale ogni individuo ha una chiave pubblica accessibile a tutti, che conferma che la transazione è stata autenticata con la chiave privata, mantenuta riservata, del soggetto disponente. Infatti, ad una specifica chiave privata corrisponde esclusivamente una chiave pubblica, una transazione segnata con una certa chiave privata può essere stata eseguita unicamente dal possessore della chiave pubblica corrispondente. L'uso di chiavi crittografate garantisce che ogni partecipante di una DLT possa essere riconosciuto tramite una sequenza numerica. Questo particolare consente di eseguire operazioni che implicano lo scambio di cripto-attività (anche di grande valore) mantenendo una forma di "semi-anonimato". Questo aspetto ha presumibilmente incentivato l'adozione delle prime cripto-attività per scopi non leciti.

[109] La creazione del concetto di "*smart contract*" è da ricondurre Nick Szabo, il quale nel 1994 scrisse: «uno *smart contract* è un protocollo di transazione computerizzato che esegue i termini di un contratto. Gli obiettivi generali del disegno dello *smart contract* sono il soddisfacimento di condizioni contrattuali comuni (come, ad esempio, i termini di pagamento, i privilegi, la riservatezza e anche l'esecuzione), la riduzione al minimo delle eccezioni sia dannose che accidentali e la minimizzazione della necessità di intermediari fiduciari. Gli obiettivi economici correlati includono l'abbassamento dei costi di perdita a causa di frodi, di arbitrato, di esecuzione e degli altri costi di transazione» N. SZABO, «*Smart Contracts*», 1994, in szabo.best.vwh.net.

[110] M. NICOTRA, *«Diritto della Blockchain, Intelligenza Artificiale e IoT»* (Ipsoa, 2018).

all'interno di una DLT, operando in modo autonomo rispetto a chi lo ha programmato o agli altri membri della rete[111].

Da questa prospettiva, si comprende meglio il motivo per cui la definizione normativa di "*smart contract*", come delineata dall'art. 8-*ter* del Decreto Semplificazioni, sottolinea maggiormente la loro natura di *software* piuttosto che quella di contratti[112]. Gli *smart contract*, infatti, sono applicazioni che operano grazie a un *computer* decentralizzato e virtuale, reso possibile dalla capacità computazionale offerta dai partecipanti alla rete[113]. Data questa distribuzione e gestione collettiva, una volta che uno *smart contract* è stato attivato, non è più possibile *ad nutum* impedirne l'esecuzione[114].

Va sottolineato, come si è detto, che una volta registrato un dato su una DLT, esso non può essere alterato.

La fondamentale proprietà di inalterabilità delle informazioni salvate su una DLT si estende quindi anche agli *smart contract* realizzati su di essa[115]. Due delle più importanti caratteristiche di uno *smart contract* sono, dunque, l'immutabilità e l'interminabilità. È però scorretto sostenere l'impossibilità *assoluta* di interrompere il funzionamento di uno *smart contract* lanciato su una *blockchain* qualunque siano le previsioni contenute al suo interno. Sarà però necessario ottenere il consenso alla modifica da parte della maggioranza dei partecipanti all'intera rete. Questa operazione prende il nome di "*fork*" in quanto ha come risultato un vero e proprio sdoppiamento

---

[111] S. L. FURNARI, «*Validità e caratteristiche degli smart contract e possibili usi nel settore bancario finanziario* in E. CORAPI - R. LENER (a cura di), *I diversi settori del Fintech. Problemi e prospettive*, *2019*», 2019, 89–110.

[112] *Cit.* Art. 8 ter. decreto-legge 21 giugno 2022, n. 73: "Tecnologie basate su registri distribuiti e smart contract" 1. Si definiscono «tecnologie basate su registri distribuiti» le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili. 2. Si definisce «smart contract» un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o piu' parti sulla base di effetti predefiniti dalle stesse. Gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto. 3. La memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'articolo 41 del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014.

[113] M. L. PERUGINI, P. DAL CHECCO, «*Introduzione Agli Smart Contract (Introduction to Smart Contract)*», SSRN Scholarly Paper (Rochester, NY, 8 dicembre 2015), https://doi.org/10.2139/ssrn.2729545.

[114] M. RASKIN, «*The Law and Legality of Smart Contracts*», SSRN Scholarly Paper (Rochester, NY, 22 settembre 2016), https://doi.org/10.2139/ssrn.2842258.

[115] M. MAUGERI, «*Smart Contracts e disciplina dei contratti - Smart Contracts and Contract Law*» (Il Mulino, 2021).

della rete. Infatti, i soggetti che acconsentiranno alla modifica manterranno nella loro copia del *database* la "versione" modificata in cui il funzionamento dello *smart contract* è stato interrotto, mentre la versione originale resterà memorizzata nel computer dei partecipanti contrari alla modifica[116]. Chiarito cosa si intende per tecnologia basata su registri distribuiti e cosa sono e come funzionano gli *smart contract,* non rimane che descrivere l'ultimo elemento su cui si basa l'esistenza di una cripto-attività: il *token*.

## 1.3 Aspetti tecnici e giuridici dei *token* alla base delle cripto-attività

Tecnicamente, un *token* rappresenta una registrazione digitale su una DLT, assegnata a un certo soggetto che diviene pertanto il "possessore" del *token*. Detenendo questa specifica registrazione, il detentore del *token* può svolgere varie attività e ha associati certi diritti legati alla *blockchain* correlata o allo *smart contract* da cui è stato creato. Riflettendo sul *token* come una "mera scritturazione", si può approfondire il meccanismo di possesso di un *token,* e di come questa attività non necessiti di per sé dell'intermediazione di soggetti terzi che svolgano il ruolo di "depositari". L'unico elemento che può essere oggetto di deposito presso soggetti terzi (i c.d. *wallet service provider*[117]) è la chiave privata, la quale è necessaria per autenticare le operazioni relative ai *token*. Questa chiave, che è costituita da una combinazione di simboli, può

[116] Sebbene ciò non sia teoricamente impossibile (si veda fra tutti il caso "The DAO" in cui il *fork* ha generato uno sdoppiamento della rete Ethereum, con la nascita di Ethereum Classic) sembra molto difficile che ciò possa avvenire a seguito dell'intervento dell'autorità giudiziaria. Infatti, quando sono conosciuti e non eccessivamente numerosi, è probabile che i partecipanti a una DLT appartengano a paesi diversi. Una DLT, assicura standard di sicurezza così elevati che solo venendo a conoscenza della chiave privata di un determinato utente è possibile disporre delle criptoattività che questo detiene. Come recenti casi di cronaca hanno dimostrato, data l'inesistenza di un gestore centrale della rete, non esiste alcun modo, diverso da un *fork,* per spogliare il possessore dalla disponibilità di un bene senza conoscerne la chiave privata. In G. FINOCCHIARO «*Le cripto-valute come elementi patrimoniali assoggettabili alle pretese esecutive dei creditori*», Rivista di diritto processuale, 1, 2019.

[117] La denominazione "*wallet*" allude simbolicamente al luogo in cui le criptovalute vengono detenute. Si differenziano principalmente in due tipologie di *wallet*: i "*cold wallet"*, nei quali la chiave privata è conservata su un supporto tangibile e non connesso al web, come potrebbe essere un pezzo di carta; e gli *"hot wallet"* sono soluzioni digitali offerte da aziende terze, spesso indicate come *"wallet service provider",* che detengono la chiave privata per conto dell'utente. La distinzione fondamentale tra questi due metodi di custodia sta nel fatto che, con i *cold wallet*, se il supporto *offline* contenente la chiave privata viene perso e l'utente non riesce a ricordarla, il saldo e le criptovalute in esso contenute andranno irrimediabilmente perdute. Per gli *hot wallet*, invece, la dimenticanza della "*password*" del servizio non comporta la perdita delle criptovalute, poiché esistono modalità definite dal servizio stesso per recuperare la chiave. Naturalmente, questo comporta una maggiore vulnerabilità agli attacchi, dato che individui con intenzioni malevole potrebbero penetrare le protezioni del fornitore di servizi di *wallet* e sottrarre le chiavi private dallo stesso detenute.

essere conservata in diversi modi: ricordata, annotata, archiviata digitalmente o su una memoria esterna.

L'aspetto rivoluzionario di questi mezzi è la loro capacità di funzionare senza intermediari. Un *token* dà al suo detentore la capacità di usare i diritti ad esso collegati in totale indipendenza. Questa libertà è potenziata dalle caratteristiche di sicurezza delle DLT. Interagendo con gli *smart contract*, i *token* possono assicurare l'attuazione di servizi specifici, consolidando la fiducia tra il possessore del *token* e chi lo ha prodotto. I diritti concessi dai *token* sono ampiamente variabili e dipendono dalle esigenze del programmatore o della struttura che rilascia il *token*. Tali diritti possono includere il possesso di proprietà, l'accesso a servizi specializzati o la capacità di esercitare diritti economici o decisionali. Un *Token* può essere scambiato con semplicità e posseduto senza un intermediario. Questa semplicità contrasta con i metodi tradizionali di scambio, che spesso implicano costi o processi complicati, rendendo l'uso non conveniente per investimenti minori.

Descritta la natura del *token*, appare essenziale distinguere tra cripto-attività e *token* stessi. Utilizzando una similitudine, questa distinzione si avvicina a quella tra un titolo di credito e il suo supporto fisico. Infatti, come il supporto cartaceo è semplicemente il mezzo "fisico" e tecnico che incarna il "titolo" e autorizza l'esercizio dei diritti ad esso collegati, il *token* rappresenta il mezzo digitale e "virtuale" che, in combinazione con altri elementi come gli *smart contract* e la DLT, consente l'attivazione dei diritti assicurati da una cripto-attività. Ricapitolando, la presenza della cripto-attività, deriva: dalla DLT quale infrastruttura che ne permette l'esistenza materiale, dagli *smart contract* quali meccanismi che permettono a chi li conferisce l'esercizio dei diritti correlati e dai *token* come mezzi che permettono sempre il medesimo esercizio di diritti, ma dal punto di vista di chi li riceve[118].

In altre parole, una cripto-attività potrebbe essere descritta come una rappresentazione di diritti incorporati in un *token*, utilizzabili attraverso tecnologie basate su un registro distribuito e sostenute da uno o più *smart contract*.

[118] S. L. FURNARI, «*La finanza decentralizzata. Cripto-attività, protocolli, questioni giuridiche aperte*» (Minerva Bancaria), luglio 2023.

## 1.4 Analisi delle definizioni delle Autorità nel contesto delle cripto-attività

Malgrado le numerose proposte avanzate nel corso degli anni da varie autorità, al momento non esiste tuttavia né a livello nazionale né europeo, una definizione giuridica dettagliata di cripto-attività. Al contrario, le definizioni proposte dalle autorità nazionali ed europee presentano un grado di vaghezza che potrebbe ampliare eccessivamente l'ambito di applicazione di tali regolamenti, generando ambiguità nella loro implementazione.

Nel contesto nazionale, si possono citare gli approcci definitori della Banca d'Italia e della CONSOB. La Banca d'Italia ha approfondito le cripto-attività principalmente in relazione all'aspetto monetario e alle ripercussioni sulla stabilità finanziaria. L'Autorità ha inizialmente rilasciato diversi avvisi sui pericoli legati all'uso delle criptovalute[119] (anche se usando il termine più generico di "valute virtuali"[120]); in seguito ha discusso del tema nei suoi rapporti sulla stabilità finanziaria[121], culminando in una comunicazione specifica riguardo la finanza decentralizzata il 15 giugno 2022, nella quale l'Autorità definisce le cripto-attività come «*una rappresentazione digitale di valore o di diritti che possono essere emessi, trasferiti e memorizzati elettronicamente, utilizzando la tecnologia di registro distribuito o una tecnologia analoga*[122]», riprendendo chiaramente la definizione proposta dal Regolamento MiCA di cui si tratterà in seguito nel corso dell'elaborato. Più rilevanti invece sono gli interventi della CONSOB in materia. L'Autorità ha lanciato nel 2019 una consultazione pubblica sul fenomeno delle cripto-attività, pubblicando i risultati all'inizio del 2020. Uno degli obiettivi di tale consultazione era di stabilire una definizione di cripto-attività che includesse solamente quelle applicazioni al di fuori dell'ambito dei prodotti e strumenti finanziari.

La CONSOB ha sottolineato che per rispettare la gerarchia delle fonti normative, non poteva operare in contrapposizione a quanto già stabilito a livello europeo o nazionale.

---

[119] BANCA D'ITALIA*, «Avvertenza sull'utilizzo delle cosiddette "valute virtuali"*», 30 gennaio 2015, Roma.
[120] BANCA D'ITALIA, «*Avvertenza per i consumatori sui rischi delle valute virtuali da parte delle Autorità europee*», 19 marzo 2018, Roma.
[121] BANCA D'ITALIA, «*Rapporto sulla stabilità finanziaria n. 1 - 2018*»,
[122] BANCA D'ITALIA, «*Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività*».

Altre definizioni possono essere individuate nelle dichiarazioni rilasciate da varie autorità europee. L'ESMA, per esempio, classifica le cripto-attività come «*un'asset privato che si basa principalmente sulla crittografia e sulla Tecnologia a Registro Distribuito (DLT)»,* specificando inoltre che un «*crypto-asset non è emesso da una banca centrale»*[123]. e sottolinea altresì che quelle cripto-attività che non si adattano alle categorie legali esistenti, dovrebbero essere sottoposte a esame da parte del legislatore europeo a causa delle potenziali minacce per gli utenti[124].

L'*European Banking Authority* (EBA) non si discosta dalla definizione precedente, identificando le cripto-attività come «*asset che si appoggiano principalmente su crittografia e tecnologia di registro distribuito per il loro valore percepito o intrinseco, e che non sono garantiti o emessi da una banca centrale o da un'entità pubblica, e possono essere utilizzati come mezzo di scambio o per investimento o per accedere a un bene o servizio»*[125]

Basandosi su queste definizioni preliminari, il 9 giugno 2023, è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea, il testo del MICA, cioè il Regolamento (UE) 2023/1114 "*Market in Crypto Asset*", approvato in via definitiva dal Parlamento Europeo il 31 maggio 2023, e successivamente ratificato sia dal Parlamento Europeo che dal Consiglio. L'articolo 3, paragrafo 1, punto 5 del Regolamento MiCA definisce una cripto-attività come «*una rappresentazione digitale di un valore o di un diritto che può essere trasferito e memorizzato elettronicamente, utilizzando la tecnologia a registro distribuito o una tecnologia analoga*». Questa interpretazione differisce leggermente dalle definizioni dell'EBA e dell'ESMA e, a differenza della lettura proposta dalla CONSOB, non esclude che le cripto-attività siano classificabili come strumenti o prodotti finanziari. Nonostante sia più dettagliata delle altre menzionate, la definizione del Regolamento MiCA omette però di citare elementi chiave come *token* e *smart contract*, terminando con un riferimento generico a "tecnologie analoghe".

---

[123] ESMA, «*Advice on Initial Coin Offerings and Crypto-Assets*», 2019.

[124] «*Where crypto-assets do not qualify as financial instruments (or where they do not fall within the scope of other EU rules applicable to non-financial instruments such as the e-money directive as identified in the EBA's report and advice on crypto-assets), ESMA believes that the absence of applicable financial rules leaves consumers exposed to substantial risks. ESMA believes that EU policymakers should consider possible ways to address the risks in a proportionate manner*». L'ESMA riafferma espressamente il principio per cui le cripto-attività avente natura finanziaria sono soggette alle già esistenti norme europee, preoccupandosi comunque di non lasciare le 'altre' cripto-attività senza regolamentazione. ESMA, cit., p. 5.

[125] EBA, «*reports on crypto-assets*», 9 gennaio 2019.

## 1.5 Disamina delle Categorie di Cripto-attività: Dall'Impatto Giuridico alle Considerazioni Normative

Una volta definito cosa si intende con il termine cripto-attività è possibile procedere con la disamina della classificazione delle stesse in modo da comprenderne la natura giuridica.

La classificazione tradizionale[126], riconosciuta anche da alcune autorità europee[127], distingue tre tipi principali categorie di cripto-attività. La prima è quella delle criptovalute, ovvero le cripto-attività che non conferiscono al loro detentore particolari diritti ma che si prestano, in base alle regole che gestiscono la loro emissione, a essere utilizzate come corrispettivo di uno scambio di beni e servizi.

La seconda categoria sono gli *utility token*, che conferiscono al *tokenholder* diritti specifici legati a beni o servizi offerti da chi le emette. L'ultima è quella degli *investment token*, che conferiscono diritti economici o amministrativi nei confronti dell'emittente. Esiste anche una categoria di cripto-attività ibride che combinano caratteristiche delle categorie precedenti.

Le criptovalute sono utilizzate principalmente come mezzo di scambio di beni e servizi[128]. Pur svolgendo una funzione simile alla moneta, non hanno un riconoscimento ufficiale equivalente alla moneta tradizionale (moneta *fiat*[129]). Il mercato ha manifestato un notevole interesse per lo scambio di beni o servizi attraverso il loro impiego. Tale diffusione può essere facilmente ricondotta al fatto che questo particolare tipo di cripto-attività è "strutturalmente" capace di svolgere le principali

---

[126] P. HACKER, C. THOMALE, *«Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law»*, SSRN Scholarly Paper (Rochester, NY, 22 novembre 2017), https://doi.org/10.2139/ssrn.3075820.

[127] EBA: *Advice on Initial Coin Offerings and Crypto-Assets*, 2019, p. 6-7, in cui si dis- tingue fra: "*Payment/exchange/currency tokens*" definite anche come "*virtual currencies*", descritte come «*tokens for payment-type purposes*»; "*Investment tokens*" cui ci si riferisce in questi termini «'*investment' or 'security' tokens representing debt or equity claims on the issuer*»; e, infine, "*Utility tokens*" ovvero «'*utility' tokens used to provide access to applications or services (commonly involving DLT)*». Relativamente all'ESMA, cit, p. 8, «*investment-type' crypto-assets may have some profit rights attached, like equities, equity-like instruments or non-equity instruments. Others, so-called 'utility-type' crypto-assets, provide some 'utility' or consumption rights, e.g., the ability to use them to access or buy some of the services/products that the ecosystem in which they are built aims to offer. Others, so-called 'payment-type' crypto-assets, have no tangible value, except for the expectation they may serve as a means of exchange or payment to pay for goods or services that are external to the ecosystem in which they are built. Also, many have hybrid features or may evolve over time*.».

[128] Cfr. M. CIAN, «*La criptovaluta – alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*», 2019.

[129] *«Il termine "fiat" si relaziona con la mancanza di valore intrinseco della moneta, alla sua inconvertibilità e, dunque, alle norme di un singolo ordinamento che impongono di accettarla per l'adempimento delle obbligazioni*» in M. CIAN, C. SANDEI, *«Diritto del Fintech*» (Cedam, 2020).

funzioni tipiche della moneta, potendo fungere da unità di conto e da mezzo di pagamento. Si dubita, invece, del fatto che le criptovalute possano svolgere anche la terza funzione "tipica" della moneta, ovvero quella di fungere da riserva di valore[130], a causa dell'elevata volatilità di alcune fra le criptovalute più conosciute.

L'obiettivo fondamentale di ogni infrastruttura di valuta digitale è quello di consentire lo scambio di "valori" attraverso un sistema non centralizzato, ovvero un modello che elimini la necessità di un'entità centrale o di vari intermediari e che, allo stesso tempo, sia capace di rimanere inalterato a fronte di interferenze esterne.

Nel contesto delle valute digitali, il beneficio della minimizzazione degli intermediari si traduce in costi di transazione ridotti e non solo. Le valute digitali sono la prima (e forse la più diffusa) implementazione di un sistema decentralizzato capace di rappresentare un'unità di conto[131]. Gli attuali servizi proposti da istituti bancari o intermediari finanziari presuppongono sempre una figura centrale responsabile della gestione dei dati e degli aggiornamenti continui dei bilanci degli utenti. L'eliminazione di questa entità permette, infatti, di ridurre i rischi nonché i costi ricollegati agli azzardi morali di questi intermediari all'interno del mercato.

Nella categoria degli *utility token*, rientrano le cripto-attività che conferiscono al titolare il diritto ad ottenere una utilità completa, legato a un interesse di "consumo", rispetto ai prodotti o ai servizi proposti dall'ente emittente. In altre parole, chi prende parte a un'offerta pubblica di attività digitali (*Initial Coin Offering* o ICO) e ottiene un *utility token,* può utilizzarlo per ottenere una utilità concreta dal diritto ricevuto come l'ottenimento di un *asset* virtuale o la possibilità di utilizzare un servizio offerto dall'emittente. In questa prospettiva, chi acquisisce un *utility token* durante un'ICO è considerato come un consumatore o, più ampiamente, come un cliente dell'entità offerente.

La tecnologia sottostante alle cripto-attività e ai *token* ha permesso ulteriori sviluppi grazie alle applicazioni decentralizzate (*dApps*), le quali sono applicazioni *open-source* che funzionano in modo autonomo. La Finanza decentralizzata (*DeFi*), ad esempio, sfrutta la tecnologia per incentivare metodi alternativi basati sulla *blockchain* per servizi finanziari tipici della finanza tradizionale (*TradFi*).

L'adozione su larga scala delle valute digitali dipende in gran parte dalla capacità delle infrastrutture tecnologiche di mantenere un equilibrio tra efficienza, sicurezza e

[130] R. DE BONIS, M. I. VANGELISTI, *«La moneta. Dai buoni di omero ai Bitcoin»* (Il Mulino, 2019).
[131] S. CAPACCIOLI, *«Criptovalute e bitcoin: un'analisi giuridica»* (Giuffrè Francis Lefebvre, 2015).

*privacy*. È essenziale che gli utenti abbiano fiducia nelle piattaforme che utilizzano, sia per quanto riguarda la protezione dei loro dati personali, sia per la garanzia della sicurezza dei loro investimenti. Mentre il settore continua a maturare, è probabile che vedremo una crescente integrazione di funzionalità di sicurezza avanzate, così come la creazione di *standard* normativi più stringenti per garantire che queste piattaforme operino in modo etico e trasparente.

Infine, è fondamentale ricordare che, sebbene le valute digitali rappresentino una rivoluzione in termini di potenzialità e innovazione, esse portano con sé anche sfide e rischi. Gli utenti, gli investitori e le entità regolatrici devono collaborare per garantire che l'adozione di queste tecnologie avvenga in modo responsabile e sostenibile, mettendo sempre al primo posto gli interessi e la sicurezza dei consumatori.

La semplicità con cui questi strumenti possono essere scambiati ha sollevato questioni sulla necessità di introdurre normative per regolamentare l'emissione degli *utility token*, anche se, per natura, questi servono principalmente ai fini di consumo piuttosto che di investimento. Questo è quanto emerge dal documento di discussione pubblicato dalla CONSOB il 2 gennaio 2020, che sottolinea come, pur non potendo regolare direttamente le cripto-attività che rientrano nei prodotti o strumenti finanziari, potrebbe esserci una crescente attenzione verso la regolamentazione di tali strumenti in futuro. Anche la FINMA, (l'Autorità svizzera di vigilanza dei mercati), ha espresso il suo punto di vista sulla questione, suggerendo che certi *utility token*, che al momento della loro emissione non concedono all'acquirente l'uso diretto del servizio offerto, potrebbero necessitare di una regolamentazione[132]. L'argomento principale sostenuto dalla FINMA è che, in tale contesto, la capacità di scambiare liberamente questi *token* potrebbe prevalere sulla loro funzione principale come strumento di consumo. Infine, come si vedrà nel capitolo successivo, le preoccupazioni legate ai potenziali rischi associati alla negoziazione di *utility token* hanno spinto l'Unione Europea ad includere questa categoria nel Regolamento MiCA.

Nella categorizzazione delle cripto-attività, gli *investment token* emergono invece per il loro profilo spiccatamente finanziario e d'investimento, contrapponendosi a quelli di consumo. Pertanto, in questa nozione dovrebbero rientrare quei *token* che offrono al detentore diritti patrimoniali e/o diritti amministrativi verso l'impresa emittente, nonché le cripto-attività il cui valore è collegato a quello di un sottostante.

[132]FINMA, «*FINMA publishes ICO guidelines*», 2018.

Data la vasta gamma di funzionalità che un *investment token* può incarnare, è possibile suddividerli ulteriormente in sottocategorie. Ci sono, ad esempio, gli "*equity token*", che forniscono diritti simili a quelli di un azionista. Mentre i "*debt token*" possono essere visti come analoghi alle tradizionali obbligazioni. Alcuni di questi potrebbero dare al possessore una frazione dei guadagni futuri di una società o altri diritti.

Un altro termine frequentemente usato è "*security token*", che indica gli *investment token* con le caratteristiche dei tradizionali strumenti finanziari. Di qui proviene anche l'espressione "*security token offering*" (STO), che descrive l'introduzione al mercato di questi strumenti finanziari in formato digitale.

È evidente che gli *investment token* hanno molte somiglianze con i prodotti finanziari classici. In alcuni contesti, le differenze tra le due categorie possono essere minime, portando a regolamentazioni più rigide ed onerose rispetto, ad esempio, alle pure criptovalute o agli *utility token*.

Mentre la categoria degli *utility token* può generare incertezze normative, gli *investment token* mostrano una maggiore esigenza di regolamentazione. Questo potrebbe derivare dalla necessità di adeguare le leggi esistenti alle peculiarità della tokenizzazione o dalla sorveglianza degli operatori del settore di questi *asset*.

Diverse autorità di regolamentazione finanziaria condividono la visione che, se una cripto-attività rientrasse nella categoria degli strumenti finanziari, le leggi corrispondenti dovrebbero applicarsi indipendentemente dalla tecnologia sottostante in ossequio al principio di neutralità tecnologica. Questa posizione è stata inizialmente sostenuta dalla SEC negli USA nel 2017, attraverso un documento sul caso "The DAO"[133].

Dopo qualche tempo, anche le autorità europee hanno ribadito che le cripto-attività che corrispondono alla definizione europea di strumento finanziario dovrebbero essere sottoposte alle relative regolamentazioni tradizionali[134].

[133] US SECURITY EXCHANGE COMMISSION,*«Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*»,
https://www.sec.gov/files/litigation/investreport/34-81207.pdf.
[134] Vedi diffusamente *infra.*

## 1.6 Sistemi di Custodia

Per comprendere i vari sistemi di custodia delle cripto-attività è necessario soffermarsi sugli aspetti tecnologici, funzionali e procedurali. La custodia di cripto-attività come è stato già evidenziato, è basata sulla tecnologia DLT, in particolare sopra il "libro mastro" di riferimento, (la *blockchain),* sulla quale sono registrate tutte le transazioni ed i criteri con cui possono essere trasferite le cripto-attività.

Come è noto, la *blockchain* non è tendenzialmente modificabile, poiché per alterare la catena di blocchi sarebbe necessaria una quantità di energia (con conseguente dispendio economico) ed una capacità computazionale sostanzialmente utopistica.

La sicurezza delle singole transazioni è affidata alla crittografia asimmetrica, basata su una coppia di chiavi: una pubblica ed una privata. Le due chiavi sono algebricamente collegate e svolgono un ruolo complementare in un protocollo di firma digitale: la chiave privata è utilizzata per generare la firma digitale, la chiave pubblica è utilizzata da chiunque per verificare la genuinità della firma digitale prodotta dalla corrispondente chiave privata. Quest'ultima è fondamentale, poiché consente lo scambio e la spendibilità delle cripto-attività associate al *wallet.*

Le cripto-attività possono essere considerate come un bene al portatore: se si perde la chiave privata, tutte le attività associate al *wallet* andranno perse definitivamente. Come si avrà modo di vedere, i *centralized exchange* hanno grande successo, oltre che per l'elevata *user experience*, anche per la garanzia di una entità centrale che custodisca la chiave privata e fornisca delle *password* sostitutive che seguono le regole di recupero dei tradizionali *account* che conosciamo. Per le motivazioni sin qui esposte, possiamo suddividere i *wallet* in due macrocategorie: *cold wallet* (quando le informazioni riservate sono custodite *offline*) e *hot wallet* (quando le informazioni riservate sono custodite *online*)[135]. Sul punto ci sono opinioni contrastanti, che dividono i fruitori di queste nuove tecnologie; tra i puristi della decentralizzazione si sente spesso la frase: "*not your keys, not your coins*", per indicare che la gestione diretta delle chiavi private è l'unica garanzia di possesso reale; anche Peter Wuille, ad oggi il più rilevante sviluppatore del protocollo bitcoin, ha sostenuto

[135] P. MAZZOCCHI, «La Custodia Sicura Di Bitcoin», febbraio 2023, Il Sole 24 ore.

fermamente l'utilizzo dei *cold wallet*[136]. La centralità di questo servizio risiede nelle meccaniche proprie di funzionamento delle cripto-attività, poiché permette al prestatore, in possesso delle chiavi private del cliente, di firmare transazioni per suo conto e dunque "movimentare" gli *asset* depositati.

MiCA definisce il servizio come "la custodia o il controllo, per conto dei clienti, delle cripto-attività o dei mezzi di accesso a tali cripto-attività, se dal caso sotto forma di chiavi crittografiche private"[137].

Il servizio di custodia e amministrazione di cripto-attività per conto dei clienti è quello che, unitamente allo scambio delle cripto-attività con valuta corrente o altre cripto-attività, si è maggiormente diffuso nel mercato. Si può anche affermare che si tratta di uno dei servizi più problematici, sia per gli aspetti relativi alla confusione del patrimonio del prestatore con quello dei propri clienti, pratica emersa in occasione dei vari fallimenti che si sono verificati negli ultimi anni, sia per le vicende che hanno visto ingenti sottrazioni di fondi custoditi dai prestatori in conseguenza di vulnerabilità dei sistemi informatici da essi utilizzati, nonché scarsa trasparenza delle condizioni applicate nei confronti della clientela[138].

## *2. Centralized exchange* e *Decentralized exchange*

### *2.1* Differenze operative tra *Centralized Exchange* (CEX) e *Decentralized Exchange* (DEX) nel contesto *FinTech*

Nel campo della Finanza Decentralizzata, le attività di scambio di cripto-attività avvengono tipicamente attraverso due differenti "intermediari": i *centralized exchange* (CEX) e i *decentralized exchange* (DEX).

Entrambi consentono lo scambio di una cripto-attività con un'altra, a seconda delle scelte effettuate dal *tokenholder*. Tuttavia, esistono notevoli differenze operative tra loro che influiscono sulle regole applicabili.

---

[136] "*Proprietà e controllo non sono la stessa cosa. Non intendo solo in senso legale: sarei sorpreso se molta gente ritenesse che il possesso di qualcosa sia necessariamente collegato al suo controllo*" cfr. F. AMETRANO, «*La custodia sicura di Bitcoin: aspetti tecnologici, funzionali e regolamentari»,* 28 settembre 2021.

[137] MiCA, art 3, comma 1, n.17.

[138] M. NICOTRA, F. SARZANA, S. IPPOLITO, M. SIMBULA, «*Il MiCar, Guida al Regolamento Europeo sui mercati delle cripto»* 91-93 (Giuffrè Francis Lefebvre, 2023).

I CEX agiscono come un mercato regolamentato, proponendo due tipi di servizi: il servizio di "gestione" del mercato (e, di conseguenza, di scambio di cripto-attività) e quello di custodia delle stesse per conto dei *tokenholder*.

Il servizio di scambio è realizzato attraverso il metodo dell'*order book*. Un CEX raccoglie tutti gli ordini di acquisto e vendita di una specifica cripto-attività e ne favorisce l'incontro, effettuando anche il *settlement* di ogni ordine. L'incrocio tra domanda e offerta determina il prezzo di scambio della cripto-valuta in questione.

Nei CEX, in genere, lo scambio di cripto-attività non viene registrato volta per volta sulla DLT associata; questo permette un uso più efficiente del sistema dell'*order book*, ed una maggiore rapidità dell'operazione con costi di transazione ridotti.

Per intraprendere uno scambio, è necessario creare un *account* ed un conto sul CEX, dove sarà possibile depositare denaro tradizionale o altre cripto-attività per le operazioni di *trading*. I CEX, offrono anche un servizio di custodia delle cripto-attività. Questa attività determina una situazione di rischio, dovuta al fatto che il cliente non detiene le chiavi private dei *wallet* in cui le cripto-attività sono depositate. Tale metodologia di custodia è ciò che principalmente distingue i CEX dai DEX.

Al contrario dei primi, i DEX infatti, permettono al detentore di *token* di mantenere le proprie cripto-attività, operando in modalità "*non-custodial*".

Utilizzando un DEX, quindi, il cliente non concede la disponibilità delle proprie cripto-attività a un soggetto terzo, potendo usufruire ugualmente di un servizio di scambio particolarmente efficiente. Inoltre, i DEX raramente utilizzano il sistema dell'*order book*, e nei rari casi in cui viene utilizzato, esso non è altrettanto efficiente[139]; invece di essere gestite da sistemi informativi "centralizzati" del CEX, in un DEX le operazioni sono effettuate da *smart contract* e ciò comporta che ogni singola operazione venga registrata, ogni volta, sulla DLT correlata. La dinamica di un DEX si basa principalmente su uno (o più) *smart contract* che, autonomamente, amministrano il "mercato", garantendo che ogni operazione avvenga direttamente all'interno della DLT di riferimento. La registrazione diretta *on-chain* accresce così la sicurezza e minimizza potenziali rischi.

Gli *exchange* centralizzati, per motivi di efficienza e celerità nella gestione degli ordini, tendono a gestire alcuni procedimenti *on-chain*[140] (come quelli che attengono

[139] V. MOHAN, «*Automated market makers and decentralized exchanges: a DeFi primer*», *Financial Innovation* 8, fasc. 1 (14 febbraio 2022): 20, https://doi.org/10.1186/s40854-021-00314-5.

[140] "I processi *off-chain* sono soggetti a opacità, azzardo morale, conflitto di interessi dei partecipanti; i secondi (*on-chain*) sono trasparenti e verificabili, ma necessariamente più rigidi e "incompleti", nel senso che non sono in grado – per definizione – di includere processi decisionali non individuabili ex

al deposito di cripto-attività presso i conti gestiti dall'*exchange*), e a gestirne altri *off-chain* (come le procedure di *matching* degli ordini e della loro esecuzione)[141]. Questa distinzione rende l'*exchange* suscettibile di potenziali attacchi *hacker* che potrebbero interferire con i processi gestiti *off-chain* e perturbare l'operatività del sistema.

La differenza tra DEX e CEX può essere letta come un compromesso tra efficienza e sicurezza. I DEX, da un lato, sono ritenuti più sicuri poiché ogni transazione avviene sulla DLT e non c'è bisogno di confidare la chiave privata del proprio *wallet* a una terza parte (lo stesso *exchange* o un fornitore di servizi di portafoglio ad esso collegato). D'altro canto, queste peculiarità rendono il sistema decisamente più lento, poiché per considerare una transazione completamente finalizzata si deve attendere la conferma da parte dell'intera DLT di riferimento. Un'altra tematica importante riguardo la sicurezza dei DEX, pone l'attenzione sulle transazioni, le quali sono interamente gestite da *smart contract*, quindi, la supervisione sugli algoritmi utilizzati riveste una importanza fondamentale. Un errore nel sistema (*bug*) potrebbe permettere a chiunque di sfruttarlo a proprio vantaggio. In questo contesto, la trasparenza della DLT associata può essere vista sia come un vantaggio che come uno svantaggio. Mentre, grazie al cosiddetto "*wisdom of the crowd*"[142], una maggiore trasparenza garantirebbe la possibilità di segnalare, anche prima del lancio ufficiale, qualsiasi dubbio o problematica che qualsiasi "esperto" del settore possa riscontrare nel codice informatico utilizzato; al contrario, vi è la possibilità che qualche soggetto, invece di segnalare l'errore, possa utilizzare le proprie conoscenze per sfruttarlo a proprio favore[143].

Infine, mentre i CEX operano in modo simile ai mercati regolamentati, il funzionamento dei DEX presenta particolari sfide regolamentari[144]. Per comprendere meglio ciò, è essenziale esaminare i dettagli dei sistemi informatici che consentono a un DEX di operare.

---

ante. Inoltre, le decisioni assunte da sistemi di governance algoritmica potrebbero essere fonte di effetti automatizzati indesiderabili e potenzialmente non controllabili.", BANCA D'ITALIA (n. 94).

[141] S. L. FURNARI, «La finanza decentralizzata. Cripto-attività, protocolli, questioni giuridiche aperte» Minerva Bancaria, 2023.

[142] "La saggezza della folla (o intelligenza della folla) è una teoria sociologica secondo la quale una massa di individui inesperti sarebbe comunque in grado di fornire una risposta adeguata e valida a una domanda più di quanto non siano in grado di farlo gli esperti (purché questi, a loro volta, non costituiscano una "folla". In J. SUROWIECKI, *«La saggezza della folla»*, Fusi Orari,2007.

[143] N CARTER, *«Decentralized Finance: The Future of Crypto and Open Finance?»,* in *Open Banking*, a c. di L. JENG (Oxford University Press, 2022).

[144] N. P. VAN VALKENBURGH, «*There's No Such Thing as a Decentralized Exchange*»,The Block (3 ottobre 2020).

Il sistema di *smart contract* che nei DEX consente di effettuare gli scambi è noto con il nome *Automated Market Maker* (AMM)[145]. In via generale, i sistemi di AMM permettono ai DEX di favorire gli scambi grazie al contributo essenziale di altri utenti che, in maniera non professionale, forniscono la liquidità necessaria per permettere gli scambi[146]. Per fornire liquidità, ogni utente deposita coppie di cripto-attività, aventi il medesimo valore al momento del deposito, in c.d. *pool* di liquidità gestito da *smart contract.* L'esistenza di una specifica "coppia di liquidità" consente di effettuare uno scambio fra le due cripto-attività che costituiscono la coppia, senza la necessità di individuare, in uno specifico momento, un soggetto disposto a effettuare lo scambio.

Quando un individuo trasmette un ordine di scambio allo *smart contract*, il sistema prende in custodia la cripto-attività che l'utente desidera scambiare. Contemporaneamente, fornisce all'utente un valore equivalente dell'altra cripto-attività che fa parte di quella specifica coppia di scambio. Questa operazione non avviene a caso, ma è regolata da una precisa formula matematica codificata all'interno dello *smart contract*. La maggior parte degli *Automated Market Makers* (AMM) adotta un principio specifico: il valore complessivo delle cripto-attività in una coppia di liquidità deve essere costante[147].

Coloro che mettono a disposizione le loro cripto-attività, depositandole nei *pool* di liquidità, ricevono una porzione delle commissioni generate da ogni operazione di scambio. Questa distribuzione è proporzionale all'ammontare depositato da ogni utente. Molti DEX incoraggiano questo comportamento offrendo ai depositanti una ricompensa supplementare, spesso sotto forma di altre cripto-attività, molte delle quali sono emesse dallo stesso DEX (cd. *Yield farming*). Pertanto, i depositanti non solo beneficiano delle commissioni delle transazioni ma anche di ulteriori rendimenti grazie a queste ricompense. Gli algoritmi AMM hanno introdotto un nuovo modo di stabilire il prezzo delle cripto-attività. Mentre i tradizionali sistemi basati su *order book* determinano il prezzo attraverso il semplice incontro tra domanda e offerta, l'AMM integra le formule algebriche nei processi di determinazione dei prezzi. Ogni singolo

[145] DINGLE, SIMON, E S. BOYKEY SIDLEY, *«Beyond Bitcoin, Decentralised Finance and the End of Banks»*, 2022.
[146] A. ASPRIS, S. FOLIS, L. WANG, *«Decentralized exchanges: The "wild west" of cryptocurrency trading»*, International Review of Financial Analysis, 77 (1 ottobre 2021), https://doi.org/10.1016/j.irfa.2021.101845.
[147] V. MOHAN, «*Automated Market Makers and Decentralized Exchanges: A DeFi Primer*», SSRN (Rochester, NY, 30 ottobre 2020), https://doi.org/10.2139/ssrn.3722714.

scambio effettuato all'interno di una coppia di liquidità genera, infatti, un momentaneo disallineamento fra il prezzo di scambio rilevato all'interno di quel DEX e quello che è possibile rilevare in un CEX o in un altro DEX. Ciò permette di sfruttare questi disallineamenti per effettuare operazioni di *trading* prive di rischi che consentono, allo stesso tempo, di riallineare il quantitativo di cripto-attività presente all'interno di una specifica coppia di liquidità.

Il sistema strutturato con i *book* di negoziazione, non è diverso da quanto avviene in un mercato regolamentato o in un MTF. In altri casi il gestore consente, in via esclusiva o fuori dal *book* di negoziazione, la contrattazione diretta tra le parti (*direct trading platform*). Anche in questo caso è utile ricordare che modalità di negoziazione diretta tra le parti, al di fuori del "*book*", sono consentite anche sulle *trading venue* di strumenti finanziari (funzionalità "*request for quote* RFQ o gli ordini c.d. *crossing*)[148]. Meno diffuse invece sono le piattaforme come "*dealer type model*", in cui i terzi possono negoziare in via esclusiva con il *dealer*-gestore della piattaforma.

Nei sistemi multilaterali centralizzati, il *trading* è organizzato (sia nel caso di *book* di negoziazione che nel caso di *direct trading*) su una piattaforma separata dalla DLT e in genere fornita dal gestore del sistema medesimo.

L'esecuzione dei contratti avviene mediante una annotazione su un registro provvisorio predisposto dal gestore della piattaforma in vista poi di una eventuale registrazione sul registro DLT, a richiesta di chi risulti in un dato momento intestatario del *token* sul registro dell'*exchange*[149]. Quest'ultimo offre quindi, un servizio di "custodia".

In altre parole, gli *exchange* centralizzati potrebbero avere le medesime caratteristiche dei mercati tradizionali; tuttavia, ci sono alcuni caratteri radicalmente differenti. Nei mercati tradizionali regolamentati, per esempio, l'investitore non può accedere direttamente al mercato; chi intende comprare o vendere delle azioni è costretto a passare attraverso un soggetto terzo, il quale, da un lato deve prendere parte al sistema delle stanze di compensazione e garanzia per gestire il rischio di controparte e, dall'altro, dovrà indirizzare la stessa proposta di negoziazione verso il listino nel quale può avvenire la *best execution* dinamica.

[148] F. P. LOPS, C. MOTTI, «*La circolazione della ricchezza nell'era digitale*» (Pacini Editore, 2021).
[149] S. A. CERRATO, «*Negoziare in rete: appunti su contratti e realtà virtuale nell'era della digitalizzazione*», Diritto comunitario e degli scambi internazionali: *1/2, 2018*, 2018, 233–66, https://doi.org/10.1400/273571.

Nei CEX invece non avviene nessuno scambio reale di cripto-attività, infatti, il consumatore dopo essersi registrato ed aver aperto un conto di *trading* presso la piattaforma, potrà acquistare cripto-attività, le quali risulteranno nell'area riservata dell'*exchange*. Tuttavia, *il token* non è nella sua reale disponibilità, poiché le operazioni che avvengono sulla piattaforma centralizzata sono solo scritture contabili. Le cripto-attività rimangono, infatti, in possesso dell'*exchange* e ciò rappresenta una criticità che potrebbe comportare elevati rischi per l'investitore *retail* sia per quanto riguarda gli attacchi *hacker*, sia per quanto riguarda la *mala gestio* degli *exchange,* come la storia ci insegna [150].

Nei DEX, invece, il *trading* è organizzato direttamente sulla piattaforma DLT; i contratti vengono registrati volta per volta sul registro distribuito, neutralizzando i rischi di conflitti di interesse e di comportamenti opportunistici sopracitati. La tempestiva annotazione comporta però, costi maggiori.

Gli intermediari nel campo delle cripto-attività stanno guadagnando un ruolo sempre più rilevante nel mondo della Finanza Decentralizzata. Oltre alla gestione del mercato secondario, questi intermediari si stanno occupando anche del collocamento sul mercato primario, tramite la sempre maggiore diffusione delle IEO[151] e delle IDO[152].

---

[150] V. CARLINI, «*Dalle piattaforme di scambio ai token, essenziale conoscere»*, Finanza digitale #2/cripto, Il Sole 24 Ore, ottobre 2022.

[151] "*Initial exchange offering*: A differenza delle ICO, i *token* nelle offerte iniziali di scambio non vengono lanciati tramite la piattaforma di un progetto, ma tramite un *exchange* che fa da intermediario. Così, non sono solo coinvolti gli emittenti e gli investitori, ma ci sono piuttosto tre attori: gli emittenti, gli investitori e un exchange di di criptovalute. Come suggerisce il nome, una Initial Exchange Offering, prevede l'uso di un *exchange* di criptovalute per raccogliere fondi per un nuovo progetto. Il *trading* di *asset* è comune su queste piattaforme, ma generalmente avviene solo dopo che gli sviluppatori hanno raccolto fondi per avviare i propri progetti. Con una IEO, potenziali investitori possono comprare questi *asset* prima che siano disponibili sul mercato. Con l'aiuto dell'*exchange* che agevola la vendita di *token*, gli utenti registrati potranno comprare *token* prima che inizi il *trading* sul mercato libero."
Dato che la IEO è agevolata da un *exchange*, le *startup* che scelgono questa opzione dovranno essere serie in merito al loro *whitepaper*. Nella maggior parte dei casi, la proposta di IEO è sottoposta a un controllo rigoroso da parte dell'*exchange* coinvolto. In un certo senso, gli *exchange* mettono in gioco la loro reputazione per ogni IEO che decidono di offrire." «*Cos'è una Initial Exchange Offering (IEO)?*», BINANCE ACADEMY, https://academy.binance.com/it/articles/what-is-an-initial-exchange-offering-ieo.

[152] "Una IDO è una offerta di token attraverso un exchange decentralizzato (DEX). Le pool di liquidità (LP) svolgono un ruolo fondamentale durante una IDO creando liquidità in seguito alla vendita. Una tipica IDO consente agli utenti di bloccare dei fondi in cambio di nuovi token, durante l'evento di generazione di tale token. Alcuni dei fondi raccolti vengono quindi aggiunti insieme al nuovo token per creare una LP, prima di essere restituiti in un secondo momento al progetto. Le IDO forniscono ai progetti un modo semplice ed economico per distribuire i propri token. Una IDO utilizza un exchange decentralizzato (DEX) per facilitare la vendita del token. Un progetto crypto fornisce i propri token al DEX, gli utenti impegnano i propri fondi attraverso la piattaforma e il DEX completa la distribuzione e il trasferimento finali. Questi processi sono automatizzati e avvengono tramite degli smart contract scritti sulla *blockchain*.
Le regole e le fasi di una IDO dipendono dal DEX utilizzato, ma ci sono alcuni step comuni:

## 2.2 Nozione di "*exchange*" nel quadro normativo UE

Gli *exchange* sono ben noti alle autorità europee. L'ESMA definisce un *exchange* di cripto-attività come «*any trading platform where crypto-assets can be bought and sold, regardless of their legal status. Crypto-assets may be traded or exchanged for fiat currencies or other crypto-assets»*[153].

L'ESMA ha anche delineato diversi modelli di *business* tra gli *exchange*, che corrispondono alla distinzione sopra evidenziata[154]. Da un punto di vista normativo, gli *exchange* decentralizzati (DEX), sono soggetti di particolare attenzione.

Secondo l'ESMA, un DEX non detiene cripto-attività per conto dei suoi clienti, ma mette semplicemente in contatto gli utenti tra loro. La transazione avviene direttamente sulla rete DLT, ovvero "*on-chain*". I DEX funzionano senza un intermediario che detenga le chiavi private dei titolari di *token* o che gestisca gli ordini di acquisto e vendita. Tuttavia, l'ESMA non approfondisce le modalità con cui i DEX permettono gli scambi o come funzionano gli algoritmi AMM.

Per quanto riguarda le normative applicabili ai CEX e DEX, oltre alle leggi antiriciclaggio, è importante soffermarsi sull'applicabilità delle leggi europee e nazionali relative alle sedi di negoziazione. Se un *exchange* venisse classificato come un "mercato regolamentato" o categorie giuridiche affini, infatti, dovrebbe seguire le normative vigenti, ottenere le necessarie autorizzazioni e rispettare onerosi obblighi[155].

---

1. Dopo un processo di controllo, il progetto è accettato per eseguire una IDO su un DEX. I fondatori del progetto offrono una *supply* del *token* a un prezzo fisso e gli utenti bloccano i loro fondi in cambio di questi *token*. In seguito, gli investitori riceveranno i *token*, durante l'evento di generazione del *token* (TGE). 2. Di solito, c'è una *whitelist* degli investitori. Potrebbe essere necessario completare alcune azioni di *marketing* per iscriversi alla lista o è semplicemente necessario fornire l'indirizzo di un *wallet*. 3. Alcuni dei fondi raccolti vengono utilizzati per creare una *pool* di liquidità insieme al *token* del progetto. Il resto dei fondi viene assegnato al *team*. Gli investitori possono quindi scambiare i token dopo il TGE. In genere, la liquidità fornita è bloccata per un determinato periodo
4. Durante il TGE, i token vengono trasferiti all'utente e diventa possibile fare trading nella LP." *«Cos'è una IDO (Initial DEX Offering)?*», BINANCE ACADEMY,
https://academy.binance.com/it/articles/what-is-an-ido-initial-dex-offering.

[153] ESMA*,* «*Advice on Initial Coin Offerings and Crypto-Assets*» 2019.

[154] ESMA, cit., p. 24, 44-45. In particolare, l'ESMA distingue fra *«(i) those that have a central order book and/or match orders under other trading models (ii) those whose activities are similar to those of brokers/dealers and (iii) those that are used to advertise buying and selling interests*».

[155] Tra gli obblighi più rilevanti e costosi vi sono i requisiti di capitale minimo previsti per le imprese di investimento o per i gestori dei mercati, soddisfare precisi requisiti organizzativi (gestione dei conflitti di interesse, sicurezza dei dati e informatica delle strutture utilizzate, continuità del servizio offerto, previsione di regole trasparenti per l'esecuzione degli ordini), nonché regole miranti alla protezione degli investitori e riguardanti l'accesso al sistema.

L'art. 4, comma 1, n. 21, della Direttiva MiFID II, fornisce una definizione di "mercato regolamentato": *«Sistema multilaterale, amministrato e/o gestito da un gestore del mercato, che consente o facilita l'incontro, al suo interno e in base alle sue regole non discrezionali, di interessi multipli di acquisto e di vendita di terzi relativi a strumenti finanziari, in modo da dare luogo a contratti relativi a strumenti finanziari ammessi alla negoziazione conformemente alle sue regole e/o ai suoi sistemi, e che è autorizzato e funziona regolarmente e conformemente al titolo III della presente direttiva»*. Dalla lettura della definizione, emergono chiaramente due elementi fondamentali per determinare l'applicabilità di queste normative agli *exchange*. Il primo elemento riguarda il fatto che gli scambi hanno ad oggetto strumenti finanziari; il secondo consiste nel requisito che la piattaforma di interscambio sia diretta da un "gestore del mercato". Riguardo al primo punto, è evidente che le considerazioni fatte in precedenza sulla classificazione legale delle diverse tipologie di cripto-attività abbiano ripercussioni anche sugli organizzatori di tali scambi. Pertanto, un CEX che permette gli scambi di *investment token*, rientrerà nella definizione menzionata e dovrà ottenere le adeguate autorizzazioni per funzionare. La questione è più complessa quando gli scambi coinvolgono *utility token*. In particolare, la decisione che verrà adottata riguardo alla loro definizione legale influenzerà le piattaforme che gestiscono esclusivamente scambi di questa specifica categoria di cripto-attività.

Mentre per i CEX le suddette questioni possono essere affrontate in modo relativamente chiaro, i DEX presentano sfide maggiori, in particolare riguardo all'identificazione del soggetto che possa qualificarsi come "gestore del mercato"[156]. Nei DEX, infatti, gli *smart contract* eseguono gli scambi con il supporto dei *tokenholder* che effettuano l'attività di *liquidity provider*, depositando cripto-attività nelle coppie di liquidità. Questo solleva dubbi sull'identificazione di una singola entità come "gestore del mercato", rendendo difficile l'applicazione delle normative attuali, anche se all'interno dei DEX si scambiano *investment token*.

[156] Per le riflessioni in merito a imputazione e responsabilità nei casi in cui un servizio sia offerto a un cliente da parte di un algoritmo, cfr. A. GUAGGERO , *Automazione dei processi e dei servizi, imputazione e responsabilità*, in M. CIAN . e C. SANDEI (a cura di), Diritto del Fintech, Milano, 2020, p. 66-70 dove l'Autore sostiene che con riferimento all'ipotesi in cui l'esecuzione del contratto sia conclusa da un algoritmo, imputazione dell'atto compiuto e responsabilità dovranno comunque essere dell'impresa che include quello specifico algoritmo all'interno della propria organizzazione. Rimane quindi senza risposta il quesito nel caso in cui non sia possibile individuare una impresa cui l'algoritmo dovrebbe fare riferimento.

All'interno di un AMM, numerosi sono gli attori che partecipano al funzionamento del DEX e altrettanti sono coloro che beneficiano della sua attività. È pertanto essenziale pensare a un approccio regolamentare differente rispetto a quello tradizionale di porre obblighi sul "padrone" del *software*.

Considerata l'impossibilità di regolamentare in modo convenzionale questi *exchange*, si dovrebbe proporre l'emanazione di *standard* tecnici cui i DEX dovrebbero attenersi. L'aderenza a tali criteri, verificabile da tutti grazie alla trasparenza della DLT, potrebbe portare all'assegnazione di un *label* o all'inserimento automatico in un apposito registro, consultabile da chi è alla ricerca di un DEX affidabile.

In un settore così esposto al rischio di truffe, o al fatto che il codice informatico impiegato contenga dei *bug*, un sistema di *labeling*, basato sulla verifica del rispetto di appositi *standard* tecnologici, aiuterebbe ad aumentare la fiducia degli investitori senza imporre costi regolamentari eccessivi sulle piattaforme[157].

Da qui un eventuale ruolo proattivo delle autorità di vigilanza, magari con l'assistenza di società private specializzate, le quali potrebbero esaminare, grazie alla trasparenza di tali sistemi, i processi digitali adottati e la loro affidabilità. L'assenza di un ente regolatore che possa "chiedere" un'autorizzazione, pare non lasciare margine per una metodologia normativa alternativa. Una volta eseguito l'esame suddetto, l'ente dovrebbe individuare la sicurezza o il rischio di un determinato DEX. In presenza di rischi, si potrebbe considerare adeguato un semplice annuncio pubblico ai detentori di *token*.

[157] Volendo, poi, aumentare la tutela degli investitori, un ordinamento potrebbe ricorrere al potere repressivo dell'oscuramento del sito web in caso di mancato rispetto degli standard tecnologici, sebbene la misura dovrebbe considerarsi eccessivamente oppressiva e dovrebbe essere impiegata, così come oggi la impiega Consob, solo in situazioni di effettivo pericolo per gli investitori. Il potere di oscuramento, in particolare, è stato previsto a favore della Consob dall'art. l'art. 7-octies t.u.f. che attribuisce all'Autorità il potere, «nei confronti di chiunque offre o svolge servizi o attività di investimento tramite la rete internet senza esservi abilitato ai sensi del presente decreto» di: (i) «rendere pubblica, anche in via cautelare, la circostanza che il soggetto non è autorizzato [alla prestazione nei confronti del pubblico di uno dei servizi o delle attività di investimento ai sensi del t.u.f., n.d.r.]»; e di (ii) «ordinare di porre termine alla violazione». La norma appena riportata è stata, poi, inizialmente integrata dall'art. 36, comma 2-terdecies, D.L. 30 aprile 2019, n. 34 (come convertito dalla L. 28 giugno 2019, n. 58), che stabilisce che «la Consob ordina ai fornitori di connettività alla rete internet ovvero ai gestori di altre reti telematiche o di telecomunicazione, o agli operatori che in relazione ad esse forniscono servizi telematici o di telecomunicazione, la rimozione delle iniziative di chiunque nel territorio della Repubblica, attraverso le reti telematiche o di telecomunicazione, offre o svolge servizi o attività di investimento senza esservi abilitato. I destinatari degli ordini comunicati ai sensi del primo periodo hanno l'obbligo di inibire l'utilizzazione delle reti delle quali sono gestori o in relazione alle quali forniscono servizi. La Consob può stabilire con regolamento le modalità e i termini degli adempimenti previsti dal presente comma».

Per concludere, vale la pena indicare che i servizi di interscambio di cripto-attività possono anche operare attraverso modelli che non replicano la dinamica dei mercati tradizionali, e pertanto, non rientrano nella legislazione attuale. Uno di questi modelli, è quello delle "bacheche elettroniche"[158]. Per essere riconosciuto come tale, l'*exchange* non deve gestire o coordinare direttamente le negoziazioni, ma solamente presentare le proposte fatte dai propri membri. Data l'avanzata capacità tecnologica del settore, questa opportunità regolamentare potrebbe rappresentare un'apertura per nuovi attori del mercato, i quali intendono posticipare l'adempimento dei costosi oneri regolamentari previsti dalla legge attuale.

# 3. Il caso FTX: dalle origini al oeclino. analisi delle fasi cruciali

## 3.1 FTX e Alameda Research: la nascita di un gigante delle criptovalute

Dopo aver analizzato le caratteristiche degli *exchange* e le differenze tra i vari sistemi di custodia, è possibile introdurre quello che è stato definito come la "*Lehman Brother delle criptovalute*". Si tratta del caso FTX, il quale fino ai primi giorni di novembre 2022 era uno dei principali *exchange* centralizzati del mondo, facente capo a Sam Bankman-Fried (di seguito "SBF"). La questione legata a FTX è molto complessa per svariate ragioni e le indagini ed i relativi procedimenti giudiziari sono ancora in corso.

[158] Si veda, sul punto il Considerando 8 del Regolamento (Ue) N. 600/2014 del Parlamento Europeo e del Consiglio del 15 maggio 2014 sui mercati degli strumenti finanziari e che modifica il regolamento (UE) n. 648/2012 il quale recita « Allo scopo di rendere i mercati finanziari dell'Unione più trasparenti ed efficienti nonché di definire condizioni eque tra le varie sedi che offrono servizi di negoziazione multilaterale è opportuno introdurre una nuova categoria di sede di negoziazione, quella di sistema organizzato di negoziazione (OTF), per le obbligazioni, i prodotti finanziari strutturati, le quote di emissione e gli strumenti derivati, così come provvedere a che sia adeguatamente regolamentata e applichi regole non discriminatorie in relazione all'accesso al sistema stesso. Tale nuova categoria è ampiamente definita in modo tale da essere in grado, ora e in futuro, di comprendere tutti i tipi di esecuzione organizzata e organizzazione di negoziazione che non corrispondono alle funzionalità o alle specifiche normative delle sedi esistenti. Di conseguenza è opportuno applicare requisiti organizzativi e regole di trasparenza appropriati a sostegno di un'efficiente determinazione dei prezzi. La nuova categoria comprende sistemi per la negoziazione di derivati sufficientemente liquidi e ammessi alla compensazione. Non dovrebbe includere sistemi in cui non ha luogo un'autentica esecuzione od organizzazione della negoziazione, quali bacheche elettroniche usate per pubblicizzare interessi di acquisto e di vendita, altre entità che riuniscono o raggruppano potenziali interessi di acquisto e di vendita, servizi elettronici di conferma post-negoziazione o compressione del portafoglio, che riduce i rischi non di mercato in portafogli di strumenti derivati esistenti senza modificare il rischio di mercato dei portafogli stessi».

Tutto ha avuto inizio con la fondazione di Alameda Research nel settembre 2017, da parte di SBF e Tara Mac Aulay; questa era una *quantitative trading firm*, la quale inizialmente svolgeva principalmente attività di *arbitrage trading*[159], approfittando della differenza tra i prezzi del bitcoin tra Stati uniti e Giappone[160]. Tra la fine del 2018 e il 2019, Alameda registrava movimenti per più di 25 milioni di dollari al giorno e in ragione dell'elevata crescita effettuata, cominciò a raccogliere capitali da investitori esterni, promettendo ritorni di capitale elevati (15%).

Questa proposta ha permesso ad Alameda di raccogliere ingenti capitali. Nel 2019 i profitti erano tali da far sì che SBF insieme a Gary Wang[161] potessero lanciare il proprio *exchange* di cripto-attività: FTX.

Inizialmente il nuovo CEX era attrattivo poiché permetteva di effettuare operazioni più rischiose e con maggiore leva finanziaria[162], rispetto a quelle di altre piattaforme già presenti sul mercato.

FTX, inoltre, era pioniere nell'offrire molti strumenti di *trading* come i *futures* per una moltitudine di cripto-attività, opzioni scambiabili istantaneamente sul mercato ed il mercato dei pronostici che permetteva di fare *trading* sulla base di previsioni del mondo reale.

FTX raccoglieva capitale sul mercato con il primo *seed round*[163]*,* tra cui anche l'investimento strategico da parte di Binance[164] per il valore del 5% del capitale sociale di FTX. Nello stesso anno viene sviluppato dal *team* di FTX il *token* nativo FTT[165].

Al di là dei servizi di scambio sia su FTX che sulle maggiori piattaforme *exchange*, il *token* era caratterizzato dalla presenza di numerose funzionalità accessorie; le più rilevanti ai fini del presente elaborato e dell'evoluzione fallimentare

---

[159] L'arbitraggio è una strategia di *trading* relativamente a basso rischio che approfitta delle differenze di prezzo tra un mercato e l'altro.

[160] M. KRUPPA, «*Crypto exchange FTX secures backing from venture capital and hedge funds*», *Financial Times*, 20 luglio 2021, sez. Cryptocurrencies, https://www.ft.com/content/a3a90a4f-54e4-4b4f-b1df-2d9d8ca7712d.

[161] ha lavorato come ingegnere software per Google, Facebook e molte altre società *tech* di rilievo; ha ricoperto la carica di CTO di FTX, nonché quella di CTO di Alameda Research.

[162] Attraverso l'utilizzo della leva finanziaria (o "*leverage*") un soggetto ha la possibilità di acquistare o vendere attività finanziarie per un ammontare superiore al capitale posseduto e, conseguentemente, di beneficiare di un rendimento potenziale maggiore rispetto a quello derivante da un investimento diretto nel sottostante ma, di converso, di esponendosi al rischio di perdite molto significative.

[163] Il *seed round* o *seed capital* è la primissima fase di raccolta fondi. È quando la *startup* è ancora alle prese con *il business plan*, analisi di mercato, quando il prodotto o servizio non è ancora finalizzato e il personale ancora ridotto.

[164] la principale piattaforma di compravendita di criptovalute e beni digitali in termini di volume di scambi, capace di offrire un'ampia gamma di funzioni e servizi ai suoi utenti. Cfr. https://www.binance.com/it/blog/ecosystem/guida-binance-per-principianti-3741372155113856065.

[165] A. BELLELLI, «*Comprare FTX Token (FTT): cos'è il progetto, grafico e previsioni*», *Finanza Digitale*, 21 giugno 2022, https://www.finanzadigitale.com/comprare-ftx/.

della vicenda FTX, sono *FTX Staking* e *FTX Pay*. La prima funzione permetteva di "mettere in *stake*", ossia vincolare per un determinato periodo i propri *token* FTT o parte di essi, in modo da ottenere ricompense dovute al mantenimento per lungo tempo della posizione[166]. La seconda funzionalità rilevante era un vero e proprio processore di pagamento veloce, sicuro e a basso costo; permetteva di ricevere pagamenti in criptovalute e valute *fiat* tradizionali[167]. È necessario ricordare che gli *asset* degli investitori, lasciati nel *wallet* dell'*exchange,* non sono nella loro reale disponibilità e la loro iscrizione solo virtualmente sulle scritture contabili. Dal punto di vista giuridico è inesistente la separazione patrimoniale tra i *token* degli investitori e quelli delle piattaforme centralizzate di scambio[168].

Nel periodo tra ottobre 2021 e gennaio 2022, SBF chiuse un *round* di investimento per circa 800 milioni di dollari tra investitori e grandi *venture capital* (tra i più rilevanti: Sequoia Capital[169], Tamasek[170], Softbank[171]); il gruppo societario contava circa 130 società. La controllante e la sua controllata FTX Digital markets Ltd hanno sede alle Bahamas[172] e la seconda è regolata dalla Securities Commission delle Bahamas, mentre negli Stati Uniti il gruppo operava tramite FTX US, società di servizi monetari registrata presso la *Financial Crimes Enforcement Network* (FinCEN), nonché tramite FTX US Derivates[173]. L'ultimo *round* di investimenti ha portato la piattaforma di SBF ad essere valutata 32 miliardi di dollari, e quindi terzo *exchange* al mondo nonché primo al di fuori della Cina[174].

---

[166] Ci si chiede se il tentativo di convincere gli utenti a depositare fondi proprio su FTX non possa essere considerato parte di una truffa. L'altro processo che Bankman-Fried dovrà affrontare è quello da parte della *Securities and Exchange Commission,* che lo ha accusato di aver truffato i suoi investitori, cioè di aver raccolto finanziamenti per la sua azienda FTX facendo promesse false.

[167] I. WRIGHT «*Cos'è il token FTX (FTT)? Prezzo, storia e come acquistarlo*», https://coinkickoff.com/it/ftx-token-ftt/.

[168] V. CARLINI, «*Cripto, dopo la tempesta di Ftx boom per robot e autocustodia*», *Il Sole 24 ORE*, 2 dicembre 2022, 36, sez. Finanza e Mercati.

[169] Sequoia Capital è una società di *venture capital* con sede in California che si focalizza principalmente sul settore industriale tecnologico. Lanciata nel 1972, considerato il pioniere del venture capital nella Silicon Valley, ha finanziato società diventate icone dell'*high-tech* USA come Apple, Google, Cisco, PayPal e YouTube.

[170] *Holding* di proprietà del governo di Singapore

[171] SoftBank Group Corporation è una *holding* finanziaria multinazionale giapponese con sede a Tokyo; È stata classificata nell'elenco Forbes Global 2000 come la 39ª più grande azienda al mondo.

[172] J. OSSINGER, «*Crypto-Derivatives Exchange FTX Leaves Hong Kong for Bahamas*», Bloomberg, 24 settembre 2021 s.d., https://www.bloomberg.com/news/articles/2021-09-24/bankman-fried-s-crypto-exchange-ftx-leaves-hong-kong-for-bahamas?leadSource=uverify%20wall.

[173] B. Elder, A. SCAGGS, «*The FTX bankruptcy filing in full (updated)*», *Financial Times*, 17 novembre 2022, sez. FT Alphaville, https://www.ft.com/content/c236d6f9-da5a-4da7-8dc8-5cd450dfe39d.

[174] C. DE ANGELIS, «*L'exchange dell'under 30 più ricco del mondo raccoglie 400 milioni di dollari. Ora vale 32 miliardi*», *Forbes Italia*, 1° febbraio 2022, https://forbes.it/2022/02/01/ftx-sam-bankman-fried-raccolgono-400-milioni-dollari/.

## 3.2 Il tracollo di FTX, le vicende che hanno portato al fallimento

Nel 2022, anno molto turbolento per il mercato delle cripto-attività[175], FTX non solo sembra rimanere indenne ma a fine agosto 2022, tramite il *report* dei risultati, comunica una crescita in termini di ricavi del 1000% rispetto all'anno precedente[176].

In ragione della sua crescente credibilità, SBF si ergeva a faro e guida del mercato per tutte le aziende nel mondo dei *digital assets*; ha concesso al prestatore di criptovalute BlockFi una linea di credito da 250 milioni di dollari[177], ha rilevato il *broker* di cripto-attività in bancarotta Voyager Digital[178], ha lanciato il suo fondo *venture* FTX ventures, il quale gestiva un patrimonio di circa 2 miliardi di dollari. Da ultimo, ha provato ad assistere Elon Musk, volendo partecipare all'acquisto di Twitter con 3 miliardi di dollari (superando di ben 6 volte il suo *competitor* Binance, che proponeva 500 milioni di dollari). Sembrava insomma, che Bankman-Fried fosse uscito dal *bear market* delle criptovalute più forte dei suoi concorrenti, soprattutto trasformando la perdita di qualcun altro nella sua opportunità.

Non è da sottovalutare la grande influenza mediatica e politica, ottenuta tramite le sponsorizzazioni milionarie di squadre sportive e finanziamenti politici[179]; Bankman-Fried è stato infatti uno dei maggiori finanziatori individuali di Joe Biden nel 2020 e il sesto donatore individuale in assoluto per le elezioni *midterm* del 2022, contribuendo con quasi 40 milioni di dollari elargiti a vari candidati[180]. Proprio grazie a queste attività ha fatto accrescere la sua credibilità a livello mondiale, tanto che tra il 2020 e il 2022 è stato il principale interlocutore del Congresso e della Casa Bianca in merito alla questione della regolamentazione delle cripto-attività.

Tutto ciò culmina in data 19 ottobre 2022 con la pubblicazione sul blog di FTX di un documento scritto di suo pugno, dal titolo: "*Possible Digital Assets Industry*

---

[175] Cfr. *S. SMERALDI, G. RIPELLINO, «bitcoin e altre valute digitali: una nuova primavera dopo il cripto-winter*» Rivista Bancaria-Minerva Bancaria (marzo 2023). E W. FERRI, «*Il terribile 2022 delle criptovalute*», Money.it, 31 dicembre 2022, https://www.money.it/il-terribile-2022-delle-criptovalute.

[176] S. SINCLAIR, «*FTX Revenue Exploded 1,000% to Beyond $1B Last Year: Report*», *Blockworks*, 22 agosto 2022, sez. Markets, https://blockworks.co/news/ftx-revenue-exploded-1000-to-beyond-1b-last-year-report.

[177] V. CACIOPPOLI, «*Il prestito di FTX a BlockFi*», The Cryptonomist, 22 giugno 2022. https://cryptonomist.ch/2022/06/22/prestito-ftx-blockfi/.

[178] S. INDAP, S. CHIPOLINA, «*Voyager Digital spurns 'lowball' joint bid from FTX*», *Financial Times*, 25 luglio 2022, sez. Cryptofinance, https://www.ft.com/content/ab23e979-8e71-4d5c-85cd-98572d0aedc0.

[179] M. VALSANIA, «*Ftx, scoppia il caso delle donazioni bipartisan: soldi ai politici Usa per regole più blande*», 28 febbraio 2023, Il Sole 24 Ore.

[180] N. POPLI, «*Sam Bankman-Fried's Political Donations: What We Know*», Time, 14 dicembre 2022, https://time.com/6241262/sam-bankman-fried-political-donations/.

*Standards*[181]", ovvero una proposta di regolamentazione del mercato delle cripto-attività, con cui detta alcune possibili linee guida che sperava che potessero essere acquisite da altri attori dell'industria, riviste ed adottate completamente a livello istituzionale".

Tutto questo castello di carte creato *ad hoc* da SBF e i suoi *advisors,* entra in crisi il 2 novembre 2022, a seguito di un articolo[182] pubblicato su Coindesk[183]. Analizzando i bilanci della società Alameda Research, l'articolo affermava "*ancora al 30 giugno gli asset di Alameda Research ammontano a 14,6 miliardi di dollari. L'asset maggiore è costituito da 3,66 miliardi di dollari in FTT non vincolati. La terza voce più importante sui loro registri? Una montagna da 2,16 miliardi di dollari in FTT collaterali"*. Con queste dichiarazioni Coindesk puntava il dito contro la società Alameda Research, facendo notare come i loro documenti finanziari evidenziassero attività per circa 14,6 miliardi di dollari e circa 8 miliardi di dollari di passività. Il problema che veniva sottolineato è che tra le attività, circa 6 miliardi di dollari erano FTT (*token* interni all'ecosistema ftx) e oltre 1 miliardo di dollari erano in SOL (*token* di Solana, creato sulla *blockchain* Solana da team interni ad FTX, quindi con un valore sostanzialmente auto-generato). Il *report*, inoltre, mostra come le attività non riuscissero a coprire le passività, a meno di una massiccia vendita sul mercato che avrebbe comportato un crollo del prezzo a discapito del *token* e dei *tokeholder.*

Nel giorno 6 novembre 2022 viene pubblicato dall'allora CEO di Binance, Chanpeng Zhao (CZ), un tweet che recitava così: "*As part of Binance's exit from FTX equity last year, Binance received roughly $2.1 billion USD equivalent in cash (BUSD and FTT). Due to recent revelations that have came to light, we have decided to liquidate any remaining FTT on our books. 1/4*[184]". CZ, dopo aver annunciato ad oltre 7 milioni di follower l'intenzione di liquidare l'intera posizione in FTT del CEX

[181] La versione originale non è più presente, in quanto il sito originario non è più accesibile. Per i punti salienti si veda: E. BOWTIED , «*Sam Bankman-Fried Proposes Centralized Crypto Industry Standards*», BowTied Island, 24 ottobre 2022, https://bowtiedisland.com/sam-bankman-fried-proposes-centralized-crypto-industry-standards/.

[182] I. ALLISON, «*Divisions in Sam Bankman-Fried's Crypto Empire Blur on His Trading Titan Alameda's Balance Sheet*», 2 novembre 2022, Coindesk, https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/.

[183] CoinDesk è il portale web leader mondiale di notizie e informazioni sulle criptovalute. La piattaforma fornisce le ultime notizie, il valore attuale, le funzionalità convenienti e l'analisi di tendenze, tecnologie, cambiamenti e aziende nel mondo della valuta digitale.

[184] CZ ◆ Binance [@cz_binance], «As Part of Binance's Exit from FTX Equity Last Year, Binance Received Roughly $2.1 Billion USD Equivalent in Cash (BUSD and FTT). Due to Recent Revelations That Have Came to Light, We Have Decided to Liquidate Any Remaining FTT on Our Books. 1/4», Tweet, *Twitter*, 6 novembre 2022, https://twitter.com/cz_binance/status/1589283421704290306.

Binance, induce una reazione nota ai mercati tradizionali e cioè la "corsa agli sportelli". A nulla, infatti, sono servite le dichiarazioni per rassicurare il mercato, effettuate da SBF e dalla CEO di Alameda Research, Caroline Ellison, con la quali veniva dichiarato che FTX muovesse in ottime acque e le riserve di capitale fossero idonee a sostenere una eventuale corsa agli sportelli.

Dopo 24 ore, Binance liquida 411 milioni di dollari ma l'*outflow* per FTX dovuto al panico del mercato ammonta a 451 milioni.

Anche sul fronte della società Alameda Research la situazione si apprestava a diventare critica; infatti, gli investitori cominciarono a chiedere indietro i loro soldi, ma riducendosi il valore di FTT si riduceva drasticamente anche il valore del collaterale che Alameda aveva utilizzato per molti prestiti[185]. Per riuscire a fornire le nuove ed ulteriori garanzie richieste, SBF ordinava di utilizzare i fondi depositati dagli investitori sull'*exchange* FTX al fine di permettere ad Alameda di rimanere solvibile[186].

L'8 novembre 2022 SBF fu costretto a bloccare i prelievi poiché non vi erano più riserve in cassa; in ragione della critica crisi di liquidità di uno dei maggiori *exchange* centralizzati globali, perviene da parte di Binance un *non binding agreement* finalizzato all'acquisizione della piattaforma[187]. Quello che poteva sembrare l'ancora di salvezza in realtà si dimostrò essere una vana speranza; infatti, di lì a poco Binance dopo aver esaminato i libri contabili, si ritira dall'accordo dichiarando: "*As a result of corporate due diligence, as well as the latest news reports regarding mishandled customer funds and alleged US agency investigations, we have decided that we will not pursue the potential acquisition of FTX.com*[188]." Binance quindi dichiara che a

---

[185] L'*Economist* solleva il sospetto che il tutto non fosse un piano di emergenza, ma un piano fin dall'inizio: "*Forse Alameda ha usato FTX come salvadanaio tutto il tempo, depositando i token emessi dall'exchange stesso (FTT) come garanzia al fine di inviare ad Alameda delle criptovalute del valore più affidabile, come bitcoin, ether o qualche stablecoin*." In *«The failure of FTX and Sam Bankman-Fried will leave deep scars*», THE ECONOMIST, 17 novembre 2022, https://www.economist.com/briefing/2022/11/17/the-failure-of-ftx-and-sam-bankman-fried-will-leave-deep-scars.

[186] Cfr. S. STIMOLO, «*Caroline Ellison: "l'insider per eccellenza" testimonia sul caso del crypto-exchange FTX*», *The Cryptonomist*, 16 ottobre 2023, https://cryptonomist.ch/2023/10/16/caroline-ellison-caso-crypto-exchange-ftx/.

[187] CZ ◆ BINANCE [@CZ_BINANCE], «*This Afternoon, FTX Asked for Our Help. There Is a Significant Liquidity Crunch. To Protect Users, We Signed a Non-Binding LOI, Intending to Fully Acquire Http://FTX.Com and Help Cover the Liquidity Crunch. We Will Be Conducting a Full DD in the Coming Days.* », Tweet, *Twitter*, 8 novembre 2022, https://twitter.com/cz_binance/status/1590013613586411520.

[188] *BINANCE [@BINANCE], «As a Result of Corporate Due Diligence, as Well as the Latest News Reports Regarding Mishandled Customer Funds and Alleged US Agency Investigations, We Have Decided That We Will Not Pursue the Potential Acquisition of Http://FTX.Com*.», Tweet, *Twitter*, 9 novembre 2022, https://twitter.com/binance/status/1590449161069268992.

seguito della *Due Diligence* volta a valutare l'acquisizione, sono emersi problemi "al di fuori del loro controllo e della loro capacità di aiutare".

Di conseguenza, l'11 novembre 2022, FTX, Alameda Research e altre 130 società affiliate hanno presentato l'istanza di protezione dal Fallimento ai sensi del *chapter 11* presso la Corte Federale del Delaware[189].

La procedura del *Chapter 11, title 11*, ha visto Sam Bankman-Fried dimettersi dal ruolo di amministratore delegato ed essere sostituito da un nuovo amministratore, l'avvocato John J. Ray III, che ha gestito alcune tra le maggiori crisi societarie statunitensi e che ha riferito alla corte di "*non aver mai assistito in quarant'anni di carriera, ad una situazione tanto disastrosa*[190]". Sembra infatti, che nel gruppo sia stata rilevata la totale mancanza di una qualsivoglia struttura di *governance*, che arriva addirittura a sfociare nella mancanza totale di riunioni dei consigli di amministrazione oltre alla carenza di un sistema dei controlli interni e di revisione (esterna) dei bilanci.

Insieme alla mancanza di bilanci adeguatamente revisionati, è poi emersa la mancanza di una corretta tenuta delle scritture contabili ed un ordinato registro dei flussi di cassa[191], specie per quanto riguarda uscite delle società del gruppo a favore dei dipendenti e consulenti. In particolare, nelle società del gruppo con sede alle Bahamas, si ha prova dell'elargizione di cifre a favori di dipendenti (per le quali non è presente alcuna registrazione a titolo di prestito), che sarebbero state usate per l'acquisto di case o altri beni personali.

Quanto alla gestione degli *asset* digitali, si è accertato l'uso di circuiti totalmente privi di *password* e protezioni, così come il mancato aggiornamento della *blockchain* a garanzia dell'ordinata registrazione delle transazioni e dei trasferimenti; per questo motivo, è stato possibile rintracciare e mettere sotto sequestro solo una parte delle cripto-attività (470 milioni di dollari)[192]. Tutte le scritture contabili e i registri sono

---

[189] FTX [@FTX_OFFICIAL], «*Press Release*» Https://T.Co/rgxq3QSBqm», Tweet, *Twitter*, 11 novembre 2022, https://twitter.com/FTX_Official/status/1591071832823959552.

[190] LA STAMPA «*Fallimento FTX, Ceo John Ray: "Mai visto un fallimento così in 40 anni*"», s.d., https://www.teleborsa.it/News/2022/11/18/fallimento-ftx-ceo-john-ray-mai-visto-un-fallimento-cosi-in-40-anni--39.html.

[191] J. DORSEY, giudice del tribunale fallimentare: "*Voglio assicurarmi di fare la cosa giusta. Abbiamo un elenco di persone che potrebbero essere clienti, potrebbero essere creditori o potrebbero essere entrambe le cose*" in V. LOPS, «*Ftx, spuntano asset liquidi per 5 miliardi*», Il Sole 24 ORE, 12 gennaio 2023.

[192] «*1 milione Gli investitori coinvolti Il fallimento di Ftx che si è consumato in questi giorni coinvolge una scia di oltre 1 milione di creditori in attesa di una risposta, secondo quanto si legge nei documenti con cui l'azienda del trading in criptoasset ha fatto richiesta per il Chapter 11. 32 miliardi Il valore bruciato. Ftx, la terza piattaforma di valute digitali al mondo aveva una valutazione pari a 32 miliardi di dollari ancora a febbraio 2022. L'11 novembre ha dichiarato fallimento. Molti analisti parlano*

stati tenuti con una tale negligenza che, al momento del subentro del nuovo amministratore, non esisteva nemmeno la lista dei primi cinquanta creditori della società. La predetta situazione si aggiungeva al tema più generale della creazione di valori arbitrari e non giustificati o giustificabili da alcun reale controvalore, unitamente alla facilità con cui investitori più o meno professionali, accettavano senza compiere nessuna reale verifica.

Si può concludere quindi, che la causa del crollo di FTX è connessa in gran parte alla scarsa o inesistente regolamentazione della materia, ma ancor più all'assenza di sistemi di controllo (interni ed esterni) della gestione del gruppo societario. Se l'attività di deposito e quella della compravendita delle cripto-attività fosse stata maggiormente regolamentata e sottoposta ai controlli delle autorità, difficilmente si sarebbero potuti tenere certi comportamenti[193].

## 3.3 FTX: un esame dettagliato delle cause del collasso e punti di contatto con le esternalità della finanza tradizionale

A seguito dell'evoluzione dell'ecosistema delle criptovalute, sono emersi anche i fallimenti del mercato e le esternalità della finanza tradizionale.

Viene ad evidenziarsi un processo definito da alcuni studiosi del settore, "*financialization*" delle cripto-attività[194], ovvero il manifestarsi di aspetti tipici e patologici della finanza tradizionale quali: conflitti di interesse, asimmetria informativa e rischi di agenzia, operativi e finanziari.

Il 2022 è stato un *annus horribilis* per l'ecosistema cripto, ancor prima del collasso di FTX[195].

---

*apertamente di "Lehman Brothers delle criptovalute*"». In *V. LOPS, «Da JP Morgan a BofA e BlackRock: tanti big nella rete del crack Ftx*», Il Sole 24 Ore, 19 novembre 2022.

[193] Michele Mandelli, Managing Partner di CheckSig: "operazioni tra parti correlate quali quelle che hanno portato al naufragio dello stesso FTX sarebbero finite, in un contesto di finanza tradizionale, sotto la lente di vigilanza e organi regolamentari, evitando così la crisi repentina di un colosso del settore." In V. CARLINI, «*Le cripto imprese alzano la voce: "Regole per isolare il business opaco"*», 12 novembre 2022, Il Sole 24 Ore.

[194] D. W. ARNER, D. A. ZETZSCHE, R. P. BUCKLEY, J. KIRKWOOD «*The Financialization of Crypto*: *Lessons from FTX and the Crypto Winter of 2022-2023*», *SSRN Electronic Journal*, 2023, https://doi.org/10.2139/ssrn.4372516.

[195] P. FITZGERALD E A. NEENAN, «*Annus Horribilis 2022: Regulation may be the only way out of crypto's 'Horrible Year'*», 5 dicembre 2022, CITY AM, https://www.cityam.com/annus-horribilis-2022-regulation-may-be-the-only-way-out-of-cryptos-horrible-year/.

In un solo anno, infatti, le criptovalute hanno perso circa 2 trilioni di dollari in valore di mercato[196], mentre bitcoin, criptovalute e finanza decentralizzata, erano state presentate come un'alternativa ai fallimenti della finanza tradizionale, intesi come secoli di crisi finanziarie e culminate nella Crisi Finanziaria Globale del 2008.

Mediante l'utilizzo di un *framework* tecnologico trasparente, le cripto-attività sono state progettate proprio per evitare gli svantaggi della finanza tradizionale: conflitti d'interesse da parte degli intermediari, asimmetrie informative, centralizzazione di funzioni cruciali, oligopolio di pochi grandi intermediari spesso interconnessi, un'abbondanza di partecipanti al mercato poco informati e troppo entusiasti (c.d. comportamento irrazionale), così come rischi di agenzia, operativi e finanziari, e ovviamente frodi, manipolazioni e condotte illegali.

La regolamentazione e la supervisione finanziaria tradizionali si sono evolute nel corso dei secoli per cercare di migliorare la stabilità finanziaria, garantire una adeguata protezione degli investitori, depositanti e consumatori, promuovere equità, efficienza e integrità del mercato ed indirizzare il sistema finanziario verso la crescita economica, l'inclusione finanziaria e lo sviluppo sostenibile.

Anche le cripto-attività, nonostante la loro natura concettuale riconducibile alla finanza decentralizzata[197], evolvendosi hanno mostrato in meno di 15 anni, l'emergere dei classici rischi e situazioni patologiche che caratterizzano la finanza tradizionale.

Il futuro delle cripto-attività è attualmente uno dei *focus* principali dell'agenda normativa. Il *Financial Stability Board* (FSB)[198], il Fondo Monetario Internazionale

---

[196] D. FANTATO, «*Crypto & Digital Assets Summit*», Financial Times Event, 28 novembre 2022, https://www.ftadviser.com/events-awards/2022/11/28/crypto-digital-assets-summit/.

[197] *"La DeFi nel senso stretto del termine è caratterizzata da transazioni peer-to-peer e dall'assenza di un intermediario centralizzato. Attraverso gli smart contract, le transazioni tra domanda e offerta dovrebbero essere eseguite automaticamente e tutti i server che supportano il funzionamento dei protocolli ('nodi'), o i detentori di token, a seconda dei casi, hanno uguale accesso ai dati e uguali diritti di governance (o l'equivalente tecnologico dei diritti di governance). Un simile sistema può anche essere definito come Organizzazione Autonoma Decentralizzata (DAO). Se una piattaforma di trading è governata da un DAO, nel gergo delle criptovalute si parla di Scambi Decentralizzati (DEX). Tuttavia, in tutto il settore delle criptovalute, gli intermediari centralizzati spesso forniscono funzioni importanti all'ecosistema DeFi. Ad esempio, Binance, Coinbase, e altri sono gestiti da entità centralizzate e quindi sono definiti Exchange Centralizzati (CEXs). Dal punto di vista del settore DeFi, questi costituiscono una sorta di Finanza Centralizzata (CeFi). Tuttavia, questi CEXs consentono a) l'investimento iniziale di valuta fiat in token e b) la negoziazione di token. A loro volta, i CEXs forniscono la maggior parte del volume di trading per i token emessi secondo presunti protocolli DeFi e influenzano la valutazione degli asset criptati che potrebbero poi essere utilizzati dai protocolli DeFi".* In *ARNER , «The Financialization of Crypto*» 2.

[198] FINANCIAL STABILITY BOARD, «*Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative Report*», 11 ottobre 2022, https://www.fsb.org/2022/10/regulation-supervision-and-oversight-of-crypto-asset-activities-and-markets-consultative-report/.

(FMI)[199] e la Bank for International Settlements (BIS)[200] hanno emesso documenti sull'argomento, mentre il G20 predilige un approccio coordinato a livello internazionale. Le principali giurisdizioni stanno implementando o progettando nuove misure.

Per quanto riguarda l'Unione Europea, il nuovo Regolamento MiCA, introduce uno schema di licenze per gli intermediari delle cripto, regole di prospetto, norme per contrastare gli abusi di mercato e le pratiche di *insider trading* e una legislazione *ad hoc* per le *stablecoin*[201].

Tornando al caso FTX, l'*exchange* era stato valutato 32 miliardi di dollari nel suo *round* di finanziamento di gennaio 2021. All'inizio del 2022, FTX era uno dei più grandi *exchange* di cripto-attività al mondo, che si definiva una "Borsa", ma in realtà era un conglomerato complesso, avendo registrato una crescita esponenziale dai 90 milioni di dollari di ricavi nel 2020 ad oltre 1 miliardo di dollari di ricavi nel 2021[202]; una crescita sorprendente di oltre il 1.000% in un anno.

Per certi versi, il fallimento di FTX è riconducibile ad una crisi di liquidità che si è trasformata in insolvenza, simile a quella di Lehman Brothers nel 2008. Quando un intermediario finanziario non è in grado di accedere a sufficiente liquidità per continuare la sua attività, questa crisi di liquidità spesso si trasforma in una crisi di solvibilità che innesca una perdita di fiducia in tutto il settore e potenzialmente una crisi finanziaria, proprio come si è potuto osservare nella seconda metà del 2022 nell'ecosistema cripto.

Tutto ciò ha portato, come nel 2008, a chiedersi se ci debba essere un "Prestatore di Ultima Istanza" (LoLR) o un "fornitore di liquidità di ultima istanza"[203]. Nel caso di FTX, come è stato sopra evidenziato, è sorta brevemente la prospettiva che Binance potesse intervenire con una iniezione di liquidità di emergenza, o addirittura rilevare FTX (come JP Morgan fece con Bear Stearns all'inizio della crisi del 2008).

---

[199] IMF, «*Elements of Effective Policies for Crypto Assets*», 23 febbraio 2023, https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-Assets-530092.

[200] M. AQUILINA, J. FROST, A. SCHRIMPF, «*Addressing the Risks in Crypto: Laying out the Options*», BIS, 12 gennaio 2023.

[201] Vedi diffusamente *infra.*

[202] K. ROONEY, «*FTX Grew Revenue 1,000% during the Crypto Craze, Leaked Financials Show*», 20 agosto 2022, CNBC, https://www.cnbc.com/2022/08/20/ftx-grew-revenue-1000percent-during-the-crypto-craze-leaked-financials.html.

[203] Cfr. D. FABER , N. VERMUNT a c. di, «*Bank Failure: Lessons from Lehman Brothers*» (Oxford, New York: Oxford University Press, 2017).

Ma, nonostante gli sforzi di FTX di garantire una continuità di liquidità di emergenza e di mantenere la fiducia del mercato (anche in ultima istanza con il tentativo di rivolgersi a Binance per assistenza d'emergenza), alla fine non è stato in grado di garantire ulteriori fondi ed è stato costretto a presentare istanza di fallimento.

Il ruolo di Binance, come principale concorrente di FTX, merita un'attenzione particolare, poiché le difficoltà di FTX sono diventate note al mondo attraverso le preoccupazioni pubblicamente espresse da Binance riguardo le (presunte) esposizioni eccessive nei confronti di Alameda. Tale annuncio è stato fatto dopo che Binance aveva venduto circa 500 milioni di dollari in FTT, (i token emessi da FTX), anticipando di fatto la crisi di liquidità e preservando il proprio bilancio dall'impatto che l'annuncio avrebbe avuto sul mercato[204].

Il ruolo di Binance in tutto ciò è stato differente da quello degli intermediari regolamentati in situazioni simili, i quali agiscono principalmente coordinandosi per mantenere la fiducia generale nel mercato.

Dopo essersi proposto come "l'ancora di salvezza", Binance ha rinunciato con un successivo comunicato pubblico, che ha reso di fatto impossibile ogni tentativo di ristrutturazione da parte di terzi. In sintesi, Binance sembra aver contribuito ad accelerare il fallimento di uno dei suoi principali concorrenti[205].

Nella finanza tradizionale, l'origine delle crisi di liquidità difficilmente si rinviene in una pubblica dichiarazione di sospetto da parte di un soggetto regolamentato verso un altro. Ciò che è accaduto nella vicenda FTX non potrebbe succedere in un mercato regolamentato, perché le normative sulle manipolazioni di mercato impediscono tale comportamento[206].

Come accade nella finanza tradizione, l'insolvenza di FTX è stata determinata dall'impossibilità di soddisfare le richieste dei clienti, creditori ed investitori.

Nel mondo delle cripto-attività, fiducia e sicurezza del mercato dovevano derivare dalla tecnologia sottostante, piuttosto che dalla regolamentazione e supervisione. Le criptovalute hanno infatti le loro radici in uno scambio di denaro *peer-to-peer* decentralizzato, progettato proprio per evitare crisi di liquidità e solvibilità.

---

[204] O. KHARIF, «*Crypto Exchange Binance To Sell $529 Million of Bankman-Fried's FTT Token*», Bloomberg, 7 novembre 2022, https://www.bloomberg.com/news/articles/2022-11-06/binance-to-sell-529-million-of-ftt-token-amids-revelations.

[205] O ALIAJ, «*Binance ditches deal to rescue rival crypto exchange FTX*», *Financial Times*, 10 novembre 2022, sez. FTX Trading Ltd, https://www.ft.com/content/ad440b22-00e2-44e9-b95d-449bb89fd504.

[206] Vedi diffusamente cap. 3

Sorge spontaneo domandarsi se la struttura originale delle criptovalute come un sistema di registrazione di transazioni *peer-to-peer* decentralizzato sia difettoso o se alcuni soggetti siano in grado di eluderlo.

In ogni caso, è chiaro che qualsiasi agenda di riforma per il settore delle cripto-attività dovrà bilanciare la struttura originale decentralizzata con l'attuale, urgente necessità di protezione centralizzata del mercato.

È utile considerare che nel settore globale delle criptovalute, mancano misure omogenee di prevenzione come le norme sulla gestione del rischio e sulle manipolazioni di mercato, e più in generale, la regolamentazione e la supervisione necessarie per mantenere la fiducia e la solidità del mercato e per mantenere riserve sufficienti per soddisfare le esigenze dei clienti, investitori e depositanti; inoltre sono assenti le misure di ristrutturazione del debito e risoluzione della crisi caratteristiche della finanza tradizionale.

Considerando le accuse di frode che sono emerse, la vicenda FTX è stata da molti paragonata al fallimento Enron[207]; in altre parole, la crisi è da addebitarsi principalmente alla struttura del gruppo societario[208].

Il *global exchange* aveva trasferito la sua sede da Hong Kong alle Bahamas nel settembre 2021 ed era registrato presso la *Securities Commission* delle Bahamas in conformità con il *Bahamas Digital Assets and Registered Exchanges Act*[209] 2020[210]. Come gruppo, FTX era comunemente considerato solo come un *exchange*, ma in realtà funzionava più come un gruppo finanziario (come Lehman brothers o Enron).

La mancanza di trasparenza ha portato a varie accuse di frode, che il fondatore di FTX, Sam Bankman-Fried, ha più volte negato[211]. Quest'ultimo è stato arrestato alle Bahamas il 12 dicembre 2022 e grazie al trattato di estradizione con gli Stati Uniti,

---

[207] M. BUSSI, «*Lo scandalo Ftx peggio di Enron - MilanoFinanza News*», MF Milano Finanza, 18 novembre 2022.

[208] S. MOLLMAN, «'*A Lot of People Have Compared This to Lehman. I Would Compare It to Enron': Larry Summers Has Some Choice Words for Sam Bankman-Fried and FTX*», *Fortune*, 11 novembre 2022, https://fortune.com/2022/11/11/larry-summers-ftx-crypto-collapse-more-like-enron-than-lehman/.

[209] cfr. C. R. ROLLE, «*Navigating The Digital Frontier: The Bahamas' Approach To Regulating Digital Assets*», IFC Review, https://www.ifcreview.com/articles/2023/september/navigating-the-digital-frontier-the-bahamas-approach-to-regulating-digital-assets/.

[210] Sam Bankman-Fried aveva affermato che la Maggiore chiarezza della regolamentazione nelle Bahamas era la ragione principale del trasferimento, in S. NAGARAJAN S. Nagarajan, «Sam Bankman-Fried Says FTX Has Moved Its HQ from Hong Kong to the Bahamas Because of Its Crypto Framework», Yahoo Finance, 27 settembre 2021, https://finance.yahoo.com/news/sam-bankman-fried-says-ftx-150947960.html.

[211] R. GOSWAMI S. MACKENZIE, «*In Defensive Interview, Sam Bankman-Fried Claims He's Broke and Committed No Fraud*», *CNBC*, 30 novembre 2022, https://www.cnbc.com/2022/11/30/former-ftx-ceo-sam-bankman-fried-says-i-didnt-ever-try-to-commit-fraud.html.

è stato posto sotto la custodia delle autorità statunitensi e accusato in un tribunale federale di New York, con sette capi d'accusa tra cui frode e cospirazione.

Ciò che è emerso dopo mesi di indagini, è che i fondi dei clienti, sono stati trasferiti da FTX ad Alameda per coprire le perdite di investimento di quest'ultima[212]. La verifica di ciò che è realmente accaduto è gravemente ostacolata dalla totale mancanza di controlli interni, strutture contabili adeguate e perfino di sistemi per tenere traccia dei conti dei clienti[213].

Mentre FTX si presentava come un *exchange*, in realtà funzionava più come un intermediario e *trader* in *asset* la cui emissione era controllata da sé stesso.

# 4. Sfide regolamentari nel settore delle cripto-attività: analisi empirica sui rischi sistemici e il fenomeno dello *shadow banking*

## 4.1 Interconnessioni finanziarie: analisi dei rischi e lezioni dal "*crypto-winter*"

Il rapido sviluppo della tecnologia *blockchain* si sta sempre più diffondendo nel settore finanziario. Diventa quindi essenziale esplorare le interconnessioni e le implicazioni tra la finanza tradizionale e quella digitale.

Probabilmente altri *exchange*, come FTX, sono stati destabilizzati da altri fallimenti dell'inizio del 2022 (soprattutto dato che FTX era coinvolta nel tentativo di ristrutturazione di alcuni di essi)[214]. Queste dinamiche dovrebbero essere assenti in un ambiente veramente decentralizzato, poiché la finanza decentralizzata è intrinsecamente progettata per evitare le interconnessioni tipiche della TradFi.

A ciò si aggiungono anche i numerosi problemi di sicurezza IT rinvenuti negli anni. In alcuni casi le chiavi private sono state sottratte attraverso l'*hacking* dei *custodial wallet* degli *exchange online* (cd. "*Hot Wallet*"), in altri gli aggressori hanno

[212] A. BERWICK, «*Exclusive: Behind FTX's Fall, Battling Billionaires and a Failed Bid to Save Crypto*», *Reuters*, 10 novembre 2022, sez. Technology, https://www.reuters.com/technology/exclusive-behind-ftxs-fall-battling-billionaires-failed-bid-save-crypto-2022-11-10/.

[213] K. SHUBBA, J. OLIVER, E S. INDAPP, «*New FTX chief says crypto group's lack of control worse than Enron*», Financial Times, 18 novembre 2022, https://www.ft.com/content/7e81ed85-8849-4070-a4e4-450195df08d7.

[214] O. KHARIF «*Crypto Billionaire Sam Bankman-Fried Eyeing Bid for Celsius Assets*», Bloomberg, 28 settembre 2022, https://www.bloomberg.com/news/articles/2022-09-27/crypto-billionaire-bankman-fried-eyeing-bid-for-celsius-assets e S. CHURCH, «*FTX's $1.4B deal for bankrupt lender Voyager is canceled*», Bloomberg *BNN*, 15 novembre 2022, sez. Company News, https://www.bnnbloomberg.ca/ftx-s-1-4-billion-deal-for-bankrupt-lender-voyager-is-canceled-1.1846741.

violato il meccanismo di *governance* e quindi acquisito i mezzi per controllare i protocolli della piattaforma (cd. "*Governance Hacks*"), riuscendo a dirottare gli *asset*.

Nel 2022, altre piattaforme hanno subito lo stesso tipo di attacco, mettendo in dubbio la capacità dell'industria di gestire e migliorare la sicurezza informatica.

Una mancanza di adeguata gestione e analisi del rischio combinata con frode e cattiva condotta è anche rinvenibile nelle ICO (*Initial Coin Offering*)[215].

In merito al processo di offerta, ciò che porta alla ICO può anche essere articolato in diverse fasi. Un primo passo riguarda la progettazione e lo sviluppo tecnico dei *token*, degli *smart contract* e, se previsto, della nuova *blockchain* che il promotore intende sviluppare.

Come già sottolineato, generare una nuova *blockchain* non è un elemento indispensabile in tutte le ICO, dato che è possibile creare nuovi *token* operando su *blockchain* preesistenti. Analogamente alle IPO, la proposta di *crypto-assets* di solito è accompagnata dalla pubblicazione di un documento "esplicativo" che ricorda molto il prospetto di una IPO. Questo documento viene comunemente chiamato "*white paper*" e ha come finalità principale quella di chiarire ai futuri detentori di *token* le finalità della raccolta e il progetto alla base di essa.

Una sezione del documento tratta dell'aspetto tecnico-informatico dei *token* o degli *smart contract* coinvolti. A differenza di un tradizionale prospetto, il *white paper* non ha ancora un formato *standard* imposto dagli organi di regolamentazione, sebbene ambisca a fornire le stesse informazioni chiave per ridurre le asimmetrie informative tra emittente ed investitore. Questo comporta un grado di rischio maggiore per coloro che partecipano all'offerta.

Il denominatore comune di molti progetti di criptovalute è la nascita di un *token* insieme ad una divulgazione inadeguata delle informazioni, supportata da promesse e

[215] "*L'acronimo comunemente usato per indicare l'offerta al pubblico di cripto-attività è ICO, il quale deriva da Initial Coin Offering. Una Initial Coin Offering è uno strumento di finanziamento alternativo di cui le imprese possono avvalersi grazie ai recenti sviluppi delle DLT. Una ICO consiste, infatti, nell'offerta al pubblico di cripto-attività in cambio di altre cripto-attività oppure di moneta avente corso legale. Il termine ICO richiama l'acronimo IPO riferibile alle Initial Public Offering. Confrontando IPO e ICO, si osserva come l'obbiettivo di entrambe sia quello di offrire al pubblico "strumenti" emessi dall'emittente, ricevendo in cambio dei fondi che verranno utilizzati per lo sviluppo di un progetto imprenditoriale. Nelle IPO, queste attività sono costituite generalmente da strumenti finanziari; nelle ICO, invece, oggetto d'offerta sono cripto-attività che, come già anticipato, possono anche non avere natura finanziaria.*" In S. L. FURNARI, «*La finanza decentralizzata. Cripto-attività, protocolli, questioni giuridiche aperte*» 2023.

annunci eccessivamente entusiastici e una tendenza ad evitare la regolamentazione finanziaria attraverso una auto-classificazione eccessivamente generosa degli *asset*.

Occorre segnalare che il problema con la bolla dell'ICO non sta nel fallimento di progetti innovativi: i fallimenti possono accadere nelle imprese innovative e le perdite sono insite nella nozione di investimento. Tuttavia, la criticità in questione è che molti fallimenti di progetti cripto sono stati causati da debolezze istituzionali che hanno portato a distorsioni operative, facilitando frodi e furti, mentre i fondi degli investitori e dei clienti erano bloccati dall'infrastruttura tecnologica (IT), il tutto senza adeguati sistemi di trasparenza e protezione degli investitori[216].

L'elemento centrale del "*Crypto Winter"* è stata la centralizzazione nei *Systemically Important Crypto Intermediaries* (SICIs)[217] che si sono rivelati *too big to fail* e anche *too connected to fail* nel contesto del loro ecosistema.

Seppur fino ad oggi le questioni nell'ecosistema *crypto* hanno avuto un impatto limitato sulla stabilità finanziaria nella finanza tradizionale, è adesso chiaro che, come già avvenuto con l'evoluzione delle istituzioni e infrastrutture finanziarie sistemicamente importanti nella finanza tradizionale, l'ecosistema crittografico si deve evolvere per generare la propria disciplina volta a limitare il più possibile il rischio sistemico.

I SICIs si formano perché tutte le transazioni di una determinata cripto-attività dipendono dall'esistenza dell'intermediario correlato.

All'interno del loro ecosistema, molti *exchange* sono esempi classici di istituzioni finanziarie non bancarie sistemicamente significative; in sintesi, rispondono al fenomeno dello "*shadow banking*[218]" o "intermediari finanziari non bancari", che hanno avuto un rilievo cruciale in molte crisi finanziarie e sono un importante *focus* nelle politiche dei principali regolatori a livello globale.

---

[216] D. A. ZETZSCHE, R. P. BUCKLEY, D. W. ARNER, L. FÖHR «*The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*», SSRN Scholarly Paper (Rochester, NY, 24 luglio 2018), https://doi.org/10.2139/ssrn.3072298.

[217] "*a new category of systemically important crypto intermediaries (SICIs) similar to traditional systemically important financial institutions (SIFIs)*" in S. ANIMASHAUN, «*Great Crypto Crisis: The Prudential Regulation of Systemically Important Crypto Conglomerates*», SSRN Scholarly Paper (Rochester, NY, 20 dicembre 2022), https://doi.org/10.2139/ssrn.4307586.

[218] Il termine "*shadow bank*" è stato coniato dall'economista Paul McCulley in un discorso tenuto in occasione del simposio finanziario annuale del 2007 ospitato dalla Federal Reserve Bank di Kansas City a Jackson Hole, nel Wyoming. McCulley si è concentrato sugli Stati Uniti e si riferiva principalmente alle istituzioni finanziarie non bancarie impegnate nella trasformazione delle passività.". In «*Shadow Banks: Out of the Eyes of Regulators*», IMF, https://www.imf.org/en/Publications/fandd/issues/Series/Back-to-Basics/Shadow-Banks.

Come è stato evidenziato in precedenza, molti modelli di *business* nel campo delle cripto-attività sono caratterizzati da elementi cruciali nella struttura e nella *governance*, centralizzate[219].

La vera Finanza decentralizzata "*Pure DeFi*" è un fenomeno attualmente non realizzato nella prassi e il mercato ha sviluppato la centralizzazione, con i conseguenti rischi di *governance* e di agenzia, già noti alla finanza tradizionale[220].

Il collasso di FTX è infatti la prova evidente: FTX, non operava in modo decentralizzato e non utilizzava la DeFi con i suoi modelli di *business* e con le sue procedure operative. FTX è stato un esempio dell'evoluzione della centralizzazione dei servizi in cripto, dei suoi fallimenti di mercato e delle esternalità negative, fenomeni con cui la regolamentazione non ha mantenuto il passo.

La centralizzazione degli *exchange* è in contrasto con la filosofia DeFi, la quale è intrinsecamente ideata per eliminare la necessità di intermediari finanziari tradizionali che concentrano nei prodotti finanziari i flussi di domanda e offerta.

La decentralizzazione dovrebbe eliminare i fallimenti di mercato e le vicende patologiche caratteristiche della finanza tradizionale. Ciò per cui le cripto-attività erano state progettate per prevenire, è venuto a caratterizzare il loro ecosistema: le economie di scopo e di scala della finanza combinate con gli effetti di rete della tecnologia hanno portato alla nascita di grandi intermediari complessi di importanza sistemica per i loro stessi utenti.

L'opacità e la complessità degli *exchange* centralizzati comportano, inoltre il rischio di *shadow banking*, *shadow finance* e arbitraggio normativo.

Alla base di questi rischi è rinvenibile una moltitudine di funzioni economiche abbinate alla mancanza di trasparenza riguardo alle operazioni effettive, nonché la mancanza di una regolamentazione appropriata di queste varie funzioni economiche. Queste criticità divengono evidenti se confrontate con i principali tipi di intermediari nella finanza tradizionale.

Le borse valori, per esempio, dopo secoli di crisi e scandali, ora sono soggette a una rigida regolamentazione dei titoli, che richiede conti separati per ciascun cliente[221].

---

[219] cfr. L. ANKER-SØRENSEN, D. A. ZETZSCHE, «*From Centralized to Decentralized Finance: The Issue of "Fake-DeFi"*», SSRN Scholarly Paper (Rochester, NY, 22 dicembre 2021), https://doi.org/10.2139/ssrn.3978815.

[220] *ibidem*

[221] cfr. THE FINANCIAL CRISIS INQUIRY COMMISSION, «*THE FINANCIAL CRISIS INQUIRY REPORT*», gennaio 2011, http://fcic-static.law.stanford.edu/cdn_media/fcic-reports/fcic_final_report_full.pdf.

Questa garanzia assicura che, in caso di insolvenza dell'intermediario, gli *asset* dei clienti siano separati dal patrimonio dell'intermediario e possano essere almeno in parte restituiti ai clienti. I requisiti di separazione patrimoniale, custodia e tutta la disciplina dei controlli operativi ai fini di garantire la sicurezza e la stabilità, sono tutti posti al centro della regolamentazione. Gli *exchange* di cripto-attività spesso si raffigurano come intermediari, ma molto raramente seguono la regolamentazione a questi destinata[222].

Se consideriamo gli organismi di investimento collettivo del risparmio (OICR), notiamo che gli *asset* gestiti da questi, sono tutti separati da quelli degli altri clienti e dell'intermediario stesso. Per qualsiasi scelta di investimento, l'interesse degli investitori collettivi, come definito nei documenti costitutivi, dovrebbe essere l'unica linea guida, identificata nella politica di investimento e strettamente distinta dagli interessi dell'intermediario coinvolto.

Qualsiasi investimento in una cripto-attività dovrebbe essere effettuato solo se tale *asset* sembri essere un buon investimento dal punto di vista del cliente (c.d. *best execution*).

I gestori di *asset* che prendono decisioni di investimento per conto del fondo (ad esempio, come, Alameda) non devono tenere conto dei benefici che l'acquisizione o la dismissione di determinati *asset* (ad esempio FTT) possono creare per un'entità correlata (ad esempio lo scambio FTX). Inoltre, le regole sui conflitti di interesse dovrebbero attivamente impedire che questo accada.

Se consideriamo invece una banca, la quale riceve fondi sotto forma di depositi e presta o investe la maggior parte di essi.

Le banche sono soggette a una serie di requisiti normativi prudenziali per aumentare la loro sicurezza e solidità e mantenere la fiducia nell'istituzione e quella del mercato, sia per sostenere il loro ruolo chiave nei pagamenti e nelle finanze (un'esternalità positiva), sia per ridurre i rischi di contagio (un'esternalità negativa).

[222]D. CHU, «*BROKER-DEALERS FOR VIRTUAL CURRENCY: REGULATING CRYPTOCURRENCY WALLETS AND EXCHANGES*», *Columbia Law Review*, 2018, https://columbialawreview.org/content/broker-dealers-for-virtual-currency-regulating-cryptocurrency-wallets-and-exchanges/.

Osservando i CEX, gli investitori potrebbero aver utilizzato i "criptoderivati" (come *forward*[223] e opzioni[224] su *cripto-asset*) al pari di sostituti del contante, e questa confusione tra investimento e contante potrebbe essere stato ulteriormente incoraggiato dalla comunicazione fuorviante da parte *exchange*. Da questa prospettiva, molte attività cripto sembrano più simili a quelle di una banca che di un *exchange*[225].

Questi *exchange* operano in altre parole, come una banca, ma non sono soggetti alla stringente regolamentazione bancaria e non hanno garanzie come l'assicurazione sui depositi, i *framework* in caso di crisi ed infine, non hanno una banca centrale come fornitore di liquidità di ultima istanza. Tutte queste misure mirano ad evitare crisi di liquidità e di fiducia, ma nessuna di queste, (inclusi i livelli minimi di capitale quelli di liquidità obbligatoria) si applicano ai CEX.

Di conseguenza si è assistito a vicende assimilabili alle corse agli sportelli, che hanno visto coinvolti numerosi CEX (per ultimo FTX, ma anche Mt. Gox[226] e altri); ciò è avvenuto logicamente a causa dell'assenza di misure progettate per prevenire gestire queste situazioni di crisi[227].

Data la *financialization* e l'aumento dei CEX di rilevanza sistemica, è improbabile che i fallimenti del 2022 siano gli ultimi fallimenti nell'ecosistema DeFi.

---

[223] *"I contratti forward sono contratti di compravendita "a termine" e si differenziano da quelli "a pronti" per il fatto che la consegna del bene oggetto del contratto (il sottostante) e il pagamento del prezzo pattuito avvengono a una data futura prefissata e non nel momento in cui le due parti raggiungono d'accordo."* BORSA ITALIANA, «*Che cosa sono i contratti forward*», https://www.borsaitaliana.it/notizie/sotto-la-lente/forward-179.htm.

[224] "*Le opzioni sono strumenti finanziari il cui valore non è autonomo ma deriva dal prezzo di una attività sottostante di varia natura (reale come nel caso di materie prime quali grano, oro, petrolio, ecc. , oppure finanziaria come nel caso di azioni, obbligazioni, tassi di cambio, indici, ecc.). Il termine "derivato" indica questa dipendenza*.". BORSA ITALIANA, «*Le opzioni: definizione e funzionamento*», https://www.borsaitaliana.it/notizie/sotto-la-lente/opzioni.html.

[225] W. D. O'CONNELL, «*Crypto Platforms Say They're Exchanges, but They're More like Banks*», *The Conversation*, 11 agosto 2022, http://theconversation.com/crypto-platforms-say-theyre-exchanges-but-theyre-more-like-banks-188339.

[226] "*Mt. Gox fallì all'inizio del 2014, gestiva circa il 70% delle transazioni Bitcoin in tutto il mondo. Senza dubbio, Mt. Gox era un intermediario di importanza sistemica per l'ecosistema Bitcoin. Una miscela di incompetenza, mancanza di gestione del rischio e promesse irrealistiche incontrò una massa di clienti crypto troppo entusiasti alla ricerca di alti rendimenti. Una volta che le capacità e le risorse del sistema furono eccessivamente stressate in ragione della grande quantità di transazioni, fu facile essere vittima di furti e frodi: nel caso di Mt. Gox ciò si manifestò nella forma di attacco all'hot wallet, apparentemente in corso dal 2011. Che un tale attacco non sia stato rilevato per oltre tre anni dimostra carenze interne nella contabilità e nell'audit. A posteriori si scoprì che queste funzioni fondamentali, non erano conformi agli standard prescritti per gli intermediari finanziari regolamentati o persino un comportamento aziendale ragionevole, particolarmente quando si tratta delle risorse altrui (il classico rischio di agenzia nella finanza).*" In M. J. CASEY, E. WARNOCK, R. SIDEL, «*Mt. Gox Halts All Transactions in New Bitcoin Setback*», 26 febbraio 2014, The Wall Street Journal, https://www.wsj.com/articles/SB10001424052702304834704579404101502619422.

[227] G. SELGIN, «*Bank and Crypto Runs: F(Ac)TX vs Fiction*» Cato Institute (21 novembre 2022), https://www.cato.org/blog/bank-crypto-runs-factx-vs-fiction.

Le ultime vicende a seguito del fallimento di FTX[228] confermano che gli *exchange* centralizzati sono esposti ai classici rischi finanziari, operativi ed ai fallimenti di mercato.

Nella finanza tradizionale, queste questioni sono mitigate dalla regolamentazione, il che solleva la questione di come regolamentare gli *exchange*.

Un'altra lezione dal passato è che la fiducia nel mercato richiede trasparenza, e protezione da frodi e abusi.

La fiducia nelle istituzioni finanziarie è complementare all'attenuazione del rischio e questa fiducia è indispensabile per l'efficienza e lo sviluppo del mercato.

Mentre alcuni sostengono che il miglior approccio è quello di separare la DeFi dalla finanza lasciandola in gran parte non regolamentata, se si segue l'approccio europeo che è culminato del MiCAR, ci si avvicina sempre di più ad un approccio regolamentare simile a quello della *TradFi*, tanto da parlare di "Mifidizzazione della MiCA[229]".

## 4.1 Rischi sistemici nelle cripto-attività: uno sguardo dettagliato alle sfide regolamentari nell'ecosistema *FinTech*

L'esistenza di una forte regolamentazione finanziaria ha spesso stimolato i tentativi di aggirarla e tale "arbitraggio normativo" è talvolta facilitato dalle complesse innovazioni finanziarie[230]. È quanto infatti accaduto nel periodo precedente la crisi del 2008, quando i *credit default swap* e le cartolarizzazioni ipotecarie si sono evolute attorno alla regolamentazione finanziaria esistente, proprio come avevano fatto decenni prima i fondi comuni del mercato monetario, poiché questi servizi fornivano equivalenti funzionali per i prodotti bancari ma operavano al di fuori della sfera bancaria regolata, sono venuti a essere conosciuti come "*shadow banking*".

Furono intrapresi pochi passi per frenare questi tipi di innovazione, e l'aumento della leva finanziaria, della rigidità del sistema e della conseguente fragilità che essi

[228] i.e. cfr. S. ELLI E P. SOLDAVINI, «*The Rock Trading, arriva la liquidazione giudiziale*», *Il Sole 24 ORE*, 14 aprile 2023, sez. Finanza, https://www.ilsole24ore.com/art/the-rock-trading-arriva-liquidazione-giudiziale-AEy0gZHD.
[229] M.T. PARACAMPO, «*I prestatori di servizi per le cripto-attività Tra mifidizzazione della MICA e tokenizzazione della Mifid»* (G. Giappichelli Editore, 2023).
[230] S. OMAROVA, «*License to Deal: Mandatory Approval of Complex Financial Products*», 63, 70 *Cornell Law Faculty Publications*, 1 gennaio 2012, https://scholarship.law.cornell.edu/facpub/1011.

crearono divenne evidente durante la crisi finanziaria del 2008. Solo dopo quella crisi legislatori e regolatori intervennero con alcune correzioni normative.

Quasi quindici anni dopo la crisi finanziaria del 2008, c'è ancora molto da apprendere dai danni che questa ha creato: ricerche recenti si sono concentrate su come quella crisi ha incrementato le disuguaglianze[231].

La crisi del 2008 non era però inevitabile. Parte della responsabilità può essere attribuita ai regolatori finanziari, per aver adottato un approccio di "*wait and see*" nei confronti dello *Shadow Banking*.

Nel suo rapporto sulle cause della crisi, la Financial Crisis Inquiry Commission[232] concluse che «fallimenti diffusi nella regolamentazione e nella supervisione finanziaria si dimostrarono devastanti per la stabilità dei mercati finanziari della nazione»[233].

La fiducia nel nostro sistema finanziario tradizionale (e nelle agenzie che lo sorvegliano) è stata giustamente scossa dalla crisi del 2008. Ciò ha comprensibilmente suscitato interesse verso un sistema finanziario alternativo, decentralizzato, dove nessuno ha bisogno di fidarsi di alcun intermediario perché gli intermediari sono stati resi superflui. Sfortunatamente, questo è un obiettivo non realistico allo stato attuale.

Le nuove tecnologie riconducibili all'ecosistema delle cripto-attività evitano gran parte della regolamentazione che tipicamente si applica ai servizi finanziari esistenti, ma hanno nuovamente molte delle fragilità rinvenibili nella finanza tradizionale prima del 2008.

In particolare, (i) la produzione illimitata di *token* può introdurre più leva nel sistema, potenzialmente superando la leva associata ai *credit default swap* nel periodo precedente alla crisi del 2008; (ii) gli *smart contract* sono progettati per essere ancora più rigidi dei meccanismi che hanno trasformato le cartolarizzazioni di mutui ipotecari in patti fallimentari durante la crisi; e (iii) le *stablecoin* condividono molte delle caratteristiche dei fondi comuni.

Oltre a queste fragilità, le applicazioni DeFi sono altamente complesse. La maggior parte degli investitori (inclusi gli intermediari finanziari) è abituata ad

---

[231] J. BRIDGES, G. GREEN, M. JOY, «*Credit, Crises and Inequality*», Bank of England Staff Working Paper SSRN Scholarly Paper (Rochester, NY, 12 novembre 2021), https://doi.org/10.2139/ssrn.3976327.

[232] La Financial Crisis Inquiry Commission era una commissione di dieci membri nominata dai *leader* del Congresso degli Stati Uniti con l'obiettivo di indagare sulle cause della crisi finanziaria del 2007-2008.

[233] THE FINANCIAL CRISIS INQUIRY COMMISSION, «*THE FINANCIAL CRISIS INQUIRY REPORT*», xviii (2011).

analizzare bilanci e divulgazioni scritte per valutare gli investimenti. Pochi, viceversa, sono in grado di leggere il codice informatico degli *smart contract* e valutarne l'effettiva genuinità[234]. Infine, un'ulteriore complessità deriva dalla struttura di *governance* spesso non trasparente. Questo comporta che se dovesse verificarsi un problema e fosse necessario un intervento di emergenza all'interno dell'ecosistema DeFi per arginare una crisi per il resto del sistema finanziario, risulterebbe difficile l'individuazione del soggetto cui fornire supporto di emergenza.

Tornando ai *Credit default swaps* (CDS) prima del 2008, questi crearono una leva finanziaria nel sistema aumentando esponenzialmente l'esposizione sullo stesso bene sottostante (tipicamente, un'obbligazione). Ciò può rappresentare un problema significativo nell'ecosistema DeFi, dove gli *asset* finanziari sotto forma di *token* possono essere creati dal nulla da chiunque abbia conoscenze di programmazione informatica, per poi essere eventualmente utilizzati come garanzia per prestiti, i quali possono essere usati a loro volta come collaterale per acquisire altri *asset*[235]*;* proprio come è avvenuto nel caso FTX. Inoltre, una capacità illimitata di creazione di *asset* finanziari pone il rischio di creare bolle speculative.

Le normative relative a requisiti di riserva, capitale, margine e compensazione sono volte a limitare la leva nel sistema finanziario tradizionale, ma vari studi hanno evidenziato che il margine massimo consentito negli scambi decentralizzati è superiore a quello negli scambi regolamentati nel sistema finanziario tradizionale[236].

Le pratiche di mercato che richiedono che le transazioni DeFi siano sovra-garantite con *stablecoin* potrebbero teoricamente agire come un vincolo sulla leva nell'ecosistema DeFi; tuttavia, quando *le stablecoin* vengono utilizzate come garanzia per prestiti, il ricavato di quei prestiti è spesso utilizzato come garanzia per altri prestiti, e così via (e in ogni caso, le pratiche di mercato intorno alla sovra-garanzia non sono le stesse delle esigenze regolamentari).

I *token* sono anche utilizzati (proprio come i CDS) per creare rappresentazioni virtuali di beni reali (*tokenizzazione*). Un recente rapporto della Bank for International Settlements, ha osservato che le versioni DeFi non regolamentate di *trading* di derivati

---

[234] S. COHNEY, D. A. HOFMANN, J. SKLAROFF, D. A. WISHNICK, «*Coin-Operated Capitalism*», Columbia Law Review 591 SSRN Scholarly Paper (Rochester, NY, 2019), https://doi.org/10.2139/ssrn.3215345.

[235] S. T. OMAROVA, «*New Tech v. New Deal: Fintech as a Systemic Phenomenon*», 735, 775*Yale Journal on Regulation* 36 (2019).

[236] S. ARAMONTE, W. HUANG, A. SCHRIMPF, «*DeFi Risks and the Decentralisation Illusion*», BIS Quarterly Review,2021.

sugli *exchange* decentralizzati stanno moltiplicando esponenzialmente la leva finanziaria nell'ecosistema DeFi[237].

I regolatori finanziari dovrebbero fare attenzione alla libertà di aumento illimitato di leva nell'ecosistema DeFi, specialmente se ci sono canali di contagio che potrebbero consentire alle pratiche di *deleveraging* nell'ecosistema DeFi di influenzare il sistema finanziario tradizionale e l'economia in generale. Recenti ricerche dell'IMF hanno riscontrato una crescente correlazione tra le *performance* degli investimenti in cripto-attività e investimenti della finanza tradizionale come le azioni[238]. Esistono inoltre anche canali più diretti per il contagio come quello degli intermediari finanziari regolamentati che investono o offrono, prodotti DeFi[239].

Un'altra criticità del settore è rinvenibile nell'eventuale situazione di crisi del sistema finanziario per eccessivo indebitamento; durante la fase recessiva, infatti, potrebbe essere necessaria una certa flessibilità per liberare i grandi intermediari dall'ottemperare alle *margin call* ed ai rimborsi richiesti, in modo da evitare che i fallimenti degli intermediari abbiano effetti a catena sull'intero sistema[240].

Gli *smart contract* dal canto loro, potrebbero rivelarsi troppo rigidi per fornire la suddetta flessibilità necessaria. Gli *smart contract*, infatti, sono progettati per eseguire istruzioni pre-programmate istantaneamente, senza attendere *input* dalle parti (o da un ente regolatore o da un tribunale). In situazioni ordinarie, ciò rende i processi più efficienti, ma queste istruzioni verranno eseguite altrettanto rapidamente in eventuali situazioni di crisi[241], favorendo gli effetti a catena.

Ci sono però delle strategie che possono essere intraprese per mitigare questi rischi, come ad esempio programmare uno *smart contract* per adattarsi ad eventi

---

[237] *Ibidem.*

[238] «The increased and sizeable co-movement and spillovers between crypto and equity markets indicate a growing interconnectedness between the two asset classes that permits the transmission of shocks that can destabilize financial markets. Our analysis suggests that crypto assets are no longer on the fringe of the financial system. Given their relatively high volatility and valuations, their increased co-movement could soon pose risks to financial stability especially in countries with widespread crypto adoption. It is thus time to adopt a comprehensive, coordinated global regulatory framework to guide national regulation and supervision and mitigate the financial stability risks stemming from the crypto ecosystem.» in T. ADRIAN, T. IYER, E M. S. QURESHI, «*Crypto Prices Move More in Sync With Stocks, Posing New Risks*» (IMF, 1 novembre 2022), https://www.imf.org/en/Blogs/Articles/2022/01/11/crypto-prices-move-more-in-sync-with-stocks-posing-new-risks.

[239] Cfr. V. PACELLI, M. FOGLIA, «*Rischi di spillover tra asset tradizionali e digitali*», BANCARIA, 10 (ottobre 2023).

[240] K. PISTOR, «*A legal theory of finance*», *Journal of Comparative Economics* 41, fasc. 2 (2013): 315–30.

[241] E. LIVNI, «*For Rules in Technology, the Challenge Is to Balance Code and Law*», *The New York Times*, 23 novembre 2021, sez. Business.

imprevisti (ad esempio, per consultare un altro *smart contract*, o una fonte di dati esterna cd. "*oracolo"*[242] controllato da un soggetto autorizzato), anche se tutto ciò farà aumentare i costi di transazione[243].

### 4.3 *FinTech*, l'illusione della decentralizzazione

Un recente *report* della Bank for International Settlements ha osservato che vi è "un'illusione di decentralizzazione" nella *DeFi*, che deriva dalla necessità inevitabile di una *governance* centralizzata in molte fasi operative intrinseche[244]. Anche il pioniere di *Internet* Tim O'Reilly ha notato che "la *Blockchain* si è rivelata la centralizzazione di una tecnologia decentralizzata più rapida che abbia mai visto"[245].

La necessità inevitabile di una *governance* centralizzata, nasce in ragione delle opportunità di profitto e dalla grandi difficoltà operative riscontrabili dal consumatore medio. La crescita degli *exchange* centralizzati sembra inevitabile. È possibile quindi affermare, che la necessità di intermediari è una questione economica, e non tecnologica; è l'economia che costringe le *blockchain permissionless* di successo a centralizzarsi[246].

È facile cadere nella fallacia secondo cui le attività decentralizzate siano completamente avulse da interventi umani[247], e trascurando il fatto che la tecnologia a registro distribuito si basa su persone per operare. Ogni livello di infrastruttura coinvolto nella fornitura di prodotti e servizi *DeFi* dipende effettivamente da azioni svolte da esseri umani[248].

La maggior parte delle decisioni relative al funzionamento di un registro distribuito sono prese dalle persone con il potere di validare le transazioni su quel registro, e dai principali sviluppatori del codice informatico che governa quel registro. Mentre il codice sottostante le *blockchain* come Ethereum e Bitcoin è *open-source*, ciò non significa che non ci sia una gerarchia in termini di programmatori informatici in

---

[242] Un oracolo è un *software* che fornisce dati agli *smart contract*. È una fonte di dati esterni su cui una *Blockchain* può fare affidamento e che può essere utilizzata per attivare o eseguire clausole contrattuali.
[243] HILARY J. ALLEN «*Driverless Finance: Fintech's Impact on Financial Stability», 99* (Oxford, New York: Oxford University Press, 2022).
[244] S. ARAMONTE, W. HUANG, A. SCHRIMPF, (n. 211).
[245] D. PATTERSON «I*nternet Guru Tim O'Reilly on Web3: "Get Ready for the Crash"*», CBS News, 10 febbraio 2022, https://www.cbsnews.com/news/web3-cryptocurrency-nft-tim-oreilly/.
[246] D. ROSENTHAL, «*Stanford's EE380 Talk*», https://blog.dshr.org/2022/02/ee380-talk.html.
[247] L SKITKA, K. MOSIER, M. BURDICK, «*Accountability and automation bias*», International Journal of Human-Computer Studies 52 (1 aprile 2000): 701–17, https://doi.org/10.1006/ijhc.1999.0349.
[248] H. J. ALLEN, «*DeFi: Shadow Banking 2.0?* », Washington College of Law Research Paper No. 2022-02 *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.4038788.

grado di modificare quel codice. Viceversa, i cosiddetti "sviluppatori principali" "funzionano come *leader* e *decision makers* in relazione al codice". Anche i validatori sono attori importanti, perché determinano la versione definitiva del registro[249].

Attualmente, i due meccanismi di validazione più comuni per i registri distribuiti sono *proof-of-work* e *proof-of-stake*. Il primo si basa su persone conosciute come "*miner*" che tentano, attraverso tentativi ed errori, di indovinare la risposta a un problema matematico relativo a un blocco di transazioni. Una volta che un *miner* ha una risposta, può sottoporla a tutti i nodi che ospitano il registro, ed è molto facile per quei nodi verificare se la risposta del *miner* funziona: se tutto è corretto, quei nodi per consenso adotteranno il blocco di transazioni che il *miner* ha proposto, aggiungendolo al registro distribuito e quindi iscrivendo quelle transazioni. Come evidenzia la Professoressa Angela Walch: "[i] *miner* selezionano, ordinano e propongono transazioni da aggiungere al registro della *blockchain*", il che significa che "[le] transazioni non compaiono nel registro della *blockchain* a meno che un *miner* non scelga di inserirle" e che "lo sfruttamento del potere di ordinamento delle transazioni può diventare un problema rilevante per l'ecosistema, poiché i *miner* possono trarre profitto dalla vendita anticipata di *slot* di elaborazione[250]". I *miner* in un sistema *proof-of-work* non sono solo persone, ma sono persone con conflitti di interesse.

È anche inesatto pensare ai *miner* come individui dispersi nel globo: negli ultimi anni, la maggior parte della potenza di *mining* di Bitcoin è stata costantemente concentrata in poche *mining pool*[251].

In definitiva, il codice informatico non gestisce l'ecosistema in via autonoma: la DeFi è governata da istituzioni e individui.

Molti intermediari centralizzati possono rivelarsi critici per l'ecosistema *DeFi;* gli *exchange*, sono fondamentali per la *DeFi*, perché consentono agli utenti di scambiare cripto-attività l'uno con l'altro.

Come si è visto in precedenza, esistono *exchange* con strutture di *governance* decentralizzate (ad es. Uniswap), i quali hanno maggiori costi di transazione; ebbene anche essi si affidano ad API per consentire ai dispositivi degli utenti di accedere al

[249] P. DE FILIPPI, A. WRIGHT, «*Blockchain and the Law — The Rule of Code*», Harvard University Press, 2019.
[250] A. WALCH, «*Committee on Banking, Housing, and Urban Affairs Cryptocurrencies: What Are They Good For?*», Responses to Questions for the Record UNITED STATES SENATE COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS, 27 luglio 2021.
[251] «*it only took six years for bitcoin to fail Nakamoto's goal of decentralization, with one mining pool controlling more than half the mining power. In the seven years since no more than five pools have always controlled a majority of the mining power*» ROSENTHAL (n. 220).

*ledger* distribuito su cui avvengono le transazioni, (le *blockchain* sono progettate come reti *peer to peer,* ma non in modo tale che sia davvero possibile per il singolo dispositivo *mobile* o il suo *browser*, accedere direttamente)[252].

Marlinspike, Commentando specificamente sui TPP's Infura e Alchemy, sottolinea che "è stato fatto tanto lavoro, per creare un meccanismo di consenso distribuito decentralizzato, ma praticamente tutti i clienti che desiderano accedervi lo fanno semplicemente fidandosi degli *output* di queste due aziende senza ulteriori verifiche.[253]".

In definitiva, una base decentralizzata rende i servizi finanziari apparentemente più efficienti e sostituisce la fiducia nelle istituzioni consolidate (come quelle governative e le banche regolamentate) con la fiducia in attori diversi, talvolta non identificati[254].

I conflitti di interesse che gli individui e le istituzioni in posizioni di autorità affrontano possono portare a grandi rischi per gli investitori DeFi. Questi, infatti, non hanno interesse a proteggere la stabilità finanziaria, che è un bene pubblico tipico della finanza tradizionale, appositamente tutelato dalle autorità del settore.

Anche se gli attori DeFi svolgessero al meglio le loro valutazioni di rischio, nel quadro odierno totalmente deregolamentato non avrebbero sufficienti informazioni sulle altre parti del sistema finanziario per valutare l'impatto delle loro azioni[255].

## 4.4 *Governance* e trasparenza: prospettive della regolamentazione finanziaria per un mercato *crypto* affidabile

La regolamentazione finanziaria determina il miglioramento del funzionamento e dell'efficienza del mercato; essa cerca di migliorare la trasparenza e di garantire la stabilità finanziaria, l'equità e l'integrità dello stesso, in modo da fornire adeguata protezione a clienti, depositanti ed investitori. Più recentemente, la regolamentazione

[252] M. MARLINSPIKE, «*My first impressions of web3*», OSnews, 7 gennaio 2022.
[253] *Ibidem.*
[254] E. NICOLLE, «*Crypto Secrecy Makes DeFi a Financial Felon's Wonderland*», Bloomberg, 27 gennaio 2022, https://www.bloomberg.com/news/articles/2022-01-27/crypto-s-cloak-of-anonymity-makes-defi-a-wonderland-for-felon.
[255] H. J. ALLEN, «*Driverless Finance: Fintech's Impact on Financial Stability»* Oxford University Press, 2 maggio 2022.

finanziaria ha cercato anche di supportare lo sviluppo del mercato e la crescita economica e di promuovere l'inclusione finanziaria e lo sviluppo sostenibile[256].

La regolamentazione finanziaria, sia macroprudenziale che microprudenziale, è fondamentale anche per prevenire o ridurre il rischio più significativo che sorge nel contesto della finanza: le crisi finanziarie e in particolare le crisi finanziarie sistemiche[257].

Anche se le cripto-attività non stanno sostituendo la finanza tradizionale, è lecito preoccuparsi per gli effetti *spillover*[258] derivanti dall'ecosistema cripto che possono ricadere sia su altri attori *FinTech* (come da un SICI all'altro) che sulla finanza tradizionale.

Per questo motivo, le autorità regolatrici intendono studiare ed attuare misure preventive, ad esempio, richiedendo *ex ante* informazioni sulle controparti e sulle esposizioni ed interconnessioni tra DeFi e TradFi.

Come si è detto, oltre alla stabilità finanziaria, la regolamentazione si concentra sulla promozione del funzionamento, della trasparenza e dell'efficienza dei mercati.

L'efficienza del mercato si basa sul raggiungimento di un elevato livello di informazione, ovvero un mercato nel quale i prezzi riflettono le informazioni pubblicamente disponibili[259].

Proprio l'efficienza del mercato desta una preoccupazione significativa nel settore delle cripto-attività; ad oggi, infatti, le informazioni sono disponibili in modo non strutturato e disorganizzato e sono diffuse attraverso canali non regolamentati, il che impedisce agli investitori, sia professionali che *retail,* di poter valutare in maniera adeguata le opportunità di investimento ed i relativi rischi.

Ne consegue che, fatta eccezione per alcuni *crypto-asset* di grande volume come ad esempio Ethereum, il sistema non è in grado di esprimere i prezzi in linea con il "prezzo corretto", ovvero quello basato sulle informazioni pubblicamente disponibili. Gli *exchange* operano su diverse *blockchain* e utilizzano *pool* di liquidità e meccanismi di negoziazione differenti, determinando una possibile frammentazione della liquidità

---

[256] T. Adrian, T. Iyer, e M. S. Qureshi, «Crypto Prices Move More in Sync With Stocks, Posing New Risks» (IMF, 1 novembre 2022), https://www.imf.org/en/Blogs/Articles/2022/01/11/crypto-prices-move-more-in-sync-with-stocks-posing-new-risks.

[257] F. ALLEN, X. GU, «*The Interplay between Regulations and Financial Stability*», *Journal of Financial Services Research* 53, fasc. 2 (1 giugno 2018): 233–48, 18 aprile 2018, https://doi.org/10.1007/s10693-018-0296-7.

[258] effetti diretti o indiretti, che le vicende possono determinare su altre attività economicamente connesse.

[259] E. F. FAMA, «*Efficient Capital Markets: A Review of Theory and Empirical Work*», *The Journal of Finance* 25, fasc. 2 (1970): 383–417, https://doi.org/10.2307/2325486.

tra le diverse piattaforme; di conseguenza, la stessa cripto-attività può avere prezzi diversi su diversi *exchange,* generando in questo modo potenziali opportunità di arbitraggio[260].

Infine, le cripto-attività sono intrinsecamente caratterizzate dall'avere informazioni non finanziarie riguardanti l'architettura IT, il *design* e la stabilità dei sistemi, che spesso sono centrali nella valutazione dei progetti.

Sebbene i *white paper* e le descrizioni dei progetti solitamente espongano alcune caratteristiche del *design* IT, solo pochi investitori sono in grado di comprendere a fondo sia il lato tecnico sia le loro implicazioni finanziarie, tanto da considerare e gestire i rischi.

La divulgazione è il principale strumento tradizionale per promuovere l'efficienza del mercato[261] e dovrebbe essere implementata anche nel sistema cripto, supportata dalla standardizzazione dei protocolli e dalla trasparenza su domanda e offerta.

La *disclosure* dovrebbe concentrarsi sulla standardizzazione dei requisiti di divulgazione e sui metodi di garanzia di qualità dell'informazione, come gli *standard* comuni di contabilità e revisione e sui dettagli tecnici dei progetti. Inoltre, la regolamentazione microprudenziale mirata a rafforzare la sicurezza e la solidità della struttura e delle operazioni degli intermediari, potrebbe ridurre le frodi ed i furti, facendo crescere la fiducia nel settore.

Un altro obiettivo centrale della regolamentazione finanziaria è la protezione degli investitori e dei depositanti. È necessario adottare una politica regolamentare volta a massimizzare il comportamento razionale[262].

La protezione degli investitori ha tre linee direttrici: i) la *disclosure*, per consentire agli investitori di prendere decisioni informate, ii) regolamentazione del settore per affrontare comportamenti patologici ampiamente riscontrati nel passato della finanza tradizionale e iii) adozione di meccanismi prudenziali per ridurre la probabilità di perdite derivanti dai possibili fallimenti degli intermediari.

Inoltre, come per la finanza tradizionale, è necessario affrontare i conflitti di interesse derivanti dalle funzioni di intermediazione.

---

[260] V. PACELLI, M. FOGLIA, «*Rischi di spillover tra asset tradizionali e digitali*», BANCARIA, 10 (ottobre 2023).
[261] C. KORSMO, «*The Audience for Corporate Disclosure*», Iowa L. Review 1581 (2017).
[262] Cfr. C. GOODHART, P. HARTMANN, D. T. LLEWLLYN, L ROJAS-SUAREZ, S. WEISBROD «*Financial Regulation: Why, How and Where Now?*», *Routledge & CRC Press*, 1998.

L'equità e l'integrità del mercato si concentrano sulla prevenzione sia dell'uso fraudolento del sistema finanziario (in particolare nel contesto del riciclaggio di denaro e del finanziamento del terrorismo) sia della frode e degli abusi.

La vicenda FTX rappresenta un caso emblematico per quanto riguarda le pratiche di *insider trading* e abusi di mercato; come è stato analizzato, Binance, in qualità di principale *competitor* di FTX, ha pubblicamente messo in dubbio l'affidabilità finanziaria di FTX[263]. Un comportamento simile non si sarebbe potuto tenere nella finanza tradizionale regolamentata dove qualsiasi affermazione simile andrebbe contro le norme in materia di abusi e manipolazione di mercato.

Emergono una serie di altre preoccupazioni nel contesto della custodia. Ad esempio, molti *exchange* hanno riutilizzato gli *asset* dei clienti detenuti in custodia senza il consenso dei clienti stessi e senza requisiti di *governance* adeguati. Questo è facilitato dal fatto che, come è stato sottolineato in precedenza, la divisione delle funzioni all'interno dell'ecosistema *crypto* non è sempre trasparente riguardo a chi funge da parte contrattuale e fornitore di liquidità. Inoltre, l'uso di conti *omnibus,* senza separazione, comporta la confusione delle attività dell'intermediario con quelle in cripto-attività di terzi.

Parte della dottrina internazionale ritiene che quando la finanza decentralizzata trova dei punti di contatto la finanza tradizionale, e allo stesso modo quando si presentano nuovi rischi derivanti dalla decentralizzazione mai affrontati prima, si debba applicare il paradigma secondo cui è necessaria una regolamentazione; la DeFi stessa richiede regolamentazione per raggiungere il suo obiettivo principale di decentralizzazione[264].

Il punto di riferimento non dovrebbe essere ciò che ha funzionato bene per la finanza tradizionale. L'obiettivo è una regolamentazione adatta (e per alcuni aspetti completamente nuova) per un'industria immatura che è tecnologicamente diversa da ciò che l'ha preceduta ma che in molti casi mostra comunque punti deboli, come fallimenti di mercato ed esternalità simili al passato.

Esistono delle teorie a mio avviso condivisibili in materia regolamentare, che uniscono le *best practice* della TradFi a nuovi paradigmi regolamentari. Il primo

[263] IL SOLE 24 ORE, «*Binance: il CEO CZ lascia la guida dopo un accordo con la giustizia americana*», 22 novembre 2023, https://www.ilsole24ore.com/art/binance-accordo-dip-giustizia-usa-zhao-si-dimette-e-si-dichiara-colpevole-AF7QuXjB.

[264] D. A. ZETZSCHE, R. P. BUCKLEY, D. W. ARNER, «*The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*», SSRN Scholarly Paper (Rochester, NY, 13 agosto 2017), https://doi.org/10.2139/ssrn.3018214.

requisito fondamentale per l'evoluzione della DeFi è la licenza, in quanto i servizi in materia di cripto-attività dovrebbero essere inibiti se non debitamente autorizzati.

Diverse prescrizioni legali possono essere associate alla licenza: definizione e delimitazione dei servizi forniti, obbligo di mantenimento costante di un'organizzazione adeguata sia per risorse umane che per IT professionali. Inoltre, sono necessarie una gestione idonea e appropriata, una condotta trasparente nelle operazioni e l'applicazione di regole prudenziali, come i requisiti di capitale minimo, le soglie di liquidità e di rischio consentito etc.[265]

L'uso del termine "*exchange*" dovrebbe essere riservato ad entità che mettono insieme la domanda e l'offerta di terze parti in un ambiente adeguatamente strutturato e gestito, mentre le attività di *broker-dealer*, *market maker*, le banche ed i gestori di *asset* dovrebbero essere tutti soggetti a requisiti su misura.

Nel redigere le regole di licenza, gli enti preposti dovranno definire precisamente i servizi e le attività correlate. In assenza di un approccio regolamentare chiaro e completo, prevarrà l'incertezza legale e gli intermediari potrebbero rimanere, (o cercare di restare), al di fuori dell'ambito della regolamentazione[266]. La certezza legale è fondamentale per garantire l'adeguato funzionamento del sistema[267].

Fondamentali per il funzionamento dei mercati finanziari sono le informazioni. Nel contesto delle cripto-attività, la *disclosure* obbligatoria finora ha ricevuto scarsa attenzione sia dai partecipanti al mercato che dagli enti regolatori[268].

In primo luogo, c'è la necessità di fornire informazioni finanziarie analoghe a quelle richieste dalla regolamentazione dei titoli tradizionali. Dovrebbe essere richiesto agli emittenti una documentazione iniziale con requisiti minimi stringenti (come quelli del prospetto) e informazioni periodiche tramite rapporti semestrali e annuali. La *blockchain* potrebbe essere un sistema molto efficiente a tale scopo, potrebbe, tramite un progetto adeguato, fornire informazioni in tempo reale agli enti regolatori[269].

---

[265] S. OMAROVA, «*Dealing with Disruption: Emerging Approaches to Fintech Regulation*», 61, *Cornell Law Faculty Publications*, 1 gennaio 2020,

[266] J. LEE, F. L'HEUREUX, «*A regulatory Framework for Cryptocurrency*», *European Business Law Review* Rev. 423 (2020).

[267] T. van der Linden, T. Shirazi, «*Markets in crypto-assets regulation: Does it provide legal certainty and increase adoption of crypto-assets?*», *Financial Innovation* 9, fasc. 1 (10 gennaio 2023): 22, https://doi.org/10.1186/s40854-022-00432-8.

[268] J. CHOU, P. AGRAWAL, J. BIRT, «*Accounting for crypto-assets: stakeholders' perceptions*», *Studies in Economics and Finance* (14 gennaio 2022), https://doi.org/10.1108/SEF-10-2021-0469.

[269] D. W. ARNER, J. BARBERIS, R. P. BUCKLEY, «*FinTech, RegTech, and the Reconceptualization of Financial Regulation*», *Northwestern Journal of International Law & Business* 37, fasc. 3 (1 gennaio 2017).

In secondo luogo, gli *exchange* autorizzati dovrebbero fornire informazioni pre e post negoziazione, oltre a rispettare i doveri di *best execution*; dovranno anche fornire informazioni sulla struttura del gruppo societario a cui appartengono e sulle attività in cui sono coinvolti, in modo che le controparti possano valutare e comprenderne i rischi.

Oltre a queste regole di *disclosure* che fanno parte del repertorio *standard* degli enti regolatori, potrebbero essere affiancate regole secondo le quali gli emittenti e gli intermediari debbano divulgare le caratteristiche della struttura operativa e dell'ambiente IT in cui l'*asset* crittografico è emesso e scambiato. Questo includerebbe la specifica distinzione delle funzioni centralizzate e decentralizzate.

Potrebbe essere utile anche richiedere di specificare come le funzioni decentralizzate essenziali funzionerebbero in caso di crisi.

Per garantire la custodia sicura degli *asset*, è anche necessario prescrivere la separazione obbligatoria della custodia da altre attività di intermediazione (come lo scambio, il *brokerage*, il *market making* e il *trading* proprietario) e sottoporre il servizio di custodia ad una apposita licenza.

Tale modello regolamentare potrebbe garantire che gli *asset*, senza il consenso del proprietario, non possano essere prestati, scambiati o utilizzati come garanzia in transazioni sul conto dell'intermediario. Qualsiasi prestito di *asset* cripto a beneficio degli investitori dovrebbe essere debitamente documentato, contrassegnato, tracciato sulla *blockchain* e monitorato dal prestatore di servizi di custodia, mentre i rischi di controparte durante le transazioni dovrebbero essere adeguatamente gestiti[270].

L'industria delle cripto-attività ha già preso l'iniziativa negli ultimi anni di creare protocolli di "*Proof of reserves"* (PoR)[271]. A tale riguardo, l'idea generale è che un *exchange* o un altro intermediario, sottoponga le proprie riserve a revisione secondo intervalli regolari. Sarebbe preferibile che tali soggetti rendessero pubblico il loro PoR, rendendolo consultabile in tempo reale, in questo modo sia gli enti regolatori che il pubblico potrebero accedere e potenzialmente monitorare la dichiarazione PoR come necessario.

[270] M. HAENTJENS, T. DE GRAAF, I. KOKORIN, «*The Failed Hopes of Disintermediation: Crypto-Custodian Insolvency, Legal Risks and How to Avoid Them*», Hazelhoff Research Paper Series No. 9, Leiden Law School, 30 april 2020, https://doi.org/10.2139/ssrn.3589381.

[271] M. MAURER, «*More Crypto Exchanges Verify Reserves, But Questions About Assets Remain*», 5 dicembre 2022, The Wall Street Journal, https://www.wsj.com/articles/more-crypto-exchanges-verify-reserves-but-questions-about-assets-remain-11670153687.

Nonostante sia molto difficile per la maggior parte del pubblico generale eseguire l'analisi *blockchain* necessaria per revisionare effettivamente il PoR, tuttavia il fatto che alcuni utenti (e soprattutto gli enti regolatori) possano farlo, dovrebbe contribuire in modo significativo a garantire che i fondi dei clienti detenuti da uno scambio cripto o da un progetto siano conservati in modo sicuro e custoditi adeguatamente.

La legislazione sulla risoluzione della crisi è cruciale per fornire continuità al sistema ed evitare effetti *spillover*[272].

Se verranno applicate ai prestatori di servizi regole che vadano a mitigare i rischi e che rendano meno opache le gestioni degli stessi e delle loro attività, i casi di insolvenza dovrebbero diminuire sensibilmente.

Nel caso in cui vi sia un SICI con una posizione dominante all'interno del mercato, non è opportuno istituire un altro *provider* come prestatore di ultima istanza a causa dei conflitti di interesse e dei rischi morali intrinseci che ne possono derivare[273]. Nel caso in cui si rendesse necessario per il sistema finanziario o per uno dei suoi segmenti, le banche centrali potrebbero avere in un prossimo futuro i mezzi per iniettare liquidità tramite *stablecoin* regolamentate, CBDC sintetiche[274] e valute digitali delle banche centrali.

Molte delle sfide rivelatesi durante il "*crypto winter"* sono ben note nella finanza tradizionale e riguardano: rischi di agenzia, conflitti di interesse, mancanza di trasparenza, rischi di controparte, rischi operativi e modalità di gestione con cui singoli intermediari spesso dominavano il *trading* e la creazione di mercato di certi *asset* crittografici. Per tutte queste questioni sarebbe ragionevole il principio "*same risk, same rules*".

Tuttavia, considerata la peculiarità del settore, le cripto-attività richiedono una regolamentazione su misura. La decentralizzazione delle cripto-attività richiede che molte entità, piuttosto che solo una, lavorino insieme per garantire la conformità, la sicurezza informatica, la custodia degli *asset* e la protezione degli investitori; tale decentralizzazione, anche parziale, pone particolari difficoltà nel garantire la

[272] Cfr. H. BENEDETTI, G. RODRÍGUEZ-GARNICA, «*Tokenized Assets and Securities*», in *The Emerald Handbook on Cryptoassets: Investment Opportunities and Challenges*, a c. di H. KENT BAKER et al. (Emerald Publishing Limited, 2023), 107–21, https://doi.org/10.1108/978-1-80455-320-620221008.

[273] Sebbene gli intermediari di criptovalute possano svolgere ruoli importanti in future ristrutturazioni, l'esempio di FTX-Binance ha dimostrato che gli intermediari di cripto-attività hanno i propri interessi e non sono quindi dei prestatori di ultima istanza affidabili.

[274] Una *central bank digital currency* (CBDC) è una tipologia di valuta digitale emessa da una banca centrale.

continuità aziendale in caso di insolvenza, poiché con l'insolvenza scompaiono gli incentivi finanziari che tendono a mantenere il sistema stabile.

A causa delle sue funzioni parzialmente decentralizzate, la DeFi è, da un punto di vista tecnico e finanziario, complessa. Richiede competenze aggiuntive da parte degli intermediari, dei *gatekeeper* (inclusi avvocati e revisori), e degli enti regolatori.

Come precedentemente spiegato, parte della dottrina ritiene che il *test* di idoneità e adeguatezza della maggior parte dei regimi di licenza, nonché la trasparenza garantita da un approccio basato sul Piano Aziendale, in aggiunta ai requisiti di *disclosure* standardizzati, siano però misure adeguate a consentire ai partecipanti al mercato e ai regolatori di controllare questa maggiore complessità.

È importante inoltre tenere sotto osservazione l'interazione tra il modello di intermediazione tradizionale e quello decentralizzato, cercando di strutturare soluzioni tecnologiche resilienti e sostenibili.

Le principali sfide riguardano proprio la definizione dei confini normativi e la definizione delle responsabilità di *governance,* in un contesto così frammentato.

L'innovazione sta ridefinendo i modelli di *business*, di supervisione e normativi che sono stati stabili per decenni, come la vigilanza per soggetti. Di conseguenza è essenziale una stretta collaborazione tra le autorità per monitorare i rischi in maniera integrata e per sfruttare le sinergie informative e di competenze, garantendo così un controllo coerente ed efficacie su tutto il sistema.

In questo scenario di rapido sviluppo tecnologico, emerge un panorama inedito che fonde elementi finanziari e tecnologici, nonché responsabilità in ambito di vigilanza prudenziale, regolamentazione dei prodotti bancari e di investimento, supervisione del sistema dei pagamenti (infrastrutture, prodotti, servizi), stabilità finanziaria e protezione del consumatore[275].

Come si è detto il tumulto del 2022 nel mercato delle cripto-attività ha evidenziato la necessità di sviluppare un quadro normativo efficace per gli emittenti e i fornitori di servizi in questi mercati. Tali episodi di *stress* non hanno comunque generato *spillover* significativi nel sistema finanziario tradizionale né nell'economia reale, grazie alla bassa interconnessione con gli intermediari finanziari tradizionali e all'uso limitato di questi *asset* per pagamenti o investimenti da parte delle famiglie e delle società. Tuttavia, ci vorrà ancora tempo per svelare tutte le ramificazioni del

[275] G. SIANI, «*La regolamentazione delle nuove tecnologie basate sulla Distributed ledger technology – DLT, tra tutela del mercato e rischi di sistema*» (BANCA D'ITALIA, 3 maggio 2022).

fallimento di FTX, che era al centro di una complessa rete di relazioni con fondi di *venture capital* e altri investitori istituzionali. Se il coinvolgimento del sistema finanziario tradizionale continuasse a crescere o le cripto-attività diventassero più popolari tra gli utenti, le vulnerabilità in questo settore potrebbero assumere un'importanza significativa per l'intero sistema.

È auspicabile in questo senso il principio di "*same risk, same regulatory outcome*" Le regole per gli emittenti di cripto-attività e i fornitori di servizi che possono essere effettivamente regolamentati dovrebbero sottostare agli stessi *standard* regolamentari di quelli previsti per gli intermediari finanziari che forniscono servizi simili nel sistema finanziario tradizionale[276]. In particolare, le attività svolte da emittenti e fornitori di servizi sono generalmente caratterizzate da questioni di protezione dei consumatori, leva finanziaria, trasformazione di liquidità e rischi legati a garanzie e concentrazioni che dovrebbero essere affrontati[277].

È necessario migliorare le pratiche di gestione del rischio nelle parti dell'ecosistema che non possono essere effettivamente regolamentate. Le autorità potrebbero riflettere su come incentivare l'adozione di pratiche di gestione del rischio sicure e solide da parte delle entità coinvolte o che operano in aree non direttamente coperte dalla regolamentazione finanziaria.

Si consideri che gli *exchange* e le *lending platforms* sono stati fattori chiave nell'amplificare il *market stress*. Come è stato analizzato, le loro debolezze erano legate sia a cattive pratiche di gestione del rischio sia alla mancanza di requisiti regolamentari che potessero mantenere la loro capacità di far fronte ai flussi di uscita degli investitori, in particolare durante i periodi di *stress* di mercato. Ciò suggerisce alcune considerazioni relative alle attività di *lending/borrowing* e degli *exchange*:

I fornitori di servizi di cripto-attività che si occupano di attività di prestito e/o che prendono in prestito cripto-attività dai clienti, dovrebbero essere soggetti a una regolamentazione adeguata che affronti i rischi di credito, di mercato e di liquidità. In particolare, un quadro normativo per queste entità dovrebbe introdurre requisiti prudenziali (requisiti di capitale e liquidità) proporzionali ai rischi assunti da questi intermediari. Le piattaforme di *lending* che effettuano trasformazioni delle scadenze (ad esempio, offrendo servizi di deposito denominati in asset crittografici rimborsabili su richiesta e fornendo prestiti in asset crittografici) dovrebbero rispettare i requisiti di

[276] FSB, «*Promoting Global Financial Stability: 2022 FSB Annual Report*», 16 novembre 2022.

liquidità. Inoltre, le attività di prestito dovrebbero essere soggette a un quadro per la misurazione e il controllo dei rischi associati alle grandi esposizioni.

Gli *exchange* dovrebbero essere soggetti allo stesso trattamento regolamentare applicato alle piattaforme di *trading* nei sistemi finanziari tradizionali. In particolare, la regolamentazione delle piattaforme di scambio di cripto-attività dovrebbe includere la segregazione operativa e legale dei fondi dei clienti, così come altre regole volte alla protezione dei consumatori e alla gestione dei conflitti di interesse.

La prima considerazione è ampiamente coerente con quelle del FSB sulle attività e i mercati delle cripto-attività. In particolare, secondo la guida all'attuazione della Raccomandazione 5[278], le Autorità dovrebbero richiedere ai fornitori di servizi di cripto-attività di identificare e gestire i rischi derivanti dalla leva finanziaria, dal credito, dalla liquidità e dalla trasformazione delle scadenze. Le autorità dovrebbero anche applicare regole, politiche e strumenti pratici che affrontino in modo completo e tempestivo questi rischi, sia in tempi normali che nei periodi di *stress*.

La seconda considerazione è invece coerente sia con le raccomandazioni del FSB sulle attività di asset crittografici sia con MiCAR, che introduce diverse regole per affrontare i rischi di protezione dei consumatori[279].

I fornitori di servizi che svolgono più attività (ad esempio, custodia dei fondi dei clienti, intermediazione, fornitura di credito per il *margin trading*, scambio, compensazione e posizionamento) dovrebbero avere una funzione di gestione del rischio che sia indipendente ed efficace per ciascuna attività o per gruppi di attività simili, in particolare quando queste attività possono creare conflitti di interesse in capo al fornitore di servizi. In altre parole, possono sorgere conflitti di interesse quando un fornitore di servizi si occupa contemporaneamente di emettere, gestire, investire e fornire prestitit *asset* detenuti dai suoi clienti[280].

Infine, la parziale decentralizzazione spesso comporta un panorama transfrontaliero che rende difficile e costosa l'applicazione delle norme. Questo può essere affrontato tramite l'utilizzo di regole precise che non lascino dubbi sulla tassonomia e sull'ambito di applicazione. È auspicabile un'azione regolamentare

[278] FSB, «*Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative Document*», 11 ottobre 2022.
[279] *Infra* cap. 3
[280] G. ABATE, N. BRANZOLI, R. GALLO, «*Crypto-asset markets: structure, stress episodes in 2022 and policy considerations*», Banca d'Italia - N. 783 Occasional Papers, Giugno 2023. https://www.bancaditalia.it/pubblicazioni/qef/2023-0783/QEF_783_23.pdf

internazionale coordinata, facilitata da quadri di cooperazione del G20, BIS[281], IOSCO[282], FSB[283], FMI[284] e FATF[285]. Un approccio regolamentare transfrontaliero ben coordinato avrebbe il vantaggio di coadiuvare l'applicazione delle norme e di renderle quindi più efficaci.

[281] Bank for International settlements.
[282] L'International Organization of Securities Commissions è un'associazione di organizzazioni che regolano i mercati mondiali dei titoli e dei futures.
[283] Financial Stability Board.
[284] Fondo Monetario Internazionale.
[285] Financial Action Taskforce.

# Capitolo 3 – Struttura della nuova regolamentazione Europea dei prestatori di servizi per le cripto-attività

Sommario: 1. Evoluzione normativa Europea in materia di cripto-attività. – 1.1 Presunzione di equivalenza dei servizi e nuove riserve di attività. – 1.2 MiCAR: ambito di applicazione. – 1.3 *E-money tokens* ed emittenti. – 1.4 Ambito di applicazione soggettivo e regime autorizzativo. – 1.5 I prestatori di diritto europeo. – 1.6 I prestatori di diritto nazionale. – 1.7 I prestatori significativi di servizi per le cripto-attività e i prestatori extra-europei. – 1.8 Il ruolo delle autorità competenti, punti in comune con il *framework* europeo *post* 2008. – 1.9 Misure e sanzioni amministrative. – 1.10. *framework* di vigilanza sovranazionale. – 1.11 *Iter* di accertamento e di adozione delle misure di vigilanza e delle sanzioni amministrative. – 1.12 Il ruolo determinante degli atti delegati nel Regolamento MiCA. – 1.13 Regime sanzionatorio e rapporti con l'ordinamento giuridico nazionale. – 2. Prevenzione degli abusi di mercato relativi alle cripto-attività. – 2.1 Introduzione e ambito applicativo. – 2.2 La nozione di informazioni privilegiate con riferimento alle cripto-attività. – 2.3 Comunicazione al pubblico di informazioni privilegiate. – 2.4 Divieto di abuso e divulgazione illecita di informazioni privilegiate. – 2.5 Divieto di manipolazione del mercato. – 2.6 Prevenzione e individuazione di abusi di mercato. – 3. Antiriciclaggio e gestione dei rischi aziendali dei prestatori di servizi di cripto-attività– 3.1 Interventi delle Autorità nazionali e sovranazionali. – 3.2 La nozione di valuta virtuale nel diritto nazionale ed europeo ai fini antiriciclaggio. – 3.3. Cenni sul *set* regolamentare europeo. – 3.4 Presidi nazionali antiriciclaggio. – 3.5 Prospettive regolatorie.

## 1. Evoluzione normativa Europea in materia di cripto-attività

Il 10 settembre 2019, Ursula Von Der Leyen, ha inviato una *Mission Letter* al commissario Valdis Dombrovskis[286], incaricandolo di sviluppare un *framework*

[286] Vicepresidente e Commissario europeo per la stabilità finanziaria, i servizi finanziari e il mercato unico dei capitali.

comune sulle cripto-attività, per comprendere come sfruttare al meglio le opportunità offerte e gestire i nuovi rischi associati.

il 13 dicembre 2019, Successivamente, il ROFIEG (Gruppo di esperti sugli Ostacoli Regolatori all'Innovazione Finanziaria - *FinTech*) ha pubblicato il suo Rapporto definitivo, sottolineando l'importanza dell'uniformità nell'approccio dell'UE alle cripto-attività, affermando che attività con rischi simili devono essere regolamentate dalle stesse norme in tutta l'UE per evitare frammentazioni, arbitraggi normativi e una corsa al ribasso in termini di rigore e tutele.

il 19 dicembre 2019, la Commissione Europea ha avviato, una Consultazione Pubblica per creare un quadro regolamentare comune europeo per le cripto-attività, proponendo un Regolamento sul mercato delle cripto-attività.

La Commissione ha rivisto i servizi finanziari e la loro accessibilità, pubblicando il 24 settembre 2020 il "*Digital finance package*", focalizzandosi su quattro priorità per promuovere la trasformazione digitale dell'UE fino al 2024. La prima era occuparsi della frammentazione del mercato unico digitale nei servizi finanziari per consentire ai consumatori europei l'accesso ai servizi transfrontalieri e supportare le imprese finanziarie europee nell'espansione delle loro operazioni digitali.

La seconda priorità era quella di garantire che il quadro normativo dell'Unione Europea favorisca l'innovazione digitale nell'interesse dei consumatori e dell'efficienza del mercato; questo implica una particolare attenzione all'utilizzo responsabile della tecnologia *blockchain* e dell'intelligenza artificiale. Tali tecnologie richiedono verifiche e adeguamenti regolamentari delle leggi dell'UE sui servizi finanziari e delle pratiche di vigilanza, per assicurare che supportino l'innovazione digitale e rimangano adeguate in contesti di mercato in continua evoluzione.

La terza priorità riguarda la creazione di uno spazio europeo di dati finanziari per promuovere l'innovazione basata sui dati, partendo dalla strategia eurounitaria.

Infine, la quarta priorità è affrontare le nuove sfide ed i rischi legati alla trasformazione digitale in un contesto in cui i servizi finanziari si spostano verso ambienti digitali con ecosistemi frammentati, compresi fornitori di servizi digitali interconnessi che in parte non rientrano nell'ambito delle normative finanziarie[287].

Occorre considerare però che la finanza digitale talvolta sfugge al quadro normativo e alla vigilanza, rendendo più difficile garantire la stabilità finanziaria, la protezione del consumatore, l'integrità del mercato, la concorrenza leale e la sicurezza.

[287] Vedi diffusamente cap. 1.

Il principio guida "stessa attività, stesso rischio, stesse norme" mira comunque a preservare la parità di condizioni di mercato tra gli attori esistenti e i nuovi partecipanti.

Le opportunità offerte dalle cripto-attività, come la velocità ed economicità nei pagamenti transfrontalieri, le nuove opzioni di finanziamento per le PMI, la maggiore efficienza dei capitali e la possibilità di pagamenti *machine-to-machine*, meritano di essere perseguite.

La Commissione Europea, insieme al *Digital Finance Package*, chiarisce l'applicazione delle norme dell'Unione Europea alle cripto-attività, introducendo un regime pilota per le cripto-attività disciplinate da tali norme e istituendo un nuovo quadro regolamentare dell'UE per quelle non disciplinate dalle previgenti normative, basato su una tassonomia di definizioni per le varie tipologie di cripto-attività.

Come è facile notare, l'analisi storica del settore, conduce all'individuazione di alcuni operatori "sistemici" che possono esporre gli utenti a perdite talvolta ingenti[288]. La storia dei vari "fallimenti" dimostra come il punto debole sia costituito dagli attori centralizzati, rappresentati dai *custodial wallet service provider*, intesi come operatori che custodiscono le chiavi private degli utenti e svolgono il servizio di conversione di moneta *fiat* in cripto-attività.

Le tre principali cause, rappresentate dai rischi associati agli attori "centralizzati", dai rischi derivanti dalla promozione delle cripto-attività e dalla presenza di un approccio eterogeneo e non armonizzato, hanno spinto le istituzioni dell'Unione Europea a emettere inizialmente una Proposta di Regolamento, successivamente approvata in via definitiva.

La necessità di conciliare tali esigenze, insieme alla crescita delle diverse piattaforme che, per loro natura, operano a livello transfrontaliero, hanno portato all'adozione del Regolamento anziché della Direttiva. Questo approccio mira a garantire agli operatori la certezza giuridica sul trattamento delle cripto-attività nei vari Stati membri, prevenendo così la frammentazione normativa che potrebbe distorcere la concorrenza nel mercato unico, consentendo l'arbitraggio normativo e complicando le operazioni transfrontaliere per le imprese.

Le legislazioni dell'Unione Europea nel settore dei servizi finanziari sono orientate dal principio di "stessa attività, stessi rischi, stesse norme" e dal concetto di neutralità tecnologica. Di conseguenza, le cripto-attività che rientrano nelle categorie

[288] Vedi diffusamente cap. 2.

di strumenti finanziari (direttiva 2014/65/UE), depositi (direttiva 2014/49/UE), depositi strutturati (direttiva 2014/65/UE), fondi (direttiva (UE) 2015/2366), posizioni verso la cartolarizzazione (Regolamento (UE) 2017/2402) o contratti di assicurazione, ramo vita, prodotti pensionistici o regimi di sicurezza sociale, rimangono soggetti alle rispettive normative di settore.

La scelta del "Regolamento" rende questa fonte direttamente efficace ai sensi del Trattato di Lisbona; tuttavia, ciò presuppone un recepimento nazionale piuttosto incisivo, poiché prevede l'intervento delle autorità preposte. È quindi un Regolamento fortemente dipendente dalla legislazione di secondo livello in ragione degli *standard* tecnici richiesti, i quali risultano essere essenziali per l'applicazione dello stesso.

Il 9 giugno 2023 è una data che segna quindi un cambio di paradigma per il settore delle cripto-attività nell'ambito dell'Unione Europea. Poiché in tale data, è stato pubblicato ufficialmente nella Gazzetta Ufficiale dell'Unione (L. 150/40) il Regolamento (UE) 2023/1114, emanato dal Parlamento Europeo e dal Consiglio il 31 maggio 2023. Il Regolamento *de quo* ha per oggetto i mercati delle cripto-attività e introduce modifiche ai regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010, nonché alle direttive 2013/36/UE e (UE) 2019/1937.

Conosciuto comunemente come MiCAR, acronimo di "*Market in Crypto Asset Regulation*", questo documento rappresenta un passo significativo nella regolamentazione del settore.

Il MiCAR ha ottenuto l'approvazione in prima battuta dal Parlamento Europeo il 20 aprile 2023 ed ha iniziato ad essere operativo dal 29 giugno 2023, ovvero solo venti giorni dopo la sua pubblicazione ufficiale. Tuttavia, preme segnalare che l'applicazione completa di molte delle sue disposizioni sarà effettiva solo nei 12 o 18 mesi successivi, a seconda delle specifiche aree trattate.

La necessità di regolamentare il settore delle cripto-attività e dei *tokens* è emersa rapidamente all'interno dell'Unione Europea, spinta dall'urgenza sentita dal legislatore europeo. Quest'ultimo era preoccupato che la diffusione di tali *asset* potesse causare instabilità nei mercati finanziari europei, portando a disuguaglianze economiche e sociali già segnalate in vari avvertimenti da parte dei regolatori dei singoli paesi membri.

Inoltre, era ormai chiaro che diversi paesi europei stessero procedendo con approcci autonomi e non coordinati nella gestione di questa materia. Questa situazione,

nonostante le iniziative comunitarie proposte, rischiava di generare frizioni nella libera circolazione di beni e servizi all'interno dell'Unione.

Tale condizione avrebbe potuto condurre a un fenomeno di arbitraggio normativo diffuso, creando discriminazioni significative tra i paesi membri e influenzando la libera circolazione dei servizi, come previsto dalla direttiva 2006/123/CE relativa ai servizi nel mercato interno e dalla direttiva 2005/36/CE sul riconoscimento delle qualifiche professionali[289].

Nei primi anni del fenomeno delle cripto-attività, l'assenza di un quadro normativo specifico per queste operazioni, unita all'incertezza sulla possibile applicazione, anche per analogia, di normative esistenti come quelle relative agli strumenti finanziari, all'offerta pubblica e ai servizi di investimento, ha contribuito ad un notevole aumento delle *Initial Coin Offerings* (ICOs) a livello globale; ovvero delle vere e proprie operazioni di "collocamento" su mercati non regolamentati di prodotti finanziari ad altissimo rischio[290]. Ciò ha portato all'ascesa di grandi piattaforme per lo scambio di *token*, creando un vasto mercato secondario che si è caratterizzato per essere in gran parte non regolamentato e poco trasparente.

Mentre le istituzioni globali, come il Financial Stability Board (FSB)[291] e la Banca per i regolamenti internazionali (BIS)[292], stanno lavorando per stabilire principi globali per la regolamentazione delle cripto-attività, l'Unione Europea ha agito proattivamente.

In un periodo relativamente breve, l'UE ha sviluppato un insieme di leggi direttamente applicabili in tutti gli Stati membri.

Già nel settembre 2020, con l'introduzione del *Digital Finance Package*, l'UE aveva intrapreso un'azione diretta in questo settore, mirando a creare una regolamentazione uniforme del mercato delle cripto-attività a livello europeo, ponendo così l'Europa in una posizione di avanguardia nella gestione di questi fenomeni.

---

[289] M. SIMBULA, «*Panoramica del Regolamento MiCA: l'Europa regola le cripto-attività*», in *Il MiCAR, Guida al Regolamento Europeo sui mercati delle cripto,* (Giuffrè Francis Lefebvre, 2023).
[290] *Ibid.*
[291] Cfr. FINANCIAL STABILITY BOARD, «*High-Level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Final Report*», 17 luglio 2023, https://www.fsb.org/2023/07/high-level-recommendations-for-the-regulation-supervision-and-oversight-of-crypto-asset-activities-and-markets-final-report/.
[292] BIS, «*The Crypto Ecosystem: Key Elements and Risks, Report Submitted to the G20 Finance Ministers and Central Bank Governors*», luglio 2023, https://www.bis.org/publ/othp72.pdf.

Il *Digital Finance Package* si articola in due direzioni strategiche: la "*Digital Finance Strategy*" e la "*Retail Payments Strategy*", entrambe destinate a convertirsi principalmente in testi legislativi direttamente applicabili in tutti gli Stati membri.

Nell'ambito della *Digital Finance Strategy* si colloca la proposta di regolamento sui *crypto-assets*, nota come "MiCA" o "MiCAR", che include anche la proposta complementare "*Pilot-Regime for DLT-based Market Infrastructures*", focalizzata sui mercati di capitali che impiegano la "*Distributed Ledger Technology*", e il "*Digital Operational Resilience Act*" (DORA) per la resilienza operativa digitale nel settore finanziario.

L'obiettivo del regolamento è quello di sviluppare un quadro giuridico chiaro ed efficace all'interno dell'Unione Europea che definisca in modo specifico il trattamento normativo delle cripto-attività, in particolare quelle non ancora disciplinate dalla legislazione esistente sui servizi finanziari. Questo approccio mira a fornire una base legale solida, tale da incoraggiare lo sviluppo dei mercati dei *crypto-asset* nell'UE.

Parallelamente, il regolamento punta a sostenere l'innovazione nel settore.

MiCA si inserisce in un contesto più ampio di sviluppo dei *crypto-asset* e di promozione della *Distributed Ledger Technology* (DLT), con l'obiettivo di stimolare l'innovazione e la concorrenza. Ciò si accompagna ad iniziative volte ad assicurare che la legislazione vigente non limiti l'adozione di nuove tecnologie, mantenendo al contempo gli obiettivi normativi rilevanti.

Un altro punto fondamentale è garantire una protezione adeguata per consumatori e investitori, nonché l'integrità del mercato. È ormai riconosciuto che i *crypto-asset* non regolati dalla legislazione attuale sui servizi finanziari presentano rischi simili a quelli degli strumenti finanziari tradizionali.

Inoltre, il regolamento mira a salvaguardare la stabilità finanziaria, considerando che alcuni *crypto-asset*, pur avendo un utilizzo e una diffusione limitati, hanno il potenziale per circolare in maniera significativa ed influenzare quindi il sistema finanziario.

Sebbene il Regolamento MiCA presenti alcune lacune e incertezze, il medesimo rappresenta ad oggi la normativa più completa e dettagliata per il mercato delle cripto-attività.

MiCA si cimenta nella complessa sfida di regolamentare il mercato delle cripto-attività, adottando un metodo piuttosto tradizionale: le tecniche regolatorie utilizzate

in altri ambiti del diritto finanziario dell'Unione Europea vengono adattate ed estese al settore delle cripto-attività.

In particolare, per quanto riguarda l'emissione e l'offerta di cripto-attività sul mercato, MiCA segue il modello delle offerte pubbliche e della normativa sui prospetti informativi, sebbene in una forma adattata e semplificata per adeguarsi a una prassi di mercato già consolidata, come quella del *White Paper*.

Per la regolamentazione dei soggetti che offrono servizi legati alle cripto-attività, il punto di riferimento principale è MiFID, dal quale vengono importati schemi, concetti e approcci regolatori e di vigilanza.

In questo modo, MiCA si propone come un regolamento che, pur affrontando un settore innovativo e in rapida evoluzione, si radica in una struttura normativa e regolatoria solida e collaudata.

Per quanto riguarda le piattaforme di scambio, il Regolamento MiCA adotta nuovamente il modello del MiFID, focalizzandosi sui sistemi di negoziazione. Per quanto riguarda la disciplina degli abusi di mercato, il regolamento si allinea alle linee guida del Regolamento sugli abusi di mercato (MAR) già esistente. Inoltre, per le cripto-attività utilizzate come mezzo di pagamento, come gli *asset-referenced token* e gli *e-money token*, il punto di riferimento diventa la normativa che regola gli enti creditizi e la moneta elettronica.

Da questa impostazione del MiCA emergono alcune considerazioni significative. Innanzitutto, il MiCA incontra alcune difficoltà nel regolamentare completamente i fenomeni legati alla finanza decentralizzata (DeFi). Questo è dovuto al fatto che, in questi contesti, spesso non è possibile identificare un soggetto o un gruppo di soggetti che possano essere definiti come "emittenti" o "prestatori di servizi", rendendo quindi non applicabili le regole appena introdotte.

Inoltre, data la sua impostazione di base e i limiti imposti dalle competenze assegnate ai legislatori dell'Unione Europea dal Trattato UE, il MiCA non regola direttamente le cripto-attività in sé, ma piuttosto il mercato di queste attività.

Di conseguenza, nel regolamento non si trovano disposizioni che chiariscano, ad esempio, la natura giuridica delle cripto-attività secondo il diritto privato o societario, o che definiscano la natura dei diritti che il titolare di una cripto-attività può vantare nei confronti della cripto-attività stessa[293].

[293] F. ANNUNZIATA, «*La disciplina delle cripto-attività*», in *La disciplina del mercato dei capitali* (G. Giappichelli Editore, 2023).

Questi aspetti, quindi, rimangono di competenza degli ordinamenti giuridici dei singoli Stati membri e sono soggetti alle regole di diritto comune che variano tra i 27 Stati. Tuttavia, è importante notare che un approccio simile è adottato anche dalla MiFID, che non fornisce definizioni specifiche per termini come "azione", "obbligazione" o altri strumenti finanziari, ma lascia tale compito alle legislazioni degli Stati membri.

In questo senso, l'acronimo MiCA segue un parallelismo con MiFID, ponendo l'accento non tanto sulla regolamentazione sostanziale del fenomeno in sé, quanto sulla disciplina dei mercati di emissione e scambio dei relativi strumenti.

Considerando la variegata natura delle cripto-attività e le loro diverse funzioni, il legislatore europeo, nel quadro del MiCA, ha dovuto affrontare la decisione su quali regole applicare alle cripto-attività che, per contenuto e funzione, coincidono con prodotti o attività già regolati dal diritto finanziario dell'Unione. Un esempio potrebbe essere un'azione emessa da una società di capitali tramite la tecnologia DLT. In questo contesto, l'approccio adottato si basa sul principio di neutralità tecnologica: indipendentemente dalla forma o dagli strumenti utilizzati per l'emissione dello strumento, se una cripto-attività è sostanzialmente un prodotto già regolato dal diritto finanziario UE, essa viene esclusa dal campo di applicazione del MiCA. Di conseguenza, le cripto-attività che sostanzialmente rappresentano o replicano "strumenti finanziari" secondo le definizioni del MiFID non rientrano nell'ambito del MiCA, essendo già disciplinate dalla MiFID stessa[294].

Per certi aspetti, è un regolamento estremamente ambizioso. Tende a coprire tutte le cripto-attività che non siano altrimenti regolamentate. Pertanto, restano fuori dall'applicazione del regolamento: gli strumenti finanziari coperti dalla MiFID, i fondi tranne i *token* di moneta elettronica, i depositi, le cartolarizzazioni, i contratti di assicurazione e i prodotti pensionistici. Rimangono esclusi anche le CBDC (e in particolare l'euro digitale), i bitcoin (poiché non hanno un emittente) e infine anche gli NFT.

Il principio di neutralità tecnologica adottato da MiCA, seppur valido, presenta alcune eccezioni. Un esempio notevole riguarda il trattamento della moneta elettronica emessa sotto forma di *token*. Sebbene il diritto dell'Unione Europea disponga già di una normativa specifica per la moneta elettronica (la *E-Money Directive* o EMD, attualmente alla sua seconda versione), MiCA introduce delle regole proprie e

[294] *Ibid.*

aggiuntive a tale disciplina. Questo approccio, benché giustificabile in termini di razionalità, solleva dubbi sull'impostazione di base del regolamento.

Tornando al fenomeno della "Mifidizzazione della MiCAR"[295] è possibile, infatti, notare delle grandi assonanze nei due testi normativi; le prime sono quelle di definizione di imprese di investimento nella MiFID II, e ancora in maniera più evidente se viene preso in esame l'elenco dei servizi per le cripto-attività contenuto dentro MICAR. Questi ultimi, infatti, sono più o meno corrispondenti ai servizi di investimento contenuti in MiFID II, al netto dell'esigenza dell'adeguamento tecnologico.

Ragionando su queste e altre assonanze è lecito domandarsi in che modo una disciplina che è improntata per molti aspetti sull'impianto MiFID, ed adeguata sulla scorta dell'aspetto tecnologico, possa essere conforme al principio di neutralità tecnologica[296].

Non è del tutto esatto, infatti, affermare che la forma tecnologica di uno strumento sia sempre irrilevante ai fini della sua regolamentazione.

La tecnologia DLT introduce questioni nuove e complesse, che non erano contemplate nei testi normativi fondamentali del diritto europeo dei mercati finanziari. In questo contesto, MiCA è stato affiancato dal Regolamento DLT Pilot, che stabilisce un regime transitorio e derogatorio rispetto alle norme del MiFID, MiFIR e CSDR. Queste deroghe sono giustificate proprio dalle caratteristiche tecniche uniche e innovative di questi fenomeni.

## 1.1 Presunzione di equivalenza dei servizi e nuove riserve di attività

Alla luce dell'impostazione in negativo evidenziata più volte, caratterizzante MiCA rispetto a Mifid 2, insieme alla presunzione unilaterale di equivalenza dei rispettivi servizi, sorge una domanda fondamentale, soprattutto considerando il processo di revisione concomitante di Mifid 2.

La presunzione di equivalenza, con tutte le sue implicazioni, opera in modo unilaterale o può generare un processo bidirezionale? In altre parole, l'equivalenza dei servizi per le cripto-attività rispetto ai servizi di investimento rappresenta un flusso

[295] Vedi n. 218.

[296] D. SALOMONE, «*I prestatori di servizi per le cripto-attività: requisiti e regime di vigilanza*» (Il Regolamento MICA nel contesto della disciplina bancaria e dei servizi di pagamento, BANCA D'ITALIA, 29 settembre 2023, Roma).

unidirezionale (da Mifid 2 a MiCA) o genera, in modo auspicabile, anche un effetto di ritorno (da MiCA a Mifid 2)?

Considerando le ricadute complessive sul sistema tradizionale, simili interrogativi possono essere estesi al rapporto tra MiCA e una serie di corpi normativi diversi da Mifid 2, elencati nell'art. 2 e collegati ad altre legislazioni finanziarie vigenti. Le conclusioni e le conseguenze di tale relazione dovrebbero riflettersi anche su altri riferimenti normativi menzionati, sia per soggetti diversi dalle imprese di investimento, che rientrano nella categoria dei beneficiari del regime di esenzione, sia per altri servizi (diversi da quelli di investimento) dichiarati equivalenti a quelli di MiCA[297].

Particolarmente rilevante è il regime di esenzione previsto per le imprese di investimento già autorizzate a prestare servizi MiCA, che a loro volta sono considerati equivalenti a quelli di Mifid. Tale regime dovrebbe essere esteso anche ai prestatori di servizi per le cripto-attività, autorizzati ai sensi di MiCA per la prestazione dei servizi oggetto della presunzione di equivalenza. Questo garantirebbe un trattamento giuridico equo e non discriminatorio, specialmente per i servizi di investimento che coinvolgono strumenti finanziari tokenizzati.

Inoltre, nel contesto dei lavori di Mifid 3, dovrebbe essere considerata l'applicazione di una presunzione di equivalenza inversa dei servizi Mifid/MiCA. Ciò consentirebbe ai prestatori autorizzati ai sensi di MiCA di fornire servizi di investimento dichiarati equivalenti. La disciplina aggiornata dei servizi di custodia e amministrazione di cripto-attività in MiCA potrebbe influenzare positivamente la considerazione di un servizio che, nel contesto di Mifid, è considerato accessorio e privo di definizione e disciplina specifica.

Infine, un regime corrispondente di esenzione dall'autorizzazione *ex* Mifid per i prestatori con passaporto MiCA dovrebbe essere implementato per coloro che intendono fornire servizi di investimento dichiarati equivalenti. Ciò richiederebbe la definizione di uno statuto normativo adatto che tenga conto dei requisiti prudenziali più rigorosi richiesti dal settore di destinazione[298].

[297] Specifiche presunzioni settoriali di equivalenza sono sancite dall'art 60 par. 2 e 5 MiCA.
[298] M.T. PARACAMPO, «*I prestatori di servizi per le cripto-attività Tra mifidizzazione della MICA e tokenizzazione della Mifid*»105 e ss. G. Giappichelli editore 2023.

Tali modifiche potrebbero contribuire a una maggiore coerenza ed omogeneità del sistema finanziario nel suo complesso, adattandosi all'osmosi operativa tra vecchi e nuovi attori del settore[299].

Gli effetti positivi si rifletterebbero anche nella certezza del trattamento giuridico e in un nuovo *level playing field* tra i prestatori di servizi, provenienti da fonti normative diverse ma connesse, in un contesto in cui i confini tra servizi legati a cripto-attività, strumenti finanziari e mercati "equivalenti" sono sempre più sfumati.

La soluzione favorevole alla reciprocità o biunivocità sembra essere suggerita quindi sia dalla crescente sfumatura dei confini tra i servizi relativi alle cripto-attività o strumenti finanziari e i mercati considerati "equivalenti", sia dalle finalità sottese alla regolamentazione del relativo funzionamento. Tale approccio potrebbe evitare l'insorgere di ulteriori forme di arbitraggio normativo nel caso in cui le situazioni concrete relative alle cripto-attività non risultino chiare e definite.

Considerando il vero obiettivo dell'equivalenza, identificato nelle stesse finalità di tutela degli investitori e dei mercati, il collegamento implicito alla presunzione discende dalla necessità di attivare automaticamente una serie di misure attraverso i medesimi presidi di protezione già implementati a tale scopo. La possibile reciprocità tra i sistemi normativi offre uno spunto di riflessione sulla persistente centralità di Mifid nell'ambito finanziario.

Infatti, l'esperienza normativa consolidata come modello di base, ha confermato più volte il ruolo di *benchmark* normativo di MIFID da replicare in contesti finanziari consolidati (es. IDD, MCD, PEPP) o di nuova creazione (es. MiCA)[300].

La centralità di questo modello potrebbe però gradualmente indebolirsi e perdere di rilevanza all'avanzare del processo di tokenizzazione dell'economia, che in MiCA apre solo una fase interlocutoria, per studiare e valutare ulteriori sviluppi, come indicato dal dettagliato elenco degli indicatori di monitoraggio a disposizione delle autorità e della Commissione europea.

Si prevede che MiCA lasci un'impronta e sposti progressivamente l'attenzione verso un nuovo ecosistema, potenzialmente assumendo il ruolo di un concorrente normativo rispetto a Mifid. Questo potrebbe forgiare e regolamentare un nuovo settore, quello delle cripto-attività, che si distingue per la sua trasversalità rispetto a tutti i

[299] Il che si pone in linea con il panorama Open Finance che progressivamente sta interessando sempre maggiormente i servizi per le cripto-attività.
[300] Cfr. F. ANNUNZIATA, «*Towards an EU Charter for the Protection of End Users in Financial Markets*», SSRN Scholarly Paper 25 agosto 2022, https://doi.org/10.2139/ssrn.4200502.

settori finanziari, inclusi quelli esplicitamente disciplinati da MICA e quelli attualmente esclusi dal suo ambito normativo.

## 1.2 MiCA: ambito di applicazione oggettivo

Ai sensi del regolamento, per "cripto-attività" si intende una rappresentazione digitale di un valore o di un diritto che può essere traferito e memorizzato elettronicamente, utilizzando la tecnologia a registro distribuito o una tecnologia analoga[301].

La definizione adottata risulta essere più concisa e di conseguenza la categoria molto più ampia rispetto a quanto precedentemente previsto a livello comunitario dalla disciplina *anti-moneylaundering*[302], che aveva introdotto per la prima volta una definizione formale dei *crypto asset*, in particolare definendo le criptovalute o "valute virtuali"[303].

Per quanto riguarda le categorie di cripto-attività, ne esistono diverse.

I *token* di moneta elettronica, i quali si propongono di mantenere un valore stabile facendo riferimento al valore di una valuta ufficiale (*fiat*) emessa da una banca centrale o da un'altra autorità monetaria. Diversamente, esistono i *token* collegati ad attività, che si propongono di mantenere un valore stabile rifacendosi a un altro valore, diritto o una combinazione di entrambi, inclusa la valuta ufficiale di un Paese. Infine, esistono gli *utility token* destinati a fornire accesso a un bene o servizio offerto dal loro emittente.

Riguardo alla funzione dei *token* di moneta elettronica, il legislatore ha inteso equipararli alla moneta elettronica tradizionale, vista come un valore monetario memorizzato elettronicamente, rappresentato da un credito nei confronti

[301] Art. 3, comma 1, n. 5, MiCA.
[302] Cfr. d.lgs. 231/2007, art 1 comma 1 lett. qq): "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".
[303] Vedi *infra*.

dell'emittente, emesso in cambio di fondi per effettuare operazioni di pagamento[304] e accettato da soggetti diversi dall'emittente stesso[305].

Come per le monete elettroniche, alcune cripto-attività funzionano come equivalenti elettronici di monete e banconote, utilizzabili per transazioni di pagamento. Tuttavia, esistono differenze sostanziali tra queste e le monete elettroniche tradizionali. Ad esempio, i detentori di moneta elettronica sono sempre titolari di un credito nei confronti dell'emittente e hanno il diritto contrattuale di ricevere un rimborso del valore monetario in qualsiasi momento. Al contrario, alcune cripto-attività, pur avendo una valuta ufficiale come riferimento, non conferiscono ai loro possessori un credito simile nei confronti degli emittenti. Questo può escluderle dall'ambito di applicazione della direttiva 2009/110/CE. Altre cripto-attività possono non offrire un credito al valore nominale della valuta di riferimento o imporre limitazioni sul periodo di rimborso. Questa mancanza di garanzie rappresenta un ostacolo significativo, generando sfiducia nei detentori di tali cripto-attività.

Pertanto, per prevenire l'elusione delle norme stabilite nella direttiva 2009/110/CE, il legislatore ha deciso di adottare una definizione più ampia del *token* di moneta elettronica. Ciò permette di includere una gamma più vasta di cripto-attività.

Tra le cripto-attività rientranti nelle due categorie restanti, ed in particolare in quella dei *token* collegati ad attività si trovano le altre cripto-attività con valore sostenuto da attività, diverse dai *token* di moneta elettronica, mentre nell'ultima ricadono tutte le cripto-attività che non rientrano nelle due precedenti, tra cui principalmente i c.d. "*utility token*".

Il legislatore ha inoltre affrontato le nuove sfide normative legate ai vari rischi e opportunità derivanti dalle cripto-attività, introducendo nel Regolamento norme specifiche per gli offerenti, per le persone che chiedono l'ammissione alla negoziazione di cripto-attività diverse dai *token* collegati ad attività o dai *token* di moneta elettronica, nonché per gli emittenti di *token* collegati ad attività e di *token* di moneta elettronica[306].

---

[304] Ossia quell'atto, disposto dal pagatore o dal beneficiario, di collocare, trasferire o ritirare fondi, indipendentemente da eventuali obblighi sottostanti tra il pagatore o il beneficiario, ai sensi dell'art 4 punto 5) della direttiva 2007/64/CE.

[305] Per la definizione di fondi il regolamento in esame rinvia all'art 4, punto 25, della direttiva (UE) 2015/2366, la quale per la definizione di moneta elettronica a sua volta rinvia all'art. 2, punto 2), della direttiva 2009/110/CE.

[306] G. M. TULLIO E S. CAPACCIOLI, «*Crypto-asset: Regolamento MiCa e DLT Pilot Regime. analisi ragionata su token, stablecoin, CASP».* (Giuffrè Francis Lefebvre, 2023).

Queste norme tengono conto del fatto che gli emittenti di cripto-attività possono essere persone fisiche, giuridiche o altre imprese. Un caso particolare è quello degli emittenti che richiedono l'ammissione alla negoziazione di tali cripto-attività o l'autorizzazione per l'offerta al pubblico.

Nel contesto delle cripto-attività, la decisione di acquisto viene affidata ai potenziali possessori, richiedendo loro di valutare l'opportunità dell'investimento. Questo processo implica una notevole autonomia e responsabilità da parte degli acquirenti nel determinare il valore e la potenziale utilità delle cripto-attività che considerano.

Parallelamente, esiste un insieme diversificato di soggetti che offrono servizi legati alle cripto-attività, conosciuti come prestatori di servizi per le cripto-attività.

A differenza degli emittenti di cripto-attività, questi soggetti devono essere persone giuridiche o altre imprese, e si specializzano nella prestazione di uno o più servizi per le cripto-attività ai clienti su base professionale, essendo autorizzati dalle autorità competenti[307].

Tra i servizi offerti si trovano quelli legati alla custodia e all'amministrazione di cripto-attività per conto dei clienti. Questo include il controllo delle cripto-attività stesse o delle chiavi crittografiche private per accedervi.

Un altro servizio cruciale è la gestione di piattaforme di negoziazione di cripto-attività, ossia la gestione di sistemi multilaterali che facilitano l'incontro di diversi interessi di terze parti ai fini dell'acquisto o vendita di cripto-attività.

I prestatori di servizi possono anche occuparsi dello scambio di cripto-attività con fondi o con altre cripto-attività, utilizzando il capitale proprio del prestatore di servizi. Ciò include la realizzazione di transazioni che coinvolgono l'acquisto o la vendita di cripto-attività in cambio di fondi o di altre cripto-attività.

Inoltre, possono eseguire ordini di cripto-attività per conto dei clienti, un'attività che racchiude, l'acquisto, la vendita o la sottoscrizione di cripto-attività, nonché la gestione di operazioni di vendita di cripto-attività in occasione della loro offerta al pubblico o dell'ammissione alla negoziazione.

[307] In conformità con quanto previsto dall'art. 59 del presente Regolamento, il quale prevede che un soggetto possa prestare un servizio per le cripto-attività all'interno dell'Unione solo qualora si tratti di una persona giuridica o un'altra impresa autorizzata come prestatore di servizi per le cripto-attività, ai sensi dell'art. 63, ovvero sia un ente creditizio, un depositario centrale di titoli, un'impresa di investimento, un gestore del mercato, un istituto di moneta elettronica, una società di gestione di un OICVM o un gestore di un fondo di investimento alternativo autorizzato a prestare servizi per le cripto-attività a norma dell'art. 60.

I prestatori di servizi possono anche essere coinvolti nel collocamento di cripto-attività, commercializzandole per conto dell'emittente o di un soggetto ad esso collegato.

Gli "altri servizi" includono la ricezione e la trasmissione di ordini di cripto-attività per conto dei clienti, la fornitura di consulenza sulle cripto-attività, la gestione di portafogli di investimento che includano cripto-attività e la prestazione di servizi di trasferimento di cripto-attività per conto dei clienti. Questa varietà di servizi mostra la complessità e la molteplicità degli utilizzi delle cripto-attività, sottolineando il ruolo essenziale dei prestatori di servizi nel facilitare e normare le transazioni e le interazioni in questo ambito.

Il legislatore mette in evidenza[308] il fatto che numerosi prestatori di servizi per le cripto-attività possono offrire servizi aggiuntivi, come il trasferimento di cripto-attività; i servizi in oggetto, potrebbero essere integrati in attività quali la custodia e l'amministrazione di cripto-attività per i clienti, lo scambio di cripto-attività con fondi o altre cripto-attività, nonché l'esecuzione di ordini di cripto-attività per conto dei clienti.

A seconda delle specifiche caratteristiche dei servizi legati al trasferimento di *token* di moneta elettronica, tali servizi potrebbero rientrare nella categoria dei servizi di pagamento definiti dalla direttiva (UE) 2015/2366[309]. In questi casi, i trasferimenti dovrebbero essere effettuati da un'entità autorizzata a fornire detti servizi di pagamento secondo la direttiva menzionata.

Inoltre, alcuni servizi per le cripto-attività, come la custodia e l'amministrazione di cripto-attività per i clienti, il collocamento ed i servizi di trasferimento per conto dei clienti, potrebbero sovrapporsi con i servizi di pagamento. In questo ambito, è importante notare che diverse entità possono svolgere attività di prestatori di servizi di

[308] Cfr. considerando n. 90.

[309] Cioè, una tra quelli elencati nell'allegato I della direttiva 2015/2366: 1. Servizi che permettono di depositare il contante su un conto di pagamento nonché tutte le operazioni richieste per la gestione di un conto di pagamento. 2. Servizi che permettono prelievi in contante da un conto di pagamento nonché tutte le operazioni richieste per la gestione di un conto di pagamento. 3. Esecuzione di operazioni di pagamento, incluso il trasferimento di fondi, su un conto di pagamento presso il prestatore di servizi di pagamento dell'utente o presso un altro prestatore di servizi di pagamento: *a)* esecuzione di addebiti diretti, inclusi addebiti diretti *una tantum*; *b)* esecuzione di operazioni di pagamento mediante carte di pagamento o analogo dispositivo; *c)* esecuzione di bonifici, inclusi ordini permanenti. 4. Esecuzione di operazioni di pagamento quando i fondi rientrano in una linea di credito accordata ad un utente di servizi di pagamento: *a)* esecuzione di addebiti diretti, inclusi addebiti diretti *una tantum*; *b)* esecuzione di operazioni di pagamento mediante carte di pagamento analogo dispositivo; *c)* esecuzione di bonifici, inclusi ordini permanenti. 5. Emissione di strumenti di pagamento e/o convenzionamento di operazioni di pagamento. 6. Rimessa di denaro. 7. Servizi di disposizione di ordine di pagamento, 8. Servizi di informazione sui conti.

pagamento[310], tra cui enti creditizi, istituti di moneta elettronica, uffici postali autorizzati, istituti di pagamento, la BCE e le banche centrali nazionali (ove non agiscano in quanto autorità pubbliche), gli Stati membri o le autorità regionali o locali (ove non agiscano in quanto autorità pubbliche), oltre a persone fisiche o giuridiche che beneficino di una specifica esenzione[311].

Il contesto *de quo* richiede di considerare una definizione più dettagliata di alcuni di questi concetti, iniziando dall'istituto di pagamento. Quest'ultimo può essere unicamente una persona giuridica autorizzata a operare come istituto di pagamento, trattandosi di un soggetto stabilito in uno stato membro[312].

Gli enti creditizi, sono autorizzati a norma della direttiva 2013/36/UE; la loro attività consiste nel raccogliere depositi o altri fondi rimborsabili dal pubblico e nel concedere crediti per proprio conto[313]. All'interno del Regolamento, gli enti creditizi sono talvolta considerati come custodi dei fondi[314], altre volte come emittenti di *token* con relativa offerta al pubblico e richiesta di ammissione alla negoziazione del *token* stesso[315].

Ma gli enti creditizi non sono gli unici soggetti rilevanti[316]: anche le imprese di investimento, gli istituti di moneta elettronica, le società di gestione di un OICVM[317] o i gestori di fondi di investimento alternativi autorizzati a prestare servizi per le cripto-attività.

Il Regolamento rinvia alla Direttiva 2014/65/CE per la definizione di impresa di investimento, descrivendola come un soggetto giuridico che si occupa professionalmente e su base autorizzata a prestare uno o più servizi di investimento a terzi e/o all'effettuare una o più attività di investimento[318]. La stessa Direttiva fornisce

---

[310] Definizione di cui all'art. 4, punto 11, della direttiva (UE) 2015/2366.

[311] Gli Stati membri infatti possono esentare o autorizzare le loro autorità competenti a esentare le persone fisiche o giuridiche che prestano i servizi di pagamento, qualora: *a)* la media mensile, calcolata sui precedenti 12 mesi, del valore complessivo delle operazioni di pagamento eseguite dalla persona interessata, compreso qualsiasi agente di cui è pienamente responsabile, non superi il limite fissato dallo Stato membro e in ogni caso non ammonti a più di 3 milioni di EUR. Tale condizione è valutata in base all'importo complessivo delle operazioni di pagamento previsto nel suo piano aziendale a meno che le sici competenti non richiedano un adeguamento di tale piano e *b)* nessuna delle persone fisiche responsabili della gestione o del funzionamento dell'impresa abbia subito condanne per crimini legati al riciclaggio o al finanziamento del terrorismo o altri reati finanziari.

[312] Art. 4, punto 4, della direttiva (UE) 2015/2466.

[313] Art. 4, par. 1, del regolamento (UE) n. 575/2013.

[314] Es. Art. 37 MiCAR.

[315] Es. Art. 17 MiCAR.

[316] Art. 59 MiCAR.

[317] OICVM: Organismo di Investimento Collettivo in Valori Mobiliari.

[318] Definizione di impresa di investimento rinvenibile nell'art. 4, par. 1, punto 1, della direttiva 2004/39/CE, al quale rinvia l'art. 4, paragrafo 1, punto 2, del regolamento (UE) n. 575/2013: "«impresa di investimento», un persona secondo la definizione di cui all'articolo 4, paragrafo 1, punto 1, della

inoltre criteri per identificare gli investitori qualificati, definiti come persone o soggetti elencati nell'allegato II, sezione I, punti da 1 a 4[319], così come quelli ad essi collegati da stretti legami[320].

Per quanto riguarda la riserva di attività, questa è definita come il paniere di attività che garantisce il credito nei confronti dell'emittente[321]. All'interno del Regolamento, viene introdotta anche la figura del gestore di fondi di investimento alternativi (GEFIA), descritto come una persona giuridica che gestisce uno o più FIA[322], raccogliendo capitali per investirli a beneficio degli investitori pur non necessitando di un'autorizzazione specifica.

Tra i vari soggetti che possono essere abilitati a fornire servizi legati alle cripto-attività, rientrano gli istituti di moneta elettronica. Questi sono persone giuridiche

direttiva 2004/39/CE che è soggetta agli obblighi stabiliti da tale direttiva, ad eccezione: *a)* degli enti creditizi; *b)* delle imprese locali; *c)* delle imprese che non sono autorizzate a prestare servizi accessori di cui all'allegato 1, sezione B, punto 1, della direttiva 2004/39/ CE, che prestano soltanto uno o più servizi e attività di investimento elencati all'allegato I, sezione A, punti 1, 2, 4 e 5, di tale direttiva e che non sono autorizzate a detenere fondi o titoli appartenenti ai loro clienti e che, per tale motivo, non possono mai trovarsi in situazione di debito con tali clienti".

[319] "1) i soggetti che sono tenuti ad essere autorizzati o regolamentati per operare nei mercati finanziari. Si intendono inclusi nell'elenco sottostante tutti i soggetti autorizzati che svolgono le attività caratteristiche dei soggetti menzionati, che si tratti di soggetti autorizzati da uno Stato membro a norma di una direttiva europea, di soggetti autorizzati o regolamentati da uno Stato membro senza riferimento ad una direttiva europea o di soggetti autorizzati o regolamentati da un paese terzo: *a)* enti creditizi; *b)* imprese di investimento; *c)* altri istituti finanziari autorizzati o regolamentati; *d)* imprese di assicurazione; *e)* organismi di investimento collettivo e società di gestione di tali organismi; *f)* fondi pensione e società di gestione di tali fondi; *g)* negoziatori per conto proprio di merci e strumenti derivati su merci; *h)* singoli membri di una borsa; *i)* altri investitori istituzionali;
2) le imprese di grandi dimensioni che ottemperano, a livello di singola società, ad almeno due dei seguenti criteri dimensionali: — totale di bilancio: EUR 20.000.000 — fatturato netto: EUR 40.000.000 — fondi propri: EUR 2.000.000;
3) i governi nazionali e regionali, compresi gli enti pubblici incaricati della gestione del debito pubblico a livello nazionale o regionale, le banche centrali, le istituzioni internazionali e sovranazionali come la Banca mondiale, la BCE, la BEI e altre organizzazioni internazionali analoghe;
4) altri investitori istituzionali la cui attività principale è investire in strumenti finanziari, compresi gli enti dediti alla cartolarizzazione di attivi o altre operazioni finanziarie."

[320] Per stretti legami si intende una situazione nella quale due o più persone fisiche o giuridiche Sono legate: da *a)* da una «partecipazione», vale a dire dal fatto di detenere, direttamente o tramite un legame di «controllo», il 20% o più dei diritti di voto o del capitale di un'impresa; *b)* da un legame di «controllo» ossia dalla relazione esistente tra un'impresa madre e un'impresa figlia, in tutti i casi di cui all'art, 22, parr. 1 e 2, della direttiva 2013/34/UE, o relazione analoga esistente tra persone fisiche e giuridiche e un'impresa, nel qual caso ogni impresa figlia di un'impresa figlia è considerata impresa figlia dell'impresa madre che è a capo di tali imprese; *c)* da un legame duraturo tra due o tutte le suddette persone e uno stesso soggetto che sia una relazione di controllo (art. 4, par. 1, punto 35, della direttiva 2014/65/UE).

[321] M. T. GIORDANO, «*Oggetto, ambito di applicazione e definizioni»,* in *Crytpo-asset: Regolamento MiCA e DLT Pilot Regime; analisi ragionata su token, stablecoin, CASP* (Giuffrè Francis Lefebvre, 2023).

[322] "Fondi di investimento alternativi".

autorizzate ad emettere moneta elettronica in conformità con le disposizioni del titolo II della direttiva 2009/110/CE[323].

Soffermandosi invece sui destinatari dei servizi per le cripto-attività, il Regolamento distingue tra clienti e detentori al dettaglio. I clienti sono definiti come persone fisiche o giuridiche che ricevono servizi per le cripto-attività, mentre i detentori al dettaglio sono soggetti che acquistano cripto-attività per scopi estranei all'attività commerciale, imprenditoriale, artigianale o professionale.

I clienti, così come i detentori di cripto-attività, hanno la possibilità di accedere ai servizi correlati tramite diverse piattaforme digitali. Questi possono includere vari tipi di *software*, come siti *web*, sezioni specifiche di siti *web* o applicazioni *mobile*. Tali piattaforme sono gestite direttamente dagli offerenti o dai prestatori di servizi per le cripto-attività, o per loro conto, e sono comunemente note come interfacce *online*[324].

È importante anche considerare le implicazioni relative al trattamento dei dati personali nell'ambito dell'emissione, dell'offerta o della richiesta di ammissione alla negoziazione di cripto-attività, nonché nella prestazione di servizi ad esse correlati. I dati personali includono qualsiasi informazione che riguarda una persona fisica identificata o identificabile[325].

Pertanto, qualsiasi trattamento di dati personali che avviene nell'ambito del Regolamento deve essere svolto in conformità con le leggi vigenti dell'Unione Europea in materia. Questo assicura che le informazioni relative alle persone fisiche siano gestite in modo sicuro e responsabile, rispettando la loro *privacy* e i loro diritti[326].

Il legislatore, tramite il Regolamento, pone enfasi sulla necessità di una gestione efficace dei servizi connessi alle cripto-attività, per proteggere gli interessati. Al fine di assicurare questa efficacia, è preferibile che la gestione sia localizzata all'interno dell'Unione Europea, così da non compromettere la vigilanza prudenziale e garantire la tutela degli investitori.

Tuttavia, la semplice presenza all'interno dell'Unione non è considerata sufficiente. Questa gestione dovrebbe essere accompagnata da un'adeguata supervisione da parte delle autorità di vigilanza con un contatto diretto con la direzione

[323] Artt. 3-9, Condizioni per l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica.
[324] Vedi diffusamente cap. 1.
[325] Una persona è considerata identificabile se può essere riconosciuta direttamente o indirettamente, in particolare tramite riferimenti a identificativi come il nome, un numero di identificazione, dati di ubicazione, un identificativo online o caratteristiche specifiche della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
[326] Cfr. *Supra* cap.1.

responsabile dei prestatori di servizi per le cripto-attività. Di conseguenza, il legislatore ha assegnato alle autorità nazionali competenti il potere di autorizzare e supervisionare tali prestatori. Le Autorità *de quo*, devono essere nominate da ciascuno Stato membro sia per gli offerenti che per coloro che richiedono l'ammissione alla negoziazione di cripto-attività diverse dai *token* collegati ad attività o dai *token* di moneta elettronica, nonché per gli emittenti di *token* collegati ad attività o di prestatori di servizi per le cripto-attività. Questo include anche l'applicazione della Direttiva 2009/110/CE riguardante gli emittenti di *token* di moneta elettronica.

Gli Stati membri hanno l'obbligo di comunicare ogni nomina di nuovo operatore all'EBA[327] e all'ESMA[328]. Se uno Stato membro designa più di un'autorità competente, deve chiarire i compiti specifici di ciascuna e individuare un'autorità come punto di contatto unico per la cooperazione amministrativa transfrontaliera con le altre autorità competenti e con l'EBA e l'ESMA.

In un'ottica di vigilanza e controllo, diventa fondamentale l'identificazione dello stato membro d'origine, per la quale il Regolamento in oggetto individua i seguenti criteri:

*a)* se l'offerente o la persona che richiede l'ammissione alla negoziazione di cripto-attività, diverse dai *token* collegati ad attività o dai *token* di moneta elettronica, ha sede legale all'interno dell'Unione Europea, lo Stato membro di riferimento è quello in cui si trova la sede legale;

*b)* nel caso in cui l'offerente o la persona richiedente non abbia una sede legale nell'Unione, ma operi tramite una o più succursali all'interno dell'Unione, lo Stato membro sarà quello selezionato dall'offerente tra quelli dove ha succursali;

*c)* se l'offerente o la persona richiedente è stabilita in un paese terzo senza succursali nell'Unione, lo Stato membro d'origine sarà il primo Stato membro in cui si propone di offrire le cripto-attività al pubblico oppure, secondo la scelta

[327] L'Autorità Bancaria Europea (ABE), fondata nel 2011 dal Regolamento (UE) n. 1093/2010 del Parlamento europeo e del Consiglio, è parte del Sistema europeo di vigilanza finanziaria (SEVIF), insieme all'Autorità europea delle assicurazioni e delle pensioni aziendali e professionali (AEAP) e all'Autorità europea degli strumenti finanziari e dei mercati (AESFEM), istituite rispettivamente dai regolamenti (UE) n. 1094/2010 e 1095/2010. Queste autorità hanno significativamente rafforzato la cooperazione tra le autorità di vigilanza bancaria nell'Unione Europea. L'ABE ha giocato un ruolo cruciale nella creazione di un insieme unificato di normative sui servizi finanziari all'interno dell'Unione e ha avuto un impatto significativo nell'assicurare un'attuazione coerente della ricapitalizzazione di importanti enti creditizi dell'Unione, seguendo la decisione presa nel vertice dell'Unione dell'ottobre 2011. Questo processo è stato realizzato in conformità con le linee guida e le condizioni relative agli aiuti di Stato stabilite dalla Commissione Europea. Per maggiori dettagli, si può consultare il Regolamento UE 1024/2013.

[328] L'ESMA, infatti, pubblica sul proprio sito *web* un elenco delle autorità competenti designate a norma dei commi 1 e 2 dell'art. 93.

dell'offerente, il primo Stato membro in cui presenta la domanda di ammissione alla negoziazione di tali cripto-attività;

*d)* per gli emittenti di *token* collegati ad attività, lo Stato membro d'origine è identificato dalla sede legale dell'emittente di tali *token*.

*e)* per gli emittenti di *token* di moneta elettronica, lo Stato membro d'origine è quello in cui l'emittente è autorizzato come ente creditizio o istituto di moneta elettronica secondo la direttiva 2009/110/CE;

*f)* per i prestatori di servizi per le cripto-attività, lo Stato membro d'origine è quello in cui il prestatore di servizi per le cripto-attività ha la propria sede legale.

La definizione di Stato membro d'origine è distinta da quella di Stato membro ospitante, che si riferisce allo Stato in cui un offerente o una persona che chiede l'ammissione alla negoziazione ha presentato un'offerta al pubblico di cripto-attività o richiede l'ammissione alla negoziazione, oppure in cui un prestatore di servizi per le cripto-attività svolge la sua attività, se diverso dallo Stato membro d'origine.

Questo Regolamento si applica a persone fisiche, persone giuridiche e ad altre imprese coinvolte nell'emissione, nell'offerta al pubblico, nell'ammissione alla negoziazione di cripto-attività o che prestano servizi connessi alle cripto-attività nell'Unione Europea. Tuttavia, è esclusa l'applicazione per coloro che forniscono servizi per le cripto-attività esclusivamente alle loro *holding*, alle loro filiali o ad altre filiali delle loro società madri, ai curatori o agli amministratori che agiscono in procedure di insolvenza, a meno che non si tratti di piani di rimborso previsti dall'art 47 MiCAR, alla BCE, alle Banche Centrali degli Stati membri quando agiscono come autorità monetarie, ad altre autorità pubbliche degli Stati membri, alla Banca europea per gli investimenti e alle sue controllate, al fondo europeo di stabilità finanziaria e al meccanismo europeo di stabilità, nonché alle organizzazioni internazionali pubbliche. Questa esclusione è dovuta al fatto che tali operazioni, essendo interne a un gruppo o coinvolgendo enti pubblici, non presentano rischi per la tutela degli investitori, l'integrità del mercato, la stabilità finanziaria, il funzionamento dei sistemi di pagamento, la trasmissione della politica monetaria o la sovranità monetaria.

Inoltre, il regolamento non include nel suo ambito le cripto-attività che si distinguono per la loro unicità e quindi non sono fungibili con altre, come l'arte digitale e gli oggetti da collezione[329], inclusi i cd. *Non Fungible Token* (NFT).

[329] Si veda in proposito il Considerando 10 del Regolamento in esame.

La motivazione di questa esclusione si trova nelle specifiche caratteristiche di queste cripto-attività: anche se esse possono essere scambiate sui mercati e accumulate con scopi speculativi, non sono tuttavia facilmente scambiabili l'una con l'altra e il valore di ogni singola cripto-attività, essendo questa unica, non è comparabile con altre attività di mercato o attività equivalenti. Un ulteriore elemento distintivo degli NFTs è la loro presunta inadeguatezza a fungere da investimenti, ad esempio, se il detentore dell'NFT non ha diritto a ricevere una remunerazione dalla sua proprietà, come avviene per i prodotti finanziari tradizionali. Tuttavia, i confini tra NFTs e *utility token* rimangono incerti, così come la relazione con la nozione domestica di prodotto finanziario. Infine, il Regolamento non fornisce una definizione precisa di "fungibilità", lasciando aperta l'interpretazione di questa nozione in base al diritto nazionale applicabile a seconda del caso[330].

Queste peculiarità riducono significativamente la loro applicabilità nel contesto finanziario e i rischi correlati, sia per i detentori sia per il sistema finanziario in generale, il che ha portato il legislatore ad escluderle dal regolamento[331]. Tuttavia, questo non esclude in futuro la possibilità di considerarle come strumenti finanziari.

Le cripto-attività escluse dal regolamento sono anche quelle che rientrano nelle definizioni di strumenti finanziari, depositi (compresi i depositi strutturati), fondi (a meno che non siano classificati come *token* di moneta elettronica) e posizioni relative a cartolarizzazioni. Per queste ultime categorie, è importante ricordare che, secondo la visione del legislatore europeo, la legislazione sui servizi finanziari dovrebbe seguire il principio di "stessa attività, stessi rischi, stesse regole" e di neutralità tecnologica. Di conseguenza, le cripto-attività che rientrano nella legislazione dell'Unione Europea vigente sui servizi finanziari, dovrebbero continuare ad essere regolate dal quadro normativo esistente, a prescindere dalla tecnologia usata per la loro emissione o trasferimento, anziché essere incluse nel nuovo regolamento[332].

Gli strumenti finanziari definiti nella sezione C dell'Allegato I della direttiva 2014/65/UE comprendono: valori mobiliari, strumenti del mercato monetario, quote di organismi di investimento collettivo, diversi tipi di contratti derivati come opzioni, contratti finanziari a termine standardizzati (*futures*), *swap* e altri accordi su strumenti derivati legati a valori mobiliari, valute, tassi di interesse, rendimenti, quote di

[330] F. RAMPONE, «*NFT e token crittografici*», Dialoghi di Diritto dell'Economia, Diritto Bancario, giugno 2023.
[331] Cfr. art. 2, par. 3 e considerando 10 e 11.
[332] Cfr. il Considerando n. 9 del Regolamento.

emissioni e altri strumenti finanziari derivati, indici finanziari o misure finanziarie, regolabili sia con consegna fisica sia con pagamento di differenziali in contanti e contratti derivati connessi a merci, regolabili in diversi modi e negoziati in specifici mercati regolamentati[333].

Un deposito può invece essere descritto[334] come un saldo creditore generato da fondi allocati in un conto bancario o da transazioni che emergono da operazioni bancarie *standard*. Questi fondi sono soggetti a rimborso da parte dell'istituto bancario in conformità con le condizioni legali e contrattuali stabilite e includono sia depositi a termine che depositi di risparmio. Non si considera un saldo creditore in situazioni dove la sua presenza è verificabile esclusivamente attraverso uno strumento finanziario, tranne nel caso di un prodotto di risparmio rappresentato da un certificato di deposito nominativo esistente in uno Stato membro alla data del 2 luglio 2014; se il principale non è rimborsabile al valore nominale; o se è rimborsabile al valore nominale solo sotto specifiche garanzie o accordi forniti dalla banca o da una terza parte.

[333] «1) valori mobiliari; 2) strumenti del mercato monetario; 3) quote di un organismo di investimento collettivo; 4) contratti di opzione, contratti finanziari a termine standardizzati («*future»*) «*swap*», accordi per scambi futuri di tassi di interesse e altri contrati su strumenti derivati connessi a valori mobiliari, valute, tassi di interesse o rendi. menti, quote di emissioni o altri strumenti finanziari derivati, indici finanziari o misure finanziarie che possono essere regolati con consegna fisica del sottostante o attraverso il pagamento di differenziali in contanti; contratti di opzione, contratti finanziari a termine standardizzati («*future*»), «*swap*», contratti a termine («*forward*») ed altri contratti su strumenti derivati connessi a merci quando l'esecuzione deve avvenire attraverso il pagamento di differenziali in contanti oppure possa avvenire in contanti a discrezione di una delle parti (per motivi diversi dall'inadempimento o da un altro evento che determini la risoluzione); contratti di opzione, contratti finanziari a termine standardizzati («*future*»), «*swap*» ed altri contratti su strumenti derivati connessi a merci che possono essere regolati con consegna fisica purché negoziati su un mercato regolamentato, un sistema multilaterale di negoziazione o un sistema organizzato di negoziazione, eccettuati i prodotti energetici all'ingrosso negoziati in un sistema organizzato di negoziazione che devono essere regolati con consegna fisica; contratti di opzione, contratti finanziari a termine standardizzati («*future*»), «*swap»*, contratti a termine («*forward*») ed altri contratti su strumenti derivati connessi a merci che non possano essere eseguiti in modi diversi da quelli citati al punto 6 della presente sezione e non abbiano scopi commerciali, aventi le caratteristiche di altri strumenti finanziari derivati; strumenti finanziari derivati per il trasferimento del rischio di credito; contratti finanziari differenziali; contratti di opzione, contratti finanziari a termine standardizzati («*future*»), «*swap*», contratti a termine sui tassi d'interesse e altri contratti su strumenti derivati connessi a variabili climatiche, tariffe di trasporto, tassi di inflazione o altre statistiche economiche ufficiali, quando l'esecuzione debba avvenire attraverso il pagamento di differenziali in contanti o possa avvenire in tal modo a discrezione di una delle parti (invece che in caso di inadempimento o di altro evento che determini la risoluzione del contratto), nonché altri contratti su strumenti derivati connessi a beni, diritti, obblighi, indici e misure, non altrimenti citati nella presente sezione, aventi le caratteristiche di altri strumenti finanziari derivati, considerando, tra l'altro, se sono negoziati su un mercato regolamentato, un sistema organizzato di negoziazione o un sistema multilaterale di negoziazione; quote di emissioni che consistono di qualsiasi unità riconosciuta conforme ai requisiti della direttiva 2003/87/CE (sistema per lo scambio di emissioni).» in M. T. GIORDANO, S. CAPACCIOLI, «*Crypto-asset: Regolamento MiCa e DLT Pilot Regime. analisi ragionata su token, stablecoin, CASP»* 63 Giuffrè Francis Lefebvre, 2023.

[334] Definizione di cui all'art. 2, comma 1, punto 3, della direttiva 2014/49/UE.

I depositi strutturati[335] sono una categoria di depositi che garantiscono il rimborso completo del capitale alla scadenza, con i termini che determinano il ritorno di interessi o premi basati su: un indice o una combinazione di indici (esclusi quelli a tasso variabile direttamente correlati a un tasso di interesse come l'Euribor o il Libor), una combinazione di strumenti finanziari, merci o una combinazione di merci o altri beni non fungibili, sia materiali che immateriali, oppure un tasso di cambio o una combinazione di tassi di cambio.

Nel contesto della legislazione europea, il termine "fondi", è specificatamente orientato a riferirsi a banconote, monete, moneta scritturale e moneta elettronica[336].

Infine, si definisce cartolarizzazione[337] quell'operazione o struttura in cui il rischio di credito legato a una singola esposizione o a un portafoglio di esposizioni è suddiviso in diverse *tranche*. Questo processo implica che i pagamenti all'interno dell'operazione o della struttura dipendono dalle *performance* delle esposizioni mentre la subordinazione delle *tranche* determina la distribuzione delle perdite durante la durata dell'operazione o della struttura; infine, l'operazione o lo schema non devono creare esposizioni recanti tutte le caratteristiche specificate nell'articolo 147, comma 8, del Regolamento (UE) n. 575/2013[338].

Proseguendo con le eccezioni, l'articolo 2 esclude dalla sua applicazione anche un'altra serie di prodotti e contratti. Questi includono i prodotti assicurativi vita e non vita che rientrano nelle classi di assicurazione definite negli allegati I e II della direttiva 2009/138/CE[339], oltre ai contratti di riassicurazione e retrocessione contemplati dalla stessa direttiva. Sono esclusi anche i prodotti pensionistici che il diritto nazionale riconosce per il loro scopo principale di fornire un reddito durante la pensione, garantendo determinati vantaggi all'investitore. Inoltre, rientrano nelle eccezioni gli schemi pensionistici aziendali o professionali ufficialmente riconosciuti che sono coperti dalla direttiva (UE) 2016/2341 o dalla direttiva 2009/138/CE, così come i prodotti pensionistici individuali per cui il diritto nazionale impone un contributo

[335] Definizione all'art. 4, comma 1, punto 43, della direttiva 2014/65/UE.
[336] Cfr. *supra* cap.1.
[337] Nella definizione dell'art. 2, punto 1, del Regolamento (UE) 2017/2402.
[338] Ovverosia: *a)* si tratta di esposizioni verso un'entità creata *ad hoc* per finanziare o amministrare attività materiali, o di esposizioni economicamente analoghe; *b)* le condizioni contrattuali conferiscono al finanziatore un sostanziale controllo sulle attività e sul reddito da esse prodotto; *c)* la fonte primaria di rimborso dell'obbligazione è rappresentata dal reddito generato dalle attività finanziate piuttosto che dall'autonoma capacità di una più ampia impresa commerciale.
[339] L'allegato 1 individua i rami dell'assicurazione non vita, quindi infortuni, malattia, corpi di veicoli terrestri, ferroviari, aerei, marittimi, lacustri, e fluviali, merci trasportate, incendio ed elementi naturali, oltre a diverse tipologie di RC; l'allegato II individua invece i rami dell'assicurazione vita.

finanziario da parte del datore di lavoro e in cui né il lavoratore né il datore di lavoro possono scegliere il fornitore o il prodotto pensionistico. Anche il prodotto pensionistico individuale paneuropeo, definito nel Regolamento (UE) 2019/1238[340], e i regimi di sicurezza sociale menzionati nei Regolamenti (CE) n. 883/2004 e (CE) n. 987/2009 rimangono esclusi.

Al fine di integrare il regolamento, il legislatore ha delegato alla Commissione l'adozione degli atti delegati per specificare gli elementi tecnici delle definizioni ed adeguarle agli sviluppi tecnologici del mercato. Il regolamento ha anche demandato all'ESMA l'elaborazione di orientamenti sulle condizioni ed i criteri per qualificare le cripto-attività come strumenti finanziari, entro 18 mesi dalla data di entrata in vigore del regolamento[341]. Questi orientamenti sono diretti principalmente alle autorità competenti e ai partecipanti ai mercati finanziari, con lo scopo di stabilire prassi di vigilanza uniformi, efficienti ed efficaci[342]. Le autorità ed i partecipanti ai mercati finanziari sono chiamati a conformarsi a tali orientamenti e, entro due mesi dall'emanazione dell'orientamento, ogni autorità nazionale di vigilanza competente dovrà confermare se intende conformarsi oppure se lo abbia già fatto.

Il regolamento MiCA mantiene la validità del Regolamento (UE) n. 1024/2013, che conferisce alla Banca Centrale Europea specifiche responsabilità riguardo la vigilanza prudenziale degli enti creditizi. Questa scelta riflette un impegno continuo nella costruzione di un'unione bancaria, basata su un insieme completo e dettagliato di norme per i servizi finanziari nell'intero mercato interno.

Il presente *framework* include un meccanismo unico di vigilanza, nonché nuove strutture per la garanzia dei depositi e la gestione delle crisi bancarie[343].

La BCE, in qualità di banca centrale della zona euro e istituzione con ampie competenze in ambito macroeconomico e di stabilità finanziaria, è ritenuta l'ente più adatto per svolgere le funzioni di vigilanza necessarie a proteggere la stabilità del sistema finanziario dell'Unione Europea. Il ruolo *de quo* le permette di contribuire

[340] Quindi un prodotto pensionistico individuale di risparmio a lungo termine offerto da un'impresa finanziaria ammissibile, a norma dell'articolo 6, paragrafo 1, nell'ambito di un contratto PEPP e sottoscritto da un risparmiatore in PEPP o da un'associazione indipendente di risparmiatori in PEPP a nome dei suoi membri a fini pensionistici, con nessuna possibilità di rimborso o con possibilità strettamente limitate, registrato in conformità del presente regolamento;

[341] il 29 gennaio 2024 è stato pubblicato il terzo ed ultimo pacchetto di consultazioni con il termine ultimo del 29 aprile 2024.

[342] L'ottica è, quindi, quella dell'articolo 16 del regolamento (UE) n. 1095/2010.

[343] Considerando n. 11 del regolamento 1024/2013,

significativamente all'integrità e alla sicurezza del settore finanziario nell'ambito dell'UE[344].

Il Regolamento MiCA adotta un approccio che potrebbe essere definito "negativo"; in altri termini, tende ad escludere dalla sua portata ciò che è già disciplinato da altri testi normativi. Questo metodo, sebbene apparentemente semplice, porta con sé complessità e difficoltà interpretative, soprattutto a causa della natura intricata dei *crypto-asset* e delle incertezze che ancora oggi circondano alcune definizioni chiave nel diritto UE dei mercati finanziari, come quella di "strumento finanziario" delineata dalla MiFID[345].

Un esempio significativo di queste problematiche interpretative è la nozione di "negoziabilità" dello strumento finanziario, un elemento centrale che genera ambiguità nell'identificazione dell'ambito di applicazione del MiCA. Questa incertezza non deriva tanto dalla mancanza di chiarezza di MiCA, ma piuttosto dalla mancanza di definizioni precise negli altri testi normativi dell'Unione Europea che dovrebbero servire come riferimento. La questione di classificazione e delimitazione tra MiCA e altri testi normativi UE rappresenta una delle debolezze del nuovo quadro regolamentare.

Per colmare queste lacune, si prevede che numerose iniziative di *soft law*, emanate dalle Autorità europee, giocheranno un ruolo chiave nell'interpretazione e nell'applicazione delle norme[346].

---

[344] Cfr. il considerando n. 13 del regolamento 1024/2013.

[345] "Ad oggi dopo 30 anni che conosciamo la disciplina sui servizi di investimento, non sappiamo esattamente cosa sia uno strumento finanziario, poiché le nozioni di strumento finanziario sono state elaborate 30 anni fa e in dottrina e giurisprudenza non esistono pronunce della corte di giustizia che aiutino a capire cosa esso sia realmente. Se non sappiamo esattamente cos'è uno strumento finanziario, la tassonomia MiCAR vacilla e si potrebbero aprire delle falle nel sistema con ripercussioni su cosa vada regolato, a chi spetti regolare e vigilare." F. ANNUNZIATA, «*La tassonomia del Regolamento MiCA: ARTs, EMTs e utility tokens. Criteri di identificazione e definizioni*.» (Il Regolamento MiCA nel contesto della disciplina bancaria e dei servizi di pagamento, Roma: BANCA D'ITALIA, 29 settembre 2023).

[346] «L'art. 2, par. 5, di MiCA prevede che, entro il 30 dicembre 2024, l'ESMA elabori orientamenti - conformemente all'art. 16 del Regolamento (UE) n. 1095/2010 - sulle condizioni e sui criteri per la qualificazione delle cripto-attività come strumenti finanziari. Fa così ingresso, anche sul piano della qualificazione dei *crypto-asset*, la *soft law*, che si conferma quale strumento sempre più diffuso e di rilievo ormai determinante sul piano delle azioni delle Autorità dell'Unione. Ulteriori previsioni, a testimonianza di quanto sia delicata la questione delle tassonomie, risultano dall'art. 97 del Regolamento (Promozione della convergenza nella classificazione delle cripto-attività), e segnatamente: in base all'art. 97, par, 1, entro il 30 dicembre 2024, le AEV emanano congiuntamente orientamenti (in conformità dell'art. 16 dei rispettivi regolamenti istitutivi) per specificare il contenuto e la forma della spiegazione che accompagna il *White Paper* sulle cripto-attività di cui all'art. 8, par. 4, e dei pareri legali sulla qualificazione dei *token* collegati ad attività di cui all'art. 17, par. 1, lett. b), punto ii), e all'art. 18, par. 2, lett. e). Gli orientamenti includono un modello per la spiegazione e il parere nonché un *test* standardizzato per la classificazione delle cripto-attività;- in base all'art. 97, par. 2, in conformità agli art. 29 dei rispettivi Regolamenti istitutivi, le Autorità europee promuovono la

La relazione tra il Regolamento MiCA e gli ordinamenti giuridici nazionali, in termini di classificazione e definizioni, si rivela complessa a causa della presenza di nozioni diverse nei sistemi giuridici interni, le quali potrebbero interferire con la portata del Regolamento. Ad esempio, in Italia, la definizione di prodotto finanziario secondo l'articolo 1, lettera *u)* del Testo Unico della Finanza (TUF) è estremamente ampia e basata su un criterio funzionale. Questa definizione mira a comprendere la funzione o lo scopo dell'operazione di investimento economica, sottoponendola alle norme relative all'offerta al pubblico e al prospetto informativo nazionale. Tale definizione si differenzia da quella eurounitaria di strumento finanziario, che è generalmente più limitata e specifica; La nozione italiana è invece aperta ed adattabile, potenzialmente in grado di includere qualsiasi operazione, contratto o attività che rispecchi le caratteristiche di un investimento finanziario.

Nonostante la definizione di prodotto finanziario abbia storicamente presentato sfide interpretative, l'introduzione della disciplina MiCA e della sua tassonomia ha accentuato queste difficoltà, specialmente nel contesto delle cripto-attività. Si consideri il caso di una cripto-attività che possiede le caratteristiche di uno strumento di partecipazione per l'emittente, simile a un titolo azionario, ma che non soddisfa gli elementi qualificanti di uno strumento finanziario, come la negoziabilità. In questa situazione, la normativa derivante dalla MiFID non sarebbe applicabile, in quanto lo strumento non potrebbe essere classificato come uno strumento finanziario secondo i criteri ivi stabiliti. Questo evidenzia la complessità e le sfide interpretative legate all'integrazione del regolamento MiCA con le normative nazionali esistenti.

Se nel suddetto esempio, lo strumento venisse emesso in forma crittografica su una tecnologia di registro distribuito, ci si interroga su quale possa essere la normativa pertinente per la sua introduzione nel mercato e per i servizi correlati offerti dai fornitori nel settore delle cripto-attività, come la consulenza, la gestione e la custodia.

---

discussione tra le autorità competenti sulla classificazione delle cripto-attività, compresa la classificazione delle cripto-attività escluse dall'ambito di applicazione di MiCA Le AEV identificano inoltre le fonti di potenziali divergenze negli approcci adottati calle autorità competenti riguardo alla classificazione di tali cripto-attività e, nella misura del possibile, promuovono un approccio comune al riguardo;- in base all'art. 97, par. 3, le Autorità competenti dello Stato membro d'origine o dello Stato membro ospitante possono chiedere all'ESMA, all'EIOPA o all'EBA, a seconda dei casi, un parere sulla classificazione delle cripto-attività, comprese quelle escluse dall'ambito di applicazione di MiCA a norma dell'art. 2, par.3; infine, in base all'art. 97, par. 4, le Autorità europee redigono congiuntamente una relazione annuale sulla base delle informazioni contenute nel registro di cui all'art. 109 e dei risultati delle loro attività di cui ai parr. 2 e 3 del presente articolo, che individua le difficolta incontrate nella classificazione delle cripto-attività e le divergenze emerse negli approcci adottati dalle Autorità competenti.» in F. ANNUNZIATA, «*La disciplina del mercato dei capitali»* (G. Giappichelli Editore, 2023).

Il Regolamento MiCA potrebbe essere il riferimento normativo, adeguato, che classifichi tale strumento come un "*utility token*". Tuttavia, emerge un'incertezza riguardo all'adeguatezza della definizione di *utility token* in MiCA, in quanto lo strumento suddetto potrebbe non rientrare nel campo di applicazione del Regolamento.

In questo contesto, si apre lo spazio per le legislazioni nazionali. Se un'attività crittografica non rientrasse sotto MiCA, le normative nazionali potrebbero trovare applicazione.

Il punto critico nel caso di specie, è l'assenza di una nozione equivalente di prodotto finanziario nella normativa europea. Pertanto, una cripto-attività potrebbe essere considerata secondo la normativa nazionale, come un'altra forma di investimento di natura finanziaria[347], dando luogo ad un conflitto con le regole MiCAR.

In verità, dopo la data di attuazione di MiCAR, questo possibile conflitto dovrebbe essere risolto a favore del suddetto regolamento UE, nel rispetto della sua natura di massima armonizzazione e anche in linea con il principio del primato del diritto UE su quello nazionale. Tuttavia, non tutte le problematiche di attribuzione di disciplina sarebbero superate nel caso in cui un prodotto finanziario circolasse sia come *token* (cioè come rappresentazione digitale di un contratto di investimento finanziario iscritto in un registro distribuito) sia in forma tradizionale, con possibile asimmetria di trattamento per la coesistenza di due discipline[348].

Questo esempio evidenzia la necessità di adattare i quadri normativi all'innovazione nel settore finanziario digitale.

La disamina della classificazione domestica di strumenti finanziari, prodotti finanziari e cripto-attività, rivela l'importanza fondamentale della tassonomia per l'adeguata applicazione delle relative normative. In Italia, sia la prassi della CONSOB[349] che le decisioni della Suprema Corte[350] hanno già stabilito che, in

[347] La dottrina nazionale si è interrogata, a questo proposito, sulla capacità della condizione di negoziabilità di trasformare un *utility token* in un prodotto finanziario. Cfr. C. SANDEI, «*L'offerta iniziale di cripto-attività»* G. Giappichelli Editore, 2022, 45-59.

[348] G. D'AGOSTINO, «*MiCAR: rischi e opportunità per le istituzioni finanziarie che prestano servizi su crypto-asset nella UE*», Bancaria, fasc. 12/2023 (dicembre 2023): 32–44.

[349] Cfr. Delibera n. 19968 del 20 aprile 2017, Delibera n. 20346 del 21 marzo 2018, Delibera n. 20693 del 14 novembre 2018, Delibera n. 20694 del 14 novembre 2018.

[350] Con la sentenza n. 44378 del 22 novembre 2022, la seconda sezione penale della corte di cassazione, ha affermato che le criptovalute sono assimilabili a prodotti finanziari. Le criptovalute, infatti, posseggono caratteri propri dell'investimento finanziario, ovvero si caratterizzano per a) l'impiego dei capitali; b) l'aspettativa di un rendimento; c) un rischio direttamente correlato all'impiego di capitali. Questa impostazione conferma quella tenuta dalla Suprema Corte con la sentenza n. 26807 del 17 settembre 2020. Cfr. *«Criptovalute sono prodotti finanziari per la Cassazione*», Diritto Bancario, 23 novembre 2022.

determinate condizioni, Bitcoin (che non rientra nel Regolamento sui Mercati di Cripto-Attività, MiCA, a causa della sua natura completamente decentralizzata) debba essere considerato un prodotto finanziario e, come tale, soggetto alla normativa specifica per l'offerta pubblica.

Queste conclusioni, benché possano non essere unanimemente accettate, rappresentano dei precedenti significativi. Riflettono le difficoltà di un sistema normativo che si confronta con la crescente diffusione delle cripto-attività e cerca di definire criteri chiari per la loro classificazione e regolamentazione. Il contesto evidenzia le sfide nel bilanciare l'innovazione tecnologica con i requisiti legali e regolamentari esistenti, sottolineando la necessità di un'evoluzione normativa che possa adeguatamente incorniciare e governare tali strumenti emergenti nel settore finanziario[351].

## 1.3 *E-money tokens* ed emittenti

Il regolamento MiCA applica a tutte le cripto-attività che fanno riferimento ad un'unica valuta ufficiale, le regole della EMD2[352].

Come è stato evidenziato, il principio che anima la direttiva, e che è comune alla legislazione Eurounitaria, è quello della neutralità tecnologica. Questo principio viene declinato sia come mancata regolazione e cioè necessità di astenersi dal regolare una specifica tecnologia, che per evitare una discriminazione normativa in ragione della tecnologia utilizzata. Per queste ragioni restano fuori dall'ambito di applicazione MiCAR tutti gli strumenti finanziari[353] che sono già regolati dalla Mifid. Questa è l'affermazione di principio fatta dal regolatore.

Volendo entrare nel merito del discorso è necessario partire dalle definizioni, mettendo a confronto la definizione di moneta elettronica che è già in vigore sulla base

[351] Nella letteratura accademica, emergono incertezze riguardanti la distinzione e sovrapposizione tra le nozioni di strumento finanziario e prodotto finanziario. È stato osservato come talvolta caratteristiche tipiche dei prodotti finanziari vengano applicate agli strumenti finanziari, confondendo quest'ultima categoria, che è generalmente una categoria chiusa e definita, con la nozione più ampia e flessibile del prodotto finanziario. È essenziale che il quadro normativo del MiCA, mantenga una coerenza con le definizioni adottate a livello dell'Unione Europea. Le normative nazionali dovrebbero intervenire solo laddove le definizioni e le normative euro-unitarie si dimostrino inadeguate o inapplicabili, come interpretate secondo il diritto dell'Unione. In Italia, ad esempio, la nozione di prodotto finanziario è circoscritta principalmente all'ambito dell'offerta al pubblico, escludendo la prestazione di servizi relativi ai prodotti finanziari. Cfr. M. CIAN, «*Manuale di diritto commerciale*», V (G. Giappichelli Editore, 2023).

[352] Direttiva 2009/110/CE. Seconda direttiva sulla moneta elettronica.

[353] Vedi *infra.*

della suddetta direttiva del 2009 e la definizione di *token* di moneta elettronica. Preme evidenziare come entrambe siano sostanzialmente una rappresentazione digitale di un valore o di una valuta ufficiale con la peculiarità che il *token* utilizza una tecnologia a registro distribuito o una tecnologia analoga. Quindi il *token* di moneta elettronica è considerato moneta elettronica e i *token* sono da ricomprendersi anch'essi nella nozione di fondi.

La funzione del *token* è molto simile a quella della moneta elettronica e analogamente a questa, si tratta di un surrogato tecnologico di monete e banconote utilizzate per fare pagamenti.

La disciplina che regola entrambi gli strumenti non ha valenza finanziaria perché questi prodotti sono emessi al valore nominale al momento del ricevimento dei fondi e deve essere assicurato il loro rimborso al valore nominale. Gli emittenti ma anche i CASP che svolgono servizi nel campo delle cripto-attività non possono concedere interessi o benefici di altra natura legati al possesso di questi prodotti e quindi sono strumenti improduttivi per loro natura.

Gli emittenti sono tenuti alla segregazione patrimoniale dei fondi ricevuti per l'emissione degli strumenti prepagati al fine di assicurarne il rimborso. Entrambi sono quindi strumenti di pagamento la cui emissione è rimessa all'attività di istituzioni finanziarie private autorizzate.

L'accettazione di questi strumenti è da ricondurre all'autonomia privata. In ogni caso sia la moneta elettronica tradizionale che quella tokenizzata sono ricomprese nella vigilanza della Banca Centrale Europea tramite il PISA *framework*[354].

Fatta questa premessa generale, volta ad accostare e sottolineare le similitudini tra questi due strumenti, è necessario esaminare alcuni dettagli della disciplina.

I soggetti emittenti di *e-money token* secondo MiCAR sono solo banche e IMEL[355]; analizzando invece la disciplina contenuta nella direttiva, emittenti di

[354] ECB EUROSYSTEM, «*Eurosystem Oversight Framework for Electronic Payment Instruments, Schemes and Arrangements*», novembre 2021, https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf.

[355] Gli istituti di moneta elettronica (IMEL) sono imprese, diverse dalle banche, che emettono moneta elettronica. Gli IMEL, oltre ad emettere moneta elettronica, possono altresì prestare servizi operativi strettamente connessi con l'emissione di moneta elettronica, quali ad esempio: *a)* progettazione e realizzazione di procedure, dispositivi e supporti relativi all'attività di emissione di moneta elettronica; *b)* prestazione, per conto di terzi emittenti di moneta elettronica, di servizi connessi con l'emissione di moneta elettronica; *c)* prestare i servizi di pagamento previsti dai punti da 1 a 8 dell'art.1, comma 2, lett. h-septies.1), TUB anche non connessi con l'emissione di moneta elettronica, nonché le relative attività accessorie; *d)* concedere finanziamenti relativi ai servizi di pagamento entro i limiti indicati nelle disposizioni di vigilanza applicabili; *e)* esercitare altre attività d'impresa non connesse alla prestazione dei servizi di pagamento o all'emissione di moneta elettronica; in questo caso, la legge

moneta elettronica sono anche le Poste, la Banca Centrale Europea e le Banche Centrali Nazionali che non agiscono in veste di autorità monetaria, gli Stati membri e altri enti territoriali in veste di autorità pubblica.

Per quanto riguarda Il regime di vigilanza, è noto il riparto di competenze proprio del settore bancario, tra Autorità nazionali competenti (Anc) e vigilanza sovranazionale.

La vigilanza c.d. "di tutela" relativa ai servizi di pagamento è concentrata presso le ANC e per determinati soggetti specializzati nell'emissione di moneta elettronica convergono nelle ANC entrambe le vigilanze sia prudenziali che di tutela.

Nel MiCAR si introduce un concetto nuovo che è quello della emissione significativa. La significatività viene collegata dal regolamento alla emissione. Non è più significativo il soggetto come avviene in materia bancaria, ma è significativa l'emissione. La significatività ha carattere dinamico, poiché la valutazione viene fatta con cadenza annuale da parte dell'EBA. Viene considerato il valore complessivo di mercato; non si fa riferimento, infatti, all'emissione del singolo emittente, ma al *token* di pagamento in generale. Di conseguenza se più emittenti emettono quello strumento, sarà preso in considerazione il valore complessivo di mercato del *token* con le medesime caratteristiche.

I criteri per stabilire la significatività sono molteplici; riguardano: criteri che sottolineano il grado di diffusione, l'entità dei *token* emessi, il grado di utilizzo giornaliero come strumento di pagamento, l'interconnessione del *token* con il sistema finanziario, l'interconnessione con almeno un servizio di cripto-attività o con la fornitura di servizi di piattaforma.

Al ricorrere di almeno 3 di questi requisiti scatta la valutazione di significatività che viene operata dall'EBA. Per effetto della valutazione *de quo* avviene il passaggio di vigilanza sull'IMEL (non anche per le banche) alla vigilanza dell'EBA ma con possibilità nell'anno successivo se questa significatività venisse meno di retrocedere alla vigilanza nazionale. La significatività porta con sé oltre allo spostamento di competenza anche obblighi aggiuntivi sui quali l'EBA dovrà vigilare per contrastare i rischi di liquidità ed i rischi operativi di gestione.

Al superamento di determinate soglie potrebbero essere applicate anche le restrizioni quantitative di emissione di EMTs significativi.

---

prevede che i servizi di pagamento e l'emissione di moneta elettronica siano svolti attraverso un patrimonio destinato che l'intermediario (c.d. ibrido commerciale) deve costituire.

Micar impone che l'emissione di *token* sia al valore nominale solo al momento del ricevimento dei fondi; avviene questa conversione per effetto della quale i detentori sono titolari di un diritto di credito nei confronti dell'emittente e CASP, i quali non concedono interessi. In questo senso la disciplina contenuta nel regolamento e quella sulla moneta elettronica sono del tutto sovrapponibili; l'elemento di diversità sta nella regolamentazione del diritto al rimborso. La direttiva tradizionale sulla moneta elettronica prevede che il contratto relativo alla moneta elettronica possa disciplinare le condizioni del rimborso, quindi, anche spese e commissioni.

Ciò di cui si fa obbligo all'emittente è che prima della sottoscrizione del contratto informi il detentore delle condizioni di rimborso.

Di certo la direttiva richiede il convenzionamento qualora il cessionario della moneta elettronica non sia un consumatore. Il negoziante per poter chiedere un rimborso della moneta elettronica ha necessità di un convenzionamento con l'emittente che può essere diretto o avvenire attraverso un altro intermediario.

Vi è quindi, una contrattualizzazione sia nella fase di emissione della moneta cioè quando lo strumento prepagato viene acquisito, sia nella fase di riscossione da parte del beneficiario di questo pagamento.

Per gli EMT, il Regolamento prevede invece un diritto al rimborso permanente *ope legis* al valore nominale di moneta di banca centrale o moneta scritturale senza commissioni[356]; la possibilità di applicare commissioni pare essere esclusa dal regolamento anche se poi si precisa che le condizioni del rimborso devono essere rese note nel *white paper*[357]. Quindi queste condizioni potrebbero essere sia temporali che relative a spese e commissioni. Appare quindi necessario coordinare le previsioni dei rimborsi in modo che non siano contestabili in sede contrattuale. Si noti che la responsabilità relativa alla veridicità e correttezza delle informazioni contenute nel *white paper* grava sull'emittente e sui membri sull'organo amministrativo, che ne devono asseverare la conformità ai requisiti formali e sostanziali dell'art. 51 MiCA[358]. La notifica sembrerebbe strumentale ad una verifica formale concernente il rispetto delle voci informative prescritte nel regolamento e non implicherebbe anche un esame di merito del suo contenuto negoziale.

[356] Considerando 19 MiCA.
[357] Artt. 46, 47, 55 MiCA.
[358] Questo, impone la notifica del white paper alla autorità competente ma non ne richiede l'approvazione.

Nel caso dei *token* di pagamento, dove la contrattualizzazione verosimilmente manca nel momento in cui il *token* passa di mano e viene acquisito da un beneficiario che non è legato da un contratto di convenzionamento all'emittente, l'unica disciplina è quella del *white paper* che quindi, in caso di violazione, porterà ad una responsabilità di tipo extracontrattuale, mancando un contratto che lega il beneficiario finale e lo stesso emittente.

Volendo concludere, si nota un disallineamento nella individuazione dei soggetti emittenti nel confronto tra le due discipline e un disallineamento per la vigilanza per questa peculiarità relativa alle emissioni significative in particolare al regime di vigilanza. Si introduce il *white paper* come strumento informativo per tutti i possessori, quindi, sia per i consumatori che per la clientela *business*. Il dubbio che ancora una volta sorge è se il principio di neutralità tecnologica, richiamata dalla direttiva, effettivamente trovi applicazione, tenuto conto che all'identità funzionale dei due strumenti e alla sostanziale identità di disciplina poi corrispondono regole non sempre coincidenti[359].

## 1.4 Ambito di applicazione soggettivo e regime autorizzativo

In merito all'aspetto soggettivo, il Regolamento sui Mercati di Cripto-Attività si rivolge principalmente a due categorie di soggetti: gli emittenti di cripto-attività (inclusi quelli al di fuori del settore finanziario) ed i fornitori di servizi di cripto-attività.

Per gli emittenti di cripto-attività, MiCA stabilisce obblighi focalizzati sulla trasparenza e la divulgazione di informazioni. Questi includono la necessità di redigere e pubblicare un *White Paper* prima di procedere con l'offerta di cripto-attività sul mercato. Per i fornitori di servizi di cripto-attività, invece, il Regolamento stabilisce norme che seguono il modello dei fornitori di servizi finanziari tradizionali all'interno dell'Unione Europea. Queste norme comprendono l'ottenimento di un'autorizzazione iniziale, il rispetto di regole prudenziali e di condotta, nonché l'osservanza di requisiti di trasparenza.

I soggetti che emettono *crypto-asset* e forniscono servizi correlati, come nel caso degli *asset referenced token* (ARTs) e dei *token* di moneta elettronica (EMTs), devono

[359] V. PROFETA «*Gli e-money tokens e la disciplina sulla moneta elettronica*» (Il Regolamento MiCA nel contesto della disciplina bancaria e dei servizi di pagamento, BANCA D'ITALIA, Roma, 29 settembre 2023).

rispettare un insieme di requisiti che combinano entrambi i regimi: la trasparenza nella fase di emissione e nella fase di prestazione dei servizi. Per gli ARTs e gli EMTs, la normativa è quindi più complessa. L'emissione di questi tipi di *token* è considerata un'attività esclusiva, accessibile solo ad enti che ricevono autorizzazione da parte delle Autorità competenti, come gli enti creditizi e gli istituti di moneta elettronica nel caso degli *e-money token*; gli emittenti di *asset-referenced token*, sono invece autorizzati in conformità alle disposizioni del MiCA.

Nel contesto delle cripto-attività, diversi soggetti partecipano sia alla fase di emissione sia a quella di distribuzione. Benché queste due fasi siano interconnesse e funzionalmente legate all'interno di un processo dinamico di diffusione e circolazione delle cripto-attività presso il pubblico, le medesime possono essere considerate separatamente per quanto riguarda la regolamentazione, delineando perimetri soggettivi[360] con caratteristiche specifiche all'interno del quadro normativo[361].

Ogni fase del ciclo delle cripto-attività, insieme agli attori che rivestono un ruolo chiave, è oggetto di attenta supervisione e analisi. Questo controllo è esercitato sia dalle Autorità nazionali competenti sia dalle Autorità europee EBA e ESMA, le quali agiscono in base alla distribuzione delle competenze in relazione alla materia trattata[362]. Al fine di includere i protagonisti dei nuovi mercati cripto-finanziari nell'ambito della vigilanza e supervisione, parimenti a quanto accade agli altri settori finanziari, è essenziale il processo di autorizzazione per l'accesso al mercato. Questo processo si configura come un elemento fondamentale del futuro panorama finanziario basato su tecnologie crittografiche.

Nonostante l'autorizzazione costituisca una fase iniziale fondamentale, in particolare per l'integrazione di nuove attività in un contesto armonizzato, influenzando elementi correlati come il passaporto europeo e il regime normativo specifico dei fornitori di servizi per le cripto-attività, la normativa MiCA la regola in modi diversi, come verrà illustrato.

Il regime giuridico correlato, delineato nel Capo 1 del Titolo V del MiCAR, stabilisce la procedura *standard* di autorizzazione, che tuttavia presenta diverse

[360] I.e. il considerando 22 precisa: "Qualora le cripto-attività non abbiano un emittente identificabile, esse non dovrebbero rientrare nell'ambito di applicazione dei titoli II, III o IV del presente regolamento. I prestatori di servizi per le cripto attività che prestano servizi in relazione a tali cripto-attività dovrebbero tuttavia rientrare nell'ambito di applicazione del presente regolamento".
[361] M. T. PARACAMPO, «*Los proveedores de servicios de criptoactivos entre antiguos y nuevos players*», in *Dinero Digital y Gobernanza IIC en la UE* (Thomson Reuters Aranzadi, 2022).
[362] Vedi *infra*.

eccezioni per specifiche categorie di fornitori e situazioni operative. Il quadro normativo, dunque, non è uniforme ma piuttosto variegato, poiché contempla sia prestatori sia nuovi che già attivi sul mercato e prevedendo un mercato aperto ad una serie di *players* con differenti *background*.

## 1.5 I prestatori di diritto europeo

L'accesso al mercato delle cripto-attività subisce alcune eccezioni in relazione a talune particolari categorie soggettive che, giusta presunzione di equivalenza dei servizi MICA a quelli ex Mifid 2, usufruiscono di regimi di esenzione dalla procedura ordinaria di autorizzazione.

Questi operatori possono essere classificati come prestatori di servizi di diritto europeo; un gruppo che rappresenta un numero chiuso di attori nel panorama dei soggetti disciplinati dal MiCA, ognuno con le proprie peculiarità ed origine normativa. Essi hanno in comune la caratteristica di essere già attivi nel mercato, fornendo servizi in linea con quelli specificati dal MiCA e considerati equivalenti a quelli del Mifid 2 in virtù della loro autorizzazione secondo la legislazione finanziaria europea.

I prestatori in questione, selezionati preliminarmente dal legislatore del MiCA sulla base del loro passaporto europeo e della loro capacità operativa, possono beneficiare di un regime di esenzione, a condizione che soddisfino determinati requisiti, che variano in base alla loro provenienza normativa.

Questo aspetto rappresenta un punto chiave nella definizione delle presunzioni di equivalenza, agendo come un filtro selettivo per l'accesso di certi operatori al mercato delle cripto-attività e stabilendo una serie di regimi di esenzione dalla procedura altrimenti obbligatoria per tutti i prestatori su richiesta. Paradossalmente, sono le stesse presunzioni di equivalenza a facilitare il riconoscimento del passaporto europeo di tali categorie, creando un collegamento diretto tra i servizi già prestati e quelli che si intendono offrire nel mercato delle cripto-attività.

Di conseguenza, è da queste presunzioni di equivalenza che si deve partire nell'analizzare e comprendere l'accesso al mercato delle cripto-attività e le relative eccezioni alla procedura di autorizzazione.

L'analisi delle equivalenze tra i servizi MiCA/Mifid 2 evidenzia una quasi completa corrispondenza con l'elenco dei servizi di investimento[363]. Alcune lacune sono state successivamente colmate, in particolare dal Consiglio d'Europa, che ha apportato due cambiamenti rilevanti. Innanzitutto, ha riposizionato la presunzione di equivalenza in un contesto più adeguato, ossia quello dell'accesso al mercato. Inoltre, ha modificato la formulazione originale, introducendo novità significative, come l'aggiunta di un nuovo articolo (art. 60), dedicato specificamente ai servizi su cripto-attività forniti da soggetti che possono beneficiare dell'esenzione dall'autorizzazione.

La nuova disposizione sembra mirata a stabilire un trattamento giuridico alternativo alla procedura ordinaria di autorizzazione, approfittando anche dell'occasione per diversificare e ampliare sia l'elenco dei soggetti inclusi nel perimetro di esenzione, sia il *range* di servizi che rientrano nella presunzione di equivalenza.

La presunzione di equivalenza, quindi, sembra perseguire un duplice scopo:

*a)* "omologare" i criteri definitori e i contenuti dei servizi MiCA con quelli già sperimentati dalla Mifid 2, rendendola un *benchmark* normativo fondamentale;

*b)* utilizzare tale omologazione come base per l'attuazione del regime di esenzione dalla procedura autorizzativa *standard*, diversamente prevista per i nuovi prestatori.

In seguito alla nuova collocazione sistematica[364] della presunzione di equivalenza nel titolo V, emerge come la sua finalità principale sia quella di collegare

[363] in particolare di: custodia e amministrazione di strumenti finanziari; gestione di sistemi multilaterali di negoziazione; gestione di sistemi organizzati di negoziazione; negoziazione per conto proprio; esecuzione di ordini per conto dei clienti; assunzione a fermo di strumenti finanziari e/o collocamento di strumenti finanziari sulla base di un impegno irrevocabile; collocamento di strumenti finanziari senza impegno irrevocabile; ricezione e trasmissione di ordini riguardanti uno o più strumenti finanziari; consulenza in materia di investimenti; gestione di portafogli.

[364] considerando 78: "Talune imprese soggette agli atti legislativi dell'Unione in materia di servizi finanziari dovrebbero essere autorizzate a prestare tutti o alcuni servizi per le cripto-attività senza essere tenute a ottenere un'autorizzazione come prestatore di servizi per le cripto-attività a norma del presente regolamento se notificano alle loro autorità competenti determinate informazioni prima di prestare tali servizi per la prima volta. In tali casi, tali imprese dovrebbero essere considerate prestatori di servizi per le cripto-attività e ad esse dovrebbero applicarsi i pertinenti poteri amministrativi previsti dal presente regolamento, compresa la facoltà di sospendere o vietare determinati servizi per le cripto-attività. Tali imprese dovrebbero essere soggette a tutti i requisiti applicabili ai prestatori di servizi per le cripto-attività a norma del presente regolamento, ad eccezione dei requisiti di autorizzazione, dei requisiti di fondi propri e della procedura di approvazione per quanto riguarda gli azionisti e i soci che detengono partecipazioni qualificate, in quanto tali questioni sono disciplinate dai rispettivi atti legislativi dell'Unione a norma del quali sono state autorizzate. La procedura di notifica per gli enti creditizi che intendono prestare servizi per le cripto-attività a norma del presente regolamento dovrebbe lasciare impregiudicate le disposizioni del diritto nazionale di recepimento della direttiva 2013/36/UE che stabiliscono procedure per l'autorizzazione degli enti creditizi a prestare i servizi elencati nell'allegato I di tale direttiva".

le circostanze soggettive di ogni prestatore nell'accesso al mercato con quelle oggettive dei servizi già offerti sul mercato secondo Mifid 2 e considerati equivalenti a quelli ora definiti nel contesto del MiCA.

Il collegamento tra la presunzione di equivalenza e il regime di esenzione nel contesto del MiCA è fondamentale e deve essere tenuto in considerazione. Tale collegamento è rafforzato dalle conseguenze, sia positive che negative, che riguardano il soggetto beneficiario del regime di esenzione fin dalla sua origine[365].

L'esenzione normativa è strettamente connessa alle presunzioni basate sull'equivalenza dei servizi tra MiCA e Mifid 2. Questo processo inizia con la verifica preliminare dell'equivalenza tra i servizi definiti dal MiCA e quelli del Mifid 2, per cui le imprese di investimento sono già autorizzate[366], in forza della loro effettiva operatività.

La preventiva autorizzazione alla fornitura di servizi nel contesto originario di provenienza dei soggetti diventa lo strumento per una "sanatoria diretta", che fornisce un'abilitazione immediata per l'erogazione dei servizi corrispondenti, dichiarati "equivalenti" nel MiCA[367].

Nella struttura delle esenzioni delineate dall'articolo 60, i regimi applicabili si articolano su più livelli e direzioni, creando un trattamento giuridico complesso, multilivello e composito. Tuttavia, presi singolarmente, questi regimi sono personalizzati e specifici, in base alle caratteristiche individuali e alla capacità operativa di ciascun soggetto.

Il regime di esenzione si basa su tre principali criteri:

*a)* soggettivo: riguarda la distinzione tra i vari soggetti autorizzati.

*b)* oggettivo: si focalizza sulla presunzione di equivalenza dei servizi.

*c)* operativo: include il numero e la tipologia di informazioni che devono essere fornite in anticipo all'autorità competente, per supportare il trattamento giuridico in questione.

---

[365] Con il riferimento si intendono tutte le vicende che riguardano sia l'autorizzazione (i.e. revoca, decadenza, rinuncia), sia il novero dei servizi prestati.

[366] Tanto si desume dal disposto dell'art. 60, par. 3:" Un'impresa di investimento può prestare servizi per le cripto-attività nell'Unione equivalenti ai servizi e alle attività di investimento per cui è specificamente autorizzata a norma della direttiva 2014/65/UE se comunica all'autorità competente dello Stato membro d'origine le informazioni di cui al paragrafo 7 almeno 40 giorni lavorativi prima di prestare tali servizi per la prima volta".

[367] M.T. PARACAMPO, «*I prestatori di servizi per le cripto-attività Tra mifidizzazione della MICA e tokenizzazione della Mifid»* G. Giappichelli Editore, 2023.

Un elemento chiave comune a tutti e tre questi aspetti è la proporzionalità, che si manifesta nella graduazione delle regole applicabili. Questo principio è cruciale sia nella valutazione comparativa tra i servizi *core* e non, e rispetto a quelli considerati "equivalenti" nel MiCA, sia nella selezione dei soggetti beneficiari del regime di esenzione.

Il regime di esenzione si distingue per diverse sfumature a seconda della natura e della qualificazione dei soggetti inclusi, con una geometria variabile che si adatta alla capacità operativa riconosciuta a ciascuna categoria.

Si può parlare di una pluralità di regimi di esenzione che, pur avendo la stessa *ratio*, si differenziano in base all'estensione del passaporto europeo dei soggetti inclusi tra i prestatori di diritto europeo. Le esenzioni sono concesse in relazione alla specifica prestazione del servizio equivalente, e si distinguono per il diverso ambito trattato, ovvero le cripto-attività anziché gli strumenti finanziari.

L'equivalenza dei servizi implica quindi anche l'equivalenza dei passaporti europei, entro i limiti specificati, con le imprese di investimento autorizzate a fornire solo i servizi MICA correlati (o equivalenti).

Ciò è una diretta conseguenza del regime di esenzione, che non si applica in modo generalizzato a tutti i servizi elencati nel MiCA, ma soltanto a quelli per i quali l'impresa è stata precedentemente autorizzata nel suo contesto originario. Questo suggerisce che la presunzione di equivalenza funge effettivamente da "passaporto", o più esattamente da chiave universale, per operare anche nel contesto del MiCA.

Una analisi letterale dell'articolo 60, paragrafo 3[368], sembra confermare questa interpretazione. Questa disposizione collega direttamente i servizi specificamente

[368] "La correlazione tra servizi inclusi nel passaporto europeo e servizi considerati equivalenti da MICA si evince chiaramente dal disposto dell'art. 60, par. 3 (quale "Un'impresa di investimento può prestare servizi per le cripto-attività nell'Unione equivalenti ai servizi e alle attività di investimento per cui è specificamente autorizzata a norma della direttiva 2014/65/UE se comunica all'autorità competente dello Stato membro d'origine le informazioni di cui al paragrafo 7 almeno 40 giorni lavorativi prima di prestare tali servizi per la prima volta"), che pone l'accento sull'avverbio "specificamente", onde rafforzare il rapporto diretto, ai fini della preventiva autorizzazione, tra servizi Mifid e MICA.
Parimenti si giustifica previsione di identico tenore di cui al par. 5 relativamente alle società di gestione di OICVM ed ai gestori di fondi alternativi di investimento ("Una società di gestione di un OICVM o un gestore di fondi di investimento alternativi possono prestare servizi per le cripto-attività equivalenti a servizi di gestione di portafogli di investimento e servizi accessori per cui sono autorizzati a norma delle direttiva 2009/65/CE o della direttiva 2011/61/UE se comunicano all'autorità competente dello stato membro d'origine le informazioni di cui al paragrafo 7 almeno 40 giorni lavorativi prima di prestare tali servizi per la prima volta")". In M. T. PARACAMPO, «*I prestatori di servizi per le cripto-attività*», 32, in *I prestatore di servizi per le cripto-attività; tra mifidizzazione della MiCAe tokenizzazione della Mifid* (G. Giappichelli Editore, 2023).

autorizzati secondo Mifid 2 con quelli che un'impresa di investimento può offrire in base al MiCA, proprio perché considerati equivalenti.

Le implicazioni operative di questa situazione hanno importanti conseguenze in caso di successiva estensione del perimetro oggettivo dei servizi offerti. In tale scenario, possono emergere tre situazioni distinte:

*a)* se l'estensione riguarda i servizi Mifid, la presunzione di equivalenza dei servizi MiCA dovrebbe implicare automaticamente la loro copertura, previa notifica all'Autorità competente e registrazione presso l'ESMA;

*b)* se l'estensione coinvolge solo i servizi MiCA, forse in seguito a un cambiamento del modello di *business* verso le cripto-attività, l'impresa non potrebbe fare affidamento sul regime di esenzione e dovrebbe seguire la procedura *standard* per ottenere l'autorizzazione a fornire ulteriori servizi MiCA;

*c)* se l'estensione è limitata a specifici servizi MiCA esclusi dalla presunzione di equivalenza, l'impresa dovrà ottenere le necessarie autorizzazioni iniziali per operare nel mercato.

Infine, un ulteriore aspetto da considerare riguarda la revoca dell'autorizzazione originaria[369], che potrebbe annullare il regime di esenzione e influenzare il riconoscimento del passaporto europeo originale per la prestazione dei servizi MiCA. In questo caso, la revoca avrebbe un effetto a catena, con ripercussioni sia sull'esenzione sia sulla capacità dell'impresa di operare nel contesto del MiCA.

Poiché quindi la legge opera una selezione tra i soggetti già autorizzati a operare sui mercati secondo le normative europee nel campo finanziario, l'accesso al regime di esenzione per i soggetti coinvolti avrà duplice natura: soggettiva in quanto riguarderà categorie di operatori già preventivamente selezionate, e oggettiva con riferimento alla prestazione effettiva sul mercato di uno o più servizi considerati equivalenti dal MiCA.

[369] Il venir meno del presupposto fondante del regime di esenzione incide inevitabilmente anche su quest'ultimo. In tal senso depone il disposto di cui all'art. 60, par. 11: "Il diritto di prestare servizi per le cripto-attività di cui ai paragrafi da 1 a 6 del presente articolo è revocato al momento della revoca della relativa autorizzazione che ha consentito al rispettivo soggetto di prestare servizi per le cripto-attività senza essere tenuto a ottenere un'autorizzazione a norma dell'articolo 59". Va peraltro evidenziato come gli effetti conseguenti alla revoca dell'autorizzazione nel settore finanziario di nascita siano inspiegabilmente duplicati (i.e. revoca dell'autorizzazione di un prestatore di servizi per le cripto-attività), sebbene con riferimenti parziali e specifici agli istituti di moneta elettronica e agli istituti di pagamento, nell'art. 64, par. 2, lett. b). *ibid*.

La diversa origine finanziaria dei soggetti, insieme ai due fattori suddetti, diventa così l'obiettivo di una regolamentazione graduale e di statuti normativi personalizzati, che tengono conto della legislazione originaria di autorizzazione.

Un altro elemento significativo che influisce sui regimi di esenzione è la loro modularità; in primo luogo, si considera la specifica estensione operativa del passaporto europeo e, in secondo luogo, il suo contesto all'interno del MiCA. Questo consente un approccio calibrato su uno o più servizi, facilitando la configurazione e la differenziazione dei prestatori di diritto europeo tra quelli con "capacità multipla" e quelli con "capacità ridotta"[370].

In un ordine decrescente di operatività sul mercato, tra tutti i prestatori di diritto europeo, gli enti creditizi (art. 60, par. 1) sono quelli con la più ampia operatività, seguiti dalle imprese di investimento che operano in base ai servizi Mifid, considerati equivalenti a quelli MiCA (par. 3).

Le società di gestione di un OICVM e i gestori di fondi di investimento alternativi, pur sempre nel contesto dei servizi Mifid, hanno una portata operativa più limitata, in quanto sono autorizzati a fornire consulenza, gestire portafogli e ricevere e trasmettere ordini.

Più settoriali e specifici sono i ruoli di altri prestatori: i depositari centrali di titoli (par. 2) per la custodia e amministrazione di cripto-attività per conto dei clienti; i gestori di mercato per la gestione di piattaforme di negoziazione di cripto-attività (par. 6), gli istituti di moneta elettronica per la custodia e amministrazione di cripto-attività per conto dei clienti, oltre ai servizi di trasferimento di cripto-attività in relazione agli *e-money tokens* di propria emissione (par. 4).

Oltre al passaporto europeo già posseduto dai soggetti menzionati e la loro inclusione nel perimetro di vigilanza delle autorità, è richiesta una valutazione preventiva dell'equivalenza necessaria dei presidi di protezione e controllo, sia quelli prescritti da Mifid 2 sia quelli derivanti da altre normative europee pertinenti alla natura finanziaria dei soggetti.

Questi presidi di controllo, a meno che non sia richiesta una loro integrazione con ulteriori requisiti specifici per le cripto-attività e le tecnologie correlate, sono implicitamente considerati adeguati sia per garantire lo stesso livello di tutela degli investitori sia per gestire e prevenire rischi analoghi a quelli degli strumenti finanziari.

[370] F. ANNUNZIATA, «*La disciplina del mercato mobiliare» 130,* (G. Giappichelli Editore, 2021).

In tale contesto, le esigenze di protezione richieste sia in Mifid 2 sia in MiCA, insieme ai processi di controllo e strutture organizzative simili (anche in questo caso implicitamente "equivalenti"), giustificano l'applicazione di un regime di esenzione.

In definitiva, l'equivalenza dei passaporti, in linea con il principio di proporzionalità, può essere interpretata in diversi modi e aspetti, in particolare per quanto riguarda i requisiti organizzativi, al fine di evitare altresì un aumento degli oneri burocratici, a meno che non emergano ulteriori esigenze di tutela regolamentare[371].

La conseguenza di questa situazione è che la struttura operativa e in espansione dei soggetti autorizzati a fornire servizi per le cripto-attività non si limita a creare un ulteriore settore verticale a fianco di quelli finanziari preesistenti. Piuttosto, essa contribuisce ad evidenziare una caratteristica trasversale di questi servizi rispetto agli altri settori del sistema finanziario. Questo processo getta le basi per lo sviluppo di un ecosistema finanziario più complesso e multidimensionale, le cui potenzialità sono ancora in fase embrionale, ma già visibili. Tale ecosistema promette di integrare le cripto-attività in modo più profondo e interconnesso con il panorama finanziario globale, dando luogo ad un'evoluzione significativa nel modo in cui le finanze e le tecnologie si intersecano e si influenzano reciprocamente.

Le revisioni effettuate durante il processo legislativo, precedentemente l'adozione del regolamento, hanno influenzato il regime di esenzione sotto due aspetti principali: l'elenco dei soggetti che possono beneficiarne e i dettagli del trattamento giuridico che sostituisce la normale procedura di autorizzazione.

Queste modifiche hanno migliorato e chiarito alcuni punti che nella proposta originale del regolamento erano trattati in maniera superficiale e ambigua.

Inizialmente, infatti, il testo si rivolgeva solo agli enti creditizi e alle imprese di investimento, delineando separatamente le norme applicabili a ciascuna categoria.

Nella versione definitiva del regolamento, si osserva un'estensione dei soggetti coinvolti e una modifica delle disposizioni alcune delle quali non si applicano più. Viene così introdotto un nuovo regime normativo, incentrato sugli aspetti informativi,

[371] A detta finalità, unitamente a quella diretta ad alleggerire l'onere burocratico a carico del prestatore, risponde anche il disposto dell'art. 60, par. 9, che previene forme di duplicazione nelle informazioni trasmesse all'Autorità, qualora quelle precedentemente inviate siano rimaste invariate.

relativamente omogeneo per tutti i prestatori di diritto europeo[372] e flessibile, poiché si adatta ai servizi specifici che intendono offrire[373].

Anche il lasso di tempo entro il quale i prestatori devono informare l'autorità competente della loro intenzione di offrire servizi per le cripto-attività è uniforme, e viene fissato in almeno 40 giorni lavorativi prima dell'inizio dell'attività. Questo processo è accelerato per i soggetti già attivi nel mercato e sotto vigilanza, poiché le autorità possono utilizzare le informazioni già in loro possesso, purché aggiornate e conformi ai requisiti di notifica, come specificato nell'articolo 60, paragrafo 9 del regolamento.

L'agevolazione concessa ai prestatori e la prevenzione di duplicazioni superflue e oneri burocratici eccessivi, costituiscono aspetti salienti di questa disposizione.

La semplificazione del processo di riconoscimento del regime di esenzione e del passaporto già in possesso avviene attraverso una notifica informativa, sottoposta a valutazione nei tempi stabiliti dalla normativa. Tale valutazione costituisce una verifica oggettiva delle informazioni richieste e della completezza della documentazione richiesta[374]. Ciò suggerisce un procedimento snello, che, in caso di riscontro positivo, conduce direttamente alla comunicazione all'ESMA per l'annotazione nel registro di cui all'art.109.

Tuttavia, nonostante quanto previsto dalla normativa, a seconda della natura del prestatore, l'autorità competente non potrà esimersi dal condurre una valutazione riguardante u sana e prudente gestione. Questa valutazione deve essere considerata alla luce dell'intera attività svolta sul mercato (*core* e *non core*) dal prestatore di servizi per le cripto-attività.

Tra le categorie soggettive che potrebbero assumere un ruolo chiave nello sviluppo dei mercati delle cripto-attività, e che al contempo potrebbero essere più

[372] Le informazioni da notificare all'autorità competente sono elencate nel par. 7 e soggette alla valutazione dell'autorità medesima.

[373] Il pacchetto informativo include dettagli sui requisiti organizzativi da implementare. Tuttavia, non si trovano riferimenti a politiche specifiche per la separazione dei servizi per le cripto-attività da quelli di investimento o da altri servizi finanziari. Nonostante questo, informazioni su come gestire la separazione tra questi diversi tipi di servizi, che potrebbero rientrare in parte nelle politiche per la gestione dei conflitti di interesse, sarebbero state utili. Questo avrebbe aiutato a chiarire i percorsi normativi e sulla relativa *compliance*.

[374] Si legga la formulazione dell'art. 60, par. 12: "Le autorità competenti comunicano all'ESMA le informazioni specificate all'articolo 109, paragrafo 5, dopo aver verificato la completezza delle informazioni ricevute in conformità del paragrafo 7. L'ESMA rende disponibili tali informazioni nel registro di cui all'articolo 109 entro la data di inizio della prestazione prevista dei servizi per le cripto-attività."

significativamente influenzate dall'entrata in vigore di MICA, rientrano i prestatori di natura bancaria.

Questi attori saranno protagonisti del nuovo regime normativo, distinguendosi tuttavia in modo peculiare dagli altri prestatori di diritto europeo, sia per la loro ampia capacità operativa in ogni settore dell'ecosistema finanziario, sia per la possibilità di agire, nel contesto MICA, sia nell'emissione che nella distribuzione delle cripto-attività.

Questo ruolo distintivo emerge anche dall'articolazione del regime di esenzione dall'autorizzazione, che per le banche assume una configurazione propria, derivante direttamente dalla fonte normativa di abilitazione (direttiva 2013/36/UE).

A differenza di altri settori, come le imprese di investimento, il regime in questione non si basa su presunzioni di equivalenza dei servizi[375], focalizzandosi piuttosto sui servizi che la banca intenderà offrire sul mercato[376].

Di conseguenza, tali presunzioni non costituiscono una giustificazione preliminare per il regime di esenzione, come nel caso delle imprese di investimento, ma intervengono successivamente per "supportare" l'operatività bancaria, attraverso la prestazione di servizi per le cripto-attività considerati equivalenti a quelli disciplinati dalla Mifid.

Pertanto, il ruolo primario che le banche potranno svolgere lungo l'intera filiera della cripto-attività, dall'emissione alla distribuzione sul mercato, comporterà un aumento delle complessità dei rischi che il consiglio di amministrazione dovrà valutare e affrontare, soprattutto nel contesto della prevenzione e gestione di conflitti di interesse di varia natura, amplificati rispetto a quelli già presenti nel sistema tradizionale.

In definitiva, nonostante le banche abbiano mostrato un crescente interesse nel settore cripto, spinte dalla domanda crescente della clientela, l'accesso al mercato si

[375] L'art. 60, par. 1, dispone: "Un ente creditizio può prestare servizi per le cripto-attività se comunica le informazioni di cui al paragrafo 7 all'autorità competente del suo Stato membro d'origine, almeno 40 giorni lavorativi prima di prestare tali servizi per la prima volta". Il presente disposto, a differenza dei successivi paragrafi, ognuno dedicato ad una categoria di *incumbent*, non riporta alcuna fonte normativa di riferimento, rinviandola implicitamente alla definizione di ente creditizio di cui all'art. 3, n. 28), quale "definito all'articolo 4, paragrafo 1, punto 1, del regolamento (UE) n. 575/2013 e autorizzato a norma della direttiva 2013/36/UE".

[376] L'art. 146 reca contemporanea modifica della direttiva 2013/36/UE tramite integrazione delle attività e dei servizi elencati dall'allegato I con i seguenti: "15. Emissione di moneta elettronica, compresi i *token* di moneta elettronica ai sensi dell'articolo 3, paragrafo punto 7...,16. Emissione di *token* collegati ad attività quale definita all'articolo 3, paragrafo 1, punto 6, 17. Servizi per le cripto-attività come definiti all'articolo 3, paragrafo 1, punto 16, …".

presenta come una sfida considerevole. Ciò è particolarmente evidente alla luce dei costi elevati necessari per entrare nel panorama dei prestatori di servizi per le cripto-attività, in concorrenza con i pionieri del settore, e per l'adeguamento o l'implementazione delle infrastrutture necessarie.

Le sfide principali per i prestatori provenienti dal settore bancario includono gli investimenti in tecnologie e competenze specifiche, la sostenibilità dei costi e le implicazioni legate all'esternalizzazione di alcune funzioni a terze parti o accordi di *partnership* con società esterne. Tali sfide richiedono una revisione dei modelli di *business*, della strategia bancaria, della *corporate governance* e della struttura organizzativa. Inoltre, è necessario rafforzare le funzioni di *audit*, *risk management* e, soprattutto, di *compliance*.

Il processo di riorganizzazione, sia interno che esterno, dovrà affrontare le nuove sfide legate al mondo *crypto*, compresa come si è detto la gestione dei conflitti di interesse, distinta rigorosamente anche a causa della separazione dei percorsi MICA e MiFID 2. Tuttavia, il parametro fondamentale da considerare è la sana e prudente gestione, che deve guidare sia i prestatori che le autorità di vigilanza[377].

La Banca Centrale Europea, nel contesto della trasformazione digitale delle banche, sta già seguendo da vicino gli sviluppi operativi e normativi sulle cripto-attività[378] e ha già annunciato l'assunzione di diverse iniziative che vanno oltre il trattamento prudenziale, concentrandosi sulla *governance* delle banche[379] e sull'armonizzazione delle licenze per le banche cripto[380]. Ciò prefigura uno statuto

[377] La centralità del principio della sana e prudente e gestione ai fini della vigilanza prudenziale è tale da condizionare l'apparato organizzativo e l'attività del prestatore in tutti gli ambiti operativi dei servizi per i quali risulti abilitato, sino ad includere aspetti traversali, quali quelli relativi alla sostenibilità, di crescente attenzione nella supervisione delle banche. Per "sana e prudente gestione sostenibile" Si veda R. LENER, P. LUCANTONI, «*sostenibilità esg e attività bancaria*», Banca, borsa, tit. cred., I (gennaio 2023).

[378] EUROPEAN CENTRAL BANK, «*Banks' Digital Transformation: Where Do We Stand?* », 15 febbraio 2023, https://www.bankingsupervision.europa.eu/press/publications/newsletter/2023/html/ssm.nl230215_2.en.html.

[379] EUROPEAN CENTRAL BANK, «*Crypto-Assets: A New Standard for Banks*», 15 febbraio 2023, https://www.bankingsupervision.europa.eu/press/publications/newsletter/2023/html/ssm.nl230215_1.en.html.

[380] Pertanto, particolare attenzione sarà dedicata, oltre ai requisiti patrimoniali, a: 1) *business models: how the proposed activity matches the overall activity and risk profile of the institution; 2) internal governance: whether the institution's policies and procedures are adequate to identify and assess risks unique to crypto-assets; 3) fit and proper assessments: here the same general fit and proper criteria apply as in any licensing procedure, including IT competence.The higher the complexity or relevance of the crypto business, the higher the level of knowledge and experience in the field of crypto should be. Senior managers or board members with relevant IT knowledge and chief risk officers with robust experience in this area are im-portant safeguards*. Infine, sorvegliati speciali saranno altresì i rischi operativi ed informatici, parimenti a frodi, antiriciclaggio e antiterrorismo: "*crypto-assets put the spotlight on certain types of risk, starting with operational and cyber risks, and the ECB is also working*

normativo speciale, attualmente in fase di definizione legislativa nell'ambito del pacchetto Basilea III[381], che integrerà il *framework* di MICA, con paritolare attenzione ai requisiti patrimoniali specifici che le banche dovranno adottare, attualmente in fase di definizione da parte del Comitato di Basilea[382].

## 1.6 I prestatori di diritto nazionale

Un'altra categoria soggettiva che gode di un regime di esenzione, temporaneo in questo caso, riguarda i "prestatori di diritto nazionale", i cui poteri operativi sono circoscritti al mercato nazionale, in conformità con le leggi adottate a livello nazionale.

Questa categoria, che è attualmente in attesa della futura regolamentazione post-MICA, rappresenta la tipologia soggettiva più complessa, poiché manca di elementi normativi di identificazione immediata ed univoca, richiedendo quindi un'analisi caso per caso.

Inizialmente, la configurazione di questa categoria può essere interpretata alla luce dell'art. 143, che contiene misure transitorie giustificando, seppure temporaneamente, la coesistenza dei regimi nazionali con quello europeo (ossia MICA), suscitando però osservazioni critiche sulla mancanza di chiarezza nel trattamento normativo riservato a tali soggetti e sui potenziali vantaggi competitivi non giustificati.

La revisione di questo articolo, presenta un nuovo panorama soggettivo configurato in modi differenti e abilitato dal diritto nazionale, rischiando di sovrapporsi a quello europeo, con possibili effetti svantaggiosi per i prestatori di diritto

---

*to assess these. They include, for instance, cryptographic key theft or compromise of login credentials, as well as risks linked to the use of special technology and outsourcing arrangements to third-party providers. Likewise, as crypto-assets are considered prone to risks associated with anti-money laundering/combating the financing of terrorism (AMI/CFT), internal governance arrangements and processes need to take account of the crypto-asset AMI/CFT risk profile of the institution. Here the ECB relies on input from national anti-money laundering authorities and Financial Intelligence Units".*
EUROPEAN CENTRAL BANK, «*Licensing of Crypto-Asset Activities*», 17 agosto 2022, https://www.bankingsupervision.europa.eu/press/publications/newsletter/2022/html/ssm.nl220817_2.en.html.

[381] Cfr. Proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) n. 575/2013 per quanto concerne i requisiti per il rischio di credito, il rischio di aggiustamento della valutazione del credito, il rischio operativo, il rischio di mercato e *l'output floor* [COM(2021) 664 final del 27 ottobre 2021], rivista alla luce degli emendamenti apportati dal Parlamento europeo (su cui si veda da ultimo la relazione del 9 febbraio 2023) che ha introdotto in materia l'art. 451 ter, recante "Informativa sulle esposizioni verso cripto-attività e sulle attività correlate" e l'art. 461 ter sul "Trattamento prudenziale delle cripto-attività".

[382] Il Comitato di Basilea ha tracciato i contorni del trattamento prudenziale delle esposizioni su cripto-attività. Si veda: BIS «*Prudential treatment of cryptoasset exposures*», https://www.bis.org/bcbs/publ/d545.pdf.

europeo e per la competizione tra attori di diversa natura nel mercato delle cripto-attività.

Questa situazione presenta sfumature normative a discrezione degli Stati membri, graduando l'accesso al mercato in base alla priorità temporale dei prestatori. Questo potrebbe favorire la capitalizzazione e il consolidamento sui mercati nazionali, fungendo da trampolino di lancio verso quelli europei, a discapito dei soggetti che accedono al mercato europeo solo in un secondo momento, sperimentando un ritardo competitivo.

Nella categoria dei "beneficiari" di questo specifico regime di esenzione, potrebbero rientrare i "*first movers*", cioè i pionieri del settore e le rispettive giurisdizioni nazionali, che si sono mossi tempestivamente aprendo un mercato destinato a conservare e incrementare il suo potenziale di sviluppo e crescita, con inevitabili implicazioni nella competizione tra soggetti e nei rispettivi ordinamenti nazionali.

Il meccanismo di riconoscimento e conseguente "sanatoria", pressoché automatizzato in mancanza di ulteriori previsioni regolamentari, per i soggetti inclusi in questa tipologia potrebbe però generare effetti indesiderati, violando le regole per una sana concorrenza tra gli attori, che dovrebbero invece competere su un piano di parità con regole omogenee e armonizzate. Potrebbe cioè crearsi, contrariamente alle intenzioni del legislatore, un *unlevel playing field*.

Tali potenziali conseguenze indesiderate hanno sollevato diverse preoccupazioni, con riferimento a quelle che potrebbero essere considerate "clausole di salvaguardia".

Introdotte dai paragrafi 1 e 2 dell'articolo 143, queste clausole utilizzano come parametro temporale la data di applicazione del regolamento, per escludere dal campo di applicazione degli articoli da 4 a 15 di MICA le offerte pubbliche concluse in date antecedenti. Allo stesso tempo, queste clausole tendono a graduare il regime applicabile alle cripto-attività diverse dagli *e-money tokens* e dagli *asset-referenced tokens*, autorizzate alla negoziazione su piattaforme di *trading* di cripto-attività.

In queste circostanze, l'introduzione di un "porto franco" temporale riguarda la non applicabilità di alcune disposizioni di MICA alle cripto-attività residue, ovvero a quelle che non rientrano nella tassonomia specifica, ma che, per le loro caratteristiche, non sono escluse dal perimetro di MICA, basandosi più sui considerando iniziali che sulle disposizioni normative.

Tali cripto-attività non sono sempre facilmente identificabili e classificabili, ma possono essere incluse nell'ambito di applicazione del regolamento grazie all'approccio "*catch all*" che caratterizza MICA[383]. A causa della mancanza di indicazioni ulteriori e, soprattutto, dell'assenza di un significato univoco attribuibile al *genus* delle cripto-attività, l'ambito considerato potrebbe essere vasto e di conseguenza, influire così sulla prestazione di servizi connessi, come la negoziazione di cripto-attività, e sui prestatori autorizzati.

La cristallizzazione temporale della fine del regime di esenzione dall'applicazione del regime ordinario, coincidendo con l'entrata in vigore di MICA (cioè 18 mesi dalla data di entrata in vigore del regolamento), potrebbe incentivare comportamenti opportunistici. Potrebbe uscire così rafforzato il vantaggio competitivo e il conseguente consolidamento della posizione di mercato per i soggetti già operativi prima della data di prima applicazione del regolamento che potrebbero sfruttare le potenzialità del regime più favorevole[384].

I dubbi sono ulteriormente amplificati dalle disposizioni dell'articolo 143, che nei paragrafi 3 e 6 stabilisce un regime di esenzione temporanea per i prestatori di servizi per le cripto-attività, derogando alle norme di MICA, ma con un'estensione temporale e perimetrale più ampia rispetto ai paragrafi 1 e 2.

Il panorama normativo precedente a MICA, basato su iniziative diverse adottate da alcuni Stati membri, presenta quindi sfide interpretative ed operative, specie nel contesto di un mercato unico armonizzato e basato sulla sana concorrenza tra tutti i partecipanti, dando l'impressione di creare, a livello europeo, un mosaico operativo con regimi differenziati in termini di tempistiche.

In merito alle misure transitorie stabilite dall'articolo 143, paragrafo 3, in deroga a MICA e alle disposizioni per le altre categorie di prestatori, offre anche un meccanismo di prolungamento operativo per coloro che erano già attivi sul mercato domestico al momento dell'applicazione del regolamento, consentendo loro di

[383] Si veda il considerando 16: "Qualsiasi atto legislativo adottato nel settore delle cripto-attività dovrebbe essere specifico e pronto alle sfide del futuro, in grado di stare al passo con l'innovazione e gli sviluppi tecnologici e fondato su un approccio basato su incentivi. I termini "cripto-attività" e "tecnologia a registro distribuito" dovrebbero pertanto essere definiti nel modo più ampio possibile, in modo tale da comprendere tutti 1 tipi di cripto-attività che attualmente non rientrano nell'ambito di applicazione degli atti legislativi dell'Unione in materia di servizi finanziari".

[384] Circostanza di cui il legislatore sembra essere pienamente consapevole, come del resto confermato dall'ultima parte del considerando 4, ove si legge: "Per far fronte a questi rischi, alcuni Stati membri hanno introdotto norme specifiche per tutte le cripto-attività che non rientrano nell'ambito di applicazione degli atti legislativi dell'Unione in materia di servizi finanziari o per un sottoinsieme di esse e altri Stati membri stanno valutando l'opportunità di legiferare nel settore delle cripto-attività".

continuare ad erogare i servizi, sulla base della legislazione nazionale, per un ulteriore periodo esteso fino a 18 mesi; il termine indicato sembrerebbe finalizzato a permettere al prestatore di adeguarsi ai requisiti di MICA.

In alternativa, tale periodo temporale di riferimento potrebbe essere ridotto in analogia con quello più breve stabilito per ottenere l'autorizzazione ai sensi dell'articolo 63 di MICA, cercando così di riequilibrare le posizioni di ingresso sul mercato europeo di questi prestatori e di tutti gli altri.

Sebbene le possibili ipotesi siano numerose, tutte sono vincolate alla discrezionalità degli Stati membri, i quali hanno l'incarico di decidere se e come applicare le misure transitorie e soprattutto che tipo di soluzione offrire ai prestatori attivi nella loro giurisdizione.

Questa scelta, mancando però di indicatori precisi e univoci, potrebbe variare dalla decisione estrema di non applicare le misure transitorie di cui all'articolo 143, paragrafo 3, fino a quella più flessibile di ridimensionarne i parametri temporali.

Qualunque sia la decisione finale la medesima dovrà essere notificata alla Commissione europea e all'ESMA.

In ogni caso, la decisione finale degli Stati membri avrà un impatto discriminante sulla destinazione dei prestatori di diritto nazionale. Questa destinazione sarà soggetta a una valutazione comparativa preliminare tra i requisiti della legislazione nazionale, in termini di struttura di *governance* e adeguatezza patrimoniale, rispetto a quelli richiesti agli altri prestatori.

Questo regime potrebbe sollevare interrogativi riguardo al coordinamento tra la classificazione delle cripto-attività effettuata da MICA e quelle contemplate nell'ambito del diritto nazionale, adottato come criterio di riferimento per il regime di esenzione normativa. Questa problematica risulta particolarmente accentuata in quanto le legislazioni nazionali, come già evidenziato, considerano diversi parametri all'interno del *genus* delle cripto-attività, talvolta più o meno estese rispetto al perimetro oggettivo delineato da MICA e con una corrispondenza variabile con le *species* incluse nella tassonomia definita dal regolamento europeo.

Emergono pertanto diversi dubbi riguardo a un sistema sovrapponibile a quello ordinario, considerando che l'assenza di chiarezza riguardo a regole uniformi cui gli Stati membri dovrebbero attenersi aumenta il rischio di compromettere la parità di trattamento tra i prestatori a scapito della protezione dei consumatori, che potrebbero essere esposti a rischi qualora si creassero zone grigie e situazioni poco trasparenti

Nell'ambito delle disposizioni transitorie fornite agli Stati membri, l'articolo 143, paragrafo 6, presenta una valida alternativa rispetto a quanto delineato nel paragrafo 3. In questo caso, l'esenzione è specificamente limitata agli articoli 62 e 63 di MICA, che riguardano la procedura di autorizzazione per i prestatori ordinari. Questa deroga favorisce coloro che presentano richiesta di autorizzazione durante il periodo compreso tra l'inizio dell'applicazione di MICA[385] e i successivi 18 mesi[386]. L'agevolazione è concessa a coloro che risultano autorizzati a prestare servizi per le cripto-attività in base a una normativa nazionale in quel periodo.

In altre parole, il regime transitorio si basa essenzialmente su due pilastri, da un lato una esenzione temporale e dall'altro di una procedura semplificata.

L'autorizzazione può essere richiesta da persone giuridiche oppure altre imprese, come anche stabilito dalla MiFID.

L'istanza di autorizzazione va inviata all'autorità competente e deve essere corredata da un corposo numero di adempimenti, poiché essenzialmente MiCA richiede che venga allegata documentazione che sia suscettibile di provare l'idoneità del prestatore oltre agli obblighi contenuti nello statuto legale, nei confronti della clientela, requisiti prudenziali, requisiti di governance e di onorabilità. L'agevolazione è contenuta nell'art 62 paragrafo 4 del Regolamento e riguarda gli intermediari che hanno già fornito informazioni in quanto già autorizzati ad esempio da Mifid o dalla PSD, che possono essere quindi esonerati dal fornire nuovamente le medesime informazioni.

Questa norma richiede determinati temperamenti; il primo problema si ravvede nel dialogo tra autorità poiché non è certo che l'autorità competente ai fini MiCAR sia la stessa competente per gli altri servizi. Il secondo chiarimento è che qui siamo nell'ambito del procedimento dell'autorizzazione ordinaria e molti dei soggetti in questione possono godere del regime agevolato della comunicazione preventiva. Quindi nulla esclude che i soggetti autorizzati su base della mera comunicazione, possano, se ne hanno i requisiti, chiedere sulla scorta del meccanismo di comunicazione ordinario di essere autorizzati allo svolgimento anche di altri servizi.

Preme sottolineare che nell'ambito della disciplina finanziaria, l'adeguata considerazione degli interessi della clientela dovrebbe essere deputata ai rapporti giusprivatistici; nel presente regolamento invece, essa fa parte del processo

[385] 30 dicembre 2024.
[386] Data ultima: 1° luglio 2026.

amministrativo e diventa possibile titolo di diniego dell'autorizzazione, evidenziando quindi l'importanza centrale della clientela nell'ambito del regolamento.

Per quanto riguarda il regime agevolato, ci sono taluni soggetti già autorizzati sulla scorta di altri plessi normativi (banche, istituti di moneta elettronica e altri soggetti finanziari) che possono prestare in tutto o in parte servizi di cripto-attività sulla scorta non di una autorizzazione ma di una comunicazione preventiva.

Questi soggetti, devono comunicare determinate informazioni alle autorità competenti almeno 40 giorni prima dell'avvio del servizio stesso.

In realtà all'interno di questo regime agevolato vi sono almeno 3 ulteriori modelli di *business* che possono essere analizzati in ordine decrescente.

Quello più ampio riguarda le banche, esse per il solo fatto di avere la licenza bancaria sono autorizzate a svolgere tutti i servizi per le cripto-attività; in questo caso il regolamento non si pone nessun problema di equivalenza dei servizi, poiché è intervenuto direttamente con una modifica/integrazione dell'allegato 1 della CRD IV con un richiamo espresso a tutti i servizi per le cripto-attività.

Il modello intermedio, si basa sulle equivalenze tra servizi (è il caso delle imprese di investimento e di gestione di fondi); questi soggetti saranno autorizzati a svolgere non già tutti i servizi ma solamente quelli che il regolamento stesso considera equivalenti a quelli per cui erano già autorizzati.

Infine, il modello più restrittivo tramite il quale è possibile prestare soltanto uno o più specifici servizi.

Vi è quindi, un'uniformità a monte tre modelli e uniformità a valle; in quanto il regime agevolato si risolve non soltanto in una agevolazione all'accesso nel mercato ma anche in esenzioni, come l'esenzione per il procedimento di autorizzazione, oppure per il rispetto dei requisiti prudenziali e per partecipazioni qualificate.

Da queste disposizioni è possibile ricavare la *ratio* del regime agevolato e cioè la concessione dell'autorizzazione sulla scorta della presunzione del possesso di adeguati presidi, in ragione dell'identità soggettiva già regolamentata da altri plessi normativi.

Ovviamente il regime agevolato nonostante l'assenza di un titolo abilitativo si caratterizzerà anche per una differente disciplina della revoca; MiCAR prevede infatti una revoca del diritto a prestare servizio in conseguenza dalla revoca dell'autorizzazione a monte.

Il punto di incertezza è se alla comunicazione preventiva debba seguire l'avvio di un procedimento amministrativo; infatti, leggendo MiCAR parrebbe che l'autorità competente debba limitarsi a ricevere le informazioni, verificarne la completezza e poi inviare la comunicazione all'ESMA affinché il prestatore sia censito nel registro.

Ma il regime transitorio non serve soltanto a gestire il passaggio dal vecchio regime al nuovo, ma è suscettibile di creare un nuovo modello di accesso. Uno dei rischi è che ad esempio un prestatore sovranazionale che non ha interesse ad ottenere il passaporto europeo, potrebbe continuare a usufruire del regime favorevole nazionale fino al primo luglio 2026.

Per questo motivo il legislatore per un verso permette agli stati membri di non applicare questo regime oppure di limitarlo temporalmente, ed in secondo luogo di applicare a costoro una procedura semplificata di autorizzazione per attribuirgli comunque il passaporto europeo. Gli Stati membri hanno quindi ampia discrezionalità nella scelta di adottare una procedura semplificata, sia nella definizione delle situazioni in cui applicarla che nei requisiti per l'ammissione. Questa discrezionalità può portare a decisioni nazionali contrastanti, con conseguenze diverse per i prestatori di diritto nazionale, che potrebbero accedere più o meno rapidamente al mercato europeo tramite una procedura semplificata o sulla base di criteri di arbitraggio regolamentare. La disposizione manca di trasparenza e rischia di diventare discriminatoria. La mancanza di linee guida chiare per l'attuazione di un'autorizzazione semplificata potrebbe creare disparità nelle regole, favorendo posizioni di vantaggio e comportamenti di concorrenza sleale

Un ulteriore rischio deriva dalla natura stessa dei soggetti che potrebbero usufruire del regime agevolato; come è stato detto, questi ricomprendono anche grandi *player* del mercato tradizionale come le banche, le quali potrebbero avere verosimilmente un grande peso nel mercato delle cripto-attività. Il rischio, pertanto è che il regime agevolato diventi sostanzialmente quello ordinario mentre quello ordinario dell'autorizzazione *ad hoc* diventi l'eccezione[387].

[387] Vedi nota n.286.

## 1.7 I prestatori significativi di servizi per le cripto-attività e i prestatori extra-europei

La categoria dei prestatori significativi di servizi per le cripto-attività costituisce una *species* ulteriore rispetto a quelle precedentemente classificate.

Questa categoria definita dall'articolo 85, presenta caratteristiche peculiari e distintive, laddove l'aggettivo "significativo" si riferisce non al soggetto autorizzato a erogare servizi per le cripto-attività, ma piuttosto alla quota di mercato acquisita e alla rilevanza dimensionale raggiunta attraverso un'operatività diffusa in Europa, dimensione fissa di almeno "15 milioni di utenti attivi, in media, in un anno civile"[388].

Questa categoria ha natura trasversale, assumendo la natura di una sottospecie identificabile successivamente all'accesso al mercato e al periodo iniziale di attività, ma anticipando la possibile distinzione tra prestatori "*significant*" e "*less significant*". Sul punto, a nuova disposizione normativa deriva dalle recenti modifiche nel processo legislativo ed giustificato dalle preoccupazioni sull'impatto in termini di stabilità finanziaria da parte di prestatori che hanno raggiunto un livello di capitalizzazione e una capacità operativa tale da richiedere una sorveglianza più attenta e rigorosa, con conseguente spostamento della vigilanza dall'autorità nazionale competente a quella europea[389].

L'aumentata attenzione sulla supervisione dei prestatori significativi ha origine anche nella necessità di bilanciare gli squilibri generati dai poteri di vigilanza ordinari, ritenuti inadeguati alla dimensione operativa assunta dai suddetti operatori sul mercato. La volatilità delle cripto-attività e i rischi associati alla loro circolazione possono essere amplificati quando la prestazione di servizi è ampiamente presente a livello europeo.

Nonostante l'obiettivo del regolamento MICA di superare la frammentazione del mercato e promuovere le attività transfrontaliere in un contesto armonizzato, alcuni prestatori potrebbero raggiungere livelli di significatività che richiedono un'attenzione aggiuntiva per possibili impatti sulla stabilità del sistema finanziario, derivanti dal consolidamento di una posizione significativa sul mercato.

In particolare, le *Big Tech* sembrano essere tra i prestatori con maggiori probabilità di rientrare in questo perimetro, data la loro vasta dimensione operativa

[388] La media viene calcolata ex art. 85, par. 1, "come media del numero giornaliero di utenti attivi nel corso dell'intero anno civile precedente".
[389] Vedi *infra*.

territoriale e la capacità pregressa anche in settori non finanziari, suscettibile di attirare utenti e generare implicazioni e dinamiche di rilevanti per le autorità europee[390].

Analogamente, vi rientreranno le banche significative, che però sono sottoposte, come è noto, al Meccanismo di Vigilanza Unico. Pertanto, qualora una fattispecie concreta coinvolga nella valutazione di significatività una banca già considerata a monte come *significant*, la BCE[391], pur se non esplicitamente menzionata nella normativa, dovrà essere consultata e avrà il suo ruolo decisionale.

Tale intervento sarà per l'appunto necessario nel caso in cui i modelli di *business* scelti per i servizi legati alle cripto-attività e il carattere significativo del prestatore possano mettere a rischio la sana e prudente gestione della banca nell'esercizio del *core business*.

Tuttavia, data la natura trasversale della sottocategoria in questione, tutti i prestatori potrebbero essere interessati, indipendentemente dal settore di provenienza.

Questi saranno tenuti a notificare alle rispettive autorità competenti il superamento della soglia media entro due mesi dal suo superamento.

Successivamente, spetterà alle autorità competenti comunicare l'informazione all'ESMA, e fornire annualmente aggiornamenti al consiglio delle autorità di vigilanza dell'ESMA riguardo agli sviluppi della vigilanza sui prestatori significativi dei servizi legati alle cripto-attività[392].

Il conferimento di poteri specifici all'ESMA, in opposizione alla supervisione diretta assegnata all'EBA per gli emittenti di cripto-attività significative, richiederà

---

[390] Vedi diffusamente *supra.*

[391] La principale preoccupazione della BCE è quella di evitare che si creino percorsi paralleli di regole sui sistemi di pagamento, come si evince dal considerando 15 ["A norma dell'articolo 127, paragrafo 2, quarto trattino, del trattato sul funzionamento dell'Unione europea (TFUE), uno dei compiti fondamentali da assolvere tramite il Sistema europeo di banche centrali (SEBC) è promuovere il regolare funzionamento dei sistemi di pagamento. Ai sensi dell'articolo 22 del protocollo n. 4 dello statuto del Sistema europeo di banche centrali e della Banca centrale europea allegato ai trattati, la Banca centrale europea (BCE) può stabilire regolamenti, al fine di assicurare sistemi di compensazione e di pagamento efficienti e affidabili all'interno dell'Unione e nei rapporti con i paesi terzi. A tal fine, la BCE ha adottato regolamenti riguardanti i requisiti per i sistemi di pagamento di importanza sistemica. Il presente regolamento fa salva la responsabilità della BCE e delle banche centrali nazionali del SEBC di assicurare sistemi di compensazione e di pagamento efficienti e solidi all'interno dell'Unione e nei rapporti con i paesi terzi. Di conseguenza, e per evitare che possano essere create normative parallele, l'ABE, l'ESMA e la BCE dovrebbero collaborare strettamente nell'elaborazione dei pertinenti progetti di norme tecniche in conformità del presente regolamento. Inoltre, è fondamentale che la BCE e le banche centrali nazionali abbiano accesso alle informazioni nello svolgimento dei loro compiti relativi alla sorveglianza dei sistemi di pagamento, compresa la compensazione dei pagamenti"], nonché dai poteri riconosciutele dalle disposizioni in tema di emissione di cripto-attività specie quando siano significative da parte delle banche.

[392] Gli aggiornamenti, forniti anche con frequenza periodica, riguardano:
"*a)* le autorizzazioni, in corso o concluse, di cui all'articolo 59; *b)* le procedure, in corso o concluse, di revoca delle autorizzazioni di cui all'articolo 64; c) l'esercizio dei poteri di vigilanza stabiliti all'articolo 94, paragrafo 1, primo comma, lettere *b)*, *c), e), f), g), y)* e *aa)*" (art. 85, par. 3).

una modifica dei regolamenti istitutivi delle due suddette Autorità europee[393]. Si noti che la ripartizione delle competenze a livello europeo, se da un lato promuove la stabilità del sistema finanziario, dall'altro involge finalità macroeconomiche.

Un tema particolarmente dibattuto all'indomani del fallimento FTX concerne l'eventualità del verificarsi di conseguenze simili a quelle registrate nel caso indicato, qualora MICA fosse già entrato in vigore con le disposizioni a protezione del consumatore.

La preoccupazione riguardo alla possibile ripetizione di situazioni del genere riguarda soprattutto la prestazione di servizi su iniziativa esclusiva del cliente, di cui all'articolo 61 del Regolamento.

Nel caso *de quo*, la provenienza dell'iniziativa assume un'importanza particolare, quando il cliente è "stabilito o residente" nell'Unione europea e il fornitore di servizi per le cripto-attività ha sede in un paese terzo non soggetto alle disposizioni di MICA.

La "distanza" territoriale tra le parti coinvolte è affrontata attraverso tre distinzioni delineate nel paragrafo 1, che riguardano una sollecitazione "attiva" da parte del cliente e una sollecitazione "passiva" (o inversa), attivata dal fornitore.

Nel tentativo di privilegiare la libertà decisionale del cliente[394] a sua iniziativa esclusiva, il legislatore propone una deroga per le imprese dei paesi terzi, evitando loro l'obbligo di richiedere l'autorizzazione, a differenza di quanto imposto agli altri fornitori europei.

Tale previsione sembra delineare un ulteriore regime temporaneo ed occasionale, applicabile a una specifica prestazione di servizio e al correlato rapporto contrattuale.

---

[393] "Dato che l'ABE dovrebbe essere incaricata della vigilanza diretta degli emittenti di *token* collegati ad attività significativi e di *token* di moneta elettronica significativi e che l'ESMA dovrebbe essere incaricata di avvalersi dei propri poteri in relazione ai prestatori di servizi per le cripto-attività significativi, e necessario garantire che l'ABE e l'ESMA siano in grado di esercitare tutti i loro poteri e compiti al fine di conseguire i loro obiettivi di tutela dell'interesse pubblico contribuendo alla stabilità e all'efficacia a breve, medio e lungo termine del sistema finanziario, per l'economia dell'Unione, i suoi cittadini e le sue imprese, e garantire che gli emittenti di cripto-attività e i prestator di servizi per le cripto-attività siano disciplinati dai regolamenti (UE) n. 1093/2010 e (UE) n.1095/2010. È pertanto opportuno modificare di conseguenza tali regolamenti". (Considerando 116).

[394] Cfr. considerando 75: Il presente regolamento non dovrebbe pregiudicare la possibilità per le persone stabilite nell'Unione di usufruire di propria iniziativa di servizi per le cripto-attività prestati da un'impresa di un paese terzo. Se un'impresa di un paese terzo presta servizi per le cripto-attività a un soggetto stabilito nell'Unione su iniziativa di quest'ultimo, tali servizi non dovrebbero essere considerati come prestati nell'Unione. Se un'impresa di un paese terzo cerca di procurarsi clienti o potenziali clienti nell'Unione o promuove o pubblicizza nell'Unione attività o servizi per le cripto-attività, i suoi servizi non dovrebbero essere considerati come prestati su iniziativa del cliente. In tal caso, l'impresa del paese terzo dovrebbe essere autorizzata come fornitore di servizi per le cripto-attività.

Questa esenzione assume un carattere occasionale, poiché un ricorso (seppur temporaneo) sistematico lascerebbe intendere diversamente le intenzioni del fornitore extra-europeo.

La problematica principale in questo contesto è la mancanza di elementi concreti per identificare le circostanze in cui si possa dimostrare che l'iniziativa è stata attivata esclusivamente dal cliente, un elemento chiave per il riconoscimento implicito di un permesso per l'operatività occasionale dell'impresa del paese terzo. Nonostante l'esistenza di clausole contrattuali e *disclaimer* con limitazioni di responsabilità, tali elementi non risultano rilevanti ai fini indicati.

La natura eccezionale di queste ipotesi, emerge dall'uso dell'aggettivo "esclusiva", il quale deve caratterizzare e rafforzare l'iniziativa del cliente, costituendo un *unicum* nel panorama normativo europeo attualmente vigente[395].

In modo analogo, il disposto del paragrafo 2 offre un'opportunità all'impresa del paese terzo di fornire il servizio richiesto direttamente dal cliente senza dover rispettare le regole ordinarie applicabili, ma allo stesso tempo vieta di promuovere attivamente al cliente la commercializzazione di nuove cripto-attività o ulteriori servizi "non richiesti".

In altre parole, l'iniziativa "esclusiva" del cliente non deve diventare un veicolo per l'impresa esterna al quadro normativo MICA per sfruttare o abusare di tale esenzione, con conseguenze negative per i consumatori e per altri prestatori in conformità con il *framework* europeo.

[395] "Tanto la normativa consumeristica (es. direttiva 2002/65/CE sulla commercializzazione a distanza dei servizi finanziari ai consumatori), quanto a cascata quella in materia finanziaria prevedono l'ipotesi di prestazione di un servizio finanziario su iniziativa (*rectius*: richiesta) del cliente, anteriormente alla lettura delle informazioni e delle condizioni preliminari attinenti al servizio o all'oggetto del servizio, da fornirsi però una volta concluso il contratto, anche ai fini della decorrenza del termine per l'eventuale esercizio del diritto di recesso. Con la precisazione che il caso ora raffigurato non esenta dalla copertura di disposizioni di tutela che vengono solo posposte a seguito della richiesta del cliente. Diversamente, nell'ipotesi configurata nel testo dell'art. 61, la specifica iniziativa del cliente esonera il prestatore dall'applicazione delle cautele a protezione del consumatore sia nel momento in cui presta il servizio, sia successivamente. Né di tanto il prestatore, proprio perché posto fuori dal perimetro di MICA, sarà tenuto ad informare il cliente che sopporterà (in)consapevolmente il rischio di qualunque pregiudizio subito a causa del comportamento della controparte contrattuale. Qualunque tipo di tutela per il cliente rimarrà alla mercé del prestatore e dell'autonomia contrattuale". In M.T. PARACAMPO, «*I prestatori di servizi per le cripto-attività Tra mifidizzazione della MICA e tokenizzazione della Mifid*» 63*,* G. Giappichelli 2023.

Tale rischio sussiste anche se il cliente accede a un servizio offerto da un fornitore di un paese terzo attraverso sollecitazioni, promozioni o pubblicità dirette nell'Unione, indipendentemente dal mezzo di comunicazione utilizzato[396].

Queste problematiche richiedono un chiarimento ulteriore e l'ESMA, ai sensi del paragrafo 3, dovrà sviluppare orientamenti di due tipologie: identificare la linea di confine delle situazioni riconducibili alla sollecitazione passiva (proveniente dall'impresa) e stabilire le *best practices* per promuovere una sorveglianza coerente a livello europeo nella individuazione e prevenzione di pratiche operative elusive della disposizione in questione.

Va sottolineato che il tema centrale è la mancanza di confini e la dimensione transfrontaliera delle cripto-attività, che, spinte da prestatori di portata internazionale, pongono la necessità di un approccio globale[397].

Nonostante le recenti problematiche emerse nel settore, i principali prestatori di servizi hanno ottenuto alti livelli reputazionali a livello mondiale, suscitando preoccupazioni sulla possibilità che il "porto franco" concesso a quelli extraeuropei possa costituire una minaccia per consumatori e mercati, favorendo così la concorrenza non regolamentata[398]. Tuttavia, la Commissione europea esaminerà questo aspetto specifico come possibile indicatore per futuri interventi normativi ai sensi dell'articolo 140, estendendo il principio del "*level playing field*" oltre i confini europei, ad esempio, attraverso l'introduzione di un "regime di equivalenza per i prestatori di servizi per le cripto-attività di paesi terzi"[399].

---

[396] Cfr. A. CANEPA, «*social media e fin-influencers come nuove fonti di vulnerabilità digitale nell'assunzione delle decisioni di investimento*», Rivista trimestrale di diritto dell'economia, gennaio 2022.

[397] Cfr. *IOSCO, «Policy Recommendations for Crypto and Digital Asset Markets. Final Report*», 16 novembre 2023, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf.

[398] Ciò traspare anche dalle parole del Presidente dell'ESMA, Verena Ross, la quale precisa, in riferimento a MICA, che: "*while it is the first comprehensive regulation of previously unregulated crypto-assets in the world, we must acknowledge that MICA is not a silver bullet. For a start, it is inevitably limited in geographic scope. Service providers outside the EU have a prominent role in crypto markets, and it seems likely that this will continue to be the case. If consumers in the EU seek out the services of providers based outside the Union, they will be outside the scope of MICA*". V. ROSS, «*Developments in AI and Blockchain – How Do We Protect Investors and Supervise Markets Effectively?*», Afore Consulting 7th Annual FinTech and Regulation Conference, 7 febbraio 2023.

[399] L'art 140, par. 2, lett. v), prevede: "una valutazione dell'opportunità di stabilire ai sensi del presente regolamento un regime di equivalenza per le entità che prestano servizi per le cripto-attività di paesi terzi, gli emittenti di *token* collegati ad attività o gli emittenti di *token* di moneta elettronica di paesi terzi".

## 1.8 Il ruolo delle Autorità competenti, punti in comune con il *framework* europeo *post* 2008

Il MiCAR, in merito alla supervisione ed *enforcement*, è disciplinato dal Titolo VII, che offre una dettagliata serie di poteri prudenziali (regolatori, di vigilanza, indagine, ispezione, intervento, sanzionatori). Tali poteri mirano a proteggere gli interessi del sistema finanziario, monetario, bancario e dei consumatori, sono distribuiti tra le autorità nazionali (ANC) ed europee[400].

Il quadro di vigilanza e applicazione delle normative per i mercati delle cripto-attività, delineato dal MiCA, rappresenta l'ultimo passo di una ridefinizione complessiva dell'ampiezza e della profondità della regolamentazione nonché del ruolo attribuito ai regolatori. Questa ridefinizione è scaturita dalla recente crisi finanziaria globale, che ha evidenziato la necessità di superare il modello precedente di vigilanza, affidato esclusivamente alle ANC, in quanto ritenuto inadeguato per fronteggiare i rischi di instabilità sistemica[401].

Successivamente alla grave crisi economica e finanziaria, la normativa europea ha identificato come *benchmark* della nuova disciplina, la necessità di superare la frammentazione del sistema di vigilanza e controllo tra diverse ANC. Questa frammentazione si è infatti rivelata incapace di fornire risposte comuni e coerenti di fronte ai rischi di instabilità sistemica. L'inadeguatezza dell'assetto preesistente ha fatto emergere la necessità di andare verso un sistema che consenta di prevenire,

[400] Il Titolo VII è suddiviso in capitoli (artt. 93-108; artt: 109-110; artt: 111-116; artt. 117-120; artt. 121-138) che disciplinano, rispettivamente: Capo I) i poteri delle autorità nazionali competenti (ANC) sugli emittenti di *token* collegati ad attività (*Asset-Referenced Tokens* - ART) e di *token* di moneta elettronica (*e-money tokens* - EMT) *dell'European Banking Authority* - EBA e dell'*European Securities and Markets Authority* - ESMA; Capo II) il registro tenuto dall'ESMA; Capo III) le sanzioni e le misure amministrative a disposizione delle ANC; Capo IV) la responsabilità di vigilanza diretta dell'EBA sugli emittenti di *token* collegati ad attività significativi (*significant asset-referenced tokens* SART) e di moneta elettronica significativi (*significant e-money tokens* - SEMT) e i requisiti per la composizione dei collegi di vigilanza; Capo V), poteri e competenze dell'EBA sugli emittenti di SART e di SEMT. Cfr. D. ALESSI, «*Il ruolo delle Autorità competenti: la collaborazione tra ABE, ESMA e Autorità nazionali*», in «*Il MiCAR, guida al regolamento Europeo sui mercati delle cripto*», a cura di M. NICOTRA, F. SARZANA, S. IPPOLITO, M. SIMBULA (Giuffrè Francis Lefebvre, 2023).

[401] Cfr. «La crisi finanziaria globale ha reso necessario un ripensamento del quadro regolamentare e, conseguentemente, del ruolo dei regolatori europei, in quanto ha fatto emergere rilevanti criticità nell'assetto istituzionale e di vigilanza che riflettono alcune peculiarità del sistema finanziario europeo. Per tale motivo, parte integrante della nuova disciplina dei mercati finanziari, adottata dal legislatore europeo al fine di prevenire nuove crisi, è la creazione di nuovi regolatori, l'attribuzione a questi di nuovi poteri e la ridefinizione dei rapporti che intercorrono tra questi ultimi e le autorità di settore nazionali» in M. PIETROLUONGO, «*I poteri di intervento temporaneo dell'ESMA*», iusinitinere.it, luglio 2019.

fronteggiare e risolvere i rischi con regole unitarie, strumenti uniformi e comportamenti comuni.

La soluzione è stata la creazione di nuove agenzie europee come autorità di vigilanza, con l'assegnazione di competenze dirette di vigilanza a istituzioni preesistenti, al fine di realizzare una vigilanza unitaria gestita congiuntamente da autorità europee e ANC[402].

Questo approccio è evidente anche nel MiCA, che adotta e rielabora le *best practices* di accentramento dei poteri di supervisione, che hanno caratterizzato la vigilanza bancaria degli ultimi dieci anni. Un esempio di ciò è rappresentato dalla scelta dell'Unione in materia di mercati finanziari di affidare direttamente la vigilanza di alcuni soggetti di nuova regolamentazione all'European Securities and Markets Authority (ESMA) e l'attribuzione alla BCE, nell'ambito dell'Unione Bancaria, di una competenza di vigilanza prudenziale su tutte le banche e di vigilanza diretta per i gruppi bancari significativi, se pure limitatamente all'eurozona.

Un'analisi dettagliata del Titolo VII del MiCA evidenzia notevoli analogie, sia a livello testuale che di contenuti, con le disposizioni di vigilanza per i mercati degli strumenti finanziari, come MiFID 2, MiFIR[403] e MAR[404].

Questa convergenza riflette l'origine stessa del MiCA, nato per regolamentare cripto-attività al di fuori del contesto normativo dei servizi finanziari dell'UE[405].

La normativa del MiCA riprende, in maniera quasi identica, gli aspetti disciplinari di MiFID 2 e MiFIR, includendo la disciplina di *product intervention*.

Ciò consente alle autorità di vigilanza nazionali e sovranazionali di limitare o vietare la distribuzione di specifici prodotti al fine di salvaguardare gli interessi degli investitori e la stabilità del mercato[406].

---

[402] Vedi il considerando 1 del regolamento n. 1095/2010: «La crisi ha evidenziato gravi lacune in materia di cooperazione, coordinamento, applicazione uniforme del diritto dell'Unione e fiducia fra le autorità nazionali di vigilanza».

[403] Regolamento UE 600/2014.

[404] Regolamento UE 596/2014.

[405] F. MURINO, *«Vigilanza ed enforcement sui mercati delle cripto-attività nella proposta di Regolamento MiCA»*, Osservatorio del diritto civile e commerciale (ISSN 2281-2628) Fascicolo Speciale, settembre 2022.

[406] La MIFID Il ed il Regolamento MiFIR hanno introdotto misure di vigilanza di cui possono disporre le autorità (ESMA, EBA e autorità nazionali) per controllare ed intervenire, sia in via preventiva che nel durante, sulla commercializzazione, distribuzione e vendita di prodotti dell'Unione. Quanto ai poteri di intervento, questi consentono all'ESMA per gli strumenti finanziari (cfr. art, 40 del Regolamento), e all'EBA per i depositi strutturati (cfr. art. 41 del Regolamento), di vietare temporaneamente o eventualmente limitare la commercializzazione, la distribuzione o la vendita di determinati strumenti finanziari o deposito strutturato, aventi particolari caratteristiche specifiche, ovvero, anche un tipo di attività o pratica finanziaria (c.d. poteri di *temporary intervention*).

A differenza di MiFIR, in cui il potere di *temporary intervention* è assegnato esclusivamente a ESMA, nel MiCA tale potere è distribuito tra ESMA e l'European Banking Authority (EBA), in base alla tipologia di prodotto.

Il MiCA si ispira al meccanismo di vigilanza unico dell'Unione Bancaria, ma si distingue per la suddivisione delle funzioni di vigilanza tra le Autorità Nazionali Competenti (ANC) e le Autorità Europee di Vigilanza (ESA), basata sul concetto di "significatività" e declinata con criteri oggettivi.

In questo contesto, il MiCA si allontana dall'architettura dell'Unione Bancaria, dove la funzione di regolazione in capo all'EBA è distinta e separata da quella di vigilanza sulle banche significative, appannaggio della BCE.

Nel MiCA, infatti, l'EBA assume solo compiti di regolazione e vigilanza diretta sugli emittenti di *significant asset-referenced token* (SART) e *significant e-money tokens* (SEMT), ed è dotata di ampi poteri di indagine, ispezione, sanzioni amministrative nonché potere di *temporary intervention* sugli *e-money token* (EMT).

L'approccio alla nuova vigilanza diretta dell'EBA nel contesto del MiCA riflette le esperienze acquisite sia nell'Unione Bancaria che nei mercati dei capitali.

Questo modello, da un lato, segue la linea già intrapresa con l'ESMA, cui sono stati conferiti poteri settoriali di vigilanza diretta sui mercati finanziari, e, dall'altro, riflette e rielabora gli sviluppi della vigilanza bancaria europea con riferimento al parametro di "significatività".

Il regolamento, come detto poc'anzi, affida alle ANC la responsabilità della vigilanza su emittenti di ARTs e di EMTs, prescrivendo che gli Stati Membri provvedano a dotarle di adeguati poteri di vigilanza e indagine[407].

L'articolo 94 del regolamento elenca i poteri di cui devono essere dotate le ANC per adempiere ai loro compiti di vigilanza.

[407] Per le ragioni a sostegno della doppia vigilanza, cfr. il Considerando n. 103: «Le autorità competenti incaricate della vigilanza a norma della direttiva 2009/110/CE dovrebbero vigilare sugli emittenti di token di moneta elettronica. Tuttavia, alla luce dell'utilizzo potenzialmente ampio dei *token* di moneta elettronica significativi come mezzo di pagamento e dei rischi che essi possono comportare per la stabilità finanziaria, è necessaria una duplice vigilanza da parte delle autorità competenti e dell'ABE sugli emittenti di tali *token*. L'ABE dovrebbe vigilare sul rispetto, da parte degli emittenti di token di moneta elettronica significativi, degli obblighi supplementari specifici stabiliti nel presente regolamento per tali *token*. Poiché gli obblighi supplementari specifici dovrebbero applicarsi solo agli istituti di moneta elettronica che emettono *token* di moneta elettronica significativi, gli enti creditizi che emettono *token* di moneta elettronica significativi, ai quali tali obblighi non si applicano, dovrebbero continuare a essere soggetti alla vigilanza delle rispettive autorità competenti. Tale duplice vigilanza dovrebbe tener conto della natura molto specifica dei rischi posti dai *token* di moneta elettronica e non dovrebbe costituire un precedente per altri atti legislativi dell'Unione in materia di servizi finanziari».

A titolo esemplificativo, le ANC possono intervenire richiedendo la correzione del contenuto del *White paper* in caso di lacune informative, garantendo la *compliance* alle normative[408] e tutelando gli interessi dei possessori di cripto-attività. Le Autorità nazionali, hanno inoltre il potere di imporre modifiche alle comunicazioni di *marketing* di soggetti come offerenti, persone che richiedono l'ammissione alla negoziazione o emittenti di ARTs e EMTs, se non conformi ai requisiti stabiliti dal regolamento di cui agli artt. 7, 29 o 53[409] . Fra i poteri di intervento più incisivi che MiCAR attribuisce alle ANC vi è la facoltà di rimuovere una persona fisica dall'organo di amministrazione di un emittente di ARTs o di un CASP[410].

Vi sono anche poteri di breve termine con una funzione principalmente "cautelare". In presenza di "fondati motivi di sospettare che il presente regolamento sia stato violato", le ANC hanno il potere di sospendere, per un massimo di "30 giorni", o richiedere a un CASP di sospendere per un periodo analogo, la prestazione di servizi per le cripto-attività, l'offerta al pubblico o l'ammissione alla negoziazione di cripto-attività; o ancora, il potere di sospendere o richiedere a un CASP che gestisce una piattaforma di negoziazione di sospendere la negoziazione di cripto-attività[411].

L'adozione di ulteriori misure cautelari, senza un termine massimo di durata, è giustificata dal fatto che la prestazione del servizio per le cripto-attività o la loro negoziazione, pregiudicherebbero gli interessi dei clienti, dei possessori di cripto-attività ed in particolare di quelli al dettaglio.

In caso di un livello potenziale di pregiudizio tale, le ANC sono autorizzate a "sospendere o richiedere a un CASP di sospendere la prestazione di servizi per le cripto-attività", "sospendere o imporre al pertinente prestatore di servizi per le cripto-attività che gestisce la piattaforma di negoziazione di sospendere la negoziazione di cripto-attività"[412].

MiCA assegna alle ANC anche il potere di vietare specifiche attività. Se le ANC constatano la violazione del Regolamento o hanno "fondati motivi di sospettare che" in assenza del loro intervento questo "sarebbe violato", possono intervenire vietando "la prestazione di servizi per le cripto-attività", "l'offerta al pubblico o l'ammissione

[408] Artt. 6, 19 o 51 MiCA.
[409] Cfr. art 94 comma 1 lett. *i) j)* MiCA.
[410] Cfr. art 94 comma 1 lett. *y)* MiCA.
[411] Cfr. art 94, comma 1 lett. *l), n)*.
[412] Cfr. art. 94, comma 1 lett. *f), t)*.

alla negoziazione di cripto-attività", "la negoziazione di cripto-attività su una piattaforma di negoziazione"[413].

Possono anche "ordinare la cessazione immediata dell'attività senza preavviso o imposizione di un termine" se c'è "motivo di presumere" che una persona stia emettendo ARTs o EMTs senza autorizzazione, o stia offrendo cripto-attività o chiedendo l'ammissione alla negoziazione di cripto-attività diverse da ARTs o EMTs senza aver notificato un *White paper* conformemente a quanto disposto dall'art. 8[414].

Il MiCA conferisce alle ANC anche il potere di rendere pubbliche le informazioni rilevanti.

La finalità di garantire la tutela degli interessi dei clienti, dei possessori di cripto-attività, in particolare dei detentori al dettaglio, o il regolare funzionamento dei mercati sottende ulteriori prerogative attribuite alle ANC, che includono la facoltà di divulgare informazioni rilevanti o richiedere ai prestatori di servizi per le cripto-attività di renderle pubbliche, qualora possano influenzare la prestazione dei servizi relativi alle cripto-attività. Le ANC sono autorizzate a rendere di dominio pubblico eventuali inadempienze da parte di CASP, offerenti, persone che chiedono l'ammissione alla negoziazione di cripto-attività o emittenti di ART o EMT. Hanno altresì il potere di richiedere che tali soggetti rendano pubbliche tutte le informazioni rilevanti che possono influire sulla valutazione delle cripto-attività offerte al pubblico o ammesse alla negoziazione[415].

Tra le numerose disposizioni contenute nell'articolo 94, emergono anche poteri incisivi di verifica e ispettivi.

Per garantire una sorveglianza completa ed efficace, le ANC sono infatti autorizzate a condurre ispezioni o indagini in loco, sia presso residenze private che in altri luoghi, allo scopo di accedere a documenti e dati in qualsiasi formato. Inoltre, hanno il diritto di esternalizzare verifiche o indagini a revisori o esperti[416].

Parallelamente, in sintonia con una vigilanza orientata alla prevenzione più che alla repressione, il MiCA consente alle ANC di attivare l'*enforcement* già in presenza di un potenziale rischio a fronte di interazioni a distanza tramite *internet*, ad esempio mediante l'oscuramento di siti, la rimozione di contenuti o l'inserimento di avvertenze[417].

---

[413] Cfr. art. 94, comma 1, lett. *c), m), o)*.
[414] Cfr. art. 94, comma 1, lett. *u)*.
[415] Cfr. art. 94, comma 1, lett. *d) r) s)*.
[416] Cfr. art. 94, comma 1, lett. *w), x)*.
[417] Cfr. CONSOB, «*Piano strategico 2022-24*»,

Questa capacità di regolamentazione *online* si riflette nella possibilità di adottare misure volte a fermare la violazione del regolamento, anche attraverso l'intervento di soggetti terzi o autorità pubbliche. Tali misure possono includere la rimozione di contenuti, la limitazione dell'accesso a un'interfaccia *online* o l'imposizione di avvertenze esplicite ai clienti e ai possessori di cripto-attività.

Inoltre, accanto ai poteri generici di sorveglianza e indagine, essenziali per adempiere ai compiti assegnati alle ANC nei Titoli da II a VI del MiCA, il Regolamento delinea ulteriori e specifici poteri, orientati principalmente verso attività di ricerca, assicurazione delle fonti di prova e provvedimenti cautelari, attivabili nell'ambito delle iniziative di prevenzione e repressione degli abusi di mercato contemplati al Titolo VI[418]

Nel contesto delle attività di sorveglianza, indagine e contrasto alle violazioni, il Regolamento stabilisce che le ANC debbano cooperare tra loro, scambiare informazioni tempestivamente e fornirsi reciprocamente assistenza.

Il MiCA assegna all'EBA e all'ESMA un ruolo di coordinamento tra le ANC e i collegi di vigilanza[419], al fine di promuovere una cultura comune della vigilanza e l'uniformità nelle prassi e procedure di sorveglianza.

Le ESAs, infatti, fin dalla loro istituzione, hanno come obiettivo principale la promozione di una cultura comune e l'adozione di prassi uniformi nel campo della vigilanza, assicurando al contempo la coerenza delle procedure e degli approcci in tutta l'Unione Europea.

Il MiCA enfatizza questo ruolo, conferendo all'ESMA un ruolo chiave in questo contesto. Concentrandoci sui compiti di regolamentazione delineati nel Titolo VII, emerge chiaramente il ruolo fondamentale delle ESAs nella promozione dello scambio efficiente di informazioni tra le ANC.

Gli articoli 95 e 96 del Regolamento assegnano specificamente all'ESMA, in stretta collaborazione con l'EBA, il compito di sviluppare proposte di norme tecniche di regolamentazione per definire nello specifico lo scambio di informazioni tra le ANC, al fine di garantire un corretto esercizio delle rispettive funzioni di *supervisory* ed *enforcement*[420].

---

https://www.consob.it/documents/1912911/1949521/ps_2224.pdf/dcc07424-55f5-d283-8b0a-4d7c8e3e0507.

[418] Cfr. art 94, comma 3.

[419] Vedi *infra*.

[420] Cfr. art 95, comma 10.

Inoltre, all'ESMA è affidato il compito di elaborare proposte di norme tecniche di attuazione per stabilire formati, modelli e procedure *standard* per la cooperazione e lo scambio di informazioni tra le ANC e tra ANC, EBA ed ESMA[421].

La Commissione Europea avrà il compito di adottare queste norme tecniche di regolamentazione e di attuazione in conformità con le disposizioni del Regolamento istitutivo dell'ESMA[422].

Inoltre, l'articolo 97 del Regolamento conferisce a tutte le ESAs un ruolo significativo nella promozione della convergenza nella classificazione delle cripto-attività. Le ESA's sono incaricate di emettere congiuntamente orientamenti in conformità dell'art 16 dei rispettivi Regolamenti istitutivi[423] per specificare il contenuto e la forma della spiegazione che accompagna il *white paper* sulle cripto-attività[424] e dei pareri legali sulla qualificazione degli ARTs[425].

Questi orientamenti includono un modello standardizzato per la spiegazione e il parere, nonché un *test standard* per la classificazione delle cripto-attività.

Le ESA's devono stimolare la discussione tra le ANC sulla classificazione delle cripto-attività, compresa la classificazione di quelle escluse dall'ambito di applicazione del MiCA[426].

Infine, alle ESAs è affidato il compito di individuare le fonti potenziali di divergenze negli approcci delle ANC alla classificazione di tali cripto-attività e di promuovere, per quanto possibile, un approccio comune su questo fronte[427].

Le ESA's hanno come attività primaria quella di assicurare l'uniformità delle procedure e la coerenza degli approcci nell'intera Unione.

---

[421] *Ibidem*.

[422] Cfr. artt. Da 10 a 15 del Regolamento (UE) N. 1095/2010. Art. 10, Norme tecniche di regolamentazione: «Se il Parlamento europeo e il Consiglio delegano alla Commissione il potere di adottare norme tecniche di regolamentazione mediante atti delegati, a norma dell'articolo 290 TFUE al fine di garantire un'armonizzazione coerente nei settori specificati negli atti legislativi di cui all'articolo 1, paragrafo 2, l'Autorità può elaborare progetti di norme tecniche di regolamentazione. L'Autorità sottopone i suoi progetti di norme all'approvazione della Commissione». Art. 15, Norme tecniche di attuazione: «L'Autorità può elaborare norme tecniche di attuazione mediante atti di esecuzione a norma dell'articolo 291 TFUE nei settori specificati negli atti legislativi di cui all'articolo 1, paragrafo 2. Le norme tecniche di attuazione sono di carattere tecnico, non implicano decisioni strategiche o scelte politiche e lo scopo del loro contenuto è quello di determinare le condizioni di applicazione di tali atti. L'Autorità sottopone i suoi progetti di norme tecniche di attuazione all'approvazione della Commissione».

[423] Art. 16 dei Regolamenti (UE) n. 1093/2010, n. 1094/2010 e n. 1095/2010.

[424] Cfr. art.8, comma 4.

[425] Cfr. art. 17, comma 1, lett. *b)*, punto ii), e art. 18, comma 2, lett. *e)*.

[426] Vedi art. 2, comma 3.

[427] Cfr. art 97, comma 2.

Le ANC di uno Stato membro possono anche richiedere all'ESMA, all'EIOPA o all'EBA, a seconda dei casi, un parere sulla classificazione delle cripto-attività, comprese quelle escluse dall'ambito di applicazione del MiCA e devono riceverlo entro 15 giorni lavorativi.

Inoltre, le ESA's devono redigere congiuntamente una relazione annuale che affronti le difficoltà e le divergenze riscontrate nella classificazione delle cripto-attività[428].

Ulteriori poteri di elaborazione di norme tecniche di regolamentazione sono attribuiti all'EBA nel Capo V, in cooperazione con l'ESMA e la BCE, l'EBA è infatti responsabile della specificazione delle condizioni rilevanti per la composizione dei collegi di vigilanza, al fine di garantirne un funzionamento coerente e uniforme[429].

L'intero quadro normativo sulla *product intervention* nel MiCA segue, l'approccio delineato nella normativa dell'Unione Europea relativa ai mercati degli strumenti finanziari. Questa normativa è inclusa nella direttiva MiFID 2 e, in particolare, negli articoli 40 e 41 del regolamento MiFIR. Tale direttiva ed il regolamento, mirando a superare la "sola filosofia della trasparenza"[430] della MiFID I, hanno potenziato la tutela degli investitori, focalizzandosi sulle diverse fasi della *product governance* che rappresenta un insieme di regole e presidi finalizzati a regolamentare la fase di ideazione, distribuzione, commercializzazione e vendita dei prodotti finanziari. Inoltre, la *product intervention* indica il potere delle autorità di vigilanza, sia a livello nazionale che sovranazionale, di vietare e/o limitare la distribuzione di specifici prodotti.

Così come il Regolamento MiFIR aveva conferito alle autorità sovranazionali ESMA ed EBA il potere di intervenire, sia in via preventiva che nel corso delle attività di commercializzazione, distribuzione e vendita dei prodotti dell'Unione, anche il Regolamento MiCA stabilisce che ESMA ed EBA possono sostituire le ANC in caso di inerzia o quando ritengono insufficienti le misure adottate dalle autorità competenti. Nel MiCA, il potere di intervento temporaneo è assegnato a ESMA ed EBA in base al tipo di cripto-attività. Gli articoli 103 e 104, che trattano dei poteri di intervento di ESMA ed EBA, presentano contenuti identici, con la differenza della competenza di ESMA sulle cripto-attività diverse da ARTs e EMTs (*utility token*) e di EBA su ARTs

[428] Cfr. art. 97, comma 4.
[429] Cfr. art 119, comma 8.
[430] Cfr. E. FRANZA, «*La product intervention del mondo MIFID II/MIFIR*» Il diritto dell'economia, fasc. n.98 (gennaio 2019) 325–51.

e EMTs. L'intervento delle due autorità europee è di natura sussidiaria e può essere attivato solo se si verificano tre condizioni fondamentali[431]:

*a)* deve essere finalizzato ad affrontare un timore significativo riguardante la tutela degli investitori o una minaccia all'ordinato funzionamento e all'integrità dei mercati delle cripto-attività o alla stabilità del sistema finanziario dell'Unione;

*b)* la minaccia in questione non venga adeguatamente affrontata con il rispetto dei requisiti regolamentari previsti dal diritto dell'Unione, che quindi non sono sufficienti a gestire la situazione;

*c)* le ANC non abbiano adottato misure adeguate ad affrontare la minaccia in questione o le misure adottate non siano adeguate a gestirla.

In sintesi, l'intervento di ESMA ed EBA è concepito come un mezzo di estrema necessità, attivabile quando gli strumenti disponibili appaiono inadeguati ed i requisiti normativi e regolamentari, della legislazione UE, risultino insufficienti.

Pertanto, ESMA ed EBA non hanno solo il potere di supplire all'inerzia delle ANC ma possono anche avocarne la competenza nel caso in cui l'ANC non si attivi in modo sufficiente, secondo una valutazione che è demandata a ESMA ed EBA stesse secondo quanto previsto dal MiCA.

Tutta via, gli interventi delle ESAs non devono generare effetti negativi sproporzionati rispetto ai benefici perseguiti per l'efficienza dei mercati finanziari o per gli investitori[432], né comportare rischi di arbitraggio normativo[433].

I presupposti che ESMA, EBA e le ANC dovranno prendere in esame saranno specificati dalla Commissione attraverso l'adozione di atti delegati, nell'esercizio del potere ad essa conferito alle condizioni stabilite dall'art. 139 della stessa MiCA[434].

I *temporary intervention powers*, consistono nella facoltà di "vietare o limitare temporaneamente" la commercializzazione, la distribuzione o la vendita di determinati ART ed EMT (EBA) o di cripto-attività diverse da ART e EMT (ESMA)[435]. Tali misure si applicano in tutta l'Unione e hanno prevalenza su eventuali misure adottate in precedenza da ANC sulla stessa questione, imponendosi così sulle autorità nazionali[436].

---

[431] Artt. 103 e 104, comma 2, lett. *a), b), c).*
[432] P. MAUME, «*The Regulation on Markets in Crypto-Assets (MiCAR): Landmark Codification, or First Step of Many, or Both?*», 2023, 243–75.
[433] Artt. 103 e 104, comma 3.
[434] Cfr, artt. 103, comma 8; art. 104, comma 8; art. 105, comma 73
[435] Cfr. artt. 103 e 104, comma 1, lett. *a)* e *b)*.
[436] Cfr. artt. 103 e 104, comma 7.

Rimane il fatto che l'intervento diretto delle ESAs, all'interno di un contesto regolamentare di competenza delle ANC, ha carattere eccezionale e sussidiario, nonché "temporaneo", come precisato nel §1 degli articoli 103 e 104 del MiCA, e consiste nei poteri di *product intervention* attribuiti "conformemente" ai Regolamenti istitutivi di entrambe le ESAs[437].

Questa disposizione del MiCA si allinea con la previsione generale contenuta nell'articolo 9, comma 5, dei Regolamenti UE n. 1093/2010 e n. 1095/2010, che riconosce alle due ESAs il potere di adottare provvedimenti di proibizione o limitazione temporanea di attività finanziarie nei casi e alle condizioni stabilite nelle norme attuative.

La temporaneità delle misure impone alle ESAs, di riesaminarle "a intervalli appropriati e almeno ogni sei mesi" e tale revisione può portare al rinnovo o alla revoca della misura; dopo almeno due rinnovi consecutivi e sulla base di un'analisi adeguata che valuti l'impatto sui consumatori, le due ESAs possono decidere di rinnovare "annualmente" il divieto o la restrizione[438]. Al contrario, le misure analoghe adottabili dalle ANC non sono soggette né a revisione periodica né a un termine finale di efficacia. La legge stabilisce semplicemente che "l'autorità competente revoca il divieto o la restrizione quando vengono meno le condizioni" che ne giustificano l'adozione[439].

Il MiCA, seguendo il modello del MiFIR, conferisce alle Autorità Nazionali Competenti gli stessi poteri di *product intervention* assegnati all'ESMA e all'EBA, posizionando l'iniziativa principale in capo alle ANC e delineando l'intervento delle ESAs come eventuale e suppletivo.

Si consideri che le ANC possono già intervenire vietando o limitando la circolazione delle cripto-attività in caso di "un timore significativo in materia di tutela degli investitori" o di una "minaccia all'ordinato funzionamento e all'integrità dei mercati delle cripto-attività" o "alla stabilità dell'insieme o di una parte del sistema finanziario di almeno uno Stato membro".

Questi poteri di intervento, simili a quelli di *temporary intervention* di ESMA ed EBA, possono essere esercitati dalle ANC all'interno dello Stato membro e possono includere la restrizione della circolazione di specifiche cripto-attività. Le ANC

[437] Cfr. art. 9, comma 5, del Regolamento (UE) n. 1095/2010 per ESMA, e Regolamento (UE) n.1093/2010 per EBA.
[438] Cfr. artt. 103 e 104, comma 6.
[439] Cfr. art. 105, comma 6.

possono intervenire solo se i requisiti regolamentari dell'Unione vigenti non affrontano adeguatamente i rischi e le minacce o se una migliore vigilanza o l'applicazione dei requisiti esistenti non sarebbe sufficiente.

Anche in questo caso, tuttavia, gli interventi delle ANC devono evitare effetti negativi sproporzionati rispetto ai benefici attesi[440], considerando la natura dei rischi, il livello di sofisticazione degli investitori o dei partecipanti al mercato interessati e il probabile impatto sugli investitori e i partecipanti al mercato. Inoltre, l'esercizio di tali poteri richiede una consultazione preventiva con le ANC degli altri Stati membri sui quali la misura "potrebbe incidere in modo significativo"[441].

Come si vede, il MiCA stabilisce una totale simmetria tra la *product intervention* delle ANC e quella delle ESAs in via sussidiaria.

È prevista anche una procedura articolata di confronto preventivo sulle misure di *product intervention* tra ESA e ANC. La ANC che intenda adottare una misura di divieto o restrizione, dovrà comunicarlo in anticipo (almeno un mese prima) alle altre ANC, all'ESMA o all'EBA (per gli ARTs e EMTs), specificando i dettagli della misura proposta[442]. Nei casi eccezionali, in cui il preavviso di un mese non sia praticabile, potrà essere adottata una misura urgente e provvisoria per un massimo di tre mesi, notificando l'entrata in vigore con almeno 24 ore di anticipo[443].

È chiaro pertanto che il regolamento MiCA stabilisce un significativo legame tra i poteri di intervento delle autorità nazionali competenti e delle agenzie europee ESMA ed EBA attraverso la procedura di parere ci cui all'articolo 106. L'assegnazione di poteri di sostituzione e revisione alle agenzie europee rispetto alle ANC evidenzia un *trend* crescente di accentramento delle funzioni di regolamentazione e vigilanza a livello comunitario.

In particolare l'ESMA e l'EBA hanno il l ruolo di "facilitazione e coordinamento" sulle misure adottate dalle ANC, ovvero queste agenzie hanno il

[440] "Con proporzionalità degli atti di vigilanza, si intende il criterio di esercizio del potere adeguato al raggiungimento del fine, con il minor sacrificio degli interessi dei destinatari. A livello generale, il principio di proporzionalità è illustrato nell'articolo 5, comma 4, del trattato sull'Unione europea. Esso mira a inquadrare le azioni delle istituzioni dell'Unione europea (Unione) entro certi limiti. in virtù di tale principio, le misure dell'Unione devono essere idonee a conseguire il fine desiderato, devono essere necessarie per conseguire il fine desiderato e non devono imporre alle persone un onere eccessivo rispetto all'obiettivo che si intende raggiungere (proporzionalità in senso stretto)". In M. T. GIORDANO, S. CAPACCIOLI, «*Crypto-asset: Regolamento MiCa e DLT Pilot Regime. analisi ragionata su token, stablecoin, CASP»* Giuffè Francis Lefebvre 2023.

[441] Cfr. art 105, comma 2, lett. *c)*.

[442] Cfr. art. 105, comma 3.

[443] Cfr. art. 105, comma 3, lett. *c)*.

compito di garantire che le misure adottate da un'autorità nazionale siano giustificate e proporzionate, e di promuovere un approccio coerente tra le autorità competenti[444].

Questo ruolo di "garante" attribuito alle ESAs si concretizza attraverso l'emissione di un parere preventivo sulle misure di intervento che le ANC intendono assumere[445].

Nonostante il parere sia obbligatorio, esso non è vincolante, perché le ANC possono discostarsene, "adottando misure contrarie ad un parere" o astenendosi "dall'adottare le misure raccomandate" purché pubblichino "immediatamente" sul loro sito *internet* un avviso in cui spieghino in modo esauriente le proprie ragioni[446]. La procedura di parere costituisce un confronto pubblico tra le ESAs e le ANC e offre un meccanismo di controllo diffuso sui rispettivi argomenti[447].

In conclusione, sebbene formalmente "non vincolante", il parere delle ESA su legittimità e proporzionalità delle misure di *product intervention* adottate dalle ANC, riflette il potere discrezionale delle ESAs di avocare la competenza e sostituirsi alle ANC qualora ritengano che queste ultime non affrontino adeguatamente la minaccia.

Il "coordinamento" tra le Autorità Nazionali Competenti e le autorità comunitarie, sottolineato nell'articolo 106, sembra quindi concretizzarsi principalmente attraverso l'utilizzo del parere, il quale assume una funzione indiretta ma sostanziale nell'orientare preventivamente l'azione delle ANC.

Ma la possibilità per le Autorità Europee di intervenire direttamente senza la necessità di rilasciare un parere, sembra delineare due percorsi alternativi a seconda che la misura in corso di adozione da parte dell'ANC sia considerata suscettibile di correzioni o irrimediabilmente inadeguata. Nel primo caso, ESMA o EBA avvieranno il processo di coordinamento come previsto dall'articolo 106, emettendo il relativo parere; invece se la misura comunicata dalla ANC sembri totalmente inadeguata, le autorità europee potranno omettere il parere e attivare i poteri di *temporary intervention* conferiti dagli articoli 103 e 104[448].

---

[444] Cfr. art. 106, comma 1.
[445] Cfr. art. 106, comma 2.
[446] Cfr. art. 106, comma 6.
[447] V. TROIANO, R. MOTRONI, «*La MiFID II: Rapporti con la clientela - regole di governance - mercat»,* (Cedam, 2016).
[448] In alternativa, è possibile che il regolamento, con la dizione «quando le autorità competenti hanno adottato una misura a norma dell'articolo 105», intenda riferirsi a misure già in vigore (e quindi già oggetto del parere preventivo delle autorità comunitarie); il che spiegherebbe, ma al contempo renderebbe persino superflua, la precisazione sulla non necessità da parte di ESMA o EBA di accompagnare la propria misura temporanea con un parere su quella della ANC ritenuta inadeguata. V. nota n.421.

## 1.9 Misure e sanzioni amministrative

Come è stato analizzato, gran parte della complessa disciplina regolatoria contenuta nel MiCA, è presidiata da un sistema di sanzioni/misure amministrative che le ANC possono adottare in caso di violazione di disposizioni.

Il Capo III del Titolo VII delinea il perimetro di tale impianto sanzionatorio, finalizzato ad intervenire sulle violazioni dei precetti contenuti nel MiCA. L'art. 111, comma 1, individua e cataloga per Titoli, alle lett. da *a)* a *e)*[449], gli articoli del regolamento la cui violazione, è valutata dal legislatore UE in maniera maggiormente rilevante[450].

Completano il catalogo delle violazioni suscettibili di sanzioni o misure amministrative, menzionate nella lettera *f*), i comportamenti di "mancata collaborazione nell'ambito di indagini, ispezioni o di richieste di cui all'articolo 94, comma 3". A differenza delle violazioni del regolamento citate nelle lettere da *a)* ad *e),* la disposizione contenuta nel MiCA si limita ad impegnare lo Stato membro a conferire poteri sanzionatori alle ANC, senza però fornire specifiche sanzioni o misure amministrative conseguenti a tali violazioni[451].

È necessario sottolineare, in particolare, il riferimento alla clausola di riserva che costituisce, per la precisione, l'inizio del comma 1, la quale recita: "salvo le sanzioni penali"[452]. L'assunto *de quo* è da interpretare in combinato disposto con la precisazione, sempre inclusa nel comma 1, che "gli Stati membri possono decidere di non stabilire norme relative alle sanzioni amministrative se le violazioni di cui al primo comma, lettere *a), b), c), d)* o *e)*, sono già soggette a sanzioni penali nel rispettivo diritto nazionale". Viene quindi lasciata alla discrezione di ciascuno Stato membro la decisione di stabilire norme in materia di sanzioni amministrative per le violazioni di cui alle lettere *a)*, *b)*, *c)*, *d)* o *e)* dell'articolo 111, comma 1, nel caso in cui tali violazioni siano già soggette a sanzioni penali. Come si vede, pertanto, il regolamento afferma la legittimità astratta della politica sanzionatoria basata su un doppio binario

[449] Violazioni del Titolo Il sulle cripto-attività diverse da ARTs e EMTs (lett. *a*), violazioni del Titolo IlI sugli ARTs (lett. *b*), violazioni del Titolo IV sugli EMTs (lett. *c*), violazioni del Titolo V sui CASP (lett. *d*), violazioni del Titolo VI in tema di prevenzione e divieto degli abusi di mercato (lett. *e*).
[450] Come si evince dall'uso dei termini "almeno" e "seguenti" di cui all'art. 111, comma 1. Ciò consente di ritenere che gli Stati membri possano prevedere, a loro discrezione, eventuali ed ulteriori fattispecie oggetto di sanzione e/o misura amministrativa.
[451] Vedi *infra*.
[452] Art. 111, comma 1.

sanzionatorio penale ed amministrativo[453], ma d'altro canto attenua il rischio di una sovrapposizione sanzionatoria.

Nel caso in cui uno Stato membro, nell'esercizio di tale discrezionalità, decida di non stabilire le sanzioni amministrative, dovrà comunicare tale decisione alla Commissione, all'ESMA e all'EBA e fornire informazioni circa le "pertinenti norme di diritto penale" vigenti nell'ordinamento interno a presidio di tali violazioni.

Una volta identificate le categorie delle violazioni rilevanti del regolamento, l'articolo 111 ai commi da 2 a 5 prosegue delineando i quadri normativi delle misure o sanzioni adottabili in relazione alle macrocategorie di violazioni individuate.

In particolare, al comma 2 vengono elencate le misure o sanzioni adottabili dalle ANC per le violazioni di cui alle lettere da *a)* a *d)*, relative alle violazioni sulle cripto-attività diverse da ARTs e EMTs, sugli ART, sugli EMT e sui CASP. Al comma 3 vengono specificate le sanzioni amministrative pecuniarie massime in caso di violazioni commesse da persone giuridiche, stabilendo una soglia massima sotto la quale lo Stato membro non può scendere. Al comma 4 vengono invece disciplinate le misure o sanzioni adottabili dalle ANC per le violazioni di cui alla lettera *e)*, relative alle violazioni in tema di prevenzione e divieto degli abusi di mercato.

Le misure adottabili dalle ANC in risposta alla violazione del regolamento, sono principalmente le seguenti: sanzioni amministrative pecuniarie, sanzioni amministrative e altre misure amministrative non pecuniarie.

In merito alle sanzioni amministrative pecuniarie, l'articolo 111, ai commi 2, 3 e 5, stabilisce parametri distinti in base al tipo di violazioni, che siano relative alle cripto-attività diverse da ARTs e EMTs, sugli ARTs, sugli EMTs e sui CASP[454], oppure alle violazioni riguardanti la prevenzione e il divieto degli abusi di mercato[455]. In entrambi i casi, vengono indicati importi massimi edittali differenti per persone fisiche e giuridiche, garantendo così una risposta sanzionatoria più proporzionata ed efficace.

Come è stato evidenziato, MiCA consente agli Stati membri di conferire alle ANC poteri sanzionatori ulteriori rispetto a quelli espressi nel regolamento e di stabilire soglie sanzionatorie massime ancora più elevate di quelle fissate nell'art. 111. Oltre alle sanzioni amministrative pecuniarie, l'articolo 111, derubricato "Sanzioni amministrative e altre misure amministrative", autorizza le ANC ad adottare

[453] V. M. SCOLETTA, «*Doppio binario sanzionatorio e ne bis in idem nella nuova disciplina eurounitaria degli abusi di mercato*» 35, Le Società, IPSOA (2016): 218 ss.
[454] Cfr. art. 111, comma 2.
[455] Cfr. art. 111, comma 5.

provvedimenti di ingiunzione, interdizione, restituzione di profitti, revoca o sospensione di autorizzazioni, senza distinguere tra "sanzioni" e "misure" e senza fornire una chiave di interpretazione delle due fattispecie[456]. Nei commi 2, 4 e 5, vengono elencati in modo indistinto tutti i provvedimenti applicabili dalle ANC in seguito a violazioni del regolamento suscettibili di sanzione e diretti a prevenire ulteriori violazioni[457]. Spetta quindi all'ordinamento domestico classificare ogni singolo provvedimento come "sanzione" o "misura".

Affinché la selezione delle sanzioni e delle misure da adottare nel caso concreto risponda ai criteri di proporzionalità, efficacia e capacità dissuasiva, l'articolo 112, comma 1, elenca i seguenti criteri a cui le Autorità Nazionali Competenti devono attenersi: *a)* la gravità e la durata della violazione; *b)* l'intenzionalità o la negligenza nella commissione della violazione; *c)* il grado di responsabilità della persona coinvolta; *d)* la capacità finanziaria, valutata attraverso il fatturato totale o il reddito annuo e patrimonio netto; *e)* i profitti realizzati o le perdite evitate; *f)* le perdite subite da terzi a causa della violazione; *g)* il livello di cooperazione con l'autorità competente, con l'obbligo di restituire i profitti o le perdite evitate; *h)* precedenti violazioni del regolamento; *i)* misure adottate per prevenire recidive; *j)* impatto della violazione sugli interessi dei detentori di cripto-attività e dei clienti dei prestatori di servizi per le cripto-attività, specialmente dei detentori al dettaglio.

I provvedimenti conseguenti, che possono essere ripristinatori, afflittivi o interdittivi, devono dimostrare efficacia nel conseguire l'obiettivo prefissato; la misura o la sanzione amministrativa dovranno essere proporzionate e limitarsi a quanto necessario per raggiungere lo scopo, bilanciando l'interesse da perseguire con la sanzione e il pregiudizio per la sfera giuridica del destinatario. L'uso del potere

[456] Analogamente, l'art. 18 del Regolamento MVU contiene un elenco di misure e sanzioni amministrative, senza fornire un criterio di differenziazione, né il complesso normativo del regolamento MVU e della CRD IV esplicita la differenziazione tra le "misure amministrative" e le "sanzioni amministrative". In M. T. GIORDANO, S. CAPACCIOLI, «*Crypto-asset: Regolamento MiCA e DLT Pilot Regime. analisi ragionata su token, Stablecoin, CASP»* Giuffrè *2023, 297 e ss.*

[457] In linea generale, si può osservare come "misure amministrative" e "sanzioni amministrative" si distinguano essenzialmente per la finalità perseguita. La misura amministrativa è intesa a riparare l'interesse danneggiato ossia ad eliminare il vantaggio acquisito tramite un comportamento non conforme alle norme, mentre la sanzione amministrativa è indirizzata ad un fine punitivo onde dissuadere il reiterare del comportamento scorretto; per una definizione normativa di misura e sanzione a livello europeo, occorre rifarsi al Regolamento (CE, Euratom) n. 2988/95 del Consiglio, del 18 dicembre 1995, relativo alla tutela degli interessi finanziari delle comunità che, agli artt. 4 e 5, contiene una distinzione fra misura e sanzione amministrativa basata sulle rispettive finalità; la misura da un lato, è volta ad eliminare il vantaggio «contrario agli obiettivi del diritto comunitario» conseguito (art.4), mentre la sanzione, dall'altro lato, è rivolta a punire il responsabile in un'ottica finalistica di dissuasione dal compimento di ulteriori azioni negative (art.5). *ibidem*.

amministrativo o sanzionatorio ha lo scopo di dissuadere l'autore dal compiere futuri illeciti amministrativi.

Il regolamento prevede altresì che, nell'esercizio dei loro poteri di imporre sanzioni amministrative e altre misure amministrative, le ANC collaborino strettamente tra di loro per garantire l'efficacia delle rispettive attività di vigilanza, indagine e imposizione di misure e sanzioni. In particolare, in situazioni transfrontaliere, le ANC devono coordinare le azioni per evitare duplicazioni e sovrapposizioni nell'esercizio dei loro poteri di vigilanza, indagine e imposizione di sanzioni[458].

L'art. 113, comma 1, infine, sottolinea l'importanza dell'adeguata motivazione delle decisioni prese dalle ANC, stabilendo il diritto all'impugnazione dinanzi a un organo giurisdizionale degli Stati membri.

È degno di nota che, nell'ambito del quadro normativo relativo alle impugnazioni, il Regolamento pone un carico specifico sugli Stati membri nell'individuare modalità di *enforcement* per ottenere l'autorizzazione. A tale riguardo, viene stabilito che il diritto di impugnazione davanti a un organo giurisdizionale si applica anche nel caso in cui le ANC non prendano una decisione di concessione o rifiuto dell'autorizzazione entro sei mesi dalla presentazione di una domanda completa di autorizzazione[459].

Infine, con l'obiettivo di accrescere la protezione dei consumatori, si richiede agli Stati membri di garantire che organismi come enti pubblici o loro rappresentanti, organizzazioni di consumatori con legittimo interesse nella tutela dei possessori di cripto-attività e organizzazioni professionali con legittimo interesse nella protezione della propria categoria possano agire in nome e nell'interesse dei consumatori stessi, presentando ricorsi davanti a tribunali o organi amministrativi competenti per assicurare l'applicazione del MiCA.

## 1.10 *Framework* di vigilanza sovranazionale

Come si è detto, il compito di vigilare direttamente sugli emittenti di ARTs significativi (SART) e EMTs significativi (SEMT) è affidato esclusivamente all'EBA,

[458] Cfr. art 112, comma 2.

[459] Trattandosi di "silenzio inadempimento", potrebbe trovare applicazione, nell'ordinamento domestico, l'art. 31 "Azione avverso il silenzio e declaratoria di nullità" del D.Lgs. n. 104/2010 (Codice del processo amministrativo).

in particolare per quanto riguarda i SART. Questa decisione è basata sull'uso potenzialmente diffuso dei SART come mezzi di scambio e nell'esecuzione di voluminose transazioni finanziarie che comportano rischi specifici per i canali di trasmissione monetaria e per la sovranità monetaria[460]. La vigilanza diretta sugli emittenti di SEMT, invece, è concorrente e coinvolge sia l'EBA sia le autorità nazionali competenti[461].

Il quadro regolamentare stabilisce una duplice vigilanza per gli emittenti di SEMT, con l'EBA responsabile della vigilanza sugli obblighi supplementari specifici per gli emittenti significativi. Le ANC continuano a esercitare la vigilanza in conformità con la direttiva 2009/110/CE e mantengono la responsabilità per tutti gli altri requisiti previsti da MiCA[462].

I servizi e le attività aggiuntive forniti dagli emittenti di cripto-attività, che non rientrano nella categoria di SART o SEMT, rimangono sotto la vigilanza dell'ANC del paese d'origine[463].

Per ogni emittente di SART o SEMT, MiCA prevede la creazione di un collegio consultivo di vigilanza[464], presieduto e gestito dall'EBA[465], coinvolgendo ESMA[466], le ANC del paese d'origine[467], autorità competenti per i CASP, autorità competenti per la custodia delle attività di riserva o dei fondi per SEMT[468], le autorità di vigilanza dei

[460] Cfr. Considerando n. 102.
[461] Con parere del 19 febbraio 2021, al punto 3.3. «*Aspetti di vigilanza prudenziale*», la BCE aveva criticato l'allora proposta di Regolamento in relazione proprio alla duplice vigilanza (EBA e ANC), osservando come per i SART e SEMT fosse più opportuno delineare un'unica vigilanza a livello europeo, maggiormente idonea a garantire un quadro completo dei rischi e un coordinamento delle azioni di vigilanza, evitando allo stesso tempo l'arbitraggio normativo. Ad avviso della BCE, la duplice vigilanza presenterebbe «gravi inconvenienti e i *token* di moneta elettronica significativi così come i *token* collegati ad attività significativi riceverebbero una migliore vigilanza a livello europeo». Inoltre «non sembra esservi alcun motivo economico per giustificare disposizioni di vigilanza differenziate tra i *token* collegati ad attività significativi (soggetti a una vigilanza armonizzata dell'ABE) e quelli di moneta elettronica significativi (soggetti a duplice vigilanza da parte dell'ABE e delle ANC». Ed ancora, quando l'emittente del SEMT è un ente creditizio, «la duplice vigilanza comporterebbe ulteriori complicazioni, in quanto l'emittente può essere un ente creditizio significativo vigilato dalla BCE ai sensi del regolamento (UE) n. 1024/2013 del Consiglio (di seguito «regolamento sull'MVU»). La proposta di regolamento assoggetterebbe l'emittente a tre diverse autorità di vigilanza: (i) la pertinente ANC, (ii) l'ABE e (iii) la BCE». La BCE in tale parere consigliava di valorizzare diversamente l'esperienza e le competenze delle ANC nella vigilanza degli emittenti e dei fornitori di SEMT, che «potrebbero essere utilmente messe a frutto nell'ambito della loro partecipazione all'organo decisionale dell'ABE e attraverso i gruppi di vigilanza congiunti nel caso di enti creditizi significativi, nonché nel collegio di vigilanza da istituire per ciascun *token* di moneta elettronica significativo».
[462] Cfr. considerando n. 103.
[463] F. MURINO, «*Vigilanza ed enforcement sui mercati delle cripto-attività nella proposta di Regolamento MiCA*», in Oss. dir. civ. comm., Bologna n. speciale, commi 5 e 6, settembre 2022.
[464] Cfr. Considerando n. 105.
[465] Cfr. art 119, comma 2, lett. *a)*.
[466] Cfr. art. 119, comma 2, lett. *b)*.
[467] Cfr. art 119, comma 2, lett. *c)*.
[468] Cfr. art 119, comma 2, lett. *d)*.

prestatori di servizi di pagamento più rilevanti, che prestano servizi in relazione a SEMT[469] e, non ultima, la BCE[470].

Il collegio consultivo è essenziale per garantire una supervisione più efficace sugli emittenti di *token* significativi e ottenere una visione completa delle criticità potenziali dei mercati delle cripto-attività. Le autorità competenti coinvolte nel collegio possono variare a seconda delle circostanze, includendo anche le autorità che garantiscono la custodia e l'amministrazione dei *token* per conto dei clienti[471]. Se l'emittente di SART o SEMT è stabilito in uno stato membro la cui moneta non è l'euro, o nel caso in cui nei SART o SEMT figuri una valuta diversa dall'euro, la banca centrale nazionale di tale stato membro fa parte del collegio[472]. Per garantire una composizione coerente e uniforme del collegio, l'EBA, in collaborazione con ESMA e la BCE, elabora progetti di norme tecniche di regolamentazione, adottati dalla Commissione per integrare MiCA. Questi progetti definiscono i criteri per l'inclusione nel collegio delle autorità competenti considerate più rilevanti per la vigilanza su una specifica cripto-attività significativa[473].

Il compito principale dei collegi è formulare pareri non vincolanti, trattando temi quali l'obbligo per un emittente di possedere fondi propri più consistenti, modifiche al *white paper* sulle cripto-attività, variazioni nel modello di *business* di un emittente di SART, modifiche all'autorizzazione degli emittenti o alle misure di vigilanza a loro applicate, nonché accordi per lo scambio di informazioni con autorità di vigilanza di paesi terzi[474].

Nel caso in cui l'EBA o un'ANC non concordino con il parere del collegio, inclusi eventuali raccomandazioni per affrontare carenze nelle misure di vigilanza, devono giustificare la propria decisione fornendo spiegazioni al collegio per ogni significativa deviazione dai pareri o raccomandazioni contenute[475].

In sintesi, la complessità della disciplina delle sanzioni richiede un'attenta valutazione nella fase di recepimento, tenendo conto di principi come la tipicità, la tassatività, la riserva di legge e la necessaria cooperazione tra le autorità nazionali ed europee. Inoltre, la questione della giurisdizione rappresenta un punto fondamentale

[469] Cfr. art 119, comma 2, lett. *f)*.
[470] Cfr. art 119, comma 2, lett. *i)*.
[471] Cfr. art 119, comma 2, lett. *h)*.
[472] Cfr. art 119, comma 2, lett. *k)*.
[473] Cfr. art 119, comma 8.
[474] Cfr. art. 120, comma 1, lett. da *a)* a *k)*.
[475] Cfr. art. 120, comma 4.

che richiede un equilibrato approccio alla luce delle recenti pronunce della Corte Costituzionale.

L'articolo 130 del regolamento contiene, ai commi 1 e 2, due elenchi di "misure" che possono essere adottate dall'EBA nei confronti degli emittenti di SART o di SEMT, qualora sia accertata o vi siano fondati motivi di sospettare la commissione di una delle violazioni elencate nei dettagli agli allegati V e VI del Regolamento MiCA.

Gli elenchi di misure, il primo applicabile ai SART e ai SEMT, risultano essere speculari. In entrambi i casi, si delineano mediante l'esercizio di un generale potere attribuito all'EBA, consentendo l'interruzione forzosa delle attività che costituiscono la violazione[476], nonché l'opzione di applicare "sanzioni amministrative pecuniarie" o penalità di mora in conformità agli articoli 131 e 132[477]. Il MiCA tratta le sanzioni amministrative pecuniarie come *species* in rapporto al *genus* delle misure di vigilanza.

Tale commistione, sebbene consueta nei regolamenti dell'Unione Europea relativi ai mercati finanziari, solleva questioni in quanto le misure di vigilanza e le sanzioni hanno natura e finalità autonome.

L'oggetto delle sanzioni pecuniarie dell'EBA è il medesimo previsto per l'adozione di tutte le altre misure/sanzioni e costituito da condotte che violano il Regolamento, elencate negli allegati V e VI del MiCA.

Trattandosi di provvedimento a carattere punitivo, l'EBA per adottare con decisione una sanzione amministrativa e tenuta previamente ad accertare, in ossequio al "principio di colpevolezza"[478], la commissione "intenzionale[479] o per negligenza",

[476] Cfr. art. 130, comma 1, lett. *a)* e comma 2 lett. *a)*.
[477] Cfr. art. 130, comma 1, lett. *b)* e comma 2 lett. *b)*.
[478] Nell'ordinamento italiano, in materia di sanzioni amministrative pecuniarie, l'elemento soggettivo dell'illecito è disciplinato dall'art. 3 della legge n. 689 del 1981, alla cui stregua «nelle violazioni cui è applicabile una sanzione amministrativa ciascuno è responsabile della propria azione od omissione, cosciente e volontaria, sia essa dolosa o colposa». La struttura dell'illecito amministrativo, nell'ordinamento domestico, prevede che il fatto tipico, per essere concretamente punibile, oltre ad essere antigiuridico, deve essere integrato necessariamente dall'elemento soggettivo. Il dettato normativo, quindi, pone una presunzione *juris tantum* in ordine alla sussistenza della colpevolezza una volta che sia stata realizzata la condotta materiale tipica e antigiuridica; il che determina un'inversione dell'onere probatorio a carico dell'autore dell'illecito, chiamato a dimostrare l'assenza dell'elemento soggettivo. Cfr., fra le tante, Consiglio di Stato, Sez. VI, 9 maggio 2011: «una volta integrata e provata dall'Autorità la fattispecie tipica dell'illecito, graverà sul trasgressore, in virtù della presunzione di colpa che permea il sistema della responsabilità da illecito amministrativo (arg. ex art. 3 1. 24 novembre 1981, n. 689), l'onere di provare di aver agito in assenza di colpevolezza».
[479] Cfr, art. 130, comma 2, contenente una precisazione in apparenza scontata, ma volta a rimarcare la necessità che la pretesa "intenzionalità" della violazione, sia suffragata da elementi soggettivi e chiaramente dimostrativi di un dolo di intensità massima: «si considera che una violazione sia stata commessa intenzionalmente se l'EBA ha accertato elementi oggettivi che dimostrano che tale emittente o un membro del suo organo di amministrazione ha agito deliberatamente per commettere tale violazione».

da parte dell'emittente di un SART o SEMT o di un membro del suo organo di amministrazione[480].

## 1.11 *Iter* di accertamento e di adozione delle misure di vigilanza e delle sanzioni amministrative

Ove nell'ambito delle sue competenze di sorveglianza, l'EBA abbia motivi chiari e oggettivi di sospettare che sia stata o sarà commessa una violazione di cui all'allegato V o VI, potrà designare un funzionario indipendente, per eseguire le indagini necessario.

Tale funzionario, al fine di svolgere le proprie mansioni investigative in modo imparziale, non dovrà aver preso parte in precedenza alla sorveglianza degli emittenti di SART o SEMT coinvolti, né potrà partecipare, alle fasi decisionali successive dell'EBA[481]. Questa disposizione relativa a un ente investigativo indipendente rispetto alle fasi di sorveglianza e decisionali riflette i principi del "giusto processo" enunciati dalla CEDU[482].

La separazione delle funzioni investigative da quelle decisionali, nei procedimenti amministrativi sanzionatori, rappresenta un principio incorporato in vari regolamenti dell'UE e in diverse giurisdizioni nazionali[483]. Nel corso dell'indagine, il

[480] Sanzioni pecuniarie in relazione alle quali il Regolamento si limita a prevedere una soglia percentuale massima; pari, rispettivamente, per gli emittenti di SART al 12,5% e per gi emittenti di SEMT al 10% del fatturato annuo dell'esercizio precedente o al doppio dell'importo dei profitti realizzati o delle perdite evitate grazie alla violazione, ove determinabili. Cfr. art 110, comma 1, lett. *a)* e *b)*.

[481] Cfr. art. 134, comma 1 e 9.

[482] Vedi, F. CINTOLI, «*Giusto processo, CEDU e sanzioni antitrust*», in Riv. dir. proc. amm., febbraio 2015, 513 e ss. e A. BIGIARINI, «*Ne bis in idem: il cortocircuito del "doppio binario" sanzionatorio in relazione a fatti di criminalità economica*», in Dir. proc pen., 2016, 262 e ss.

[483] La funzione punitiva dei provvedimenti sanzionatori e il rispetto delle garanzie dell'equo processo rendono opportuna la previsione del Regolamento per cui l'attribuzione di funzioni istruttorie e decisorie devono essere attribuite ad organi differenti, in attuazione del principio generale per cui un soggetto non può essere al tempo stesso *judge and jury*. Nell'ordinamento domestico, per alcune autorità di vigilanza è lo stesso legislatore a prevedere una separazione tra funzioni di indagine e funzioni di giudizio, Gli artt. 187-*septies*, comma 2 e 195, comma 2, del TUF statuiscono che il procedimento sanzionatorio è retto dai principi del contraddittorio, della conoscenza degli atti istruttori, della verbalizzazione e della distinzione tra funzioni istruttorie e decisorie». Per quanto, proprio con riferimento al procedimento sanzionatorio della Consob, la Corte di Strasburgo ha riscontrato l'assenza di un'autentica ed effettiva separazione tra chi formula l'accusa e chi la giudica. V. CEDU sentenza n. 18640 del 4 marzo 2014, Caso *Grand Stevens c. Italia*: «Le delibere n. 15086/2005 e n. 18750/2013 della Consob che disciplinano le potestà sanzionatorie dell'Autorità prevedono un meccanismo di accertamento della violazione ed irrogazione del provvedimento sanzionatorio che si articola in una fase di indagine dapprima dinanzi alla Divisione competente per materia e successivamente dinanzi all'Ufficio sanzione amministrative, e di una fase decisoria dinanzi la Commissione.
Tuttavia, rimane il fatto che la divisione competente per materia, l'Ufficio sanzioni e la commissione non sono che suddivisioni dello stesso organo amministrativo, che agiscono sotto l'autorità e la supervisione di uno stesso presidente. Ciò si esprime nel consecutivo esercizio di funzioni di indagine

funzionario incaricato deve analizzare attentamente gli elementi di fatto e di diritto e valutare quelli emersi durante l'attività di sorveglianza; a tal fine, egli avrà il diritto di accedere alla documentazione dell'EBA utilizzata durante l'attività di vigilanza[484] e potrà esercitare tutti i poteri generali di indagine[485].

Dopo la conclusione della fase "istruttoria" e prima di trasmettere il fascicolo con i risultati all'EBA, verrà offerta alle persone coinvolte nell'indagine l'opportunità di essere ascoltate su questioni pertinenti.

Nel momento conclusivo della fase decisionale, prima che il procedimento sanzionatorio giunga alla sua conclusione con l'emanazione del provvedimento finale, le modalità attraverso cui si assicura la partecipazione al procedimento sanzionatorio sono principalmente due: il principio del contraddittorio e il diritto di accesso. Affinché il soggetto destinatario della sanzione possa effettivamente esercitare il suo diritto di difesa, è essenziale che egli abbia piena conoscenza di tutti gli elementi di fatto e di diritto posti dall'EBA a fondamento delle proprie conclusioni[486]. Questa conoscenza dell'ipotesi di violazione è strumentale al principio stesso del contraddittorio, poiché consente al soggetto interessato di difendersi efficacemente attraverso l'esercizio del *right to be heard*[487] prima che l'EBA assuma la propria decisione.

Il diritto di difesa in fase decisionale potrà essere però limitato in presenza della necessità di intraprendere azioni urgenti per prevenire danni ingenti e imminenti alla stabilità finanziaria o ai possessori di cripto-attività, specialmente i detentori al dettaglio. In tale circostanza eccezionale, l'EBA può adottare una decisione provvisoria, riservandosi di ripristinare il diritto di difesa delle persone interessate il prima possibile, concedendo loro nuovamente la possibilità di essere sentite.

Risulta significativa la disposizione conclusiva dell'articolo 134, che impone all'EBA di astenersi dall'irrogare sanzioni amministrative pecuniarie o penalità di mora se è a conoscenza di una precedente sentenza di assoluzione o condanna, riguardante fatti identici o sostanzialmente analoghi, passata in giudicato in esito a un procedimento penale di diritto interno[488].

---

e di giudizio in seno ad una stessa». In B. RAGANELLI, «*Sanzioni Consob e tutela del contraddittorio procedimentale*», GIORNALE DI DIRITTO AMMINISTRATIVO, fasc. 4 (2015): 517.

[484] Cfr. art. 134, comma 4.

[485] Cfr. art. 134, commi 2 e 3.

[486] Cfr. art. 135, comma 1.

[487] Cfr. art. 135, comma 1.

[488] Cfr. art. 134, comma 11, secondo periodo.

La previsione normativa di un "obbligo di astensione" in capo all'EBA in presenza di un giudicato penale interno per un *idem factum* (fatto storico-naturalistico) comporta l'applicazione *ex lege*, anche alle sanzioni amministrative pecuniarie e penalità di mora relative agli emittenti di SART e SEMT, del divieto di fonte eurounitaria e convenzionale del *bis in idem* processuale[489].

Tale divieto opera non solo in riferimento a uno stesso fatto-reato, ma anche, secondo una interpretazione consolidata, a un *idem factum* sanzionato sia penalmente che da misure punitive irrogate da Autorità di vigilanza che rivestano una connotazione penale[490]. La previsione del MiCA riflette pertanto la consolidata giurisprudenza europea, secondo cui il rispetto del principio del *ne bis in idem* processuale, sancito dall'articolo 50 della Carta di Nizza, non vieta di sanzionare lo stesso fatto con diverse misure, ma richiede che ciò avvenga in un unico procedimento o attraverso procedimenti coordinati, ostacolando la possibilità di procedere quando nei confronti del destinatario è stata emessa una sentenza penale definitiva[491].

## 1.12 Il ruolo determinante degli atti delegati nel Regolamento MiCA

Per cogliere appieno l'importanza degli atti delegati nel garantire l'efficacia normativa, preme fare riferimento a principi fondanti del diritto europeo. In particolare, l'art. 290 del Trattato sul Funzionamento dell'Unione Europea stabilisce che un atto legislativo può delegare alla Commissione europea il potere di adottare atti non legislativi di portata generale che integrano o modificano specifici elementi non essenziali dell'atto legislativo.

Mentre gli elementi essenziali di un settore restano riservati all'atto legislativo e non possono essere delegati, quest'ultimo deve stabilite chiaramente gli obiettivi, il

[489] Cfr. artt. 50 CDFUE e 4 Prot. 7 CEDU Cfr. In particolare, l'art. 50 della Carta dei diritti fondamentali dell'Unione europea recita: «Nessuno può essere perseguito o condannato per un reato per il quale è già stato assolto o condannato nell'Unione a seguito di una sentenza penale definitiva conformemente alla legge»; in senso analogo, l'art. 4 del protocollo n. 7 della CEDU: «Nessuno può essere perseguito o condannato penalmente dalla giurisdizione dello stesso Stato per un reato per il quale è già stato assolto o condannato a seguito di una sentenza definitiva conformemente alla legge ed alla procedura penale di tale Stato».

[490] Cfr. M. VENTORUZZO, «*Abusi di mercato, sanzioni Consob e diritti umani: il caso Grande Stevens e altri c. Italia*», rivista delle società, 2014, 693 e ss.

[491] Cfr. fra le altre, Corte di Giustizia dell'Unione Europea, 26 febbraio 2013, *Aklagaren c. Hans Akerberg Fransson*, causa C-617/10. In dottrina, M. L. DI BITONTO, «*Il ne bis in idem nei rapporti tra infrazioni finanziarie e reati*» in Cassazione Penale, fasc. 4, 2016, p. 1335; B. LAVARINI, «*Corte europea dei diritti dell'uomo e ne bis in idem: la crisi del "doppio binario" sanzionatorio*», in Dir. pen. proc., 2014, suppl. n. 12, p. 82 ss.

contenuto, la portata e la durata della delega di potere. Questo determina le condizioni della delega, e della revoca della stessa su decisione del Parlamento europeo o del Consiglio e anche l'entrata in vigore dell'atto delegato, subordinata all'assenza di obiezioni da parte del Parlamento europeo o del Consiglio entro un termine stabilito.

Analizzando il complesso normativo del regolamento in questione ed i considerando, emerge come il legislatore europeo abbia deciso di delegare alla Commissione il potere di adottare atti delegati in base all'art. 290 TFUE, con il chiaro obiettivo di garantirne l'efficacia[492].

La delega e l'adozione dei relativi atti sono cruciali per specificare ulteriormente gli elementi tecnici delle definizioni inserite nel regolamento, in modo da adeguarli agli sviluppi tecnologici e del mercato.

Non solo, ma essi sono altresì necessari per specificare determinati aspetti, come i criteri utili, ad esempio, per stabilire se un *token* collegato ad attività o un *token* di moneta elettronica debba essere classificato come significativo. Questi atti delegati sono fondamentali anche per determinare quando vi sia un timore significativo in materia di tutela degli investitori o per il corretto funzionamento e l'integrità dei mercati delle cripto-attività o per la stabilità del sistema finanziario dell'Unione.

Gli atti delegati risultano altrettanto essenziali per specificare le norme procedurali che regolano l'esercizio del potere dell'EBA di imporre sanzioni amministrative pecuniarie o penalità di mora, comprese le disposizioni sui diritti della difesa, le tempistiche e la riscossione delle sanzioni. Infine, sono cruciali per specificare ulteriormente il tipo e l'importo delle commissioni di vigilanza che l'ABE può imporre agli emittenti di *token* collegati ad attività significative o di *token* di moneta elettronica significativi.

L'articolo 139 del presente Regolamento costituisce la disposizione preposta per delineare i limiti dell'esercizio della delega di poteri, che è conferita alla Commissione alle condizioni ivi specificate, per un periodo di 36 mesi, a partire dalla data di entrata in vigore del regolamento.

Almeno nove mesi prima della scadenza di tale periodo, la Commissione è tenuta a redigere una relazione in merito. Occorre sottolineare che la delega di poteri è tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga, al massimo tre mesi prima della scadenza di ciascun periodo.

[492] Si veda il considerando 108 del Regolamento.

Conformemente alla previsione normativa esplicita, la Commissione è investita del potere di adottare gli atti delegati menzionati negli articoli 3, comma 2, 43, comma 11, 103, comma 8, 104, comma 8, 105, comma 7, 134, comma 10, e 137, comma 3 del Regolamento. Tuttavia, è anche importante evidenziare che l'articolo 139 del Regolamento stabilisce anche la possibilità di revocare la delega di potere in qualsiasi momento da parte del Parlamento europeo o del Consiglio. La decisione di revoca comporta inequivocabilmente la cessazione della delega di potere, come indicato nella decisione, con effetti che decorrono dal giorno successivo alla sua pubblicazione nella Gazzetta Ufficiale dell'Unione Europea o dalla data successiva ivi specificata; tale decisione non pregiudica la validità degli atti delegati già in vigore.

Per quanto riguarda la procedura di adozione degli atti delegati, una volta che l'atto è stato adottato, la Commissione è tenuta a notificarlo tempestivamente al Parlamento europeo e al Consiglio. Inoltre, l'atto delegato, entra in vigore solo in assenza di obiezioni da parte del Parlamento europeo e del Consiglio entro un periodo di tre mesi dalla data in cui è stato loro notificato o se, prima della scadenza di tale termine, il Parlamento europeo e il Consiglio informano la Commissione della loro intenzione di non sollevare obiezioni. Tale termine può essere prorogato di tre mesi su iniziativa del Parlamento europeo o del Consiglio.

La Commissione europea è incaricata altresì di precisare il contenuto e il formato delle informazioni che le autorità competenti devono fornire almeno due volte all'anno all'EBA e alla BCE[493] ai fini della valutazione sui criteri sopra menzionati. Questa disposizione si estende anche alle informazioni trasmesse trimestralmente dall'emittente all'autorità competente riguardo ai *token* collegati ad attività di valore superiore a 100.000.000 euro.

In aggiunta, conformemente all'articolo 103, comma 8, la Commissione è chiamata a adottare atti delegati per integrare il regolamento al fine di precisare i criteri ed i fattori che l'ESMA è tenuta a considerare nel determinare l'esistenza di un timore significativo in materia di tutela degli investitori o di una minaccia all'ordinato funzionamento e all'integrità dei mercati delle cripto-attività o alla stabilità finanziaria dell'Unione.

Questi interventi dell'ESMA, tra cui divieti o limitazioni temporanee di determinate attività legate alle cripto-attività, sono condizionati al soddisfacimento di tutti i requisiti previsti dal comma 2, lettera a), dell'articolo 103. Lo stesso principio si

[493] A norma del comma 4 del presente articolo, e dell'art. 56, comma 3.

applica all'articolo 104, comma 8, che prevede che la Commissione deve adottare atti delegati per specificare gli elementi che l'EBA deve considerare nel determinare se vi sia un timore significativo in materia di tutela degli investitori o di minaccia all'ordinato funzionamento e all'integrità dei mercati delle cripto-attività o alla stabilità finanziaria dell'Unione.

Ancora, l'articolo 105, comma 7, stabilisce che la Commissione deve adottare atti delegati per integrare il regolamento definendo i criteri e i fattori che le autorità competenti devono considerare nel determinare la presenza di un timore significativo in materia di tutela degli investitori o di una minaccia all'ordinato funzionamento e all'integrità dei mercati delle cripto-attività o alla stabilità finanziaria di almeno uno Stato membro, ai fini del comma 2, lettera *a)*.

Inoltre, l'articolo 134, comma 10, prevede che la Commissione debba adottare atti delegati entro 12 mesi dall'entrata in vigore del regolamento per integrarlo in materia di imposizione di sanzioni amministrative pecuniarie o penalità di mora, comprese le disposizioni sui diritti della difesa, le disposizioni temporali, le disposizioni sulla riscossione delle sanzioni amministrative pecuniarie o delle penalità di mora e sui termini di applicazione delle stesse. L'articolo 134 riguarda in particolare l'indagine condotta da un funzionario nominato dall'ABE nel caso in cui vi siano chiari e dimostrabili motivi di sospettare che sia stata o sarà commessa una violazione da parte di un emittente, che potrebbe portare all'adozione di una misura di vigilanza o a una sanzione amministrativa pecuniaria.

Infine, l'articolo 137, comma 3, impone alla Commissione di adottare atti delegati entro 12 mesi dall'entrata in vigore del regolamento per integrarlo in tema di commissioni economiche applicabili, sulle fattispecie per cui sono esigibili, sull'importo e sulle modalità di pagamento, nonché sulla metodologia per calcolare l'importo massimo dovuto per soggetto che può essere irrogato dall'ABE [494]. Queste commissioni vanno a coprire i costi sostenuti dall'ABE nelle sue attività di vigilanza sugli emittenti, come anche i rimborsi dei costi eventualmente sostenuti dalle autorità competenti nell'adempimento delle attività loro delegate dall'ABE[495].

Il legislatore europeo ha anche previsto che la Commissione, prima dell'emanazione dell'atto delegato, sia tenuta a consultare esperti designati da ciascuno Stato membro, nel rispetto dei principi stabiliti nell'accordo interistituzionale

[494] Cfr. art .137, comma 2.
[495] Ai sensi dell'art 138 del regolamento.

"Legiferare meglio" datato 13 aprile 2016; stipulato tra il Parlamento europeo, il Consiglio dell'Unione europea e la Commissione europea, con l'obiettivo di garantire una cooperazione leale e trasparente per l'intero processo legislativo.

Nel caso in cui sia richiesta una conoscenza più approfondita, la Commissione dovrebbe rivolgersi a gruppi di esperti, coinvolgere specifici portatori di interesse e condurre consultazioni pubbliche, secondo le circostanze.

Il legislatore europeo ha quindi sviluppato il presente regolamento rispettando questi principi, ritenendo essenziale che la Commissione conduca consultazioni adeguate durante la fase preparatoria. Al fine di garantire la parità di partecipazione nella preparazione degli atti delegati, il Parlamento europeo ed il Consiglio ricevono contemporaneamente i documenti agli esperti degli Stati membri, e gli esperti delle istituzioni europee hanno accesso alle riunioni pertinenti dei gruppi di esperti della Commissione.

Concludendo, sono rilevanti le considerazioni espresse dal legislatore europeo riguardo ai poteri delegati assegnati alla Commissione in merito a questo Regolamento. Viene attribuita considerevole importanza alla specifica dei contenuti normativi, fino ad arrivare alla possibilità di prorogare la data di applicazione del regolamento, che potrebbe essere rinviata al fine di consentire l'adozione delle norme tecniche di regolamentazione, delle norme tecniche di attuazione e degli atti delegati necessari per precisare taluni elementi del presente regolamento.[496]

Non sorprende, quindi, che il legislatore preveda un dettagliato conferimento di poteri alla Commissione per l'adozione di norme tecniche di regolamentazione elaborate dall'EBA e dall'ESMA[497].

---

[496] Considerando n. 119.

[497] Ciò riguarda specificamente: *a)* Il contenuto, le metodologie e la presentazione delle informazioni contenute in un *White Paper* sulle cripto-attività, focalizzandosi sui principali impatti negativi sul clima e altri effetti negativi legati all'ambiente del meccanismo di consenso utilizzato per emettere le cripto-attività, nonché la procedura di approvazione dei *White Paper* presentati dagli enti creditizi al momento dell'emissione di *token* collegati ad attività. *b)* Le informazioni contenute nella domanda di autorizzazione per l'emissione di *token* collegati ad attività. *c)* La metodologia utilizzata per stimare il numero trimestrale medio e il valore aggregato medio delle operazioni giornaliere associate a usi di *token* collegati ad attività e *token* di moneta elettronica denominati in una valuta diversa da quella di uno Stato membro come mezzo di scambio in ciascuna area monetaria unica. *d)* I requisiti, modelli e procedure per la gestione dei reclami dei possessori di *token* collegati ad attività e dei clienti dei prestatori di servizi per le cripto-attività, insieme ai requisiti per le politiche e le procedure volte a identificare, prevenire, gestire e comunicare i conflitti di interesse degli emittenti di *token* collegati ad attività, includendo dettagli e metodologia per il contenuto di tale comunicazione. *e)* La procedura e i tempi per l'adeguamento di un emittente di *token* collegati ad attività e di *token* di moneta elettronica significativi ai requisiti di fondi propri più elevati, i criteri per richiedere fondi propri più elevati, i requisiti minimi per l'elaborazione dei programmi relativi agli *stress test*, i requisiti di liquidità della riserva di attività e gli strumenti finanziari in cui può essere investita la riserva di attività. *f)* Il contenuto dettagliato delle informazioni necessarie per valutare il progetto di acquisizione della partecipazione

## 1.13 Regime sanzionatorio e rapporti con l'ordinamento giuridico nazionale

Il Regolamento, da un primo sguardo, presenta apparentemente una struttura sanzionatoria; Come è stato analizzato, si tratta di un regolamento dalle maglie ampie, che sottolinea altresì un marcato ruolo della *soft law*[498]. Pertanto, se in generale il ruolo di questa fonte sembra più affine ad una direttiva che a un regolamento, ossia una norma che assegna a soggetti diversi compiti senza definire condotte, precetti e sanzioni specifiche, il contesto sanzionatorio si presenta alquanto problematico.

Come si è visto, trovano applicazione in materia sanzionatoria, i principi europei convenzionali e quelli dell'Unione, recepiti dalla CEDU in materia di sanzioni.

Si fa riferimento soprattutto agli articoli 6 e 7 della Convenzione CEDU, che richiamano i principi tradizionali di legalità, tassatività e tipicità, sia delle fattispecie illecite che delle relative sanzioni.

Questo Regolamento, richiede un elevato grado di garanzie, come evidenziato nei considerando 6 e 9, che sottolineano rispettivamente la necessità di un elevato livello di tutela ed il principio di neutralità sotteso al Regolamento; in modo da evitare

---

qualificata in un emittente di *token* collegati ad attività. *g)* I requisiti per gli obblighi aggiuntivi per gli emittenti di *token* collegati ad attività significativi. *h)* Le informazioni notificate alle autorità competenti da enti creditizi, depositari centrali di titoli, imprese di investimento, gestori del mercato, istituti di moneta elettronica, società di gestione di OICVM e gestori di fondi di investimento alternativi che intendono prestare servizi per le cripto-attività. *i)* Le informazioni contenute in una domanda di autorizzazione del prestatore di servizi per le cripto-attività. *l)* Il contenuto, le metodologie e la presentazione delle informazioni che il prestatore di servizi per le cripto-attività mette a disposizione del pubblico relative ai principali impatti negativi sul clima e altri effetti negativi legati all'ambiente del meccanismo di consenso utilizzato per emettere ciascuna cripto-attività. *m)* Le misure per garantire la continuità e la regolarità della prestazione dei servizi per le cripto-attività e le registrazioni da mantenere per tutti i servizi per le cripto-attività, gli ordini e le operazioni effettuati. *n)* I requisiti per le politiche volte a identificare, prevenire, gestire e comunicare i conflitti di interesse dei prestatori di servizi per le cripto-attività, insieme ai dettagli e alla metodologia per il contenuto di tale comunicazione. o) Il modo in cui devono essere presentati i dati sulla trasparenza del gestore di una piattaforma di negoziazione e il contenuto e il formato delle registrazioni nel *book* di negoziazione relativi alla piattaforma di negoziazione. *p)* Il contenuto dettagliato delle informazioni necessarie per valutare il progetto di acquisizione della partecipazione qualificata in un prestatore di servizi per le cripto-attività. *q)* I dispositivi, sistemi e procedure adatti per monitorare e individuare gli abusi di mercato, il modello di notifica per la segnalazione di sospetti di abusi di mercato e le procedure di coordinamento tra le autorità competenti per l'individuazione di abusi di mercato. *r)* Le informazioni che le autorità competenti sono tenute a scambiarsi. *s)* Un modello di documento per gli accordi di cooperazione tra le autorità competenti degli Stati membri e le autorità di vigilanza di paesi terzi. *t)* I dati necessari per la classificazione dei *White Paper* sulle cripto-attività nel registro dell'ESMA e le modalità pratiche per assicurare che tali dati siano leggibili meccanicamente. Le condizioni alle quali taluni membri del collegio delle autorità di vigilanza per gli emittenti di *token* collegati ad attività significativi e gli emittenti di *token* di moneta elettronica significativi sono da considerare come i più rilevanti nella loro categoria, le condizioni alle quali si ritiene che i *token* collegati ad attività o i *token* di moneta elettronica siano utilizzati su larga scala ai fini della qualifica di taluni membri di tale collegio e i dettagli delle modalità pratiche di funzionamento di tale collegio.

[498] M. PERASSI, «*Il Regolamento MiCA nel contesto della disciplina bancaria e dei servizi di pagamento*» (Centro Convegni Carlo Azeglio Ciampi, Roma: BANCA D'ITALIA, 2023).

disomogeneità di tutela tra gli ordinamenti giuridici degli Stati membri che possa determinare una concorrenza basata su regimi sanzionatori più o meno favorevoli[499].

Premesso che la definizione del sistema sanzionatorio, delle violazioni, delle sanzioni e dei relativi procedimenti rientra nella competenza dei legislatori nazionali, nel presente contesto, emergono diverse tematiche, a partire dal tema dei principi di legalità e identificazione delle fattispecie illecite.

L'articolo 111, al primo comma, dovrebbe individuare tutte le fattispecie illecite, ma la tecnica utilizzata dal legislatore europeo consiste nel delineare le violazioni in relazione agli articoli "almeno"[500] da 4 a 14, da 16 a 25, da 27 a 41 e 46, 47 rendendo praticamente ogni violazione del Regolamento un illecito amministrativo. Tale formulazione entra in conflitto con l'articolo 7 della CEDU[501], che prevede il principio del "*nullum crimen sine lege*", sia per le sanzioni penali che amministrative[502].

È chiara l'esigenza di un ulteriore intervento normativo non solo a livello nazionale ma anche a livello sovranazionale, che coinvolga le diverse autorità.

Ad esempio, l'articolo 31 attribuisce al 5° comma all'EBA e all' ESMA la cooperazione nella stesura di norme tecniche di regolamentazione. Le stesse norme tecniche sono richieste per molte disposizioni successive, come l'articolo 32 e l'articolo 34.

Dall'analisi di queste disposizioni emerge la complessità delle relazioni tra le disposizioni del Regolamento, le norme tecniche da elaborare e la norma nazionale che, recependo il regolamento e assegnando la necessaria copertura della riserva di legge, necessario per un potere sanzionatorio, individui l'illecito norma per norma mediante l'integrazione di una fonte non normativa ordinaria ma riconducibile alla regola tecnica. Ciò è possibile, ma richiede un considerevole lavoro di recepimento e attuazione.

---

[499] Questo è un caso tipico in cui la severità di una sanzione e l'efficacia del regime sanzionatorio possono influenzare gli spostamenti nei mercati a discapito degli Stati membri più rigorosi. Cfr. A. ZOPPINI, «*La concorrenza tra ordinamenti giuridici*», vol. 68, Percorsi (Laterza, 2004).

[500] Cfr. art. 111, comma 1.

[501] "1. Nessuno può essere condannato per una azione o una omissione che al momento in cui fu commessa non costituisse reato secondo il diritto interno o secondo il diritto internazionale. Non può del pari essere inflitta alcuna pena superiore a quella che era applicabile al momento in cui il reato è stato commesso. 2. Il presente articolo non ostacolerà il rinvio a giudizio e la condanna di una persona colpevole d'una azione o d'una omissione che, al momento in cui fu commessa, era criminale secondo i princìpi generali di diritto riconosciuti dalle nazioni civili."

[502] A. POLICE, «*Lo speciale regime sanzionatorio di MiCA applicabile agli emittenti di ARTs e EMTs*» (Il Regolamento MiCA nel contesto della disciplina bancaria e dei servizi di pagamento, Centro Convegni Carlo Azeglio Ciampi, Roma: BANCA D'ITALIA, 29 settembre 2023).

L'art. 111, comma 2 e 3, delineando la tipologia di sanzioni e l'entità delle pene e delle ammende, stabilisce tetti massimi ma non minimi; questa mancanza di limiti minimi è manifestamente problematica se l'obiettivo è quello di garantire il massimo livello di tutela e l'omogeneità della stessa tra i paesi membri[503].

Se consideriamo " le altre misure" alla stregua di sanzioni accessorie, si pone il problema della tipicità, della tassatività e della riserva di legge, presupposto indispensabile per l'esercizio di questo potere, non solo in questo ordinamento ma in tutti quelli dell'Unione.

Il tema delle "altre misure" è caratterizzato dall'assenza di indicazioni di criteri per l'imposizione di tali misure, a meno che non si legga attentamente l'*incipit* del primo e secondo paragrafo dell'articolo 112, secondo cui, quando si tratta dell'esercizio di poteri di vigilanza e sanzionatori, sia le sanzioni che le altre misure sono adottate sempre con gli stessi criteri impiegati per l'irrogazione delle sanzioni. Pertanto, sanzioni e misure accessorie alle sanzioni dovrebbero godere dello stesso regime sostanziale di tipicità della fattispecie e condotta illecite, così come della tipicità della sanzione prevista per ciascun illecito, e conseguentemente del procedimento per l'esercizio del potere sanzionatorio.

Per quanto riguarda il procedimento, vige l'articolo 6 della CEDU, recepito nell'ordinamento dell'Unione e nazionale, il quale stabilisce tutte le garanzie procedimentali minime. I modelli, i criteri e le regole previsti per l'esercizio della potestà sanzionatoria amministrativa in altri ambiti potrebbero essere trasposti per il modello procedimentale da seguire, individuando l'autorità competente per l'esercizio di questo potere con tutte le garanzie procedimentali proprie delle sanzioni amministrative.

È opportuno sottolineare lo specifico regime sulla pubblicazione delle decisioni, di cui all'articolo 114; la decisione che impone sanzioni o altre misure alternative per una violazione del presente regolamento deve essere pubblicata. Anche queste forme di pubblicità costituiscono un ulteriore chiaro riflesso del carattere afflittivo di sanzioni e altre misure, e dimostra che anche queste ultime godono delle stesse garanzie di tipo sostanziale e procedimentale.

In questo contesto, si pone naturalmente anche il tema dei parametri nell'esercizio della potestà sanzionatoria della pubblica amministrazione. Mentre

[503] La previsione dell'articolo 112, paragrafo 1, che individua i criteri per la decisione sulla determinazione della sanzione, non affronta appieno questa problematica. *Ibidem*.

l'illecito potrà essere definito, si pone il tema di quegli *standard* tecnici, la cui mutevolezza e possibile variabilità nel tempo sollevano anche la questione della scelta del regime giuridico applicabile alla fattispecie oggetto della sanzione. Questo è un tema delicato che occorrerà tenere in conto nel recepimento.

Vi sono poi altri due temi da considerare: da un lato, il rapporto tra l'esercizio della potestà sanzionatoria, di competenza degli Stati membri e delle autorità amministrative individuate a livello nazionale, e la cooperazione richiesta dall'articolo 115 del regolamento. Il regolamento, infatti, sin dai primi considerando, richiede una forma intensa di cooperazione tra il livello europeo e le diverse autorità nazionali.

L'articolo 115 prevede la segnalazione delle sanzioni amministrative e delle altre misure ad ESMA e EBA. Questo determina un effetto aggiuntivo significativo piuttosto nuovo rispetto alle tipiche sanzioni amministrative di livello nazionale. La comunicazione sulle infrazioni diventa così parte integrante di questa collaborazione, al fine di migliorare l'attività di regolamentazione di queste Autorità.

Più volte la dottrina giuspublicista ha dimostrato come le sanzioni costituiscano uno strumento di regolazione; in particolare quando alcune autorità regolano esclusivamente attraverso le sanzioni, come nel caso delle autorità *antitrust*[504].

In questo caso, la potestà sanzionatoria degli Stati membri alimenta l'attività di regolamentazione, almeno per la definizione degli *standard* tecnici, che si evolvono velocemente. Si evidenzia così il collegamento tra potere sanzionatorio e potere di regolazione, con rilevanti ricadute pratiche.

Un'attenzione particolare infine va dedicata al tema delle impugnazioni, anch'esso trattato dall'articolo 113 del regolamento il quale, nel clima di neutralità delle scelte del legislatore europeo rispetto alle tutele giurisdizionali, lascia all'ordinamento nazionale la scelta delle tutele, prevedendo esclusivamente il diritto all'impugnazione.

[504] Cfr. per un maggiore approfondimento: *G. LEGNINI, P. MOROSINI, «Le giurisdizioni e le autorità indipendenti»* (Consiglio Superiore della Magistratura, 2018), https://www.csm.it/documents/21768/41479/Le+giurisdizioni+e+le+autorit%C3%A0+indipendenti/4c3a6fce-720e-0df7-b993-ddbdd7d7a497.

## 2. Prevenzione degli abusi di mercato relativi alle cripto-attività

### 2.1 Introduzione ed ambito applicativo

In tema di abusi di mercato, le cripto-attività presentano sia rischi comuni ad altre attività economiche tradizionali che aspetti peculiari. Si pensi in particolare, all'*insider trading*, caso in cui un vantaggio operativo derivante dall'asimmetria informativa può tradursi in un profitto per chi detiene informazioni privilegiate, direttamente o indirettamente.

Fino ad oggi, le piattaforme di *trading* di cripto-attività presentano caratteristiche peculiari, essendo strutture private non sottoposte al controllo di autorità di vigilanza, spesso di dimensioni ridotte[505] e con operatori perlopiù anonimi. Queste peculiarità facilitano comportamenti abusivi e manipolativi rispetto ai mercati tradizionali, complicando l'individuazione e la repressione dei soggetti responsabili. Da ciò scaturisce la decisione di dedicare una sezione specifica di MiCA alla prevenzione e al divieto degli abusi di mercato[506], come delineato nel Titolo VI negli articoli dall'86 al 92 del Regolamento.

L'analisi dei considerando di MiCA evidenzia i punti focali che hanno guidato il legislatore europeo, ovvero la salvaguardia dell'integrità del mercato[507] insieme alla volontà politica di favorire lo sviluppo del settore[508].

---

[505] Se paragonati ai mercati regolamentari tradizionali.

[506] Il considerando n. 95 al Regolamento afferma: «E 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 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 degli utenti 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. Tali norme specifiche per gli abusi di mercato commessi in relazione alle cripto-attività dovrebbero essere applicate anche nei casi in cui le cripto-attività sono ammesse alla negoziazione».

[507] Si veda, in particolare, il considerando n. 4, in cui è affermato che «l'assenza di tali norme fa sì che i possessori di tali cripto-attività siano esposti a rischi, in particolare nei settori non disciplinati dalle norme in materia di tutela dei consumatori. L'assenza di tali norme può anche comportare rischi sostanziali per l'integrità del mercato, anche in termini di abuso di mercato e di criminalità finanziaria».

[508] Si veda il considerando n. 5: «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».

Per quanto possibile, il legislatore europeo ha replicato la normativa esistente in materia di mercati finanziari, privilegiando l'approccio preventivo rispetto a quello repressivo. In particolare, tanto sul piano delle definizioni che su quello delle condotte vietate, è agevole rilevare il tendenziale adattamento alle cripto-attività delle disposizioni esistenti nella *Market Abuse Regulation* (MAR)[509] e nella *Market Abuse Directive* (MAD)[510] in materia di strumenti finanziari.

Questa scelta è giustificata dal principio di proporzionalità, considerando l'evoluzione del settore delle cripto-attività[511] e la necessità di legiferare prima rispetto ad altri Paesi. Il richiamo diretto di MAR e MAD da parte degli emittenti e fornitori di servizi in materia di cripto-attività sarebbe stato probabilmente troppo gravoso in termini di oneri organizzativi, strutturali e regolatori per un settore in via di sviluppo[512].

Il Regolamento prevede un intervento sanzionatorio amministrativo sugli abusi di mercato in cripto-attività, lasciando ai Paesi membri la scelta di adottare eventuali misure di diritto penale. Tuttavia, è auspicabile che, per una tutela efficace del mercato delle cripto-attività e per garantire coerenza con il mondo degli strumenti finanziari, il legislatore europeo valuti interventi legislativi ulteriori, eventualmente attraverso direttive, che inducano gli Stati membri a prevedere sanzioni penali per le violazioni delle disposizioni sugli abusi di mercato. Per quanto concerne l'ambito di applicazione del Titolo VI di MiCA, l'articolo 86 stabilisce confini di carattere concettuale, di applicazione pratica e territoriale.

Sotto il primo aspetto, il primo paragrafo dell'articolo 86 stabilisce che il Titolo VI si applica a tutti gli atti compiuti da qualsiasi individuo relativamente alle cripto-attività ammesse alla negoziazione o in relazione alle quali è stata presentata una richiesta di ammissione alla negoziazione. Tale disposizione anticipa la soglia di tutela anche alle cripto-attività per le quali è stata presentata una richiesta di ammissione alla negoziazione, seguendo un approccio analogo a quanto previsto dall'articolo 2, comma 1, lettere *a)* e *b)* del Regolamento MAR per gli strumenti finanziari. Tale scelta

[509] Regolamento 596/2014.
[510] Direttiva 2014/57/UE, recepita nell'ordinamento italiano con il D.Lgs. 10 agosto 2018 n. 107.
[511] «la gran parte degli emittenti e dei fornitori di servizi in materia di cripto-attività sono piccole e medie imprese» in C. GORTSOS, «*The Commission's 2020 Proposal for a Markets in Crypto-Assets Regulation ('MiCAR'): A Brief Introductory Overview*», SSRN Scholarly Paper (Rochester, NY, 7 maggio 2021), https://doi.org/10.2139/ssrn.3842824.
[512] M. BENCINI, L. FANFANI, «*Prevenzione degli abusi di mercato relativi alle criptoattività*», in *Crypto-asset: Regolamen to MiCA e DLT Pilot Regime. Analisi ragionata su token, stablecoin, CASP* (Giuffrè Francis Lefebvre, s.d.), 249 e ss.

è giustificata, dall'esigenza di garantire una tutela effettiva anche nelle fasi precedenti alla negoziazione propriamente detta.

Dal punto di vista dell'applicabilità, il secondo paragrafo dell'articolo 86 stabilisce che le norme del Titolo VI si applicano a qualsiasi operazione, ordine o condotta, indipendentemente dalla sua esecuzione in una piattaforma di negoziazione. Questa estensione dell'applicazione al di fuori delle piattaforme di negoziazione è mirata a prevenire possibili tentativi di elusione delle norme finalizzate a contrastare gli abusi di mercato in riferimento alle cripto-attività.

Il terzo paragrafo dell'articolo 86, infine, disciplina l'ambito territoriale, stabilendo che il Titolo VI del Regolamento trova applicazione alle azioni e omissioni riguardanti le cripto-attività menzionate nel paragrafo 1, sia nell'Unione Europea che nei Paesi terzi.

## 2.2 La nozione di informazioni privilegiate con riferimento alle cripto-attività

L'articolo 87 del Regolamento propone la definizione di "informazioni privilegiate" in gran parte in linea con l'articolo 7 del Regolamento MAR[513], adattandola al contesto specifico delle cripto-attività.

Ai sensi di MiCA, le informazioni privilegiate sono quelle informazioni precise, non rese pubbliche, che riguardano direttamente o indirettamente uno o più emittenti, offerenti o coloro che chiedono l'ammissione alla negoziazione di cripto-attività, ovvero informazioni relative a una o più cripto-attività che, ove rese pubbliche, potrebbero avere un effetto significativo sui prezzi di tali cripto-attività o su cripto-attività collegate.

Nel caso di persone incaricate dell'esecuzione di ordini per conto di clienti, sono considerate informazioni privilegiate anche le informazioni precise trasmesse da un cliente e relative ai propri ordini pendenti in cripto-attività, che possono riguardare emittenti, offerenti o soggetti che chiedono l'ammissione alla negoziazione.

Gli elementi maggiormente significativi della nozione sono quindi la precisione e la non pubblicità dell'informazione, nonché la sua *price sensitivity*. Altro aspetto meritevole di attenzione è la suddivisione tra i c.d. *insider* primari o secondari, vale a

[513] Per una analisi approfondita sull'argomento, cfr. M. BENCINI, L. FANFANI, S. PELLIZZARI, V. TODINI, «*Profili penali della tutela del risparmio : truffa, abusi di mercato e gestione patrimoniale»* (Giuffrè Francis Lefebvre, 2021) cap. 3.

dire coloro che vengono a conoscenza di un'informazione privilegiata per ragioni professionali.

Il secondo comma dell'articolo 87, precisa che le informazioni sono considerate precise se fanno riferimento a circostanze esistenti o ragionevolmente previste, o a eventi accaduti o ragionevolmente prevedibili; esse devono essere sufficientemente specifiche da consentire di trarre conclusioni sull'effetto potenziale di tali circostanze o eventi sui prezzi delle cripto-attività. Questa nozione è in linea con quanto stabilito dall'articolo 7, comma 2, del Regolamento MAR. In altre parole, le informazioni devono riferirsi a circostanze o eventi già verificatisi o probabili[514].

La notizia deve possedere anche un grado di dettaglio tale da renderla "sufficientemente specifica", cioè precisa e dettagliata al punto da fornire elementi di valutazione affidabili e utilizzabili nell'ottica di un investimento. Gli eventi, le circostanze e gli elementi devono essere caratterizzati da un certo grado di oggettività e certezza, affinché sia possibile trarre conclusioni sull'effetto potenziale di questo complesso di circostanze o di tale evento sui prezzi delle cripto-attività.

Al di fuori della definizione di "informazione precisa" rientrano le notizie troppo vaghe e non supportate da dati oggettivi, come voci di mercato e *rumors*, nonché le "*very soft information*"[515], ovvero "previsioni di natura soggettiva o meramente congetturali riguardanti eventi e circostanze possibili ma improbabili"[516]. La loro influenza sui prezzi delle cripto-attività non sarebbe ragionevolmente prevedibile, come chiarito anche dalla giurisprudenza[517], anche se con riferimento agli strumenti finanziari.

Rilevanti possono essere anche le informazioni parziali o incomplete relative a una singola fase di un processo decisionale prolungato, come nel caso delle informazioni legate alle fasi intermedie dell'autorizzazione di un *white paper*.

Il concetto di sviluppo progressivo delle informazioni, già trattato dalla Corte di Giustizia dell'Unione Europea nel caso Daimler[518], è stato introdotto anche nel MAR.

---

[514] Cfr. F. MUCCIARELLI, «*L'insider trading della nuova disciplina del D.lgs 58/98*»,in Riv. trim. dir. pen. ec. 2000, 935. e F. SGUBBI, «*Il risparmio come oggetto di tutela penale*», in Giur. comm. 2009, 349 e ss.

[515] F. MUCCIARELLI, «*L'insider trading nella rinnovata disciplina UE sugli abusi di mercato*», in Soc. 2016, 193.

[516] E. AMATI, «*Abusi di mercato e sistema penale*», Torino, 2012, 91. E S. GIAVAZZI, «*l'abuso di informazioni privilegiate*» in Diritto penale delle società, I, Padova 2014, 702.

[517] Cfr. Cass. Pen., 7 dicembre 2012, n. 49362, in CED, rv.254063.

[518] Corte di Giustizia dell'Unione Europea, sez. II, 28 giugno 2012, Markus Geltl vs. Daimler AG (C-19/11). Per un commento della sentenza si rinvia a S. LOMBARDO, «*Acquisto di partecipazioni di controllo, fattispecie a formazione progressiva, informazione privilegiata e insider secondario*», in Soc., 2014, 707 ss.

Secondo questo principio, se la realizzazione di una particolare circostanza o evento futuro richiede un processo prolungato per concretizzarsi, le tappe intermedie di tale processo possono essere considerate informazioni precise e, in presenza degli altri requisiti, costituiscono informazioni privilegiate. Questo principio è stato integrato nell'articolo 87, comma 1, di MiCA.

Per qualificarsi come "privilegiata" ai sensi della disposizione in commento, l'informazione non deve essere di pubblico dominio. Si considera di pubblico dominio la notizia alla quale il pubblico ha avuto la concreta possibilità di accedere, indipendentemente dal fatto che sia stata formalmente comunicata o che il pubblico l'abbia effettivamente conosciuta[519].

La verifica dell'effettiva accessibilità dell'informazione privilegiata è strettamente legata alle modalità con cui essa è reperibile. Pertanto, il carattere "pubblico" dell'informazione è escluso quando le modalità di diffusione non permettono un accesso rapido, completo e tempestivo, come esplicitato nell'art. 17, comma 1 del MAR, con riferimento agli strumenti finanziari[520].

Il riferimento al "pubblico" come destinatario della notizia è interpretato in senso ampio, includendo la generalità dei potenziali investitori, secondo l'accezione precisata dalla giurisprudenza[521].

Passando all'effetto significativo sul prezzo delle cripto-attività, il comma 4 dell'art. 87 specifica che le informazioni privilegiate sono quelle che «un possessore di cripto-attività ragionevole probabilmente utilizzerebbe come elemento decisionale per gli investimenti».

Analogamente a quanto osservato per gli strumenti finanziari, il criterio dell'investitore ragionevole appare vago e discrezionale[522], con l'uso dell'avverbio "probabilmente" che non apporta di certo maggiore rigore definitorio. Inoltre, il riferimento all'informazione *price sensitive* come "uno degli elementi" (e quindi non

[519] S. SEMINARA, «*il reato di insider trading tra obbligo di astensione e divieto di utilizzazione in borsa di informazioni riservate. considerazioni su riforme ordite, abortite e partorite*», Banca Borsa, II (1998): 325 e ss.
[520] Cfr. F. D'ALESSANDRO, «*Regolatori del mercato, enforcement e sistema penale»,* (G. Giappichelli Editore, 2014) 121.

[521] Sul punto, Cass. pen. 23 dicembre 2008, n. 48005, la quale ha precisato che «per pubblico deve intendersi solo quello dei potenziali investitori sul mercato telematico, che non può certo coincidere con i soggetti […] i quali, nella loro qualità di collaboratori dell'intermediario, vengano a conoscenza delle informazioni privilegiate, concernenti gli ordini da eseguire, a causa dell'esercizio della loro attività professionale, dal momento che questi ultimi non sono certo obbligati, tra di loro, a tenere riservate le notizie apprese, essendo tale obbligo riferibile solo nei confronti dei terzi».
[522] F. SGUBBI, «*Abusi di mercato*» Annali, fasc. II Enc. Dir. (2008): 20 e ss.

il solo) sul quale il possessore di cripto-attività potrebbe basare le proprie decisioni di investimento rischia di ampliare il concetto di notizia *price sensitive* anziché restringerlo.

È quindi fondamentale abbandonare la valutazione prognostica delle scelte di investimento dell'investitore ragionevole e sostituirla con un'analisi delle condizioni del mercato e della situazione specifica della cripto-attività, verificando se l'informazione sia davvero rilevante per le decisioni di investimento[523].

## 2.3 Comunicazione al pubblico di informazioni privilegiate

L'art. 88 di MiCA regola la comunicazione al pubblico delle informazioni privilegiate, imponendo agli emittenti, offerenti e richiedenti l'ammissione alla negoziazione, l'obbligo di comunicare tempestivamente «quanto prima al pubblico le informazioni privilegiate di cui all'art. 87 che li riguardano direttamente», in modo da consentire un accesso rapido e la conseguente valutazione completa, corretta e tempestiva.

Nel primo comma dell'art. 88 viene specificato 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 della loro attività. La locuzione, non sufficientemente chiara, deve essere interpretata alla luce della versione inglese "*combine*", nel senso che l'emittente o offerente che sia, ha l'obbligo di non confondere la comunicazione verso il pubblico dell'informazione privilegiata con la comunicazione commerciale.

Il paragrafo 2 dell'articolo 88 regola le situazioni in cui è legittimo ritardare la comunicazione delle informazioni privilegiate e cioè nei casi in cui siano presenti tre specifiche condizioni. In primo luogo, la divulgazione immediata potrebbe danneggiare i legittimi interessi degli emittenti, degli offerenti o dei soggetti che richiedono l'ammissione alla negoziazione. In secondo luogo, deve essere improbabile che il ritardo abbia l'effetto di fuorviare il pubblico. In terzo luogo, gli emittenti, gli offerenti o i soggetti che richiedono l'ammissione alla negoziazione devono essere in grado di garantire la riservatezza delle informazioni. La presenza simultanea di queste tre condizioni giustifica il ritardo nella comunicazione delle informazioni privilegiate.

[523] In dottrina G. FERRARINI «*la nuova disciplina europea dell'abuso di mercato*», in Riv. Soc., 2004, 54.

È importante notare che questi sono gli stessi criteri stabiliti dall'articolo 17, comma 4, del MAR per la comunicazione ritardata delle informazioni privilegiate nel contesto finanziario.

In caso di comunicazione ritardata delle informazioni privilegiate al pubblico, l'emittente, l'offerente o il soggetto che richiede l'ammissione alla negoziazione hanno l'obbligo di notificare il ritardo all'autorità competente, fornendo una spiegazione scritta sulle condizioni che giustificano il ritardo. Questa notifica deve essere fornita "immediatamente dopo che le informazioni sono state divulgate al pubblico".

## 2.4 Divieto di abuso e divulgazione illecita di informazioni privilegiate

L'articolo 89 del MiCA disciplina invece il divieto di abuso di informazioni privilegiate, seguendo la struttura dell'articolo 8 del MAR, che tratta il divieto di *insider trading*.

Questo divieto si applica a coloro che detengono informazioni privilegiate in quanto membri di organi di amministrazione, direzione o vigilanza dell'emittente, dell'offerente o del soggetto che richiede l'ammissione alla negoziazione. Il divieto suddetto si estende anche a coloro che detengono informazioni privilegiate in virtù della loro partecipazione al capitale, dell'attività lavorativa, professione o funzione, o del loro coinvolgimento nelle tecnologie a registro distribuito o simili. Questo approccio è in linea con le tradizionali disposizioni relative ai mercati finanziari.

Gli *insider* primari sono coloro che ottengono informazioni privilegiate a causa del loro *status*, e sono suddivisi in *insider* istituzionali (*corporate insider*) e *insider* temporanei (*temporary insider*). Gli *insider* istituzionali agiscono in virtù della loro carica nella struttura societaria, mentre gli *insider* temporanei possono essere estranei alla società ma possono accedere a informazioni rilevanti per la valutazione delle cripto-attività in base all'attività lavorativa o alla posizione ricoperta, come ad esempio professionisti coinvolti nella stesura di un *white paper* o collaboratori nella parte tecnica di creazione e strutturazione delle cripto-attività.

L'articolo 89 sancisce inizialmente l'illegalità del *trading* basato sull'uso di informazioni privilegiate. Questo comportamento presuppone una correlazione strumentale tra l'acquisizione di informazioni privilegiate e l'esecuzione di operazioni relative alle cripto-attività. In altre parole, il vantaggio informativo può essere sfruttato

dall'agente per plasmare la propria decisione di investimento, senza necessariamente costituire l'unico elemento determinante.

La scelta del termine "utilizzare" evidenzia il disvalore della condotta concentrato sull'effettivo sfruttamento della notizia *price sensitive*, rafforzando il collegamento causale tra la detenzione dell'informazione privilegiata e l'attività di *trading*; "l'utilizzo" implica infatti un comportamento attivo, di natura commissiva, che si basa sullo sfruttamento diretto della notizia.

Parallelamente, l'articolo 89 vieta il "*trading* per evitare le perdite", in cui l'*insider*, a conoscenza di informazioni privilegiate sulle caratteristiche negative di una specifica cripto-attività, effettua operazioni per evitare o ridurre le perdite di un investimento; ciò include anche l'adozione di comportamenti come l'annullamento o la modifica di un ordine inserito prima della conoscenza dell'informazione privilegiata. In entrambi i casi, l'*insider* compie attivamente operazioni di negoziazione, conferendo rilevanza alla sua condotta.

L'azione proibita può essere anche eseguita "per conto proprio o per conto di terzi, direttamente o indirettamente"; l'esecuzione di quest'azione per conto di terzi, oltre ad allargare il campo di applicazione della norma, comporta l'intervento di un soggetto diverso dall'utilizzatore primario dell'informazione, la cui sfera patrimoniale subisce però gli effetti economici dell'operazione.

È importante notare che, nell'ambito della negoziazione di cripto-attività, ci sono soggetti specifici, i c.d. "*miners*", incaricati della verifica, approvazione e registrazione delle transazioni nei blocchi della *blockchain* o di altri registri distribuiti[524]. Il ruolo svolto conferisce al *miner* un punto di osservazione privilegiato, da cui può agevolmente ottenere vantaggi informativi rispetto agli utenti non qualificati, potenzialmente approfittando di tali informazioni per ottenere un vantaggio operativo.

Da un'altra prospettiva, a differenza degli strumenti finanziari, non esistono obblighi di *best execution* che vincolino il *miner* ad eseguire le operazioni nell'ordine in cui sono ricevute, né di astenersi dall'operare per proprio conto o per conto terzi in relazione alle transazioni sottoposte alla loro approvazione. Questo fenomeno è conosciuto come "*miners front running*". Risulta evidente, quindi, come il privilegio informativo possa creare opportunità concrete di vantaggio patrimoniale, sia sotto il profilo dell'*insider dealing* che della *market manipulation*, specialmente se il soggetto agente può operare nell'anonimato con una certa sicurezza.

[524] Cfr. diffusamente cap.2.

La seconda azione vietata dall'articolo 89 è il "*tuyautage*", che proibisce sia di raccomandare ad altri l'abuso di informazioni privilegiate che di indurli a farlo. In parallelo, il comma 3 stabilisce che chiunque detenga informazioni privilegiate non deve fornire raccomandazioni o indurre altri a comprare, vendere, annullare o modificare un ordine relativo a tali cripto-attività.

Infine, l'articolo 90 impone il divieto di divulgazione illecita delle informazioni privilegiate. Questa è una fattispecie speculare rispetto a quella prevista dall'articolo 10 MAR, riguardando non una raccomandazione di investimento, bensì la diffusione di informazioni privilegiate, tranne nei casi in cui tale divulgazione avvenga nell'ambito del normale svolgimento di un'attività lavorativa, di una professione o di una funzione.

La condotta in esame, nel contesto dell'*insider trading* tradizionale, è nota come "*tipping*". I divieti di raccomandazione mirano a garantire il rispetto dell'obbligo di segretezza e riservatezza dell'informazione privilegiata fino a quando non venga resa pubblica, prevenendo l'allargamento del numero di persone che possono godere del vantaggio informativo o delle istruzioni operative ad esso correlate[525].

Pertanto, il pericolo in sé non è la comunicazione, ma l'ampliamento del gruppo di individui che potrebbero approfittare di una posizione di privilegio informativo.

In questo modo, si attua una precauzionale anticipazione di tutela.

La differenza tra la condotta di *tuyautage* e quella di *tipping*[526] è che nel primo caso, le raccomandazioni e l'induzione non riguardano la comunicazione della notizia *insider*, ma piuttosto il comportamento da tenere sulla base delle informazioni privilegiate. Se la notizia *insider* viene comunicata, la raccomandazione viene assorbita e integrata nella comunicazione, che incorpora l'intero disvalore della condotta. In tal caso, l'eventuale esecuzione dell'operazione suggerita da parte di un terzo non sarebbe più il risultato della raccomandazione o dell'induzione dell'*insider*, ma una scelta specifica del soggetto che subentra nel privilegio informativo. Per perfezionare la condotta di *tuyautage*, è quindi necessario e sufficiente che l'*insider* si limiti a fornire suggerimenti a terzi riguardo a un'operazione di investimento, basandosi sulla conoscenza della notizia privilegiata. Non è nemmeno necessario che il destinatario della raccomandazione effettui effettivamente l'operazione suggerita.

[525] F. MUCCIARELLI, «*Speculazione mobiliare e diritto penale, quaderni di giurisprudenza commerciale*» (Giuffrè Francis Lefebvre, 1995).
[526] Vale ricordare che, prima del recepimento della MAD, nel diritto italiano le condotte di *tipping* e *tayautage* erano enucleate come un'unica condotta.

La raccomandazione e l'induzione devono avvenire "sulla base" dell'informazione privilegiata; quindi, deve esistere un collegamento causale tra la condotta di *tuyautage* e la notizia *insider*, escludendo tutte le ipotesi in cui la raccomandazione non dipende dall'informazione privilegiata acquisita dall'*insider*.

## 2.5 Divieto di manipolazione del mercato

L'articolo 91, comma 1, di MiCA introduce il divieto di manipolazione del mercato, vietando a chiunque di effettuare o tentare di effettuare manipolazioni di mercato. Similmente a quanto già indicato nelle disposizioni precedenti, la formulazione presenta somiglianze con l'articolo 12 del MAR, seppur con alcune peculiarità.

Il comma 2 dell'articolo 91 fornisce una descrizione dettagliata delle attività che costituiscono manipolazione. La prima proibizione, indicata dalla lettera *a)*, riguarda la conclusione di un'operazione, la collocazione di un ordine di negoziazione o qualsiasi altra condotta che fornisca indicazioni false o fuorvianti riguardo all'offerta, alla domanda o al prezzo di una cripto-attività. Inoltre, vi rientra anche l'azione volta a fissare il prezzo di una o più cripto-attività a un livello anormale o artificiale.

La lettera *b)* del comma 2 qualifica come manipolazione la conclusione di un'operazione, la collocazione di un ordine di negoziazione o qualsiasi altra attività o condotta che influenzi o possa influenzare il prezzo di una o più cripto-attività attraverso l'uso di uno strumento fittizio o di un qualsiasi altro tipo di inganno o espediente.

Infine, la lettera *c)* sottolinea l'importanza della diffusione di informazioni, tramite i *media*, compreso *Internet*, o qualsiasi altro mezzo, che forniscano segnali falsi o fuorvianti riguardo all'offerta, alla domanda o al prezzo di una o più cripto-attività, vietando la diffusione di informazioni non confermate quando chi la diffonde conosce o dovrebbe sapere che tali informazioni sono false o fuorvianti.

Queste disposizioni rappresentano un adattamento alle cripto-attività delle condotte tradizionalmente denominate "*information-based manipulation*", le quali derivano dall'effetto della divulgazione di informazioni false o fuorvianti[527].

[527] Cfr. A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, «*Diritto penale dell'economia»* (Utet Giuridica, 2019).

La destinazione al pubblico assume rilievo, anche in modo indiretto, ad esempio in situazioni come incontri con analisti, società di *rating* o altri soggetti deputati a propagare ulteriormente la notizia, configurandosi come strumento fittizio. Per quanto riguarda le informazioni, tanto quelle sull'emittente (*corporate information*) che quelle di mercato (*market information*) possono integrare una manipolazione del mercato stesso. La diffusione deve riguardare necessariamente notizie, ovvero informazioni relative a fatti, e non semplici opinioni.

Il comma 3 dell'articolo 91 descrive inoltre le condotte di manipolazione basate sul mercato, vietando l'acquisizione di una posizione dominante sull'offerta o sulla domanda di una cripto-attività, con effetti diretti o indiretti sui prezzi di acquisto o vendita o creando condizioni commerciali inique.

Il paragrafo 3, lettera *b*, del comma 3 dell'art. 91elenca invece diverse azioni, che includono l'inoltro di ordini a una piattaforma di negoziazione di cripto-attività, compresa qualsiasi cancellazione o modifica degli stessi tramite qualsiasi mezzo di negoziazione che produca gli effetti di cui al comma 2, lett. *a)*[528], attraverso il sabotaggio o il ritardo dell'operatività della piattaforma di negoziazione di cripto-attività o l'esecuzione di qualsiasi attività che possa provocare i medesimi effetti.

Le menzionate attività includono l'esecuzione di azioni finalizzate a ostacolare l'individuazione di ordini autentici sulla piattaforma di negoziazione di cripto-attività da parte di 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, la creazione di un segnale falso o fuorviante in merito all'offerta, alla domanda o al prezzo di una cripto-attività, in particolare mediante l'inserimento di ordini per avviare o aggravare una tendenza in atto.

Il comma 3, lett. *c)* descrive infine l'uso occasionale o abituale dei mezzi di informazione tradizionali o elettronici al fine di esprimere pareri su una cripto-attività, sulla quale si sono prese posizioni in precedenza, approfittando degli effetti prodotti da tali pareri sul prezzo di detta cripto-attività, senza avere nel contempo reso pubblico detto conflitto di interesse in modo adeguato ed efficace.

In sintesi, l'art. 91 di MiCA dettaglia una serie di condotte proibite, tentando di abbracciare tutte le possibili manipolazioni del mercato delle cripto-attività. Vengono

[528] Ovvero che sia suscettibile di fornire indicazioni false o fuorvianti in merito all'offerta, alla domanda o al prezzo di una cripto-attività, ovvero fissi, o sia suscettibile di fissare, il prezzo di una o più cripto-attività a un livello normale o artificiale.

così contemplate anche operazioni che non comportano una reale modifica di proprietà o profilo di rischio, negoziazioni solo apparenti (*wash trading* o *ramping*), l'inserimento contemporaneo di ordini di acquisto e vendita al medesimo prezzo (*churning*) e l'inserimento di ordini ad alta frequenza con l'intenzione di cancellarli prima dell'esecuzione, così condizionando il valore del titolo (*spoofing*).

Dato il grande numero di condotte manipolatorie ibride, la scelta del legislatore europeo di concentrarsi sugli effetti reali o potenziali di tali condotte appare del tutto fondata. Inoltre, il legislatore cerca di affrontare il rischio di conflitto di interesse derivante dall'anonimato delle transazioni, imponendo la comunicazione e la neutralizzazione delle posizioni conflittuali, come specificato nel comma 3, lett. *c).*

## 2.6 Prevenzione e individuazione di abusi di mercato

L'articolo 93 di MiCA, integrando il quadro regolatorio delineato precedentemente, istituisce gli obblighi relativi alla prevenzione e alla *compliance* in materia di abusi di mercato, applicabili nei confronti di «chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività».

Questi operatori sono tenuti a implementare dispositivi, sistemi e procedure efficaci per prevenire e individuare abusi di mercato. Sono inoltre soggetti alle norme di notifica del rispettivo Stato membro e devono comunicare prontamente all'autorità competente eventuali sospetti riguardanti ordini, operazioni o aspetti del funzionamento della tecnologia a registro distribuito, che possano indicare un abuso di mercato, sia esso reale o potenziale.

Le autorità competenti, a loro volta, sono tenute a comunicare tempestivamente le informazioni ricevute ai loro omologhi responsabili della vigilanza delle piattaforme di negoziazione interessate.

Le violazioni delle disposizioni del titolo e la mancata collaborazione durante l'esercizio dei poteri ispettivi sono anch'esse soggette a sanzioni amministrative ai sensi dell'articolo 111 di MiCA.

Tuttavia, gli Stati membri possono scegliere di non stabilire norme relative alle sanzioni amministrative se le violazioni, degli articoli da 88 a 92 siano già soggette a sanzioni penali nel diritto nazionale entro dodici mesi dall'entrata in vigore di MiCA.

Attualmente, il diritto penale italiano punisce i reati di *insider trading* e *market abuse* in relazione agli strumenti finanziari quotati[529], non quotati[530] e ai "valori ammessi nelle liste di borsa o negoziabili al pubblico mercato"[531].

Accanto alle fattispecie penali, gli artt. 187-*bis* e 187-*ter* del TUF prevedono illeciti amministrativi per i comportamenti di abuso di informazioni privilegiate e manipolazione del mercato costituenti violazione delle disposizioni del MAR.

Tutte le disposizioni citate hanno quale presupposto comune il trovarsi di fronte a uno strumento finanziario[532], differenziandone l'ambito applicativo a seconda che si tratti di strumenti quotati o meno. Come più volte ricordato, MiCA non è tuttavia applicabile, ai sensi dell'art. 2, comma 4, lett. *a)*, alle cripto-attività qualificabili come strumenti finanziari. Tale clausola di esclusione sembrerebbe *prima facie* risolvere ogni difficoltà interpretativa, creando due ambiti contigui ma distinti tra ciò che è da qualificarsi come strumento finanziario, e che quindi ricade sotto le disposizioni di MiFID II e in genere in quelle del diritto dei mercati finanziari, e ciò che invece andrà regolato ai sensi di MiCA.

In realtà, la ripartizione in questione non è affatto pacifica. Innanzitutto, la definizione se una cripto-attività debba considerarsi uno strumento finanziario o meno è affidata all'emittente mediante il *white paper*, sotto la supervisione da parte delle autorità competenti. In secondo luogo, come è stato evidenziato, la nozione di strumento finanziario è intrinsecamente complessa e sfuggente.

In base all'ordinamento italiano, l'art. 1, comma 2 del TUF classifica come strumento finanziario qualsiasi strumento elencato nella sezione C dell'allegato 1 del medesimo TUF, con la possibilità per il Ministero dell'Economia e delle Finanze di specificarlo ulteriormente tramite decreto ministeriale.

Tuttavia, esaminando l'elenco degli strumenti finanziari nella sezione C dell'allegato 1, non emerge alcun riferimento alle cripto-attività, suggerendo che queste potrebbero non rientrare nella definizione di strumento finanziario.

In aggiunta, già prima dell'entrata in vigore di MiCA, l'ordinamento italiano conosceva delle cripto-attività, i *security tokens*, che erano sicuramente riconducibili

[529] Artt. 184 e 185 del d.lgs 58/1998 (TUF).
[530] Art. 2637 c.c.
[531] Art. 501 c.p.
[532] Salvo l'art. 501 c.p., che tuttavia a ben vedere risulta pressoché privo di applicazioni pratica soprattutto in seguito alla riforma dell'art. 2637 c.c. del 2002, che di fatto avocava all'aggiotaggio societario (art. 2637 c.c.) i comportamenti sulle liste di borsa o il pubblico mercato. In questo senso, F. D'ALESSANDRO, «*L'aggiotaggio e la manipolazione del mercato*», in *Diritto e procedura penale delle società* (Giuffrè Francis Lefebvre, 2022).

alla nozione di strumenti finanziari[533]. La giurisprudenza di legittimità ha però adottato un orientamento che attribuisce maggiore importanza alla funzione della cripto-attività piuttosto che alla sua definizione formale[534].

In motivazione, la Suprema Corte ha richiamato e fatto proprio un precedente orientamento di merito del Tribunale civile di Verona, ripreso dal Pubblico Ministero nel procedimento sottoposto alla decisione di legittimità, secondo cui «caratteri distintivi dell'investimento di tipo finanziario sono: *a)* un impiego di capitali, riconducibile generalmente al danaro o, più in generale, a un capitale proprio che può corrispondere anche a una valuta virtuale; *b)* una aspettativa di rendimento; *c)* un rischio proprio dell'attività prescelta, direttamente correlato all'impiego di capitali».

Come osservato in dottrina «a rilevare è la dinamica della fattispecie, la reclamizzazione della vendita di valute virtuali, la cui natura statica forse potrebbe anche non essere quella di uno strumento finanziario: sarebbe l'invito a comprare rivolto in *incertam personam* a trasformare la criptomoneta in investimento e i destinatari della comunicazione in risparmiatori che devono poter valutare adeguatamente i rischi cui si sottopongono»[535].

Un percorso alternativo, volto a giustificare il ricorso al reato di abusivismo finanziario ai sensi dell'art. 166 del TUF, considera poi la possibilità di collocare le cripto-attività nella categoria di prodotti finanziari. Questi, secondo l'art. 1, comma 1, lett. *u)* del TUF, includono "gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria.".

Nell'elaborazione della giurisprudenza civile[536] e della Consob[537], la nozione di prodotti finanziari ricomprende quella degli strumenti, che ne rappresentano quindi una *species*, ma include anche ogni altra forma di investimento, quindi caratterizzata da impiego di capitale, aspettativa di rendimento e assunzione di un rischio.

---

[533] Cfr. P. CARRIERE, N. DE LUCA, M. DE MARI, G. GASPARRI, T. N. POLI «*tokenizzazione di azioni e azioni tokens*», quaderni giuridici consob, n. 25/2023, 53.

[534] Sul punto, è stato infatti affermato che «con riguardo all'uso della moneta virtuale come mezzo di scambio o strumento finanziario, questa Corte ha precisato (Sez. II, Sentenza n. 26807 del 17 settembre 2020, De Rosa, Rv. 279590) che ove la vendita di bitcoin venga reclamizzata come una vera e propria proposta di investimento, si ha una attività soggetta agli adempimenti di cui agli artt. 91 e ss. TUF ("La CONSOB esercita i poteri previsti dalla presente parte avendo riguardo alla tutela degli investitori nonché all'efficienza e alla trasparenza del mercato del controllo societario e del mercato dei capitali"), la cui omissione integra la sussistenza del reato di cui all'art. 166 comma 1 lett. c) TUF ».

[535] F. CONSULICH, «*Nella wunderkammer del legislatore penale contemporaneo: monete virtuali che causano danni reali*», febbraio 2022, in Dir. Proc. Pen., 154.

[536] Cass. Civ., sez. II, 12 marzo 2018, n.5911.

[537] Seppur in riferimento a un investimento in opere d'arte, delibera 17 gennaio 2018, n.5911.

Sul punto, è stato efficacemente osservato (con specifico riferimento alle criptovalute) che la finanziarietà è «uno stato di fatto, in quanto esprime l'interesse tipico della comunità all'accesso ad un determinato bene/rapporto e l'utilità sociale rivestita dal medesimo. In quanto stato di fatto, la finanziarietà può sussistere o non sussistere a seconda del contesto o a seconda del tempo in cui il bene/rapporto è trattato. In questa prospettiva, nella negoziazione di bitcoin, oggi, l'interesse a dotarsi di uno strumento di intermediazione negli scambi (denaro) sembra decisamente un interesse di retroguardia, rispetto a quello di speculare sul suo tasso di cambio, e dunque di investire capitali con l'aspettativa di una remunerazione. Non sono perciò le lusinghe suscitate dalla pubblicità che fanno della "causa concreta" dell'offerta di bitcoin una causa di investimento, bensì l'interesse tipico che oggi muove chi dispone di capitali a investire in questa criptovaluta»[538]

In linea con l'approccio adottato dalla Corte di Cassazione, si potrebbero classificare come strumenti finanziari e, di conseguenza, soggetti alle disposizioni penali pertinenti, tutte le cripto-attività in cui l'interesse di investimento prevale su quelli di riserva di valore o utilità. L'imposizione di sanzioni penali sembra dunque giustificata sia per affrontare pericoli reali di asimmetrie e manipolazioni che danneggiano gli investitori meno esperti, sia per garantire coerenza nel sistema normativo.

Ragionando in questa prospettiva, si eviterebbero situazioni paradossali in cui la manipolazione di una cripto-attività sarebbe penalmente irrilevante, mentre la manipolazione di uno strumento derivato basato sulla stessa cripto-attività sarebbe soggetta alle disposizioni del TUF, poiché riconducibile alla sezione C dell'allegato 1, n.10.

Quanto alle specifiche fattispecie di reato applicabili, risulta complesso ricondurre le cripto-attività alle disposizioni degli artt. 184 e 185 TUF, dato che le recenti modifiche all'art. 182 come sostituto dall'art 26, comma 1, lett. *a)* della l. 23 dicembre 2021, n. 238 hanno limitato notevolmente il loro campo di applicazione.

Al contrario, sembra più appropriato applicare la fattispecie di aggiotaggio di cui all'art. 2637 c.c. per le condotte di manipolazione del mercato, la quale fa riferimento agli "strumenti finanziari non quotati o per i quali non è stata presentata una richiesta di ammissione alle negoziazioni in un mercato regolamentato".

[538] M. CIAN, «*Notarelle su finanziarietà e non finanziarietà nei crypto-asset: la suprema corte sulla natura del servizio di exchange*», Banca, borsa, tit. cred., fasc. I (2023): 3.

In sintesi, seguendo l'interpretazione "finalistica" della giurisprudenza di legittimità, si può considerare una cripto-attività uno strumento finanziario se la sua funzione principale è di natura di investimento. Di conseguenza, le azioni di manipolazione della cripto-attività o della relativa piattaforma di negoziazione potrebbero essere soggette alle sanzioni previste dall'art. 2637 c.c..

Diversamente, non sarebbero sanzionabili penalmente i comportamenti di *insider trading*, mancando nel nostro ordinamento una fattispecie che incrimina l'abuso di informazioni privilegiate su strumenti non quotati.

Tali ultimi comportamenti, quindi, sarebbero sanzionabili a livello amministrativo ai sensi di MiCA, mentre con riferimento alla manipolazione del mercato potrebbe optarsi per la non applicazione delle sanzioni amministrative ai sensi dell'art. 111.

Per tali ragioni appare auspicabile che il legislatore italiano eserciti la facoltà concessa dall'art. 111 MiCA di regolare autonomamente l'eventuale piano penalistico delle violazioni degli artt. da 88 a 92, in modo da fugare ogni rischio di genericità e indeterminatezza dell'ambito applicativo delle fattispecie suddette, nonché ogni asimmetria sanzionatoria.

L'intervento del legislatore potrebbe infatti estendere l'applicazione delle disposizioni di cui agli artt. 184 e 185 TUF a talune o tutte le cripto-attività, ovvero introdurre specifiche disposizioni che sanzionino penalmente i comportamenti di abuso di informazioni privilegiate e manipolazione del mercato ove riferiti alle cripto-attività.

Così facendo, si supererebbero anche i problemi interpretativi destinati a sorgere per effetto della non agevole compresenza tra un piano regolamentare europeo, che limita l'applicazione di MiCA alle cripto-attività non qualificabili come strumenti finanziari, e un piano applicativo nazionale per cui la medesima cripto-attività può essere invece considerata strumento finanziario in virtù della sua offerta al pubblico come investimento.

# 3. Antiriciclaggio e gestione dei rischi aziendali dei prestatori di servizi di cripto-attività

## 3.1 Interventi delle Autorità nazionali e sovranazionali

La disciplina antiriciclaggio è da qualche anno a questa parte soggetta ad importanti fasi di aggiornamento, che lungi dall'esser concluse, stanno conducendo ad una vera e propria riforma sistematica della materia. L'innovazione finanziaria è stata, e continua a rimanere senza dubbio una delle spinte più rilevanti di questa metamorfosi[539]. In particolare, si è riconosciuto che i sistemi decentralizzati delle cripto-attività sono particolarmente vulnerabili a causa dello pseudo-anonimato ed espongono gli utenti a frodi oltre a facilitare il riciclaggio di denaro[540].

Una presa di consapevolezza di tali rischi risale al 12 dicembre 2013, quando l'*European Banking Authority* pubblicò un comunicato intitolato "*Warning to consumers on virtual currencies*"[541]. In cui l'EBA mise in guardia i consumatori sui rischi legati all'acquisto, detenzione e scambio di valute virtuali come Bitcoin, evidenziando la mancanza di tutele normative contro la perdita di denaro, l'*hacking* dei portafogli digitali, l'irreversibilità delle transazioni e l'eccessiva volatilità dei valori virtuali.

In quello stesso frangente, il *Financial Action Task Force* (FATF-GAFI) pubblicò un *report* intitolato "*Virtual currencies: key definitions and Potential AML/CFT Risks*", in risposta alla emersione delle valute virtuali e dei meccanismi di

[539] G. ALPA, A.M. PANCALLO, «*Le criptovalute*», in «*Diritto e intelligenza artificiale*», 2020, 591 e ss.
[540] "Secondo gli ultimi dati sui crimini commessi nel mondo dei *crypto-asset*, il 2022 è stato un anno durante il quale il volume delle transazioni illecite osservabili sulla *blockchain* ha raggiunto i 20,6 miliardi di dollari, rappresentando, in valore assoluto, il dato più alto dal 2017. E ciò, nonostante la flessione del volume delle transazioni totali legata alla crisi che ha attraversato il settore dei *crypto-asset* nel 2022, generata dai gravi scandali che hanno coinvolto importanti operatori del mercato, dall'azione di controllo e repressione sulle attività illecite condotta da alcune Autorità e dall'ondata ribassista che ha avuto inizio nel dicembre 2021 sui principali *crypto-asset* (Bitcoin ed Ethereum, entrambi determinanti nella capitalizzazione del settore). Come detto, il volume delle transazioni illecite legate ai *crypto-asset*, e osservabili come tali sulla *blockchain*, deriva dal tracciamento delle transazioni riconducibili a *wallet* legati a soggetti coinvolti in attività criminali. Le attività illecite del *cybercrime* - con oggetto *crypto-asset* utilizzati come mezzo di pagamento o come fine stesso dell'atto criminale - più incidenti sui flussi sono quelle riconducibili al furto di fondi (*hacking*), alle truffe (*scam*), all'estorsione digitale (*ransomware),* ad attività associate ad entità sanzionate e ai *darknet market*." In D. VARANI, D. LUNETTA, «*Rilevanza del mercato dei crypto-asset nell'ambito del cybercrime e dei reati di riciclaggio*», in *Cripto-attività: antiriciclaggio e gestione dei rischi aziendali* (Pacini Editore, 2024), 7.
[541] L'EBA richiamò la necessità di intraprendere iniziative di *hard law*, in relazione ai potenziali rischi.

pagamento ad esse associati, volti a fornire nuovi metodi di trasferimento di valore attraverso *internet*.

Nello specifico, la possibilità di effettuare transazioni anonime grazie all'utilizzo di sistemi (più o meno) decentralizzati, unitamente allo sviluppo di relazioni *non-face-to-face* con il cliente, vennero considerati fattori di vulnerabilità in termini di potenziale utilizzo criminale delle valute virtuali[542]. Nel suo *report* del giugno 2014, il GAFI ha definito la valuta virtuale[543] come: «rappresentazione digitale di valore che può essere ceduta/scambiata digitalmente e funzionare come mezzo di scambio, unità di conto e riserva di valore, che tuttavia non ha corso legale in alcuna giurisdizione; non è emessa o garantita da alcuna giurisdizione, riuscendo a soddisfare le predette condizioni solo attraverso l'accordo che intercorre tra la comunità degli utilizzatori della valuta virtuale»[544]

Dopo la divulgazione del suddetto "*Warning*" nel dicembre 2013, ed appena un mese dopo la pubblicazione delle "*Key Definitions*" da parte del GAFI, l'11 agosto del 2016 l'EBA pubblicò il documento: "*Opinion of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)*", con il quale mise in collegamento le perplessità e le criticità espresse precedentemente sull'incerta qualificazione giuridica delle cripto-attività , con il rischio di riciclaggio connesso, confermando così la necessità di adattare l'assetto della disciplina antiriciclaggio alle nuove tecnologie e alle soluzioni innovative derivate da queste ultime.

Sottolineando il suo ruolo istituzionale nel monitorare le attività finanziarie e stabilire linee guida per promuovere la sicurezza e la solidità dei mercati[545], l'EBA si

---

[542] "*virtual currencies provide a powerful new tool for criminals, terrorist financiers and other sanctions evaders to move and store illicit funds, out of the reach of law enforcement and other authorities*".

[543] La definizione in oggetto è stata poi ripresa dalla V direttiva AML.

[544] Cfr. http://www.fatf-gafi.org/me-dia/fatf/documents/reports/Virtual-cur-rency-key-defini-tions-and-potential-aml- cft-risks.pdf.

[545] Come noto, gli atti di *soft law* prodotti dalle agenzie europee di vigilanza dei mercati finanziari (EBA, ESMA, EIOPA) hanno da sempre alimentato un vivace dibattito circa la loro precisa natura, inducendo anche la Corte di Giustizia Europea ad esprimersi sul punto. Anche sulla scorta di quanto già affermato più in generale circa la natura *non-binding* degli atti di *soft law* (C-322/88 *Salvatore Grimaldi v Fonds des maladies professionnelles*,), la Corte ha più recentemente preso posizione circa la natura di tali atti nel caso C-911/19 FBF. Il caso riguardava la possibilità per un istituto di credito francese di presentare un ricorso ai sensi dell'art. 263 TFUE per l'annullamento degli orientamenti emanati dall'EBA ai sensi dell'art. 16 del Regolamento istitutivo dell'EBA (Regolamento 1093/2010). La Corte, nel porre come prerequisito per qualsiasi decisione sull'annullamento di strumenti di *soft law* la necessità di determinare se un atto produca effetti giuridici vincolanti, ha sostenuto che le linee guida in questione sono soggette alle stesse regole previste per le raccomandazioni emesse dall'EBA, che non sono vincolanti per i destinatari e quindi non hanno, in linea di principio, alcuna forza vincolante. La Corte ha anche fatto riferimento all'art. 16, par. 3, del menzionato Regolamento EBA, che sancisce il principio "*comply or explain*", il quale non comporta un obbligo di conformità, bensì la mera necessità di fornire spiegazioni

propone di sottolineare la necessità di sottoporre le valute virtuali e gli operatori del settore a una regolamentazione specifica in tema di antiriciclaggio.

Sebbene l'EBA riconosceva alcuni vantaggi nell'uso delle valute virtuali, come la riduzione dei costi di transazione e l'inclusione finanziaria migliorata grazie ai sistemi decentralizzati, evidenziava altresì rischi significativamente aumentati per gli utenti e il sistema finanziario rispetto agli ambiti tradizionali. I vari "*warnings*" emessi analizzano dettagliatamente oltre 70 rischi associati alle valute virtuali.

L' "*Opinion*" si conclude raccomandando alle Autorità di Vigilanza nazionali di scoraggiare gli istituti finanziari dall'acquistare, detenere o vendere valute virtuali, segnalando l'opportunità di ricondurre i partecipanti al mercato delle cripto-attività, all'interno della disciplina antiriciclaggio e per contrastare il finanziamento del terrorismo.

Nel giugno 2015 il GAFI ha emesso il documento "*Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*"[546]. Questo documento fa parte di una strategia volta a prevenire e monitorare i rischi legati al riciclaggio di denaro e al finanziamento del terrorismo, associati ai servizi e ai prodotti di pagamento basati su valute virtuali. Inizialmente, il GAFI si focalizzava sugli aspetti delle attività legate all'uso di valute virtuali come in particolare le operazioni di cambio di valute virtuali convertibili che mostravano connessioni con il sistema finanziario tradizionale.

Negli anni successivi, l'ecosistema degli "*asset* virtuali" ha subìto una rapida evoluzione, includendo una vasta gamma di prodotti, servizi, modelli di *business* e attività che non rientrano nella definizione originaria di "cambiavalute" delle valute virtuali. L'evoluzione *de quo*, ha visto una diffusione significativa delle "criptovalute basate sull'anonimato", diverse tecniche di anonimizzazione come *mixering*, *tumblering* e *clustering*, piattaforme decentralizzate e altri servizi che opacizzano l'origine e la destinazione dei flussi finanziari, insieme all'emergere di nuovi modelli di *business* come le offerte iniziali di moneta (ICO), portando con sé rischi di frode e manipolazione del mercato.

---

dettagliate in caso di inosservanza. Sulla base di queste argomentazioni, la Corte ha concluso che le linee guida non possono essere considerate come produttrici di effetti giuridici vincolanti nei confronti dei destinatari. Sul tema, si v. anche Case C-28/15 *Koninklike KPN NV and Others v Autoriteit Consument en Markt* (Second Chamber; *Belgium v Commission*, C-16/16 P. In letteratura: F. ANNUNZIATA, «*The Remains of the Day: EU Financial Agencies, Soft Law and the Relics of Meroni*», SSRN Scholarly Paper (Rochester, NY, 19 novembre 2021), https://papers.ssrn.com/abstract=3966980.

[546] Consultabile: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf.

Perciò, il 21 ottobre 2018, il GAFI ha sentito la necessità di aggiornare la propria "*Guidance*" chiarendo in maniera esplicita che le raccomandazioni ivi formulate si dovessero applicare anche alle attività finanziare che coinvolgono *virtual asset*. Nello specifico, il GAFI ha provveduto ad aggiornare l'ambito applicativo della Raccomandazione n. 15 ("Nuove tecnologie") ricomprendendovi esplicitamente anche i VASP e richiedendo alle Autorità nazionali competenti di assoggettarli alla regolamentazione in materia di lotta al riciclaggio di denaro e di finanziamento del terrorismo assoggettandone l'attività a "licenza" o "registrazione" e a sistemi efficaci di "monitoraggio" e/o "vigilanza" ed altresì a controlli di *compliance*.

Allo stesso tempo, sono state aggiunte definizioni chiave, come "*Virtual Asset*" (VA)[547] e "*Virtual Asset Service Provider*" (VASP)[548].

L'obiettivo principale di queste azioni era rafforzare l'approccio che identifica negli obblighi gravanti sui VASP l'elemento chiave per il monitoraggio dei flussi finanziari sospetti nei circuiti economico-legali.

Nel giugno 2019, il GAFI ha pubblicato una "nota interpretativa" alla Raccomandazione n. 15 per chiarire l'applicazione dell'approccio basato sul rischio alle operazioni con *virtual asset* e alle attività dei VASP. In questa occasione, il GAFI ha enfatizzato l'importanza di sottoporre i VASP a un regime autorizzativo generale (licenza o registrazione) nella giurisdizione di insediamento, mirando a prevenire il coinvolgimento di "criminali" o loro "affiliati" negli assetti proprietari dei VASP o in ruoli gestionali. Ha promosso, inoltre, l'adozione di regolamentazioni nazionali al fine di sottoporre i VASP ad una vigilanza da parte di autorità nazionali competenti, dotate di poteri di supervisione, monitoraggio ed ispezione atti a garantire la conformità ai requisiti antiriciclaggio e antiterrorismo, inclusi poteri sanzionatori come l'interdizione dall'attività.

Nell'ambito della medesima "nota interpretativa", è stato chiarito l'ambito di applicazione dell'approccio basato sul rischio alle operazioni coinvolgenti transazioni con valute virtuali e alle attività dei VASP, ai quali è stato raccomandato di apportare

[547] Una rappresentazione digitale di valore che può essere scambiata o trasferita digitalmente, e che può essere utilizzata per finalità di pagamento o di investimento. Non sono incluse nella definizione le rappresentazioni digitali di valute *fiat*, di valori mobiliari o di altri *asset* finanziari già altrimenti disciplinate dalle stesse Raccomandazioni.

[548] La definizione include i soggetti, non altrimenti disciplinati dalle Raccomandazioni, che svolgono su base professionale una delle attività o operazioni in nome o per conto di un'altra persona fisica o giuridica: *a)* conversione tra *virtual asset* e valute legali; *b)* conversione tra *virtual asset*; *c)* trasferimento di *virtual asset*; *d)* custodia e/o amministrazione di *virtual asset* o di strumenti che ne consentono il controllo; *e)* partecipazione e fornitura di servizi finanziari relativi all'offerta e/o alla vendita di *virtual asset*.

le necessarie modifiche organizzative per garantire il corretto adempimento delle misure di prevenzione del rischio di riciclaggio. Queste modifiche includono l'osservanza dell'obbligo di adeguata verifica della clientela, anche per transazioni al di sotto di soglie come 1000 euro/dollari, e l'implementazione della "*travel rule*"che prevede l'ottenimento, la conservazione e la trasmissione sicura delle informazioni sul disponente e beneficiario delle transazioni in cripto-attività, alle *Financial Intelligence Unit* (FIU) competenti a livello nazionale.

Nel giugno 2019, il FATF ha poi adottato le "Linee Guida concernenti l'applicazione dell'approccio basato sul rischio ai *virtual asset*" con l'obiettivo di assistere sia le Autorità nazionali al fine di comprendere e sviluppare risposte adeguate alle attività legate ai *virtual asset*, sia i soggetti privati interessati a intraprendere attività legate ai *virtual asset,* per comprendere i propri obblighi in materia di antiriciclaggio e le modalità per adempiere efficacemente ai medesimi.

A seguito dei moniti levati dagli *standard setters* e dalle Autorità di settore, il legislatore ha dato così forma e contenuto alle diverse preoccupazioni dedicandovi specifiche norme giuridiche[549].

In questa prospettiva, la Direttiva 2018/843/UE ha affrontato la questione aggiornando la Direttiva 2015/849/UE con l'inserimento della definizione di "*crypto currency*" e dell'espansione della lista di soggetti obbligati in modo da ricomprendere anche i fornitori di servizi per le cripto-attività.

## 3.2 La nozione di valuta virtuale nel diritto italiano ed europeo ai fini antiriciclaggio

La V Direttiva Antiriciclaggio[550] rappresenta poi il primo atto normativo dell'Unione Europea volto a occuparsi in modo esplicito delle "valute virtuali"[551], fenomeno precedentemente privo di una specifica regolamentazione. I considerando 8, 9 e 10 delineano il contesto che ha ispirato il legislatore europeo, sottolineando i seguenti aspetti chiave.

[549] Cfr. E. PEDERZINI, «*La Tracciabilità Dei Movimenti Finanziari Tra Anonimato e Pseudonimato: FinTech, Incorporazione Del Diritto Nella Tecnica e Paradigma by Design», Rivista Di Diritto Bancario*, 2022.

[550] Direttiva (UE) 2018/843 del Parlamento Europeo e del Consiglio del 30 maggio 2018 che modifica la direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo e che modifica le direttive 2009/13/CE e 2013/36/UE.

[551] Si precisa che questa è la definizione tuttora vigente nel sistema normativo antiriciclaggio, sebbene già superata nella prassi e anche nella normativa per effetto dell'approvazione, il 31 maggio 2023, del Regolamento 2023/1114, MiCAR, e del c.d. "Pacchetto VI Direttiva AML".

La direttiva premette che i prestatori di servizi, coinvolti nello scambio tra valute virtuali e legali e nella gestione di portafogli digitali, fino a quel momento erano esclusi dall'obbligo di individuare attività sospette. Tale esclusione crea la possibilità per gruppi terroristici di trasferire denaro in modo discreto all'interno del sistema finanziario dell'Unione, sfruttando un livello di anonimato.

Si evidenzia quindi il potenziale uso improprio delle valute virtuali a fini criminali, in particolare a causa dell'anonimato, che caratterizza gran parte delle transazioni in valuta virtuale[552]. La direttiva riconosce che l'inclusione di alcuni prestatori di servizi tra i soggetti controllati non risolve completamente il problema dell'anonimato, poiché gli utenti possono ancora effettuare operazioni senza coinvolgere tali intermediari[553].

La definizione di valute virtuali viene distinta con chiarezza da concetti come moneta elettronica, fondi e valute di gioco, sottolineando l'obiettivo della direttiva di coprire tutti i possibili utilizzi di valute virtuali. Si evidenzia anche l'urgenza di regolamentare il fenomeno ormai diffuso e talvolta sfruttato per scopi illeciti, pur nella consapevolezza delle sfide legate alla definizione precisa degli strumenti coinvolti.

Precedentemente la BCE, aveva cercato di fornire una definizione delle valute virtuali come un tipo di denaro digitale non regolamentato, emesso e controllato dai suoi sviluppatori, utilizzato all'interno di una specifica comunità virtuale. Tuttavia, la definizione rimaneva aperta a successivi adeguamenti in risposta a modifiche nelle caratteristiche fondamentali, riflettendo la complessità di categorizzare con precisione tali strumenti.

Il legislatore italiano ha recepito la V Direttiva Antiriciclaggio nel proprio ordinamento[554], allineando le definizioni e includendo le finalità di investimento[555]. Il recepimento ha consentito di allineare le definizioni a quelle menzionate in sede unionale.

---

[552] Cfr. Considerando 8, V Direttiva AML.
[553] Cfr. Considerando 9, V Direttiva AML.
[554] Il recepimento della V Direttiva è avvenuto attraverso il D.lgs. n. 125 del 4 ottobre 2019.
[555] Si può osservare che il legislatore italiano ha connotato la nozione di criptovaluta in modo più preciso - già nel 2017 (D.Lgs. n. 90/2017), e ancor più in fase di "ritocco" attraverso le modifiche apportate nel 2019 - di quanto non abbia inteso fare la direttiva europea a monte (cfr. art. 3, par. 1, n. 18 della Direttiva 2015/849/UE). Infatti, messa a raffronto con quella unionale, la definizione domestica si contraddistingue per due importanti differenze. La prima attiene all'aggiunta delle funzioni cui può assolvere la valuta virtuale quale mezzo di scambio: essa, infatti, è utilizzata «come mezzo di scambio per l'acquisto di beni e servizi». La seconda riguarda sempre l'esplicitazione di "come" la valuta virtuale può essere adoperata, precisando però che l'uso può essere per "finalità di investimento". Sulle conseguenze di tali differenze, anche con riguardo ai riflessi pratici, cfr. A. MINTO, «*Riflessioni sull'applicabilità della disciplina antiriciclaggio ai Non-Fungible Tokens ("NFT")*», in *Rivista di Diritto Bancario*, 2023, 41.

Le complesse vicissitudini legate alla definizione di un quadro normativo stabile per le valute virtuali hanno subito notevoli trasformazioni con l'introduzione del Regolamento (UE) 2023/1113 contestualmente al MiCAR. Tale regolamento, nella sezione concernente i dati informativi che accompagnano i trasferimenti di fondi e specifiche cripto-attività, ha apportato modifiche alla direttiva (UE) 2015/849.

Tornando alla nostra disciplina nazionale vigente, codificata nel Decreto Anti-riciclaggio, che per quanto appena detto necessita di urgenti interventi di riordino, seppure scontando una sorta di "obsolescenza genetica" nella definizione del fenomeno, ha comunque consentito di impostare le fondamenta per una regolamentazione e conseguente vigilanza sul comparto delle "valute virtuali" altrimenti destinato a perpetuare quelle caratteristiche di deregolamentazione che ne hanno consentito il rapido successo e la tumultuosa crescita in termini dimensionali; ma al contempo ne hanno enfatizzato le debolezze e i rischi sia dal punto di vista della volatilità dei valori di riferimento sia da quello dell'utilizzo di siffatti strumenti per finalità di riciclaggio e finanziamento del terrorismo.

È stato già evidenziato, infatti, come lo stesso Regolatore europeo, pur cos-sapevole della difficoltà e forse dell'oggettiva impossibilità di attrarre qualunque utilizzo delle valute virtuali all'interno di un "unico *level playing field* ", ha comunque chiaramente tracciato come strada più efficace quella di individuare gli specifici soggetti obbligati agli adempimenti antiriciclaggio e, attraverso questi, perseguire il contrasto alle attività criminose[556].

La normativa italiana, implementata attraverso il Decreto Antiriciclaggio, ha ora avviato le prime forme di vigilanza sugli operatori specializzati in valute virtuali[557]. Con un decreto del Ministero dell'Economia e delle Finanze del febbraio 2022, è stata istituita una sezione speciale all'interno del Registro dei Cambiavalute[558], previsto

[556] L. MURTAS, «*Antiriciclaggio e cripto-attività nella legislazione europea e nazionale*», in *cripto-attività: antiriciclaggio e gestione dei rischi aziendali* (Pacini Editore, 2024), 23–42.

[557] Tale categoria ricomprende, per un verso, i prestatori di servizi relativi all'utilizzo di valute virtuali ("Virtual Asset Service Providers" spesso indicati con l'acronimo "VASP"), definiti all'art. 1, co. 2, lett. *ff)* del D.Lgs. n. 231/2007 come «qualsiasi persona fisica o giuridica che fornisce a terzi, su base professionale, servizi (compresi i servizi online) funzionali all'uso, allo scambio e alla conservazione di "valuta virtuale", nonché al loro cambiamento da o in valute *fiat* o beni digitali, ... nonché all'emissione, offerta, trasferimento, compensazione e qualsiasi altro servizio funzionale all'acquisizione, negoziazione o intermediazione nello scambio di tali valute; per altro verso, i prestatori di servizi di portafoglio digitale (c.d. "*custodian wallet providers*"), definiti come «qualsiasi persona fisica o giuridica che fornisce, a titolo professionale, nei confronti di terzi, anche online, servizi di custodia di chiavi crittografiche per conto dei propri clienti, allo scopo di detenere, conservare e trasferire valute virtuali» (cfr. art. 1, co. 2, lett. *ff-bis*) d.lgs. n. 231/2007).

[558] L'allocazione prescelta evidenzia come il Legislatore italiano sia rimasto ancorato all'associazione delle "valute virtuali" alle valute in senso ampio. La rilevanza dimensionale del fenomeno, i suoi

dall'art. 17-*bis*, comma 1, del D.Lgs. 13 agosto 2010, n. 141, dedicata agli operatori di servizi relativi alle valute virtuali e ai portafogli digitali nel territorio della Repubblica Italiana.

Questa sezione speciale, tenuta dall'organismo per la gestione degli elenchi degli agenti in attività finanziaria e dei mediatori creditizi (OAM), rappresenta un passo significativo nella costruzione di un quadro di vigilanza sul settore. Il decreto del Ministero dell'Economia e delle Finanze 13 gennaio 2022, ha definito le "modalità e la tempistica con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale e i prestatori di servizi di portafoglio digitale sono tenuti a comunicare la propria operatività sul territorio italiano".

Il Decreto MEF rappresenta un'implementazione dell'art. 17-*bis*, comma 8-*ter,* del D.Lgs. n. 141/2010, introdotto insieme al comma 8-*bis* dall'art. 8, comma 1, del D.Lgs. n. 90/2017, nel quadro della trasposizione della IV Direttiva antiriciclaggio (e successivamente modificato dal menzionato decreto legislativo n. 125/2019). In modo più specifico, il comma 8-*bis* dell'art. 17-*bis* estende ai fornitori di servizi relativi all'utilizzo di valute virtuali e ai fornitori di servizi di portafoglio digitale la regolamentazione prevista dallo stesso articolo per i cambiavalute, incluso l'obbligo di registrazione in una sezione apposita del registro dei cambiavalute tenuto dall'OAM e attivo dal 16 maggio 2022[559].

Per garantire un adeguato accesso a questa sezione speciale del registro, il comma 8-*ter* affida al Decreto MEF la definizione delle modalità e dei tempi entro i quali i fornitori di servizi relativi all'utilizzo di valute virtuali e i fornitori di servizi di portafoglio digitale devono comunicare la loro attività in Italia, nonché la definizione delle forme di cooperazione tra il Ministero dell'Economia e delle Finanze e le forze di polizia per interrompere la fornitura di servizi relativi all'utilizzo di valute virtuali da parte dei fornitori che non rispettano l'obbligo di comunicazione.

L'intervento è di estremo interesse, poiché da quanto si legge: "la comunicazione costituisce condizione essenziale per l'esercizio legale dell'attività da parte dei suddetti prestatori"[560]. Inoltre, il Decreto MEF sembra istituire un regime di riserva di

connotati del tutto peculiari nonché le tendenze emergenti dalla normativa europea *in fieri*, che tratteggiano un distacco sempre più evidente da questa originaria matrice anche nel nome che sarà utilizzato (cripto-attività), lasciano pensare a una prossima rivisitazione delle forme di registrazione e di vigilanza.

[559] Cfr, la relazione illustrativa del decreto. E E. PEDERZINI, «*La tracciabilità dei movimenti finanziari: anonimato e pseudoanonimato*», in *Diritto del FinTech* (Cedam, 2020), 122 e ss.

[560] Cfr. art. 17-*bis*, co. 8-*ter*, D.Lgs 241/2010.

attività, limitando l'esercizio dei servizi relativi alle valute virtuali in Italia ai soggetti registrati nella sezione speciale del registro[561]. Di conseguenza, la prestazione di servizi relativi alle criptovalute in Italia da parte di soggetti non registrati potrebbe essere considerata abusiva[562].

Questo intervento solleva questioni sistematiche significative, poiché potrebbe rappresentare un requisito normativo in contrasto con i principi di libera circolazione propri dell'Unione Europea, soprattutto con l'entrata in vigore della disciplina armonizzata della MiCA. Questo non accadrebbe se l'istituzione del registro e le connesse incombenze in esame venissero inquadrate nel contesto della disciplina antiriciclaggio.

### 3.3 Cenni sul *set* regolamentare europeo

Gli operatori in cripto-attività devono adempiere a obblighi di verifica della clientela, conservazione dei dati e segnalazione di operazioni sospette, sebbene in una forma meno articolata rispetto a quella applicabile agli intermediari bancari e finanziari[563].

Sebbene l'impianto iniziale costituisca una base fondamentale, è probabile che nel tempo gli adempimenti antiriciclaggio richiesti a questa categoria di soggetti divengano crescenti.

Il 20 luglio 2021, la Commissione Europea aveva presentato un "pacchetto" di proposte legislative mirate a rafforzare le normative contro il riciclaggio e il finanziamento del terrorismo. Questo pacchetto includeva quattro proposte: un Regolamento che stabilisca una nuova Autorità competente per contrastare il riciclaggio e il finanziamento del terrorismo (Regolamento AMLA)[564], un

[561] Cfr. art. 3 «l'esercizio sul territorio italiano dei servizi relativi all'utilizzo di valuta virtuale o di portafoglio digitale è riservato ai soggetti iscritti nella sezione speciale del registro».
[562] Nella relazione illustrativa al decreto si precisa che la mera attività di emissione di valute virtuali non è di per sé sufficiente a rendere applicabili gli obblighi di registrazione all'OAM, qualora l'attività non sia accompagnata dall'esercizio a titolo professionale per conto della clientela di uno o più servizi relativi all'utilizzo di valute virtuali e/o di portafoglio digitale.
[563] Non trovano infatti applicazione le disposizioni contenute nei fondamentali provvedimenti attuativi del Decreto Antiriciclaggio quali, fra le altre, i Provvedimenti della Banca d'Italia del 26 marzo 2019 in materia di organizzazione, procedure e controlli interni, del 30 luglio 2019 in materia di adeguata verifica, del 24 marzo 2020 in materia di conservazione e messa a disposizione di documenti, dati e informazioni.
[564] Per una analisi delle implicazioni derivanti dall'istituzione di un'autorità europea antiriciclaggio, v. A. URBANI, «*Verso la centralizzazione della supervisione antiriciclaggio?*», *Rivista trimestrale di diritto dell'economia*, fasc. suppl. al n. 1 (2022): 172 e ss., Alla luce della rapida e profonda trasformazione che sta interessando l'attività di vigilanza antiriciclaggio, anche per effetto del processo

Regolamento che disciplini gli adempimenti dei soggetti obbligati, con particolare attenzione alla verifica adeguata della clientela e alla titolarità effettiva (Regolamento antiriciclaggio), una Direttiva che sostituisca l'attuale Direttiva 2015/849/UE (VI Direttiva AML) contenente disposizioni sulle Autorità di Vigilanza e sulle *Financial Intelligence Unit* (FIU) nazionali, e una revisione del Regolamento 2015/847/UE sui trasferimenti di fondi, finalizzato a tracciare i trasferimenti di *crypto-asset*.

Questo pacchetto di proposte intendeva modificare radicalmente non solo il quadro normativo di riferimento, ma anche i comportamenti delle Autorità nazionali e dei soggetti obbligati. L'obiettivo è quello di superare la frammentazione esistente tra gli Stati membri, derivante dall'esercizio delle discrezionalità consentite dalle direttive fino a oggi utilizzate[565].

Di particolare rilevanza in questo contesto è la proposta di revisione del Regolamento 2015/847/UE, emanata attraverso il Regolamento (UE) 2023/1113 che si concentra sul tracciamento dei dati relativi ai trasferimenti di determinate cripto-attività. La proposta si basa sulle modifiche apportate nel giugno 2019 alla Raccomandazione 15 del FATF-GAFI sulle nuove tecnologie, cercando di includere le attività virtuali e i prestatori di servizi in nuovi obblighi informativi per i trasferimenti di cripto-attività. La proposta riconosce le cripto-attività come parte integrante del concetto di "trasferimento di fondi", collegandosi al Regolamento MiCA per la definizione di cripto-attività. Lo stesso MiCA contiene rinvii alle specifiche disposizioni in materia di antiriciclaggio, cosicché i vari progetti in fase di studio che a vario titolo impattano sul tema delle cripto-attività e della finanza digitale dovranno

---

di riforma degli assetti normativi e istituzionali avviato a livello europeo, è stata costituita presso la Banca d'Italia l'Unità "Supervisione e normativa antiriciclaggio" (SNA), al fine di presidiare la crescente complessità dei compiti di vigilanza antiriciclaggio e assicurare, in prospettiva, un indirizzo unitario della funzione. La nuova Unità, collocata in *staff* al Direttorio a garanzia dell'autonomia della funzione, è chiamata a svolgere attività di analisi e di intervento in materia di riciclaggio e contrasto al finanziamento del terrorismo, curando le attività amministrative conseguenti alle risultanze cartolari e ispettive; segue altresì la produzione normativa nazionale e internazionale di rilievo per le finalità istituzionali dell'Unità, intrattenendo i rapporti con le altre Autorità competenti in ambito di contrasto del riciclaggio. L'introduzione dell'AMLA realizzerà un'architettura istituzionale che riecheggia, per molti aspetti, la grande riforma che il mercato creditizio ha conosciuto con l'introduzione del Meccanismo di Vigilanza Unica nel contesto dell'Unione Bancaria Europea. Nella letteratura sul tema, cfr. A. PIERINI, «*L'unione bancaria europea come federalizing process»* (Cedam, 2019) e R. IBRIDO, «*L'unione bancaria europea, profili costituzionali*», (G. Giappichelli Editore,2017).

[565] Queste misure mirano a perfezionare «l'attuale quadro normativo dell'UE, adeguandolo alle sfide nuove ed emergenti legate all'innovazione tecnologica, come le valute virtuali, la maggiore integrazione dei flussi finanziari nel mercato unico e la natura globale delle organizzazioni terroristiche. Queste proposte contribuiranno a creare un quadro molto più coerente per agevolare la conformità degli operatori soggetti alle norme AML/ CFT, in particolare quelli che operano a livello transfrontaliero», Così, il Comunicato Stampa della Commissione Europea, Sconfiggere la criminalità finanziaria: la Commissione riesamina le norme contro il riciclaggio e il finanziamento del terrorismo, 20 luglio 2021 reperibile su https:/ / ec.europa.eu/commission/presscorner/detail/it/ip_21_3690.

convergere in un complesso e contestuale allineamento per evitare lacune, ridondanze, sovrapposizioni e contraddizioni[566].

L'oggetto e il campo di applicazione del Regolamento 2015/847 (disciplinati rispettivamente dall'art. 1 e dall'art. 2, sono stati modificati per includere le informazioni relative al cedente e al cessionario nei trasferimenti di cripto-attività, equiparando i prestatori di servizi per le cripto-attività ai prestatori di servizi di pagamento. Questo adeguamento riflette l'approccio olistico del legislatore europeo, che considera i *token* di moneta elettronica, come definiti dal MiCAR, alla stessa stregua delle cripto-attività.

Nel definire il "trasferimento di cripto-attività", si fa riferimento all'operazione effettuata elettronicamente da un cedente ad un prestatore di servizi per le cripto-attività, al fine di mettere a disposizione delle cripto-attività al cessionario[567].

Le definizioni di "trasferimento di cripto-attività", "cripto-attività" e "prestatore di servizi per le cripto-attività" sono rinviate a quelle codificate nel MiCAR.

La parte centrale del regolamento è rappresentata dal nuovo Capo III, derubricato "obblighi dei prestatori di servizi per le cripto-attività". Gli obblighi di tracciamento dei dati dei trasferimenti di cripto-attività sono divisi tra il prestatore di servizi per le cripto-attività del cedente e quello del cessionario, seguendo il modello utilizzato per altri fondi con la distribuzione delle responsabilità tra il prestatore dei servizi di pagamento dell'ordinante e quello del beneficiario.

---

[566] "Sull'importanza del coordinamento tra comparti disciplinari, v. il considerando n. 8, il quale specifica che «Qualsiasi legislazione adottata nel settore delle cripto-attività dovrebbe essere specifica, pronta alle sfide del futuro e in grado di stare al passo con l'innovazione e gli sviluppi tecnologici. Le "cripto-attività" e la "tecnologia di registro distribuito" dovrebbero pertanto essere definite nel modo più ampio possibile, in modo tale da comprendere tutti i tipi di cripto-attività che attualmente non rientrano nell'ambito di applicazione della legislazione dell'Unione in materia di servizi finanziari. Tale legislazione dovrebbe inoltre contribuire all'obiettivo riguardante la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo. Qualsiasi definizione di "cripto-attività" dovrebbe pertanto corrispondere alla definizione di "attività virtuali" contenuta nelle raccomandazioni del Gruppo di azione finanziaria internazionale (GAFI). Per lo stesso motivo, qualsiasi elenco di servigi per le cripto-attività dovrebbe comprendere anche i servizi relativi alle attività virtuali che potrebbero sollevare preoccupazioni in materia di riciclaggio di denaro e che sono identificati come tali dal GAFI».
Ad onor del vero, la saldatura tra disciplina sostanziale delle cripto-attività e normativa antiriciclaggio non è stata sin da subito perfetta ed anzi si è profilato addirittura il rischio - a nostro avviso - di una eterogenesi dei fini. Durante le fasi intermedie che hanno scandito l'elaborazione del MiCA, infatti, il Parlamento ha suggerito di allargarne obiettivi e ambito di applicazione anche alle «misure volte ad evitare l'uso improprio delle cripto-attività a fini illeciti per proteggere il mercato interno dai rischi connessi al riciclaggio, al finanziamento del terrorismo e ad altre attività criminali» (con l'inserimento della lettera e-bis, all'art. 1). Tale integrazione è stata correttamente espunta nel c.d.
"*compromise text*" in A. MINTO, «*il sistema dei controlli interni delle banche e la gestione del rischio di riciclaggio» Cedam* 2023, 248..

[567] Cfr. Regolamento 2023/1113, art. 3.

Per quanto riguarda gli obblighi del prestatore di servizi per le cripto-attività del cedente, è richiesto di assicurare che i trasferimenti di cripto-attività siano accompagnati dai dati informativi, inclusi il nome del cedente e del cessionario, i numeri di conto pertinenti e l'indirizzo del cedente. Nel caso in cui i trasferimenti non coinvolgano un conto, è richiesto al prestatore di registrare gli identificativi dell'indirizzo del cedente e, se del caso, del cessionario, nel registro distribuito. È importante sottolineare che i dati informativi non devono essere direttamente allegati al trasferimento di cripto-attività o inclusi, ma il prestatore deve verificare la loro accuratezza basandosi su documenti o informazioni ottenuti da fonti affidabili e indipendenti[568].

La riforma organica del diritto antiriciclaggio europeo contempla diverse linee guida, tra cui quella dei presidi organizzativi interni. La Proposta di Regolamento del Parlamento e del Consiglio, del 20 luglio 2021, infatti, mira a rivedere le disposizioni della Direttiva 2015/849/UE.

Innanzitutto, va notato che la struttura della Proposta di Regolamento è più ordinata rispetto alla IV Direttiva antiriciclaggio[569], poiché consolida la disciplina in un blocco di norme già contenute nel Capo II, rubricato "Politiche, controlli e procedure interni dei soggetti obbligati". Ciò evidenzia l'importanza dei presidi organizzativi, che rappresentano il primo obbligo imposto ai destinatari della disciplina. La Proposta enfatizza in particolare lo stretto legame tra "assetti organizzativi" e "gestione del rischio antiriciclaggio". Da un punto di vista sostanziale, non si può affermare che la Proposta enuclei o in maniera esplicita specifici, nuovi obblighi organizzativi in risposta alla diffusione delle cripto-attività. Più opportunamente, essa lo fa in modo "mediato", ossia rendendo conto dell'esistenza di nuove modalità circolatorie della ricchezza e della loro idoneità ad incidere sul contenuto concreto del dovere organizzativo che incombe in capo ai destinatari della disciplina e che impone loro di adottare il protocollo organizzativo adeguato al rischio di riciclaggio cui sono esposti[570].

La centralità della gestione del rischio emerge dall'art. 7 della Proposta, che richiede ai soggetti obbligati di adottare misure adeguate che siano proporzionate alla natura e alle dimensioni dell'impresa in funzione della corretta individuazione e

[568] Cfr. Regolamento 2023/1113, art. 14, par. 4.
[569] Nel quale la materia delle misure organizzative interne è distribuita disorganicamente tra l'art.8 e poi gli artt. 45 e 46.
[570] Cfr. considerando n. 21, 22, 23 e 24.

valutazione dei rischi di riciclaggio, finanziamento del terrorismo ei rischi di mancata applicazione delle sanzioni finanziarie[571]. Secondo la proposta è importante considerare le caratteristiche dei clienti, dei prodotti, dei servizi, dei paesi e dei canali di distribuzione per affrontare efficacemente tali rischi; a tal fine, i soggetti obbligati devono tener conto delle caratteristiche dei loro clienti, dei prodotti, dei servizi o delle operazioni offerti, dei paesi o delle aree geografiche interessati oltreché dei canali di distribuzione utilizzati[572].

La necessità di tenere in considerazione i "nuovi" prodotti e servizi nel contesto di esame ed autovalutazione del rischio, si collega senz'altro a quanto plasticamente espresso nel considerando n. 6: «la tecnologia continua a evolversi, offrendo al settore privato l'opportunità di sviluppare nuovi prodotti e sistemi per scambiare fondi o valore. Tale fenomeno, seppur positivo, può generare nuovi rischi di riciclaggio e finanziamento del terrorismo, in quanto i criminali riescono continuamente a trovare modi per sfruttare le vulnerabilità al fine di occultare e trasferire fondi illeciti in ogni parte del mondo. I fornitori di servizi per le cripto-attività e le piattaforme di *crowdfunding* sono esposti all'uso improprio di nuovi canali per la circolazione di denaro illecito e si trovano nella posizione ideale per individuare tali movimenti e mitigare i rischi».

Il fornitore di servizi per le cripto-attività del cessionario, inoltre, è soggetto a diversi obblighi ai fini della verifica e del monitoraggio dei trasferimenti di cripto-attività.

Inizialmente, deve adottare procedure efficaci, eventualmente includendo il monitoraggio nella fase dei trasferimenti, per garantire l'inclusione accurata dei dati informativi nei trasferimenti di cripto-attività.

La normativa introduce una soglia di materialità, differenziando gli obblighi di verifica in base all'importo del trasferimento; se l'importo è superiore a 1000 euro[573], il prestatore di servizi per le cripto-attività del cessionario è tenuto a verificare l'accuratezza dei dati utilizzando documenti, dati o informazioni provenienti da fonti

[571] La Proposta di Regolamento introduce la nuova nozione di "sanzioni finanziarie mirate" , con la quale si intende "il congelamento dei beni e il divieto di mettere a disposizione, direttamente o indirettamente, fondi o altri beni a beneficio di persone ed entità designate a norma delle decisioni del Consiglio adottate sulla base dell'articolo 29 del trattato sull' unione europea e dei regolamenti del Consiglio adottati sulla base dell'articolo 215 del trattato sul funzionamento dell'Unione europea" (cfr. art. 2, par. 1, n. 35).
[572] Cfr. considerando n. 20.

[573] Da calcolare non soltanto su operazioni singole ma anche cumulando più operazioni che appaiano tra loro collegate.

affidabili e indipendenti. Nel caso in cui l'importo sia inferiore a 1000 euro, l'obbligo di verifica si applica solo se il prestatore di servizi per le cripto-attività del cessionario effettua pagamenti in contanti o in moneta elettronica anonima o ha ragionevoli sospetti di riciclaggio o finanziamento del terrorismo.

Inoltre, il prestatore di servizi per le cripto-attività del cessionario ha responsabilità specifiche nei casi in cui il trasferimento di cripto-attività non sia accompagnato dai dati informativi prescritti. Deve rifiutare il trasferimento o richiedere i dati mancanti relativi al cedente e al cessionario prima di mettere le cripto-attività a disposizione del cessionario. Nel caso di omissioni ripetute da parte del prestatore di servizi di pagamento nel fornire i dati richiesti, il fornitore di servizi per le cripto-attività del cessionario deve adottare misure specifiche, che possono includere richiami, diffide o addirittura la restituzione delle cripto-attività trasferite.

Infine, l'Autorità competente responsabile della sorveglianza del rispetto delle normative antiriciclaggio e antiterrorismo deve essere informata dal prestatore di servizi per le cripto-attività del cessionario in caso di violazioni dei requisiti informativi obbligatori; in questa circostanza, il prestatore di servizi segnalante deve anche fornire dettagli sulle misure adottate.

Appare utile segnalare che l'entrata in vigore del nuovo testo del regolamento ha comportato un allineamento significativo degli obblighi di tracciamento dei dati informativi per i trasferimenti di cripto-attività, pur considerando le peculiarità della tecnologia sottostante basata su registri distribuiti.

Da questa analisi emergono però alcuni limiti significativi; poichè l'obbligo di tracciamento delle transazioni, imposto ai fornitori di servizi per le cripto-attività come gli *exchange* e i *custodian wallet*[574], ciò non consente di tracciare i trasferimenti che avvengono tra *wallet* c.d. *unhosted*[575] o che non transitano attraverso una piattaforma *exchange*. Pertanto, il Regolamento non può estendersi a tracciare tutte le transazioni, specialmente quelle che avvengono su reti decentralizzate come la DeFi.

Nonostante questo limite, il Regolamento rappresenta comunque un notevole progresso nel rendere compatibile l'anonimato tipico delle *blockchain* con la necessità di divulgarne i dettagli, come richiesto dalle norme. Infatti, l'applicazione di tali regole

[574] I *wallet* si distinguono tra *provider* e *custodian* a seconda che offrano i servizi di custodia e amministrazione del conto di valute virtuali (*wallet* elettronico) e la gestione delle transazioni del cliente e/o la custodia della chiave pubblica e privata del medesimo cliente; possono essere conservati sia *online* ("*hot storage*") che *offline (*"*cold storage*"), in quest'ultimo caso con maggiori caratteristiche di sicurezza dal rischio di hackeraggio.
[575] Non detenuti tramite un *custodian*.

consentirebbe agli operatori di servizi in cripto-attività e alle autorità antiriciclaggio e antiterrorismo di accedere ai dati di transazione, anche se limitatamente a quelle coinvolgenti i fornitori di servizi.

Inoltre, i criminali che agiscono nel contesto delle cripto-attività sono spesso spinti a convertire tali *asset* in valuta *fiat* tramite i fornitori di servizi *off-ramp*[576]. Questi intermediari sarebbero tenuti a registrare tutte le transazioni in modo trasparente, contribuendo così agli sforzi di contrasto al riciclaggio e al finanziamento del terrorismo.

D'altra parte, l'accelerata tendenza verso la "tokenizzazione" degli *asset* e l'adozione sempre più diffusa della DeFi come strumento di *disruption* del sistema finanziario tradizionale richiedono l'implementazione di nuovi strumenti[577], sia a livello normativo che tecnologico, per affrontare le sfide crescenti legate al riciclaggio e per superare l'approccio centralizzato delle transazioni finanziarie.

## 3.4 Presidi nazionali antiriciclaggio

Come è noto, il Decreto Legislativo 8 giugno 2001, n. 231, ha introdotto nella legislazione italiana la "responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica".

La suddetta responsabilità amministrativa degli Enti, si basa sull'attribuzione all'Ente della responsabilità per fatti illeciti commessi da persone fisiche all'interno della sua struttura, nel suo interesse o vantaggio[578]. Questa responsabilità è autonoma rispetto a quella penale della persona fisica autrice del reato e si affianca ad essa[579].

Per essere considerato responsabile, l'Ente deve aver agevolato la realizzazione del reato, non adottando adeguate misure di prevenzione.

Nel contesto delle cripto-attività, un Ente operante in questo settore potrebbe essere chiamato a rispondere per fatti illeciti commessi da soggetti ad esso funzionalmente legati. È quindi necessario esaminare le possibili fattispecie criminose

[576] Servizi che permettono di convertire cripto-attività in valuta *fiat*.
[577] Sono attualmente in via di sviluppo *computer* quantistici che sono in grado di processare enormi quantità di dati e risolvere problemi complessi in un tempo enormemente più veloce rispetto agli attuali computer grazie alle proprietà del *qubit*. Questi potrebbero far venire meno la sicurezza raggiunta oggi dalle tecniche crittografiche in relazione all'anonimizzazione.
[578] Cfr. A. BERNASCONI e A. PRESUTTI, «*Manuale della responsabilità degli enti»,* (Giuffrè Francis Lefebvre, 2018).
[579] Cfr. G. DE SIMONE, «*La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi) d'imputazione*», 28 ottobre 2012, in Diritto Penale Contemporaneo.

previste per gli Enti operanti con cripto-attività[580], considerando reati come il riciclaggio, i reati societari, la corruzione, i delitti informatici, i reati tributari e i nuovi delitti legati agli strumenti di pagamento virtuali.

Le caratteristiche intrinseche delle cripto-attività, come l'anonimato e la difficoltà di tracciabilità e la riservatezza, le rendono adatte al perseguimento di scopi illeciti, come il riciclaggio di proventi illeciti, l'elusione fiscale e la falsificazione di informazioni societarie[581]. Queste sono solo alcune delle possibili modalità di strumentalizzazione.

L'attività di "*cyberlaundering*"[582] viene sanzionata differentemente all'interno dell'ordinamento italiano; se l'acquisto di cripto-attività avvenisse tramite denaro di provenienza illecita potrebbe costituire un reato ai sensi dell'articolo 648-bis c.p., infatti, le varie attività di sostituzione, trasferimento e utilizzo di criptovalute possono costituire ostacoli all'identificazione dell'origine criminosa dei fondi[583].

L'occultamento dell'origine illecita dei capitali può avvenire sia mediante l'acquisto iniziale di criptovalute con denaro contante (noto come "riciclaggio digitale strumentale"), convertendo così moneta fisica legale in moneta virtuale, sia mediante il "riciclaggio digitale integrale", che consiste in uno scambio diretto di cripto-attività[584].

---

[580] L'attenzione dovrà essere posta altresì su quelle fattispecie delittuose che, benché non ricomprese tra i reati presupposto della normativa 231/2001, siano ad essi strumentali o propedeutiche.

[581] A. ROSATO, «*Profili penali delle criptovalute*», in Quaderni del Centro di Ricerca Sicurezza e Terrorismo (Pacini Giuridica, 2021).

[582] Cfr. R. RAZZANTE, «*Riciclaggio e reati connessi. Applicazioni giurisprudenziali e di vigilanza»,* (Giuffrè Francis Lefebvre, 2023).

[583] «La tradizionale distinzione in tre fasi dell'attività di riciclaggio - *placement* (piazzamento materiale dei proventi ad es. dei contanti presso istituti bancari), *layering* (stratificazione tramite operazioni volte a separare il capitale dalla sua origine, ad es. spostandolo in paradisi *off shore*) ed *integration* (integrazione nei circuiti legali con investimenti leciti) - potrebbe essere ricondotta a quelle di "sostituzione", "trasferimento", "altre operazioni che ostacolano l'identificazione della provenienza"» in L. PICOTTI, «*Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*», *Cedam*, Rivista trimestrale di diritto penale dell'economia, fasc. 3–4 (2018): 590–619.

[584] Nella prima ipotesi di "riciclaggio digitale strumentale" almeno una delle tre fasi di *cyberlaundering* (collocazione - dissimulazione - integrazione) è svolta in via digitale. Al contrario, nel caso di "riciclaggio digitale integrale" tutte le fasi di riciclaggio sono realizzate digitalmente. in G.J. SICIGNANO, «*231 e criptovalute*», Pacini Editore,2021, soltanto per mezzo del "riciclaggio digitale strumentale" sarebbe possibile ostacolare l'individuazione della provenienza delittuosa del "denaro sporco", diversamente dalla seconda ipotesi, quella di "riciclaggio digitale integrale", in cui invece l'intera operazione è tracciata. e non si verifica alcuna attività evidente di dissimulazione».
Spiega dettagliatamente la distinzione di tali diverse tipologie di riciclaggio A. ROSATO, «*Profili penali delle criptovalute*», cit. e P. IOVINO, «*Le criptovalute nella fase di layering del riciclaggio*», in Giurisprudenza Penale, 3/2022, sottolinea come «la fase di *placement* ovvero l'immissione dei proventi illeciti nel circuito finanziario o bancario, senza ombra di dubbio rappresenta la fase più delicata del processo, in quanto gli obblighi dettati dalla normativa antiriciclaggio cui sono soggetti gli intermediari finanziari e non, potrebbero portare all'attivazione di *red lags* che, a loro volta, determinerebbero l'inoltro di una segnalazione per operazione sospetta all'Unità di Informazione finanziaria, con il successivo blocco dei fondi e sospensione del operazione stessa. Tale immissione può avvenire nei modi

La difficoltà nell'accertare l'origine illecita dei fondi diventa ancora più seria quando i soggetti interessati utilizzano tecniche di "*mixing*" o "*tumbling*", per confondere le tracce delle transazioni.

Se invece l'acquisto di cripto-attività con denaro illecito è compiuto dallo stesso autore del reato, si potrebbe configurare il reato di autoriciclaggio secondo l'articolo 648-ter. c.p. occorre distinguere se l'acquisto di moneta digitale sia considerato una destinazione in "attività [...], finanziarie, [...] o speculative" anziché una mera conversione o sostituzione di denaro in cripto-attività[585].

Per garantire la conformità con le disposizioni normative in materia di antiriciclaggio, i prestatori di servizi per le cripto-attività devono rispettare gli obblighi previsti dal Decreto Legislativo n. 231/2007, segnatamente degli articoli 35 e 55[586] e seguenti.

Gli operatori finanziari in cripto-attività sono soggetti alle normative che disciplinano l'utilizzo della valuta virtuale, e in caso di violazioni, possono essere chiamati a rispondere di gravi illeciti; tali obblighi includono la necessità di effettuare un'adeguata verifica dell'identità dei clienti, la conservazione delle informazioni raccolte durante le transazioni, la fornitura di informazioni veritiere e la segnalazione di operazioni sospette all'Unità di Informazione Finanziaria (UIF)[587].

In caso di mancato adempimento di tali obblighi, questi prestatori di servizi potrebbero essere soggetti a contestazioni relative non solo alla violazione delle normative antiriciclaggio ma anche al possibile concorso di persone[588] nel reato di riciclaggio, in base all'articolo 648-bis c.p. realizzato dai propri clienti[589]. Questo scenario ipotizza un'omissione volontaria nel compimento degli obblighi, configurando una posizione di garanzia nei confronti dei clienti per impedire il reato di riciclaggio[590].

---

più disparati si pensi, a titolo esemplificativo, alle tecniche di *smurfing* o *structuring*, che consistono nell'effettuare numerosi e piccoli depositi di denaro contante al fine di eludere le soglie di rilevazione da parte degli istituti di credito, oltre le quali scatterebbero gli obblighi di segnalazione di operazione sospetta» sul punto A. R. CASTALDO, M. NADDEO, «*Il denaro sporco. Prevenzione e repressione nella lotta al riciclaggio»* (Cedam, 2010).

[585] Cfr. Cass. Pen., Sez. II, 25 gennaio 2022, n.2868 e Cass. Pen., Sez. II, 13 luglio 2022, n.27023. Per un commento di quest'ultima, si veda F. COLAZZO, «*Investire i profitti della truffa per acquistare criptovalute integra il reato di autoriciclaggio*» in Antiriciclaggio e compliance (2022).

[586] Come riformato dal D.lgs. n. 125/2019.

[587] L. DI STEFANO, «*La richiesta di sospensiva di operazioni sospette da parte degli exchangers e dei wallet providers*», 2021.

[588] *Ex* art. 110 c.p.

[589] Reato presupposto dalla responsabilità amministrativa degli Enti, *ex* D.lgs. 231/2001, art. 25-*octies*.

[590] Cass. Pen., Sezione II, n.9472/2016, in materia di intermediari finanziari, richiama in particolare un caso di omessa segnalazione di operazioni sospette.

Si ritiene che, in determinate circostanze, gli *exchange* ed i *custodian wallet provider* possano addirittura rispondere di reati previsti dall'articolo 55 del D.Lgs. n. 231/2007 in concorso formale o materiale con il reato di riciclaggio, realizzandoli cioè in proprio e non in concorso con gli utenti[591].

Tuttavia, sorgono perplessità riguardo alla possibilità di assorbire l'illecito previsto dalla normativa antiriciclaggio in reati più gravi[592]. Laddove, infatti, tali prestatori di servizi pongano in essere condotte atipiche rispetto alle previsioni dell'articolo 55, essi saranno perseguibili solo per il reato di cui all'art. 648-bis c.p.[593].

In sintesi, la responsabilità amministrativa dell'Ente, ai sensi del Decreto Legislativo 8 giugno 2001, n. 231, può derivare dalla commissione di reati legati ai *crypto-asset*, come ricettazione, riciclaggio, autoriciclaggio ed impiego di denaro illecito. Affinché l'Ente possa prevenire tali reati, è cruciale adottare un efficace Modello di Organizzazione, Gestione e Controllo, come previsto dalla nuova normativa eurounitaria.

Questo rappresenta un punto di partenza fondamentale e comporta un'analisi approfondita dei rischi (c.d. *risk assessment*)[594], considerando le specifiche ipotesi di reato legate alle cripto-attività.

Il Modello deve quindi comprendere una parte generale che includa i sistemi organizzativi, le deleghe, il Codice Etico, l'Organismo di Vigilanza (ODV), ed una una parte speciale con dettagli sulle singole fattispecie di reato, principi di comportamento, protocolli e procedure di gestione del rischio.

La gestione dei sistemi informativi deve essere attentamente monitorata, anche considerando il possibile coinvolgimento di programmi informatici nei reati con criptovalute[595].

---

[591] L. DI STEFANO, «*Le criptovalute e la disciplina di cui al D.lgs. n. 231/2001*», in *Cripto-attività: antiriciclaggio e gestione dei rischi aziendali* (Pacini Editore, 2024), 126.

[592] Cfr. M. GIUCA, «*Criptovalute e diritto penale nella prevenzione e repressione del riciclaggio*» in Diritto Penale Contemporaneo (1/2021): 150 e ss.

[593] G.P. ACCINNI, «*Cybersecurity e criptovalute: rilevanza penale dopo la Quinta Direttiva*» in sistema penale (15 maggio 2020).

[594] «Ai fini del *risk assessment* 231 si evidenzia la famiglia dei reati di ricettazione, riciclaggio e autoriciclaggio, nonché - stando al tenore letterale del comma 2, art. 25-*octies*.1 - ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio», in A. DE VIVO, C. ZANICHELLI, «*Il difficile risk assessment 231 per i delitti in materia di strumenti di pagamento diversi dai contanti*», febbraio 2022.

[595] Ad esempio, deve essere integrata la predisposizione di adeguati strumenti informatici atti a prevenire la commissione di questi reati, come requisiti di autenticazione ai sistemi per l'accesso ai dati mediante la creazione di *password* etc.

L'adozione e l'aggiornamento regolare del Modello consentono alle società di prevenire la responsabilità amministrativa, fornendo un solido strumento di gestione dei rischi legati all'uso delle criptovalute.

Per ottenere l'esenzione dalla responsabilità amministrativa secondo il D.Lgs. n. 231/2001, è necessario affidare all'Organismo di Vigilanza (OdV) il compito di supervisionare l'adeguatezza, il funzionamento e l'osservanza dei Modelli Organizzativi adottati all'interno dell'ente.

L'OdV deve valutare l'efficacia, la reale capacità e la stabilità persistente del Modello Organizzativo, garantendo la prevenzione dei reati presupposti. A tale scopo, l'Organismo possiede ampi poteri di ispezione e controllo, che gli consentono l'accesso a qualsiasi informazione o dato aziendale anche attraverso strutture interne.

Pur avendo l'obbligo di segnalare condotte illecite, l'OdV non assume alcuna posizione di garanzia riguardo all'impedimento dei reati da parte dell'ente. Questa esclusione è particolarmente critica quando l'Organismo di Vigilanza coincide, almeno in parte, con il Collegio Sindacale, soggetto agli obblighi di vigilanza e comunicazione in materia di antiriciclaggio ai sensi del D.Lgs. n. 231/2007.

La sovrapposizione di funzioni tra il Collegio Sindacale e l'Organismo di Vigilanza, tuttavia, crea possibili interferenze tra le diverse cariche[596]. La coincidenza di incarichi rimane però una caratteristica peculiare nel settore bancario-finanziario-assicurativo[597].

Per quanto concerne le condotte illecite, l'OdV dovrà porre attenzione sia a quelle in cui le cripto-attività costituiscono un mero elemento accidentale della fattispecie[598] (da intendersi quale trasposizione *online* di illeciti comuni), sia a quelle in cui i *crypto-asset* rappresentino l'elemento costitutivo del reato,[599] ovvero in tutti i casi in cui la cripto-attività non è un semplice mezzo alternativo alla moneta tradizionale nel compimento del reato, bensì costituisce un tratto caratterizzante ed insostituibile della concreta manifestazione criminosa[600].

---

[596] Cfr. E. DI FIORINO, C. SANTORIELLO, «*L' organismo di vigilanza nel sistema 231»,* (Pacini Editore, 2020).

[597] Laddove la diversa scelta di affidamento delle funzioni di OdV ad organi soggettivamente distinti dal collegio sindacale deve essere supportata da "adeguata motivazione". (così Banca D'Italia, circolare n. 285/2013, "disposizioni di vigilanza per le banche", aggiornamento 23 settembre 2020, Parte I).

[598] Ovvero reati di truffa aggravata in danno allo stato, di un Ente Pubblico, dell'UE, o per il conseguimento di erogazioni pubbliche, scommesse illegali e pedopornografia (reati presupposto della responsabilità amministrativa degli Enti, *ex* Dlgs. N. 231/2001, rispettivamente agli artt. 24, 25-*quinquies* e 25-*quaterdecies*).

[599] È il caso del furto di valuta virtuale, del riciclaggio (reato presupposto ai sensi dell'art 25-*octies* del D.Lgs. 231/2001) e del finanziamento al terrorismo internazionale (in forza dell'art 25-*quater*).

[600] G.P. ACCINNI, «*Cybersecurity e criptovalute*» 15 maggio 2020, in Sistema Penale.

L'OdV deve anche vigilare sugli "altri operatori (non) finanziari" in cripto-attività, verificando la loro iscrizione nella Sezione speciale del Registro dei Cambiavalute tenuto dall'OAM.

Nonostante la mancata osservanza dell'obbligo di iscrizione costituisca un mero illecito amministrativo[601], tale circostanza potrebbe costituire per l'OdV un rilevante indice di allerta di una illegittimità operativa da parte dell'operatore.

Risulta concreto, infatti, il rischio della configurabilità del reato di abusivismo finanziario, *ex* art. 166, comma 1, lett. c), del D.Lgs. n. 58/1993 TUF, a carico dell'*exchange* di cripto-attività[602].

Tutto ciò conferma quanto importante e stretto sia il legame tra valutazione del rischio, gestione del rischio e assetti organizzativi interni.

Non è quindi un caso che il legislatore intenda adottare una serie di precauzioni proprio con riguardo al delicato momento della valutazione del rischio di riciclaggio. Per un verso, esso demanda alle autorità di vigilanza di settore l'individuazione dei criteri e della metodologia con cui l'autovalutazione deve essere effettuata; per l'altro, richiede ai soggetti obbligati l'invio periodico del *report* sull'autovalutazione alle autorità di vigilanza[603]. Si noti che dal tenore letterale della disposizione in oggetto, si tratterebbe di una condivisione funzionale[604]; Al di là di Autorità come l'UIF, la Guardia di Finanza, la Direzione Investigativa Antimafia - per le quali sembra facile intuire cosa possa significare il riferimento all'uso di questa autovalutazione del rischio per l'sercizio dei poteri repressivi e di contrasto del fenomeno criminale è lecito domandarsi se la trasmissione alla Banca d'Italia possa rappresentare un ulteriore punto di accesso del *supervisor* per esaminare e garantire più in generale la sana e prudente gestione dell'intermediario, a partire dall'analisi del rispetto della disciplina antiriciclaggio.

---

[601] *Ex* art. 17-*bis*, comma 5, del D.Lgs. n. 141/2010.

[602] Parte della dottrina è in disaccordo: "si ritiene al contrario che non siano realizzabili i reati di abusivismo bancario (articoli 130 e seguenti del TUB), non svolgendo i cambiavalute le relative specifiche attività riservate" in A. CINQUE, «*La blockchain: Smart contract - cripto-attività - applicazioni pratiche*» (Pacini Editore, 2022).

[603] «la valutazione di cui al comma 2 [dell'art. 15 d.lgs. n. 231/2007] è documentata, periodicamente aggiornata e messa a disposizione delle autorità di cui all'articolo 21, comma 2, lettera a), e degli organismi di autoregolamentazione, ai fini dell'esercizio delle rispettive funzioni e dei rispettivi poteri in materia di prevenzione del riciclaggio e di finanziamento del terrorismo» in A. Minto, *il sistema dei controlli interni delle banche e la gestione del rischio di riciclaggio*.

[604] Non si dice che la valutazione è "trasmessa" quasi si trattasse di un adempimento afferente alla vigilanza c.d. cartolare, bensì "messa a disposizione".

### 3.5 Prospettive regolatorie

Il controllo sul riciclaggio e il finanziamento del terrorismo sono divenuti una priorità assoluta per i regolatori e autorità politiche. È fondamentale che le aziende del settore, in particolare gli intermediari vigilati, implementino robusti ed efficaci presidi e controlli per garantire la *compliance* con le normative nazionali ed europee.

Come è stato evidenziato, l'approccio basato sul rischio specifico è cruciale e richiede un'attenta valutazione che consideri le caratteristiche specifiche di ciascun *crypto-asset* trattato. È fondamentale comprendere che i *crypto-asset* sono diversi tra loro e che i criminali sono in grado di sfruttare le loro specifiche proprietà. Pertanto, è essenziale sviluppare un approccio tecnico piuttosto che regolamentare generico per implementare un sistema di presidi e controlli efficace.

L'assunzione di personale adeguato e il dialogo proattivo con le autorità di regolamentazione sono cruciali per le aziende al fine di adeguarsi a normative in rapida evoluzione. In altre parole, le aziende devono essere pronte ad apportare modifiche non solo al programma di *compliance*, ma anche ai prodotti, ai servizi offerti e alle modalità di vendita.

Sebbene ci siano tecniche criminali comuni che coinvolgono le cripto-attività, ci sono sfumature e aree in cui si presentano rilevanti differenze, che non possono essere identificate utilizzando i medesimi indicatori di anomalie.

L'evoluzione del panorama normativo può richiedere modifiche ai *framework* esistenti o la creazione di nuovi regolamenti aziendali specifici per le attività in *crypto-asset*.

All'interno del panorama *crypto*, gli eventi si manifestano in modo più veloce e complesso rispetto al panorama ordinario. Le combinazioni di anonimato e *dark web* sono difficili da monitorare e presentano rischi significativi. Gli eventi recenti hanno visto un aumento esponenziale delle minacce legate a crimini come il riciclaggio, i crimini informatici ed il finanziamento del terrorismo[605].

Le conseguenze della non conformità AML per gli intermediari vigilati sono sempre più severe, con possibili multe elevate, danni alla reputazione e rischi per il fatturato. Le autorità di regolamentazione possono richiedere una revisione dei

[605] Cfr. BANCA D'ITALIA, UIF, «*Quaderni dell'antiriciclaggio dell'Unità di Informazione Finanziaria. dati statistici*», 1/2023.

processi AML/CFT e, in casi gravi di non conformità, possono sospendere o revocare la licenza all'impresa.

In sintesi, con il continuo sviluppo dei quadri normativi per le cripto-attività, le aziende e gli intermediari devono affrontare un panorama in continua evoluzione; tuttavia una delle maggiori sfide che gli intermediari sono chiamati ad affrontare, è la mancanza di una regolamentazione standardizzata a livello globale.

Essi dovranno rimanere costantemente informati sulle modifiche legislative esistenti, sulle nuove leggi, sui regolamenti in via di pubblicazione, sulle sanzioni attuali e anche su quelle previste, al fine di essere pronti ad affrontare l'imminente ondata di cambiamenti normativi.

Attualmente, la "*travel rule*" rappresenta una delle sfide più significative in termini di conformità.

Purtroppo, non esistendo una soluzione standardizzata che sia adeguata a tutti gli operatori di mercato, gli intermediari dovranno esplorare diverse opzioni per affrontare questa sfida; in particolare, è fondamentale che siano in grado di raccogliere e conservare i dati in un formato standardizzato simile allo schema di dati sviluppato dagli *InterVASP Messaging Standards (*IVMS-101)[606].

Sebbene la conformità alla *travel rule* sia importante, essa rappresenta solo una parte minima del programma complessivo di prevenzione del riciclaggio e del contrasto al finanziamento del terrorismo. La documentazione richiesta alle imprese del settore in materia di requisiti generali di licenza e conformità richiede tempo e risorse e deve coprire tutti gli aspetti del processo, dall'*on-boarding* alla valutazione del rischio, dal monitoraggio continuo (compresa la sorveglianza delle transazioni) alla presentazione di rapporti di attività sospette e alla tenuta dei registri. Le imprese del

[606] "Nell'ottobre 2018, il GAFI ha adottato alcune modifiche alle sue Raccomandazioni per chiarire esplicitamente che esse si applicano anche alle attività finanziarie che coinvolgono beni virtuali (*virtual asset*), ampliando di fatto l'ambito di applicazione ai fornitori di servizi di beni virtuali (*virtual asset service provider* o VASP) e ad altri soggetti obbligati che svolgono o forniscono attività in materia di *virtual asset*. Esiste la necessità, sostiene il GAFI, che vengano adottati approcci uniformi e vengano stabiliti *standard* comuni per consentire sia ai VASP sia agli intermediari che si affacciano a questo mondo di adempiere agli obblighi derivanti dalle Raccomandazioni. Per affrontare il problema, nel dicembre 2019 è stato costituito un gruppo di lavoro congiunto di esperti tecnici intersettoriali e interprofessionali, che ha sviluppato un nuovo *standard* tecnico di messaggistica interVASP (JWG) e di flussi informativi. Tale gruppo di lavoro è nato dalla collaborazione fra tre associazioni di settore, *leader* a livello internazionale, che rappresentano i VASP: Chamber of Digital Commerce, Global Digital Finance (GDF) e International Digital Asset Exchange Association (IDAXA). In L. GANDOLFI, «*Cripto-asset e intermediari vigilati: una guida per progettare e presentare un piano AML volto a mitigare efficacemente i rischi*», in *Cripto-attività: antiriciclaggio e gestione dei rischi aziendali* (Pacini Editore, 2024), 51 e ss.

settore devono quindi assicurarsi di avere tutta la documentazione ed il personale necessari per soddisfare i requisiti generali di licenza.

La valutazione del rischio consente di identificare e gestire i potenziali rischi legati al riciclaggio di denaro e al finanziamento del terrorismo, con l'obiettivo di mitigarli in modo efficace. Sebbene alcuni aspetti della valutazione siano simili a quelli adottati da altre istituzioni finanziarie, è essenziale valutare in modo specifico i rischi relativi ai prodotti e servizi offerti, ai tipi di clientela, e alle giurisdizioni coinvolte.

Tali aspetti critici includono l'adozione di processi accurati di verifica dell'identità dei clienti durante la fase di acquisizione, il monitoraggio attento del flusso di denaro attraverso la *blockchain*, la previsione delle aspettative delle autorità di regolamentazione e la valutazione dei rischi associati alle risorse virtuali. È fondamentale che la valutazione del rischio venga aggiornata regolarmente per tenere conto di eventi significativi come il lancio di nuovi prodotti e l'avvento delle modifiche normative.

# Considerazioni conclusive

Con il termine "*FinTech*" ci si riferisce ad un insieme vastissimo e variegato di innovazioni finanziarie, ognuna con diversi *business model.* La nozione *de quo*, in ragione degli eterogenei fenomeni che essa sottende, pone una ampio ventaglio di interrogativi; non si tratta soltanto di profili di natura regolatoria o di vigilanza - seppure questi assumano connotati di assoluto rilievo - bensì anche della individuazione delle ricadute derivanti dallo svolgimento delle attività finanziarie attraverso l'utilizzo delle nuove tecnologie, nonché del rapporto con i soggetti utilizzatori di quei servizi innovativi e dei profili della loro necessaria tutela.

Gli interpreti più attenti hanno colto la problematicità di questi aspetti, evidenziando come "*FinTech*", per definizione, rende ragione alla teoria della unitarietà dei mercati finanziari, e, in qualche modo, la esalta, portandola alle sue estreme conseguenze; se infatti una regolamentazione è necessaria od opportuna, questa non potrà non tenere conto della natura intrinsecamente integrata del mercato dei servizi offerti tramite *FinTech*.

Da questa considerazione, e da quella, ulteriore, che attraverso le nuove tecnologie vengono forniti servizi di uguale natura (*rectius*: aventi il medesimo oggetto) rispetto a quelli già resi attraverso le modalità "tradizionali", deriva l'affermazione del paradigma della c.d. "neutralità tecnologica", che si esprime nel brocardo "*stessi servizi, stessi rischi, stesse regole*", ed è sottesa all'attività regolatoria eurounitaria.

Dal momento, cioè, che la strada di una regolamentazione specifica del fenomeno *FinTech* non sarebbe percorribile e neppure efficace, si perviene alla conclusione che, laddove vengano svolte le medesime attività, dovrebbero poter continuare ad operare le medesime regole. Alla stregua di questo principio, dunque, le regole sarebbero tendenzialmente le medesime: ma si tratta di una raffigurazione realistica?

In realtà, la constatazione della natura del "*FinTech*" porta inevitabilmente a ripensare i modelli di vigilanza, conducendo ad un tramonto più o meno definitivo del modello per soggetti. L'ulteriore problema che si pone è quello che riguarda gli enti regolatori, o, ancor meglio, la pluralità dei medesimi. Il diverso "taglio" ed il nuovo approccio dei soggetti regolatori rispetto ad uno stesso oggetto (se non altro sotto il

profilo del mercato su cui il fenomeno produce il proprio impatto) non può non essere concepito come una "discrasia" del sistema normativo.

In ogni caso, appare chiaro che l'approccio regolatorio dovrà tenere conto del carattere disomogeneo del fenomeno e quindi dovrà essere caratterizzato da un notevole livello di adattabilità e di proporzionalità, oltre che di gradualità; dovrà inoltre avere un carattere di sufficiente univocità ed integrazione non potendo essere condizionato da differenti tendenze e dovrà da ultimo avere carattere transnazionale, alla luce della natura "intrinsecamente *cross-border*" dei servizi prestati.

Nell'anno 2022 si è assistito al fenomeno denominato "*crypto-winter*", caratterizzato da diversi fallimenti di soggetti operanti sul mercato, *in primis* da quello dell'*exchange* FTX.

Come si è tentato di dimostrare nel presente elaborato, al di là di ciò che si possa pensare, il fallimento in questione attiene principalmente a problematiche societarie tradizionali che non hanno a che vedere con l'ecosistema *FinTech*.

Il punto critico dalla vicenda è stata la totale assenza di norme regolamentari applicabili al caso specifico e ciò ha reso possibile condotte ed operazioni fraudolente e molto spesso irregolari.

Proprio come accaduto per Lehman Brothers nella crisi degli anni 2007/2008, FTX rappresenta l'emblema di un settore troppo grande per poter essere deregolamentato.

Il presente elaborato si è posto l'obiettivo di dimostrare la presenza di numerose analogie tra il mercato tradizionale ed il mercato *crypto*, seppur con i necessari adattamenti tecnologici.

I risultati del presente elaborato indicano che la posizione di rischio e di liquidità di FTX, soprattutto in relazione alle criptovalute emesse privatamente ed ai successivi effetti di contagio sul mercato e la maggiore interconnessione con gli *asset* tradizionali può manifestarsi attualmente in scenari negativi di portata molto più ampia. Il ruolo centrale di questi *token* non regolamentati nel fallimento di FTX e la mancanza di trasparenza nelle riserve detenute, dovrebbero servire da forte monito riguardo all'immaturità del settore delle cripto-attività e su quanto la regolamentazione sia ancora inadeguata. In altre parole, gli eventi descritti rappresentano un forte avvertimento sulla necessità di una solida regolamentazione coordinata a livello internazionale.

Sulla scia delle analogie tra mercato tradizionale e *crypto*, ritengo che sia più che necessario, in uno scenario regolamentare come quello europeo, l'intervento sul mercato della Banca Centrale. Infatti, con l'avvento dell'*open finance* e della *DeFi,* si è assistito, ad una progressiva perdita di rilevanza della moneta contante, a vantaggio di altri strumenti di pagamento; solo il contante però è direttamente coniato o stampato dal Banchiere Centrale e costituisce così un diritto di credito che può essere fatto valere nei suoi confronti, con tutte le garanzie del caso quale, *in primis*, l'impossibilità di fallire. Le altre forme di moneta, essendo in mano ai privati, presentano un alto rischio di credito; la moneta privata è stata infatti capace di evolversi e adattarsi alle esigenze di cambiamento del contesto sociale e presenta una natura dematerializzata sin dalle origini. Paradossalmente però, l'utilizzo del contante, in virtù della *traditio*, è l'unico che consente alle parti di addivenire direttamente allo scambio delle somme di denaro, senza la necessità di alcuna rete e quindi di alcun intermediario che partecipi o si inserisca nell'operazione; in tutti gli altri casi, la moneta per essere trasferita ha bisogno di un sistema che consenta la movimentazione intermediata (Banche commerciali, PSP, VASP).

Per tali motivi, in un sistema monetario come quello attuale, in cui il ruolo preponderante è assunto dalla moneta bancaria, i banchieri centrali hanno le armi spuntate verso il mercato delle criptovalute; di conseguenza vi è una progressiva perdita di controllo di base monetaria da parte del banchiere centrale. A ciò si aggiunge che, ad oggi, per lo meno potenzialmente la produzione di moneta privata non è più appannaggio esclusivo di quegli intermediari bancari rigidamente regolati, poichè le cripto-attività permettono di creare vere e proprie monete, che prescindono completamente dai sistemi monetari e di pagamento degli stati nazionali.

E' questa la prima ragione che dovrebbe indurre seriamente a riflettere circa la necessità di introdurre in tempi rapidi una valuta digitale del Banchiere Centrale ossia, una c.d. CBDC. Inoltre, il banchiere centrale nel mercato *crypto* potrebbe assumere il ruolo di prestatore di ultima istanza, nei casi di grandi crisi di liquidità come quella di FTX.

Per quanto riguarda il Regolamento europeo MiCA, il medesimo è senz'altro un prodotto normativo ambizioso, ancor di più se si tiene conto della velocità con cui il legislatore europeo vi è giunto, spinto dall'esigenza di dare una risposta non solo all'emersione di nuovi fenomeni, ma anche agli interventi normativi dei singoli legislatori nazionali dell'Eurozona, che rischiavano di creare i presupposti per

pericolosi arbitraggi regolamentari. Tuttavia, il regolamento sconta il vincolo della *ratio legis* europea, legata alla neutralità tecnologica. Le attuali definizioni di concetti fondamentali per la finanza tradizionale, quali: "servizi di investimento", "strumenti finanziari", "mercati", sono state concepite in un lontano contesto storico, nel quale determinati *business model* non erano nemmeno immaginabili; non sempre quindi risultano adeguati a catturare nuovi fenomeni caratterizzati da dematerializzazione e disintermediazione.

Evidenti sono i limiti di questa impostazione: in primo luogo essa impone un approccio *case-by-case*, ossia la necessità di verificare di volta in volta a quale categoria dovrebbe essere ricondotto il singolo *token*, prima di poter individuare la disciplina di riferimento, rischiando dunque di aumentare la situazione di incertezza.

Una dimostrazione di questo pericolo è ben evidente nello stesso regolamento che impone, come abbiamo visto, agli emittenti di individuare la natura del *crypto-asset* da loro emesso all'interno del documento denominato *white paper*, determinando così l'applicabilità del MiCAR, dichiarando che non sussistono nel caso specifico le caratteristiche di uno strumento finanziario, di una moneta elettronica o di un deposito.

In secondo luogo, essa non considera l'estrema difficoltà di perimetrazione della nozione di strumento finanziario e della stessa moneta. Come è noto, infatti, manca tutt'ora una comune definizione europea, posto che la stessa MIFID II ha lasciato ai singoli paesi membri ampia libertà in merito al suo recepimento. La stessa problematicità si annida del resto nell'individuazione di un concetto condiviso di moneta e di strumenti di pagamento.

In terzo luogo, una simile impostazione, che ritiene idonea la disciplina tradizionale di strumenti finanziari o di pagamento, non considera le peculiarità e i rischi che sono connessi a queste nuove tipologie di "prodotti".

Del resto, già l'ESMA in un suo *report* aveva messo in luce come la mera applicazione della normativa finanziaria esistente rischiasse di non essere adeguata ad affrontare le specificità poste da questo fenomeno.

Secondo parte della dottrina che, a parere di chi scrive, è condivisibile, sembra che il regolatore voglia selezionare soltanto alcune potenzialità del mondo *crypto*, cercando invece di arginarne altre, quale in primo luogo bitcoin, che pure ne rappresenta l'elemento più emblematico.

Anzi, a questo proposito, la Commissione Europea più che essere interessata alla creazione di un mercato dei *crypto-assets* sembra più attratta dal diverso fenomeno

della tokenizzazione del mercato finanziario, ossia la dematerializzazione di *assets* tradizionali - quali strumenti finanziari o di pagamento -, tramite l'uso della DLT e degli *smart contracts*, in virtù della convinzione che tale soluzione tecnologica possa avere potenzialità inimmaginabili in questi settori.

Ritengo infatti, che di fronte al cambio di paradigma che le nuove tecnologie impongono, è opportuna una nuova forma di regolamentazione rispetto a quella dei tradizionali fenomeni di intermediazione finanziaria, nella convinzione che solo così sarà possibile garantire l'effettiva gestione di una realtà complessa sia nell'ottica della stabilità finanziaria sia in quella della tutela dei consumatori/investitori.

Un punto centrale emerso nel presente elaborato, riguarda quindi il superamento della nozione di neutralità tecnologica; come si è avuto modo di sostenere questo è un settore ove un approccio di neutralità inteso come "stessi servizi, stessi rischi, stesse regole", mostra tutti i suoi limiti. Il tentativo di ricondurre le eterogenee categorie di *tokens* nell'ambito della bipartizione tra strumento finanziario e strumento di pagamento, rischia di ingenerare pericolosi equivoci e zone grigie, aumentando così l'incertezza del *framework* normativo.

Inoltre, si ha avuto modo di analizzare il fenomeno da molti operatori del settore denominato "mifidizzazione del MiCAR"; quest'ultimo è un Regolamento che sostanzialmente prende l'impianto Mifid e in qualche modo lo adegua sulla scorta dell'aspetto tecnologico. Per questo motivo appare una contraddizione in termini parlare di "neutralità tecnologica", in quanto se non per poche disposizioni di nuova creazione, ciò che distingue l'impianto Mifid dal MiCAR sono proprio le caratteristiche tecnologiche proprie della materia regolata.

In chiusura del mio elaborato e dopo un attento studio della materia, mi sento di rispondere ai fautori della deregolamentazione e dell'utopistica decentralizzazione perfetta del fenomeno *FinTech*, con le parole dell'autorevole giurista Natalino Irti: «*I liberisti della cattedra, che esaltano l'ordine spontaneo dell'economia, e vagheggiano non sappiamo quale stato minimo, non si avvedono che soltanto il diritto ha la forza di ridurre le incognite del futuro e di consentire il calcolo dell'altrui condotta. La valutazione giuridica, costante e uniforme (cioè capace di imprimere unità di forma a casi innumerevoli e particolari), rende possibile la "previsione della valutazione futura", e introduce così nel processo economico un momento di alto valore costituito dalla sicurezza.*[607]»

[607] N. IRTI, «*L'ordine giuridico del mercato*», 34, libri del tempo (Editori Laterza, 2008).

# BIBLIOGRAFIA


- ABATE G., BRANZOLI N., GALLO R. «*Crypto-asset markets: structure, stress episodes in 2022 and policy considerations*», in *BANCA D'ITALIA n.783*, giugno 2023. https://www.bancaditalia.it/pubblicazioni/qef/2023-0783/QEF_783_23.pdf.
- ACCENTURE. «*Banking Customer 2020, Report*», 2015. https://bankingblog.accenture.com/wp-content/uploads/2015/08/P1200614_Infografik_Banking_Customer.pdf
- ACCINNI G. P. «*Cybersecurity e criptovalute: rilevanza penale dopo la Quinta Direttiva*», in *sistema penale* (15 maggio 2020).
- ADINOLFI A., GAETA E. G. «*Cyberlaundering, VASPs' Regulation, and AML Policy Response*». In *The Role of Distributed Ledger Technology in Banking. From theory to practice*, 114 e ss. Cambridge university press, 2023.
- ADRIAN T., IYER T., QURESHI M.S. «*Crypto Prices Move More in Sync With Stocks, Posing New Risks*». IMF, 1° novembre 2022. https://www.imf.org/en/Blogs/Articles/2022/01/11/crypto-prices-move-more-in-sync-with-stocks-posing-new-risks.
- AL SHANTI A. M., JORDAN A., MCMILLAN D. «*The Impact of Digital Transformation towards Blockchain Technology Application in Banks to Improve Accounting Information Quality and Corporate Governance Effectiveness*», in *Cogent economics&finance* (2023). https://www.tandfonline.com/doi/epdf/10.1080/23322039.2022.2161773?needAccess=true.
- ALLEN H. J. «*DeFi: Shadow Banking 2.0?*» *SSRN Electronic Journal* Washington College of Law Research Paper No. 2022-02 (2022). https://doi.org/10.2139/ssrn.4038788.
- ALLEN H. J. «*Driverless Finance: Fintech's Impact on Financial Stability*». New York: Oxford University Press, 2022.
- ALLISON I. «*Divisions in Sam Bankman-Fried's Crypto Empire Blur on His Trading Titan Alameda's Balance Sheet*», Coindesk, 2 novembre 2022.

https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/.

- ALPA G., PANCALLO A. M. «*Le criptovalute*». In *Diritto e intelligenza artificiale*, 591 e ss., 2020.
- AMATI E. «*abusi di mercato e sistema penale*», G. Giappichelli, novembre 2012.
- AMBROSINI S., AMOROSINO S., BONFATTI S., CAPRIGLIONE F., CORTESE F., GENTILI A., GUIZZI G., «*Open Banking, Open Problems. Aspetti controversi del nuovo modello dei "sistemi bancari aperti"», in* Rivista di Diritto Bancario, dottrina e giurisprudenza commentata 2020, 46.
- AMETRANO F. «*La custodia sicura di Bitcoin: aspetti tecnologici, funzionali e regolamentari*», 28 settembre 2021.
- AMMANNATI L. «*Il paradigma del consumatore nell'era digitale : consumatore digitale o digitalizzazione del consumatore?*», in *Rivista Trimestrale di Diritto dell'Economia* (2019). https://air.unimi.it/handle/2434/655050.
- AMMANNATI L. «*La circolazione dei dati: dal consumo alla produzione*». *Astrid rassegna*, 1° gennaio 2020.
- ANIMASHAUN S. «*Great Crypto Crisis: The Prudential Regulation of Systemically Important Crypto Conglomerates*». SSRN Scholarly Paper. Rochester, NY, 20 dicembre 2022. https://doi.org/10.2139/ssrn.4307586.
- ANKER-SØRENSEN L., ZETZSCHE D. A. «*From Centralized to Decentralized Finance: The Issue of "Fake-DeFi"*». SSRN Scholarly Paper. Rochester, NY, 22 dicembre 2021. https://doi.org/10.2139/ssrn.3978815.
- ANNUNZIATA F. «*An overview of the markets in crypto-assets regulation (MiCAR)*». EBI Working Paper Series, 2023.
- ANNUNZIATA F. *«La disciplina del mercato dei capitali»*. G. Giappichelli Editore, 2023.
- ANNUNZIATA F. *«La disciplina del mercato mobiliare»*. G. Giappichelli Editore, 2021.
- ANNUNZIATA F. «*La disciplina delle cripto-attività*». In *La disciplina del mercato dei capitali*. G. Giappichelli Editore, 2023.
- ANNUNZIATA F. «*La tassonomia del Regolamento MiCA: ARTs, EMTs e utility tokens. criteri di identificazione e definizioni*». Roma: BANCA D'ITALIA, 29 settembre 2023.
- ANNUNZIATA F. «*The Licensing Rules in MiCA*». SSRN Scholarly Paper. Rochester, NY, 3 febbraio 2023. https://doi.org/10.2139/ssrn.4346795.
- ANNUNZIATA F. «*The Remains of the Day: EU Financial Agencies, Soft Law and the Relics of Meroni*». SSRN Scholarly Paper. Rochester, NY, 19 novembre 2021.

https://papers.ssrn.com/abstract=3966980.

- ANNUNZIATA F. «*Towards an EU Charter for the Protection of End Users in Financial Markets*». SSRN Scholarly Paper. Rochester, NY, 25 agosto 2022. https://doi.org/10.2139/ssrn.4200502.
- ANNUNZIATA F., CHISARI A. C., AMENDOLA P. B. «*DLT-Based Trading Venues and EU Capital Markets Legislation: State of the Art and Perspectives under the DLT Pilot Regime*». SSRN Scholarly Paper. Rochester, NY, 1 febbraio 2023. https://doi.org/10.2139/ssrn.4344803.
- ANNUNZIATA F., VARANI D. «*Cripto-attività: antiriciclaggio e gestione dei rischi aziendali*». Pacini Editore, 2024.
- ANTONUCCI A. «*I contratti di mercato finanziario - Seconda edizione*». Pacini Editore, 2022.
- AQUILINA M., FROST J., SCHRIMPF A. «*Addressing the Risks in Crypto: Laying out the Options*», BIS, 12 gennaio 2023.
- ARAMONTE S., WENQIAN H., SCHRIMPF A. «*DeFi Risks and the Decentralisation Illusion*» BIS Quarterly Review (2021).
- ARGENTATI A. «*Banche e big tech: criticità e strumenti per governare la nuova relazione competitiva. Prime riflessioni*». In *Mercati regolati e nuove filiere di valore*, 328. G. Giappichelli Editore, 2021.
- ARGENTATI A. «*Banks and new Competitive Scenario: FinTech, the Open Banking Paradigm and the Threat of Big Tech Companies*». *Mercato Concorrenza Regole*, fasc. 3 (3 dicembre 2018): 441–66.
- ARGENTATI A. «*Le banche nel nuovo scenario competitivo. Fin-Tech, il paradigma Open banking e la minaccia delle big tech companies*». In *Mercato Concorrenza Regole*, fasc. 3 (dicembre 2018).
- ARMSTRONG P. «*Financial Technology: ESMA's Approach*», 6, 2018.
- ARNER D. W., BARBERIS J., BUCKLEY R. P. «*FinTech, RegTech, and the Reconceptualization of Financial Regulation*». *Northwestern Journal of International Law & Business* 37, fasc. 3 (1° gennaio 2017): 371.
- ARNER D. W., BUCKLEY R. P., ZETZSCHE D. A., VEIDT R. «*Sustainability, FinTech and Financial Inclusion*». SSRN Scholarly Paper. Rochester, NY, 1 novembre 2019. https://doi.org/10.2139/ssrn.3387359.
- ARNER D. W., ZETZSCHE D. A,BUCKLEY R. P. , KIRKWOOD J. «*The Financialization of Crypto: Lessons from FTX and the Crypto Winter of 2022-2023*». *SSRN Electronic Journal*, 2023. https://doi.org/10.2139/ssrn.4372516.

- ASPRIS A., FOLEY S., SVEC J., WANG L. «*Decentralized exchanges: The "wild west" of cryptocurrency trading*», in *International Review of Financial Analysis* 77 (1 ottobre 2021): 101845. https://doi.org/10.1016/j.irfa.2021.101845.
- BAIRROS R. «*Discussion Paper - on Innovative Uses of Consumer Data by Financial Institutions*», 4 maggio 2016. https://policycommons.net/artifacts/2225531/discussion-paper/2982963/.
- BAKER T. H. «*Let's Stop Treating Crypto Trading as If It Were Finance*», in The CLS Blue Sky Blog Columbia University (29 novembre 2022). https://clsbluesky.law.columbia.edu/2022/11/29/lets-stop-treating-crypto-as-if-it-were-finance/.
- BANCA D'ITALIA e UIF. «*Quaderni dell'antiriciclaggio dell'Unità di Informazione Finanziaria. dati statistici*», gennaio 2023.
- BANCA D'ITALIA. «*Avvertenza sull'utilizzo delle cosiddette "valute virtuali"*», 30 gennaio 2015.
- BANCA D'ITALIA. «*Banca d'Italia - Avvertenza per i consumatori sui rischi delle valute virtuali da parte delle Autorità europee*», 19 marzo 2018. https://www.bancaditalia.it/compiti/vigilanza/avvisi-pub/avvertenza-valute-virtuali-2018/https%3A%2F%2Fwww.bancaditalia.it%2Fcompiti%2Fvigilanza%2Favvisi-pub%2Favvertenza-valute-virtuali-2018%2Findex.html%3Fcom.dotmarketing.htmlpage.language%3D102.
- BANCA D'ITALIA. «*Banca d'Italia - Comunicazione della Banca d'Italia in materia di tecnologie decentralizzate nella finanza e cripto-attività*». https://www.bancaditalia.it/media/notizia/comunicazione-della-banca-d-italia-in-materia-di-tecnologie-decentralizzate-nella-finanza-e-cripto-attivit/https%3A%2F%2Fwww.bancaditalia.it%2Fmedia%2Fnotizia%2Fcomunicazione-della-banca-d-italia-in-materia-di-tecnologie-decentralizzate-nella-finanza-e-cripto-attivit.
- BANCA D'ITALIA. «*Indagine FinTech nel sistema finanziario italiano*», 2021. https://www.bancaditalia.it/pubblicazioni/indagine-fintech/2021/2021-FINTECH-INDAGINE.pdf.
- BANCA D'ITALIA. «*La governance delle blockchain e di sistemi basati sulla tecnologia dei registri distribuiti*», in Banca d'Italia n. 773.
- BANCA D'ITALIA. «*Rapporto sulla stabilità finanziaria*», in Banca d'Italia n.1, 2018.

https://www.bancaditalia.it/pubblicazioni/rapporto-stabilita/2018-1/https%3A%2F%2Fwww.bancaditalia.it%2Fpubblicazioni%2Frapporto-stabilita%2F2018-1%2Findex.html%3Fcom.dotmarketing.htmlpage.language%3D102.

- BANCA D'ITALIA. «*Trasparenza delle operazioni e dei servizi bancari e finanziari Correttezza delle relazioni tra intermediari e clienti*», marzo 2009. https://www.bancaditalia.it/compiti/vigilanza/normativa/consultazioni/2009/resoconto-consultazione-pubblica/trasparenza_documento_consultazione.pdf.
- BARBAGALLO C. «*Il sistema bancario italiano: situazione e prospettive*», 24 marzo 2018.
- BASSAN F. «*Digital Platforms and Blockchains: The Age of Participated Regulation*». *SSRN Electronic Journal*, 2022. https://doi.org/10.2139/ssrn.4244139.
- BATTAGLINI R., GIORDANO M. T. «*Blockchain e smart contract*». Giuffrè Francis Lefebvre, 2019.
- BELLELLI A. «*Comprare FTX Token (FTT): cos'è il progetto, grafico e previsioni*». *Finanza Digitale*, 21 giugno 2022. https://www.finanzadigitale.com/comprare-ftx/.
- BENCINI M., FANFANI L, PELLIZZARI S., TODINI V. «*Profili penali della tutela del risparmio: truffa, abusi di mercato e gestione patrimoniale*». Giuffrè Francis Lefebvre, 2021.
- BENCINI M., FANFANI L. «*Prevenzione degli abusi di mercato relativi alle criptoattività*». In *Crypto-asset: Regolamen to MiCA e DLT Pilot Regime. Analisi ragionata su token, stablecoin, CASP*, 249 e ss. Giuffrè Francis Lefebvre.
- BENEDETTI H., RODRÍGUEZ-GARNICA G. «*Tokenized Assets and Securities*». In *The Emerald Handbook on Cryptoassets: Investment Opportunities and Challenges*, 107–21. Emerald Publishing Limited, 2023. https://doi.org/10.1108/978-1-80455-320-620221008.
- BERNASCONI A., PRESUTTI A. «*Manuale della responsabilità degli enti*». Giuffrè Francis Lefebvre, 2018.
- BERWICK A., WILSON T. «*Exclusive: Behind FTX's Fall, Battling Billionaires and a Failed Bid to Save Crypto*». *Reuters*, 10 novembre 2022, sez. Technology. https://www.reuters.com/technology/exclusive-behind-ftxs-fall-battling-billionaires-failed-bid-save-crypto-2022-11-10/.
- BIGIARINI A. «*Ne bis in idem: il cortocircuito del "doppio binario" sanzionatorio in relazione a fatti di criminalità economica*», 2016, 262 e ss.
- BINANCE [@BINANCE]. «*As a Result of Corporate Due Diligence, as Well as the Latest News Reports Regarding Mishandled Customer Funds and Alleged US Agency Investigations, We*

*Have Decided That We Will Not Pursue the Potential Acquisition of Http://FTX.Com.»* *Twitter*, 9 novembre 2022. https://twitter.com/binance/status/1590449161069268992.

- BINANCE ACADEMY. «*Cos'è una IDO (Initial DEX Offering)?*», https://academy.binance.com/it/articles/what-is-an-ido-initial-dex-offering.
- BINANCE ACADEMY. «*Cos'è una Initial Exchange Offering (IEO)?*», https://academy.binance.com/it/articles/what-is-an-initial-exchange-offering-ieo.
- BINANCE. «*Guida Binance per Principianti | Il blog di Binance*». https://www.binance.com/it/blog/ecosystem/guida-binance-per-principianti-3741372155113856065.
- BIS. «*BIS Quarterly Review, March 2023*», 3/2023. https://www.bis.org/publ/qtrpdf/r_qt2303.pdf.
- BIS. «*Prudential Treatment of Cryptoasset Exposures*», 16 dicembre 2022. https://www.bis.org/bcbs/publ/d545.pdf.
- BIS. «*The Crypto Ecosystem: Key Elements and Risks, Report Submitted to the G20 Finance Ministers and Central Bank Governors*», luglio 2023. https://www.bis.org/publ/othp72.pdf.
- BONUOMO M., BO A., BOSSI P. «*Prove di collaborazione tra FinTech e banche: quali sfide e come superarle?*», in *Minerva Bancaria* marzo 2023.
- BORSA ITALIANA. «*Che cosa sono i contratti forward*». https://www.borsaitaliana.it/notizie/sotto-la-lente/forward-179.htm.
- BORSA ITALIANA. «*Le opzioni: definizione e funzionamento*», https://www.borsaitaliana.it/notizie/sotto-la-lente/opzioni.htm.
- BORSA ITALIANA. «*Organismi di Investimento Collettivo del Risparmio - Glossario Finanziario*», https://www.borsaitaliana.it/borsa/glossario/organismi-di-investimento-collettivo-del-risparmio.html.
- BOSCIA V., SCHENA C. M., STEFANELLI V., «*Digital banking e FinTech: l'intermediazione finanziaria tra cambiamenti tecnologici e sfide di mercato*», in *Banca e mercati Saggi* 142. ABI Servizi, Bancaria editrice, 2020.
- BOSCIA V., SCHENA C., STEFANELLI V. «*Digital banking e FinTech, L'intermediazione finanziaria tra cambiamenti tecnologici e sfide di mercato*». Bancaria Editrice, 2020. http://www.bancariaeditrice.it/digital-banking-e-fintech.
- BOWER J., CHRISTENSEN C. «*Disruptive Technologies: Catching the Wave*», Harvard Business Review, 1995.
- BOWTIED E. «*Sam Bankman-Fried Proposes Centralized Crypto Industry Standards*». BowTied Island, 24 ottobre 2022.

https://bowtiedisland.com/sam-bankman-fried-proposes-centralized-crypto-industry-standards/.

- BREYDO L. E. «*Crypto contagion. The ftx bankruptcy, a sector's crisis & the future of digital assets*», SSRN Scholarly Paper. Rochester, NY, 2023
- BRIDGES J, GREEN G., JOY M. «*Credit, Crises and Inequality*». SSRN Scholarly Paper. Rochester, NY, 12 novembre 2021. https://doi.org/10.2139/ssrn.3976327.
- BUSSI M. «*Lo scandalo Ftx peggio di Enron - MilanoFinanza News*». *MF Milano Finanza*, 18 novembre 2022, sez. MF Online. https://www.milanofinanza.it/news/lo-scandalo-ftx-peggio-di-enron-2584455.
- CACIOPPOLI V. «*Il prestito di FTX a BlockFi*», The Cryptonomist 22 giugno 2022. https://cryptonomist.ch/2022/06/22/prestito-ftx-blockfi/.
- CADOPPI A., CANESTRI S., MANNA A., PAPA M. «*Diritto penale dell'economia*», in *Trattati giuridici*. Utet Giuridica, 2019.
- CANEPA A. «*social media e fin-influencers come nuove fonti di vulnerabilità digitale nell'assunzione delle decisioni di investimento (Social media and fin-influencers towards a new digital vulnerability in investment decisions)*», in *Rivista trimestrale di diritto dell'economia*, gennaio 2022.
- CAPACCIOLI S. «*Criptovalute e bitcoin: un'analisi giuridica*». Giuffrè Francis Lefebvre, 2015.
- CAPRIGLIONE F. «*Manuale di Diritto bancario e finanziario*». II. Cedam, 2019.
- CARLINI V. «*Cripto, dopo la tempesta di Ftx boom per robot e autocustodia*». *Il Sole 24 ORE*, 2 dicembre 2022, Finanza e Mercati edizione, sez. Finanza Personale.
- CARLINI V. «*Dalle piattaforme di scambio ai token, essenziale conoscere*». *Finanza digitale #2/cripto*, ottobre 2022, Il Sole 24 Ore.
- CARLINI V. «*Le cripto imprese alzano la voce: "Regole per isolare il business opaco"*», 12 novembre 2022, Il Sole 24 Ore.
- CARNEY M. «*The Promise of FinTech – Something New Under the Sun?*», Speech given by Mark Carney e Governor of the Bank of England Chair of the Financial Stability Board, 14. Wiesbaden: BANK OF ENGLAND, 2017. https://www.bis.org/review/r170126b.pdf.
- CARRARO G., DI RAIMO R., FIORDIPONTI F., FURNARI S. L., GALLI L., GIORGI M, LUCANTONI P., LENER R. «*FinTech: Diritto, Tecnologia e Finanza*». Minerva Bancaria, 2018.
- CARRIERE P., De Luca N., De Mari M., Gasparri G., Poli T. N. «*tokenizzazione di azioni e azioni tokens*», in *quaderni giuridici consob*, n. 25/2023, 53.

- CARTER N. «*Cryptoasset Valuation: Theory and Practice*». In *Cryptoassets*, 69–88. Oxford University Press, 2019. https://doi.org/10.1093/oso/9780190077310.003.0004.
- CARTER N. «*Decentralized Finance: The Future of Crypto and Open Finance?*» In *Open Banking*, a cura di JENG L., Oxford University Press, 2022. https://doi.org/10.1093/oso/9780197582879.003.0014.
- CASEY M. J., WARNOCK E., SIDEL R. «*Mt. Gox Halts All Transactions in New Bitcoin Setback*», 26 febbraio 2014, The Wall Street Journal. https://www.wsj.com/articles/SB10001424052702304834704579404101502619422.
- CASSANO G., DI CIOMMO F., DE RITIS M. R. «*Banche; Intermediari e FinTech*». Giuffrè Francis Lefebvre, 2021.
- CASTALDO A. R., NADDEO M. «*Il denaro sporco. Prevenzione e repressione nella lotta al riciclaggio*». Cedam, 2010.
- CAVALLARO G. «*Commentario al Testo Unico della Finanza*». Pacini Editore, 2021.
- CBI, PWC. «*The Global Open Finance Report*», marzo 2023. https://www.cbi-org.eu/Media-Events/Next-Appointments/The-Global-Open-Finance-Report.
- CERRATO S. A. «*Negoziare in rete: appunti su contratti e realtà virtuale nell'era della digitalizzazione*» in *Diritto comunitario e degli scambi internazionali : 1/2, 2018*, 2018, 233–66. https://doi.org/10.1400/273571.
- CHAINANALYSIS. «*Il report sui crimini crypto del 2023*», febbraio 2023.
- CHIOMENTI. «*Servizi di pagamento e Open finance: le proposte dalla Commissione europea*», giugno 2023.
- CHOHAN U. W. «*FTX, Sam Bankman-Fried, and the Cryptoexchange Problem*». *SSRN Electronic Journal*, 2023. https://doi.org/10.2139/ssrn.4326161.
- CHOU J., AGRAWAL P., BIRT J. «*Accounting for crypto-assets: stakeholders' perceptions*». *Studies in Economics and Finance* ahead-of-print (14 gennaio 2022). https://doi.org/10.1108/SEF-10-2021-0469.
- CHU D. «*Broker-dealers for virtual currency: regulating cryptocurrency wallets and exchanges*», in *Columbia Law Review*, 2018. https://columbialawreview.org/content/broker-dealers-for-virtual-currency-regulating-cryptocurrency-wallets-and-exchanges/.
- CHURCH S. «*FTX's $1.4B deal for bankrupt lender Voyager is canceled*». *BNN*, 15 novembre 2022, Bloomberg, sez. Company News. https://www.bnnbloomberg.ca/ftx-s-1-4-billion-deal-for-bankrupt-lender-voyager-is-canceled-1.1846741.

- Cian M. «*La criptovaluta – alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*», X convegno annuale dell'Associazione Italiana dei Professori Universitari di Diritto Commerciale "Orizzonti di Diritto Commerciale", "L'evoluzione tecnologica e il diritto commerciale". Roma, 22-23 febbraio 2019. https://www.orizzontideldirittocommerciale.it/wp-content/uploads/2021/04/Cian_La-criptovaluta.pdf.
- CIAN M. *«Manuale di diritto commerciale»*. V. G. Giappichelli Editore, 2023.
- CIAN M. «*Notarelle su finanziarietà e non finanziarietà nei crypto-asset: la suprema corte sulla natura del servizio di exchange*»,in *Banca, borsa, tit. cred.*, fasc. I (2023): 3.
- Cian M., Sandei C. «*Diritto del Fintech*». Cedam, 2020.
- CINQUE A. «*La blockchain: Smart contract - cripto-attività - applicazioni pratiche*». Pacini Editore, 2022.
- CINTIOLI F. «*Giusto processo, CEDU e sanzioni antitrust*», in *Diritto Processuale Amministrativo*, febbraio 2015, 513 e ss.
- CIOCCA P. «*FinTech e l'impatto sui servizi finanziari: dati, fiducia, regole*» Bancaria (giugno 2018): 18–22.
- CIOCCA P., PITRUZZELLA G., SORO A., ROSSI S. «*Corso di alta formazione su FinTech e diritto*». ABI Servizi, Bancaria editrice, Roma 10 maggio 2018.
- CIPOLLONE P. «*Towards PSD3: The Dynamics of Digitalized Payment Systems*», 2023.
- CIPOLLONE P. «*Towards PSD3: the Dynamics of Digitalized Payment System*», BANCA D'ITALIA, Roma, 14 aprile 2023. https://www.bancaditalia.it/pubblicazioni/interventi-direttorio/int-dir-2023/Cipollone_14042023.pdf
- CIRAOLO F. «*Open Banking, Open Problems. Aspetti controversi del nuovo modello dei "sistemi bancari aperti"*», in *Rivista di Diritto Bancario*, anno 2020, fascicolo 4, sezione 1 (2020).
- COHNEY S., HOFFMAN D. A., SKLAROFF J., WISHNICK D. A. «*Coin-Operated Capitalism*». SSRN Scholarly Paper. Rochester, NY, 2019. https://doi.org/10.2139/ssrn.3215345.
- COLAZZO F. «*Investire i profitti della truffa per acquistare criptovalute integra il reato di autoriciclaggio*», in *Antiriciclaggio e compliance* (2022).
- CONSOB. «*Piano strategico 2022-24*», https://www.consob.it/documents/1912911/1949521/ps_2224.pdf/dcc07424-55f5-d283-8b0a-4d7c8e3e0507.
- CONSULICH F. «*Nella wunderkammer del legislatore penale contemporaneo: monete virtuali che causano danni reali*», in *Diritto Penale e Processo*, febbraio 2022, 154.

- CZ ◆ BINANCE [@CZ_BINANCE]. «*As Part of Binance's Exit from FTX Equity Last Year, Binance Received Roughly $2.1 Billion USD Equivalent in Cash (BUSD and FTT). Due to Recent Revelations That Have Came to Light, We Have Decided to Liquidate Any Remaining FTT on Our Books. 1/4*». Tweet. *Twitter*, 6 novembre 2022. https://twitter.com/cz_binance/status/1589283421704290306.
- CZ ◆ BINANCE [@CZ_BINANCE]. «*This Afternoon, FTX Asked for Our Help. There Is a Significant Liquidity Crunch. To Protect Users, We Signed a Non-Binding LOI, Intending to Fully Acquire Http://FTX.Com and Help Cover the Liquidity Crunch. We Will Be Conducting a Full DD in the Coming Days*». Tweet. *Twitter*, 8 novembre 2022. https://twitter.com/cz_binance/status/1590013613586411520.
- D. ALESSI. «*Il ruolo delle Autorità competenti: la collaborazione tra ABE, ESMA e Autorità nazionali*». In *Il MiCAR, guida al regolamento Europeo sui mercati delle cripto*. a cura di NICOTRA M., SARZANA F., IPPOLITO S., SIMBULA M. Giuffrè Francis Lefebvre, 2023.
- D. VARANI D., LUNETTA D. «*Rilevanza del mercato dei crypto-asset nell'ambito del cybercrime e dei reati di riciclaggio*». In *Cripto-attività: antiriciclaggio e gestione dei rischi aziendali*, 7. Pacini Editore, 2024.
- D'AGOSTINO G. «*MiCAR: rischi e opportunità per le istituzioni finanziarie che prestano servizi su crypto-asset nella UE*», in *Bancaria*, fasc. 12/2023 (dicembre 2023): 32–44.
- D'ALESSANDRO F. «*L'aggiotaggio e la manipolazione del mercato*». In *Diritto e procedura penale delle società*. Giuffrè Francis Lefebvre, 2022.
- D'ALESSANDRO F. «*Regolatori del mercato, enforcement e sistema penale*». G. Giappichelli Editore, 2014.
- DALY. «*Crypto-Assets in Banks Between Opportunities and Legal Uncertainties*». In *The Role of Distributed Ledger Technology in Banking. From theory to practice*, 90 e ss. Cambridge university press, 2023.
- DAVOLA A. «*Algoritmi decisionali e trasparenza bancaria*». Utet Giuridica, 2020.
- DE ANGELIS C. «*L'exchange dell'under 30 più ricco del mondo raccoglie 400 milioni di dollari. Ora vale 32 miliardi*». *Forbes Italia*, 1° febbraio 2022. https://forbes.it/2022/02/01/ftx-sam-bankman-fried-raccolgono-400-milioni-dollari/.
- DE BONIS R., VANGELISTI M. R. «*La moneta. Dai buoni di omero ai Bitcoin*». Il Mulino, 2019.
- DE FILIPPI P., WRIGHT A. «*Blockchain and the Law — The Rule of Code*», in *Harvard University Press*., 2019. https://www.hup.harvard.edu/catalog.php?isbn=9780674241596.

- DE PASCALIS F. «*The Journey to Open Finance: Learning from the Open Banking Movement*», in *European Business Law Review* 33, fasc. Issue 3 (1 aprile 2022): 397–420. https://doi.org/10.54648/EULR2022018.
- DE SIMONE G. «*La responsabilità da reato degli enti: natura giuridica e criteri (oggettivi) d'imputazione*», in *Diritto Penale Contemporaneo*, 28 ottobre 2012.
- DE VIVO A., ZANICHELLI C. «*Decreto legge 231 - Il difficile risk assessment 231 per i delitti in materia di strumenti di pagamento diversi dai contanti*», febbraio 2022.
- DELMASTRO M., NICITA A. «*Big data. Come stanno cambiando il nostro mondo*». Il Mulino, 2019.
- DI BITONTO M. L. «*Il ne bis in idem nei rapporti tra infrazioni finanziarie e reati*», in *Cassazione Penale*, fasc. n.4 (2016): 1335.
- DI FIORINO E., SANTORIELLO C. «*L' organismo di vigilanza nel sistema 231*». Pacini Editore, 2020.
- DI STEFANO L. «*La richiesta di sospensiva di operazioni sospette da parte degli exchangers e dei wallet providers*», 2021.
- DI STEFANO L. «*Le criptovalute e la disciplina di cui al D.lgs. n. 231/2001*». In *Cripto-attività: antiriciclaggio e gestione dei rischi aziendali*, 126. Pacini Editore, 2024.
- DIERKSMEIER C., SEELE P. «*Cryptocurrencies and Business Ethics*», in *Journal of Business Ethics* 152, fasc. 1 (settembre 2018): 1–14. https://doi.org/10.1007/s10551-016-3298-0.
- DINGLE S., BOYKEY SIDLEY S. «*Beyond Bitcoin, Decentralised Finance and the End of Banks*». Icon Books, 2022.
- DIRECTORATE-GENERAL FOR FINANCIAL STABILITY, FINANCIAL SERVICES AND CAPITAL MARKETS UNION. «*Report on Open Finance*», 24 ottobre 2022. https://finance.ec.europa.eu/publications/report-open-finance_en#:~:text=Description,perspective%20of%20the%20Expert%20Group.
- DIRITTO BANCARIO. «*Criptovalute sono prodotti finanziari per la Cassazione*». *DB*, 23 novembre 2022.
- DIRITTO BANCARIO. «*Verso la PSD3: la posizione di Banca d'Italia*». *DB*, 17 aprile 2023. https://www.dirittobancario.it/art/verso-la-psd3-la-posizione-di-banca-ditalia/.
- DONOVAN A. «*(Shadow)Banking on the Blockchain:Permissioned Ledgers, Interoperability and Common Standards*». In *Research Handbook on Shadow Banking*, 314 e ss., 2018.
- EBA «*EBA reports on crypto-assets | European Banking Authority*», 9 gennaio 2019.
- EBA. «*EBA eport on the impact of fintech on incumbent credit institutions' business models*», 3 luglio 2018.

https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2270909/1f27bb57-387e-4978-82f6-ece725b51941/Report%20on%20the%20impact%20of%20Fintech%20on%20incumbent%20credit%20institutions%27%20business%20models.pdf?retry=1.

- ECB EUROSYSTEM. «*Eurosystem Oversight Framework for Electronic Payment Instruments, Schemes and Arrangements*», novembre 2021. https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf.
- EDPB. «*Linee guida 06/2020 sull'interazione tra la seconda direttiva sui servizi di pagamento e il GDPR Versione 2.0*», 15 dicembre 2020. https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202006_psd2_afterpublicconsultation_it.pdf.
- ELDER B., SCAGGS A. «THE FTX BANKRUPTCY FILING IN FULL (UPDATED)». *Financial Times*, 17 novembre 2022, sez. FT Alphaville. https://www.ft.com/content/c236d6f9-da5a-4da7-8dc8-5cd450dfe39d.
- ELLENA N. «*API: cosa sono e perché sono importanti per il Fintech*». Money.it, 18 gennaio 2023. https://www.money.it/API-fintech-cosa-sono-e-perche-sono-importanti.
- ELLI S., SOLDAVINI P. «*The Rock Trading, arriva la liquidazione giudiziale*». *Il Sole 24 ORE*, 14 aprile 2023, sez. Finanza. https://www.ilsole24ore.com/art/the-rock-trading-arriva-liquidazione-giudiziale-AEy0gZHD.
- ESMA «*Financial Technology: ESMA's Approach. 4th Luxemburg FinTech Conference*», 10 ottobre 2018, https://www.esma.europa.eu/sites/default/files/library/esma71-99-1051_speech_on_cryptoassets_-_pa.pdf.
- ESMA. «*Advice Initial Coin Offerings and Crypto-Assets*», 9 gennaio 2019. https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.
- EUR LEX «*EUR-Lex - L24216 - EN - EUR-Lex. Verso Un Nuovo Quadro per l'infrastruttura Delle Comunicazioni Elettroniche.*». https://eur-lex.europa.eu/IT/legal-content/summary/a-new-framework-for-electronic-communications-services.html.
- EUROPEA CENTRAL BANK «*Licensing of Crypto-Asset Activities*», 17 agosto 2022. https://www.bankingsupervision.europa.eu/press/publications/newsletter/2022/html/ssm.nl220817_2.en.html.

- EUROPEAN CENTRAL BANK «*Crypto-Assets: A New Standard for Banks*», 15 febbraio 2023. https://www.bankingsupervision.europa.eu/press/publications/newsletter/2023/html/ssm.nl230215_1.en.html.
- EUROPEAN CENTRAL BANK. «*Banks' Digital Transformation: Where Do We Stand?*», 15 febbraio 2023. https://www.bankingsupervision.europa.eu/press/publications/newsletter/2023/html/ssm.nl230215_2.en.html.
- EUROPEAN CENTRAL BANK. «*Eurosystem Oversight Framework for Electronic Payment Instruments, Schemes and Arrangements*», novembre 2021. https://www.ecb.europa.eu/paym/pdf/consultations/ecb.PISApublicconsultation202111_1.en.pdf.
- EUROPEAN COMMISSION. DIRECTORATE GENERAL FOR FINANCIAL STABILITY, FINANCIAL SERVICES AND CAPITAL MARKETS UNION., VVA., E CEPS. «*A Study on the Application and Impact of Directive (EU) 2015/2366 on Payment Services (PSD2)*». LU: Publications Office, 2023. https://data.europa.eu/doi/10.2874/996945.
- FABER D., VERMUNT N. «*Bank Failure: Lessons from Lehman Brothers*». Oxford, New York: Oxford University Press, 2017.
- FALCONE G. «*Tre idee intorno al c.d. "FinTech"*», in *Rivista di diritto bancario* (giugno 2018): 351 e ss.
- «Fallimento FTX, Ceo John Ray: "Mai visto un fallimento così in 40 anni"», in *Teleborsa*, La Stampa, 18/11/2022. https://www.teleborsa.it/News/2022/11/18/fallimento-ftx-ceo-john-ray-mai-visto-un-fallimento-cosi-in-40-anni--39.html.
- FAMA E. F. «*Efficient Capital Markets: A Review of Theory and Empirical Work*», in *The Journal of Finance* 25, fasc. 2 (1970): 383–417. https://doi.org/10.2307/2325486.
- FANTATO D. «*Crypto & Digital Assets Summit*». Financial Times Event, 2022. https://www.ftadviser.com/events-awards/2022/11/28/crypto-digital-assets-summit/.
- Ferrarini G. «*la nuova disciplina europea dell'abuso di mercato*», in *Rivista delle Società*, 2004, 54.
- FERRARINI G., GIUDICI P., BOREIKO D. «*Blockchain Startups and Prospectus Regulation*», in *European Business Organization Law Review*, (25 novembre 2019): 665 e ss.
- Ferri W. «*Il terribile 2022 delle criptovalute*». Money.it, 31 dicembre 2022. https://www.money.it/il-terribile-2022-delle-criptovalute.
- FIMMANÒ F., FALCONE G. «*FinTech*». Edizioni Scientifiche Italiane, 2019.

- FINANCIAL STABILITY BOARD «*Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative Document*», 11 ottobre 2022.
- FINANCIAL STABILITY BOARD. «*FinTech and Market Structure in Financial Services: Market Developments and Potential Financial Stability Implications*», 14 febbraio 2019.
- FINANCIAL STABILITY BOARD. «*High-Level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Final Report*», 17 luglio 2023. https://www.fsb.org/2023/07/high-level-recommendations-for-the-regulation-supervision-and-oversight-of-crypto-asset-activities-and-markets-final-report/.
- FINANCIAL STABILITY BOARD. «*Promoting Global Financial Stability: 2022 FSB Annual Report*», 16 novembre 2022.
- FINANCIAL STABILITY BOARD. «*Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative Report*», 11 ottobre 2022. https://www.fsb.org/2022/10/regulation-supervision-and-oversight-of-crypto-asset-activities-and-markets-consultative-report/.
- FINANCIAL STABILITY BOARD. «*Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative Document*», 11 ottobre 2022, https://www.fsb.org/wp-content/uploads/P111022-3.pdf
- FINMA. «*FINMA publishes ICO guidelines*», 2018. https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?sc_lang=en&hash=83EE49D77DA54DD079F314D9EDCBDC3D.
- FINOCCHIARO G. «*Le cripto-valute come elementi patrimoniali assoggettabili alle pretese esecutive dei creditori*», in Rivista di Diritto Processuale, 2019, 86-104.
- FITZGERALD P., NEENAN A. «*Annus Horribilis 2022: Regulation may be the only way out of crypto's 'Horrible Year'*», 5 dicembre 2022, CITY AM edizione. https://www.cityam.com/annus-horribilis-2022-regulation-may-be-the-only-way-out-of-cryptos-horrible-year/.
- FRAILE CARMONA A., GONZÁLEZ-QUEL LOMBARDO A., RIVERA PASTOR R., TARÍN QUIRÓS C., VILLAR GARCÍA J. P., RAMOS MUÑOZ D., CASTEJÓN MARTÍN L. «*Competition Issues in the Area of Financial Technology (FinTech)*», luglio 2018.
- FRANKLIN A., GU X. «*The Interplay between Regulations and Financial Stability*», in *Journal of Financial Services Research* 53, fasc. 2 (1 giugno 2018): 233–48. https://doi.org/10.1007/s10693-018-0296-7.

- FRANZA E. «*La product intervention del mondo MIFID II/MIFIR*», in *Il diritto dell'economia*, fasc. n.98 (gennaio 2019): 325–51.
- FRATINI PASSI L. «*Open Banking: le sfide nel mercato globale*», in Bancaria n. 7-8/2022 (agosto 2022): 93.
- FRATINI PASSI L. «*Open Finance: tendenze e innovazione collaborativa*» in, *MINERVA BANCARIA* N.3/2023 (marzo 2023), *Bancaria Editrice* 143.
- FRIGENI C. «*Il mercato primario delle cripto-attività. Offerta al pubblico e regime di trasparenza nella proposta di Regolamento MiCA*», in *Osservatorio del diritto civile e commerciale*, fasc. speciale, Il Mulino, (settembre 2022): 23 e ss.
- FTX [@FTX_OFFICIAL]. «*Press Release*» Tweet. *Twitter*, 11 novembre 2022. https://twitter.com/FTX_Official/status/1591071832823959552.
- Furnari S L. «*Validità e caratteristiche degli smart contract e possibili usi nel settore bancario finanziario*» in CORAPI E., LENER R. (a cura di), *I diversi settori del Fintech. Problemi e prospettive*, 2019», 89–110, 2019.
- FURNARI S. L. «*La finanza decentralizzata. Cripto-attività, protocolli, questioni giuridiche aperte*». Minerva Bancaria. https://rivistabancaria.it/monografia/la-finanza-decentralizzata-cripto-attivita-protocolli-questioni-giuridiche-aperte/.
- FURNARI S. L., SCHETTINI D. «*Euro digitale: primi commenti alla Proposta di Regolamento. Tra innovazione tecnologica e adozione di massa*», in *Diritto Bancario*, Luglio 2023. https://www.dirittobancario.it/wp-content/uploads/2023/07/2023-Proietti-Digital-Services-Act.pdf.
- GANDOLFI L. «*cripto-asset e intermediari vigilati: una guida per progettare e presentare un piano AML volto a mitigare efficacemente i rischi*». In *Cripto-attività: antiriciclaggio e gestione dei rischi aziendali*, 51 e ss. Pacini Editore, 2024.
- GERADIN D. «*What Should EU Competition Policy Do to Address the Concerns Raised by the Digital Platforms' Market Power?*» SSRN Scholarly Paper. Rochester, NY, 30 settembre 2018. https://doi.org/10.2139/ssrn.3257967.
- GIAVAZZI S. «*l'abuso di informazioni privilegiate*», in *Diritto Penale delle Società*, I, 2014, 702.
- GIMIGLIANO G. «*Payment Tokens and the Path Towards MiCA*», in *Italian Law Journal*, volume 8, fascicolo 1, 2022
- GIORDANO M. T., CAPACCIOLI S. «*Crypto-asset: Regolamento MiCa e DLT Pilot Regime. analisi ragionata su token, stablecoin, CASP*». Giuffrè Francis Lefebvre, 2023.

- GIORDANO M.T. «*Oggetto, ambito di applicazione e definizioni*». In *Crytpo-asset: Regolamento MiCA e DLT Pilot Regime; analisi ragionata su token, stablecoin, CASP*. Giuffrè Francis Lefebvre, 2023.
- GIUCA M. «*Criptovalute e diritto penale nella prevenzione e repressione del riciclaggio*», in *Diritto Penale Contemporaneo* (gennaio 2021): 150 e ss.
- GOODHART C., HARTMANN P., WEISBROD S., ROJAS-SUAREZ L., LLEWELLYN D. T. «*Financial Regulation: Why, How and Where Now?*» *Routledge & CRC Press*, 1998. https://www.routledge.com/Financial-Regulation-Why-How-and-Where-Now/Goodhart-Hartmann-Llewellyn-Rojas-Suarez-Weisbrod/p/book/9780415185059.
- GORTON G., METRIK A., SHLEIFER A., TARULLO D. K. «*Regulating the Shadow Banking System*», in *Brookings Papers on Economic Activity*, 261-312, 2023.
- GORTSOS C. «*The Commission's 2020 Proposal for a Markets in Crypto-Assets Regulation ('MiCAR'): A Brief Introductory Overview*». SSRN Scholarly Paper. Rochester, NY, 7 maggio 2021. https://doi.org/10.2139/ssrn.3842824.
- GRASSI L., FIGINI N., FEDELI L. «*How Does a Data Strategy Enable Customer Value? The Case of FinTechs and Traditional Banks under the Open Finance Framework*», in *Financial Innovation* 8, fasc. 1 (16 agosto 2022): 75. https://doi.org/10.1186/s40854-022-00378-x.
- GREEN E. F., AMICO J. F. «*Blockchain, marketplace lending and crowdfunding: emerging issues and opportunities in fintech*». In *Research handbook on shadow banking*, 253 e ss. Edward Elgar, 2018.
- HACKER P., THOMALE C. «*Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law*». SSRN Scholarly Paper. Rochester, NY, 22 novembre 2017. https://doi.org/10.2139/ssrn.3075820.
- HAENTJENS M., DE GRAAF T., KOKORIN I. «*The Failed Hopes of Disintermediation: Crypto-Custodian Insolvency, Legal Risks and How to Avoid Them*». SSRN Scholarly Paper. Rochester, NY, 30 aprile 2020. https://doi.org/10.2139/ssrn.3589381.
- HANSEN S. «*How Will Open Finance and the Financial Data Access Regulation Impact the Financial Sector?*», 3 agosto 2023. https://www.ey.com/en_be/financial-services/how-will-open-finance-and-financial-data-access-regulation-impact-financial-sector.
- Ibrido R. *L'unione bancaria europea Profili costituzionali*. G. Giappichelli Editore, 2017.
- IL SOLE 24 ORE. «*Binance: il CEO CZ lascia la guida dopo un accordo con la giustizia americana*», 22 novembre 2023. https://www.ilsole24ore.com/art/binance-accordo-dip-giustizia-usa-zhao-si-dimette-e-si-dichiara-colpevole-AF7QuXjB.
- IMF «*Shadow Banks: Out of the Eyes of Regulators*». In *IMF*

https://www.imf.org/en/Publications/fandd/issues/Series/Back-to-Basics/Shadow-Banks.

- IMF. «*Elements of Effective Policies for Crypto Assets*», 23 febbraio 2023.https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-Assets-530092.
- INDAP S., CHIPOLINA S. «*Voyager Digital spurns 'lowball' joint bid from FTX*». *Financial Times*, 25 luglio 2022, sez. Cryptofinance. https://www.ft.com/content/ab23e979-8e71-4d5c-85cd-98572d0aedc0.
- IOSCO. «*Policy Recommendations for Crypto and Digital Asset Markets. Final Report*», 16 novembre 2023. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf.
- IOVINO P. «*Le criptovalute nella fase di layering del riciclaggio*», in *Giurisprudenza penale*, fasc. 3 (2022).
- IRTI N. «Concetto giuridico di mercato e dovere di solidarietà», *in Rivista di diritto civile* (1997): 185 e ss.
- IRTI N. «*Dialogo su diritto e tecnica*». Laterza, 2001.
- IRTI N. «*l'essenza tecnica del diritto (ancora un dialogo con Emanuele Severino)*». In *l'uso giuridico della natura*. Laterza, 2013.
- IRTI N. «*L'ordine giuridico del mercato*». libri del tempo. Editori Laterza, 2008.
- IRTI N. «*L'uso giuridico della natura*». Laterza, 2013.
- KHARIF O. «*Crypto Billionaire Sam Bankman-Fried Eyeing Bid for Celsius Assets - Bloomberg*», 28 settembre 2022, Bloomberg.
  https://www.bloomberg.com/news/articles/2022-09-27/crypto-billionaire-bankman-fried-eyeing-bid-for-celsius-assets.
- KHARIF O. «*Crypto Exchange Binance To Sell $529 Million of Bankman-Fried's FTT Token*», 7 novembre 2022, Bloomberg.
  https://www.bloomberg.com/news/articles/2022-11-06/binance-to-sell-529-million-of-ftt-token-amids-revelations.
- KOKORIN I. «*The anatomy of crypto failures and investor protection under MiCAR*», in *Capital Markets Law Journal*, fasc. vol. 18, 4 (2023): 501 e ss.
- KORSMO C. «*The Audience for Corporate Disclosure*», in *Faculty Publications Iowa L. Review* 1581 (2017). https://scholarlycommons.law.case.edu/faculty_publications/1717.
- Kruppa M. «*Crypto exchange FTX secures backing from venture capital and hedge funds*». *Financial Times*, 20 luglio 2021, sez. Cryptocurrencies.
  https://www.ft.com/content/a3a90a4f-54e4-4b4f-b1df-2d9d8ca7712d.

- LEE J., L'HEUREUX F. «*A regulatory Framework for Cryptocurrency*» in *European Business Law Review* Rev. 423 (2020).
- Legnini G., Morosini P. «*Le giurisdizioni e le autorità indipendenti*». Consiglio Superiore della Magistratura, 2018. https://www.csm.it/documents/21768/41479/Le+giurisdizioni+e+le+autorit%C3%A0+indipendenti/4c3a6fce-720e-0df7-b993-ddbdd7d7a497.
- LEMMA V. *«Shadow Banking System: Creating Transparency in the Financial Markets»*. London: Palgrave Macmillan UK, 2016. https://doi.org/10.1057/9781137496133.
- LENER R. «*Tecnologie e attività finanziaria*», in *Rivista trimestrale di diritto dell'economia*, (marzo 2019).
- LENER R., CORAPI E. «*I diversi settori del FinTech*». Cedam, 10/2019.
- LENER R., LUCANTONI P. «*Sostenibilità ESG e Attività Bancaria*», in Banca, borsa, tit. cred., I (gennaio 2023). https://fchub.it/sostenibilita-esg-e-attivita-bancaria/.
- Lener R., LUCHENA G., ROBUSTELLA C. «*Mercati regolati e nuove filiere di valore»*. I. Diritto dell'economia, G. Giappichelli Editore, 4/2021.
- LEO S., PANETTA I. C. «*The DLT Landscape in Banking Key Features of Prominent Use Cases through Strengths and Weaknesses*». In *The Role of Distributed Ledger Technology in Banking. From theory to practice*, Cambridge university press:294 e ss., 2023.
- LINDA J. «*Open Banking*». New York: Oxford Academic, 2022. https://doi.org/10.1093/oso/9780197582879.001.0001.
- LIVNI E. «*For Rules in Technology, the Challenge Is to Balance Code and Law*». *The New York Times*, 23 novembre 2021, sez. Business. https://www.nytimes.com/2021/11/23/business/dealbook/cryptocurrency-code-law-technology.html.
- LO CONTE R. «*Valutazione del dissesto o rischio di dissesto bancario e impugnabilità delle decisioni del Single Resolution Board, note a sentenza del Tribunale dell'Unione Europea 6 luglio 2022*», in *Rivista Trimestrale di Diritto dell'Economia*, 3/2022, 100 e ss.
- LOMBARDO S. «*Acquisto di partecipazioni di controllo, fattispecie a formazione progressiva, informazione privilegiata e insider secondario*», in *Le Società: rivista di diritto e pratica commerciale societaria e fiscale*, Vol.33, pp.702-710
- Lops F. P., Motti C. «*La circolazione della ricchezza nell'era digitale*». Pacini Editore, 2021.
- LOPS V. «*Da JP Morgan a BofA e BlackRock: tanti big nella rete del crack FTX*», Il Sole 24 ORE, 19 novembre 2022.
- LOPS V. «*Ftx, spuntano asset liquidi per 5 miliardi*». Il Sole 24 ORE, 12 gennaio 2023.

- M. MAURER. «*More Crypto Exchanges Verify Reserves, But Questions About Assets Remain*», 5 dicembre 2022, The Wall Street Journal. https://www.wsj.com/articles/more-crypto-exchanges-verify-reserves-but-questions-about-assets-remain-11670153687.
- MACCARONE S. «*discorso del presidente CBI*», in The Global Open Finance Report, marzo 2023. https://www.cbi-org.eu/Media-Events/Next-Appointments/The-Global-Open-Finance-Report.
- MACCHIAVELLO E. «*FinTech e regolazione: attuali zone grigie del diritto dell'economia e la necessità di un ripensamento generale del sistema*». In *I luoghi dell'economia, le dimensioni della sovranità*, 47–67. G. Giappichelli Editore, 2019.
- MARLINSPIKE M. «*My first impressions of web3*», in *OSnews*, 7 gennaio 2022.
- MATTASSOGLIO F. «*Algoritmi e regolazione. Circa i limiti del principio di neutralità tecnologica*», in *Rivista della Regolazione dei mercati*, fasc. 2 (2018): 226 e ss.
- MATTASSOGLIO F. «*Big data: impatto sui servizi finanziari e sulla tutela dei dati personali*». G. Giappichelli Editore, 2017.
- MATTASSOGLIO F. «*Intelligenza Artificiale e moneta: grandi "poteri" e maggiori responsabilità. Alcuni motivi che inducono a riflettere circa l'urgente necessità di una moneta digitale del banchiere centrale*», in *Rivista trimestrale del diritto dell'economia*, fasc. supplemento 2 al n. 3/2021 (marzo 2021): 371 e ss.
- MATTASSOGLIO F. «*La profilazione dell'investitore nell'era dei big data. I rischi dell'estremizzazione della regola del "know your customer" (The Customer's profiling in the Era of Big Data.The Risks related to the radicalization of the "know your customer's role)*», in *Rivista Trimestrale di Diritto dell'Economia* n. 4/2016, supplemento n.1, (1° gennaio 2016): 233–54.
- MAUGERI M. «*Proposta di Regolamento MiCA (Markets in Crypto-Assets) e tutela del consumatore nella commercializzazione a distanza*»., in *Osservatorio del diritto civile e commerciale*, Il Mulino, settembre 2022, 21.
- MAUGERI M. «*Smart Contracts e disciplina dei contratti - Smart Contracts and Contract Law*». Il Mulino, 2021.
- MAUGERI M., CONSULICH F., MILIA C., POLI T. N., G. TROVATORE G. «*AI e abusi di mercato: le leggi della robotica si applicano alle operazioni finanziarie?*», in *Quaderni giuridici Consob*, 29 maggio 2023.
- MAUME P. «*The Regulation on Markets in Crypto-Assets (MiCAR): Landmark Codification, or First Step of Many, or Both?*», 2023, 243–75.
- MAZZOCCHI P. «*La Custodia Sicura Di Bitcoin*» Il Sole 24 ore (febbraio 2023).

- MINTO A. «*il sistema dei controlli interni delle banche e la gestione del rischio di riciclaggio*». In *Saggi e monografie di diritto dell'economia*. Cedam, 2023.
- MINTO A. «*Riflessioni sull'applicabilità della disciplina antiriciclaggio ai Non-Fungible Tokens ("NFT")*». In *Rivista di Diritto Bancario*, 2023, 41.
- MINTO A. «*The Legal Characterization of Crypto-Exchange Platforms*», in *Global Jurist* 22, fasc. 1 (1 aprile 2022): 137–56. https://doi.org/10.1515/gj-2020-0085.
- MOHAN V. «*Automated Market Makers and Decentralized Exchanges: A DeFi Primer*». SSRN Scholarly Paper. Rochester, NY, 30 ottobre 2020. https://doi.org/10.2139/ssrn.3722714.
- MOLLMAN S. «'*A Lot of People Have Compared This to Lehman. I Would Compare It to Enron': Larry Summers Has Some Choice Words for Sam Bankman-Fried and FTX*». *Fortune*, 11 novembre 2022. https://fortune.com/2022/11/11/larry-summers-ftx-crypto-collapse-more-like-enron-than-lehman/.
- MOTTI C. «*Mercati regolamentati, sistemi multilaterali e internalizzatori sistematici*». In *L'attuazione della Mifid in Italia*, 2010.
- MUCCIARELLI F. «*L'insider trading della nuova disciplina del D.lgs 58/98*», 2000, 935.
- MUCCIARELLI F. «*L'insider trading nella rinnovata disciplina UE sugli abusi di mercato*», 2016, 193.
- MUCCIARELLI F. «*Speculazione mobiliare e diritto penale*», in *quaderni di giurisprudenza commerciale*. Giuffrè Francis Lefebvre, 1995.
- MURINO F. «*Vigilanza ed enforcement sui mercati delle cripto-attività nella proposta di Regolamento MiCA*», settembre 2022. https://doi.org/10.4478/106719.
- MUROLO C. «*Open Banking: così le banche possono conservare il rapporto diretto con il cliente*». *Agenda Digitale*, 5 ottobre 2017. https://www.agendadigitale.eu/cittadinanza-digitale/open-banking-cosi-le-banche-possono-conservare-il-rapporto-diretto-con-il-cliente/.
- MURTAS L. «*Antiriciclaggio e cripto-attività nella legislazione europea e nazionale*». In *cripto-attività: antiriciclaggio e gestione dei rischi aziendali*, 23–42. Pacini Editore, 2024.
- NAGARAJAN S. «*Sam Bankman-Fried Says FTX Has Moved Its HQ from Hong Kong to the Bahamas Because of Its Crypto Framework*». Yahoo Finance, 27 settembre 2021. https://finance.yahoo.com/news/sam-bankman-fried-says-ftx-150947960.html.
- Nicolle E. «*Crypto Secrecy Makes DeFi a Financial Felon's Wonderland*». *Bloomberg.Com*, 27 gennaio 2022. https://www.bloomberg.com/news/articles/2022-01-27/crypto-s-cloak-of-anonymity-makes-defi-a-wonderland-for-felon.
- NICOTRA M. «*Diritto della Blockchain, Intelligenza Artificiale e IoT*». Ipsoa, 2018.

- NICOTRA M., SARZANA F., IPPOLITO S., M. SIMBULA M. «*Il MiCar, Guida al Regolamento Europeo sui mercati delle cripto*». Giuffrè Francis Lefebvre, 2023.
- O'CONNELL W. D. «*Crypto Platforms Say They're Exchanges, but They're More like Banks*», in *The Conversation*, 11 agosto 2022. http://theconversation.com/crypto-platforms-say-theyre-exchanges-but-theyre-more-like-banks-188339.
- OMARINI A. «*Banks and Fintechs: How to Develop a Digital Open Banking Approach for the Bank's Future*», in *International Business Research* 11 (10 agosto 2018): 23. https://doi.org/10.5539/ibr.v11n9p23.
- OMAROVA S. «*Dealing with Disruption: Emerging Approaches to Fintech Regulation*», in *Cornell Law Faculty Publications*, 1 gennaio 2020. https://scholarship.law.cornell.edu/facpub/1726.
- OMAROVA S. «*License to Deal: Mandatory Approval of Complex Financial Products*», in *Cornell Law Faculty Publications*, 1 gennaio 2012. https://scholarship.law.cornell.edu/facpub/1011.
- OMAROVA S. «*New Tech v. New Deal: Fintech as a Systemic Phenomenon*», in *Yale Journal on Regulation* 36 (2019).
- OMAROVA S. «The People's Ledger: How to Democratize Money and Finance the Economy», *SSRN Electronic Journal*, 2020. https://doi.org/10.2139/ssrn.3715735.
- ORTENCA A., PALMA S., OLIVER J., CHIPOLINA S., FONTANELLA-KHAN J. «*Binance ditches deal to rescue rival crypto exchange FTX*», in *Financial Times*, 10 novembre 2022, sez. FTX Trading Ltd. https://www.ft.com/content/ad440b22-00e2-44e9-b95d-449bb89fd504.
- OSSINGER J. «*Crypto-Derivatives Exchange FTX Leaves Hong Kong for Bahamas - Bloomberg*», 24 settembre 2021. https://www.bloomberg.com/news/articles/2021-09-24/bankman-fried-s-crypto-exchange-ftx-leaves-hong-kong-for-bahamas?leadSource=uverify%20wall.
- PACELLI V., FOGLIA M. «*Rischi di spillover tra asset tradizionali e digitali*», in *BANCARIA*, n. 10, (ottobre 2023).
- PAGLIANTINI S. «*La proposta MiCAR e le clausole abusive: una prima lettura*», in *Osservatorio del diritto civile e commerciale*, fasc. speciale (settembre 2022): 347 e ss.
- PARACAMPO M T. «*FinTech tra algoritmi, trasparenza e algo-governance*», in *Rivista della Banca e del Mercato Finanziario*, fasc. 2, Pacini Editore, (gennaio 2019).
- PARACAMPO M T. «*I prestatori di servizi per le cripto-attività Tra mifidizzazione della MICA e tokenizzazione della Mifid*». G. Giappichelli Editore, 2023.

- PARACAMPO M. T. «*Fintech Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*». II. Vol. I. G. Giappichelli Editore, 2021.
- PARACAMPO M. T. «*Fintech, introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*». G. Giappichelli Editore, 2019.
- PARACAMPO M.T. «*Los proveedores de servicios de criptoactivos entre antiguos y nuevos players*». In *Dinero Digital y Gobernanza IIC en la UE*. Thomson Reuters Aranzadi, 2022.
- PARACAMPO M.T. «*I prestatori di servizi per le cripto-attività*». In *I prestatore di servizi per le cripto-attività; tra mifidizzazione della MiCAe tokenizzazione della Mifid*. G. Giappichelli Editore, 2023.
- PATTERSON D. «*Internet Guru Tim O'Reilly on Web3: "Get Ready for the Crash"*», in *CBS News*, 10 febbraio 2022. https://www.cbsnews.com/news/web3-cryptocurrency-nft-tim-oreilly/.
- PATUELLI A. «Finanza, tecnologie e diritto» in *Bancaria* (giugno 2018): 16.
- PEDERZINI E. «*La Tracciabilità Dei Movimenti Finanziari Tra Anonimato e Pseudonimato: FinTech, Incorporazione Del Diritto Nella Tecnica e Paradigma by Design*», in *Rivista Di Diritto Bancario*, 2022.
- Pederzini E. «*La tracciabilità dei movimenti finanziari: anonimato e pseudoanonimato*». In *Diritto del FinTech*, 122 e ss. Cedam, 2020.
- PERASSI M. «*Il Regolamento MiCA nel contesto della disciplina bancaria e dei servizi di pagamento*». Centro Convegni Carlo Azeglio Ciampi, Roma: BANCA D'ITALIA, 29 settembre 2023.
- PERRONE A. «*Servizi d'investimento e tutela dell'investitore*», in *Banca Borsa Titoli di Credito*, 2019.
- PERUGINI M. L., DAL CHECCO P. «*Introduzione Agli Smart Contract (Introduction to Smart Contract)*». SSRN Scholarly Paper. Rochester, NY, 8 dicembre 2015. https://doi.org/10.2139/ssrn.2729545.
- PIATTELLI U. «*La regolamentazione del Fintech. Dai nuovi sistemi di pagamento all'intelligenza artificiale. Aggiornato al D.L. 17 marzo 2023 c.d. "Decreto Fintech"»*. Seconda edizione. G. Giappichelli Editore, 2023.
- PICOTTI L. «*Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*», in *Rivista trimestrale di diritto penale dell'economia*, fasc. 3–4 (2018), *Cedam*, 590–619.
- PIERINI A. «*L'unione bancaria europea come federalizing process*». Cedam, 2019.
- PIETROLUONGO M. «*I poteri di intervento temporaneo dell'ESMA*», in *Ius in itinere*, 20 marzo 2019. https://www.iusinitinere.it/i-poteri-di-intervento-temporaneo-dellesma-18944.

- PIETROLUONGO V. «*Finanza digitale: le novità del Regolamento DORA*», in *Diritto Bancario*, 30 marzo 2023. https://www.dirittobancario.it/wp-content/uploads/2023/03/2023-Pietroluongo-Panoramica-Regolamento-DORA.pdf.
- PISTOR K. «*A legal theory of finance*», in *Journal of Comparative Economics* 41, fasc. 2 (2013): 315–30.
- POLICE A. «*Lo speciale regime sanzionatorio di MiCA applicabile agli emittenti di ARTs e EMTs*». Centro Convegni Carlo Azeglio Ciampi, Roma: BANCA D'ITALIA, 29 settembre 2023.
- POWELL K. «*If You Can't Beat 'em, Join 'em: 77% of Banks Feel Pressure to Collaborate With Fintechs That They View as a Threat to Their Existence*», 12 gennaio 2023. https://www.businesswire.com/news/home/20230112005173/en/If-You-Can%E2%80%99t-Beat-%E2%80%98em-Join-%E2%80%98em-77-of-Banks-Feel-Pressure-to-Collaborate-With-Fintechs-That-They-View-as-a-Threat-to-Their-Existence.
- PROFETA V. «*Gli e-money tokens e la disciplina sulla moneta elettronica*». Roma: BANCA D'ITALIA, 29 settembre 2023.
- RADLEY-GARDNER O., BEALE H., ZIMMERMANN R., «*Fundamental Texts On European Private Law*». Hart Publishing, 2016. https://doi.org/10.5040/9781782258674.
- RAGANELLI B. «*Sanzioni Consob e tutela del contraddittorio procedimentale*», in *Giornale di Diritto Amministrativo*, fasc. 4 (2015): 517.
- RAGANELLI B.M. *«Frontiere di Diritto Pubblico dell'economia. Concorrenza, Regolamentazione, Vigilanza e Tutela»*, Cedam 3/2019.
- RAMPONE F. «*NFT e token crittografici*», in *Dialoghi di Diritto dell'Economia*, giugno 2023.
- Raskin M. «*The Law and Legality of Smart Contracts*». SSRN Scholarly Paper. Rochester, NY, 22 settembre 2016. https://doi.org/10.2139/ssrn.2842258.
- RAZZANTE R. «*Riciclaggio e reati connessi. Applicazioni giurisprudenziali e di vigilanza*». Giuffrè Francis Lefebvre, 2023.
- RICCIUTO V. «*La tutela dell'investitore finanziario. Prime riflessioni su contratto, vigilanza e regolazione del mercato nella c.d. MiFID 2*», gennaio 2016, 10.
- ROHAN. G., MCKENZIE S. «*In Defensive Interview, Sam Bankman-Fried Claims He's Broke and Committed No Fraud*». *CNBC*, 30 novembre 2022. https://www.cnbc.com/2022/11/30/former-ftx-ceo-sam-bankman-fried-says-i-didnt-ever-try-to-commit-fraud.html.
- ROLLE. C. R. «*Navigating The Digital Frontier: The Bahamas' Approach To Regulating Digital Assets*», in *IFC Review*,

https://www.ifcreview.com/articles/2023/september/navigating-the-digital-frontier-the-bahamas-approach-to-regulating-digital-assets/.

- ROONEY K. «*FTX Grew Revenue 1,000% during the Crypto Craze, Leaked Financials Show*», 20 agosto 2022, CNBC. https://www.cnbc.com/2022/08/20/ftx-grew-revenue-1000percent-during-the-crypto-craze-leaked-financials.html.
- ROSATO A. «*Profili penali delle criptovalute*». In *Quaderni del centro di ricerca sicurezza e terrorismo*. Pacini Giuridica, 2021.
- ROSENTHAL D. «*EE380 Talk*», 9/2/2022. https://blog.dshr.org/2022/02/ee380-talk.html.
- ROSS V. «*Developments in AI and Blockchain – How Do We Protect Investors and Supervise Markets Effectively?*», Afore Consulting 7th Annual FinTech and Regulation Conference, 7 febbraio 2023.
- Salomone D. «*I prestatori di servizi per le cripto-attività: requisiti e regime di vigilanza*». BANCA D'ITALIA, 2023.
- SANDEI C. «*L'offerta iniziale di cripto-attività*». G. Giappichelli Editore, 2022.
- SCOLETTA V. M. «*Doppio binario sanzionatorio e ne bis in idem nella nuova disciplina eurounitaria degli abusi di mercato*», in *Le Società*, 35, fasc. 2, IPSOA (2016): 218 ss.
- SECURITY COMMISSION OF BAHAMAS «*DARE, Consultation on the Digital Assets and Registered Exchange bill*», 2023.
- SELGIN G. «*Bank and Crypto Runs: F(Ac)TX vs Fiction*» Cato Institute (21 novembre 2022). https://www.cato.org/blog/bank-crypto-runs-factx-vs-fiction.
- SEMINARA S. «*il reato di insider trading tra obbligo di astensione e divieto di utilizzazione in borsa di informazioni riservate. considerazioni su riforme ordite, abortite e partorite*», in *Banca Borsa*, II (1998): 325 e ss.
- SGUBBI F. «*Abusi di mercato*», in Annali, fasc. II (2008): 20 e ss.
- SGUBBI F. «*Il risparmio come oggetto di tutela penale*», 2009, 349 e ss.
- SHUBBA K., OLIVER J., INDAPP S. «*New FTX chief says crypto group's lack of control worse than Enron*», 18 novembre 2022, Financial Times. https://www.ft.com/content/7e81ed85-8849-4070-a4e4-450195df08d7.
- SIANI G. «*La regolamentazione delle nuove tecnologie basate sulla Distributed ledger technology – DLT, tra tutela del mercato e rischi di sistema*». BANCA D'ITALIA, 3 maggio 2022.

https://www.bancaditalia.it/pubblicazioni/interventi-vari/int-var-2022/SIANI_3_maggio_2022.pdf.

- SIBILIO N. I., BOERO M. «*Presidio dei rischi e tecnologie innovative: sicurezza, blockchain, algoritmi, big data*», in *Bancaria* (novembre 2023).
- SICIGNANO G. J. «*231 e criptovalute*», in *231 e impresa*. Pacini Editore, 2021.
- SIMBULA M. «*Panoramica del Regolamento MiCA: l'Europa regola le cripto-attività*». In *Il MiCAR, Guida al Regolamento Europeo sui mercati delle cripto*. Giuffrè Francis Lefebvre, 2023.
- SINCLAIR S. «*FTX Revenue Exploded 1,000% to Beyond $1B Last Year: Report*». *Blockworks*, 22 agosto 2022, sez. Markets. https://blockworks.co/news/ftx-revenue-exploded-1000-to-beyond-1b-last-year-report.
- SKITKA L., MOSIER K., BURDICK M. «*Accountability and automation bias*», in *International Journal of Human-Computer Studies* 52 (1 aprile 2000): 701–17. https://doi.org/10.1006/ijhc.1999.0349.
- SMERALDI S., RIPELLINO G. «*bitcoin e altre valute digitali: una nuova primavera dopo il cripto-winter*», in *Rivista Bancaria*, Minerva Bancaria (marzo 2023).
- SORGE V, *«discorso del Vice CEO di Banca Popolare di Puglia e Basilicata*, in The Global Open Finance Report, marzo 2023. https://www.cbi-org.eu/Media-Events/Next-Appointments/The-Global-Open-Finance-Report.
- STIMOLO S. «*Caroline Ellison: "l'insider per eccellenza" testimonia sul caso del crypto-exchange FTX*». *The Cryptonomist*, 16 ottobre 2023. https://cryptonomist.ch/2023/10/16/caroline-ellison-caso-crypto-exchange-ftx/.
- Surowiecki J. «*La saggezza della folla*». Fusi Orari, 2007.
- TAGLIAMONTI I. «*L'integrità dei mercati delle cripto-attività, tra vecchie e nuove tutele*», in *Osservatorio del diritto civile e commerciale*, Il Mulino, fasc. speciale (settembre 2022).
- THE ECONOMIST. «*The failure of FTX and Sam Bankman-Fried will leave deep scars*». 17 novembre 2022. https://www.economist.com/briefing/2022/11/17/the-failure-of-ftx-and-sam-bankman-fried-will-leave-deep-scars.
- THE FINANCIAL CRISIS INQUIRY COMMISSION. «*The Financial Crisis Unquiry Report*», gennaio 2011. http://fcic-static.law.stanford.edu/cdn_media/fcic-reports/fcic_final_report_full.pdf.
- TIME. «*Sam Bankman-Fried's Political Donations: What We Know*», 14 dicembre 2022. https://time.com/6241262/sam-bankman-fried-political-donations/.

- TINA A. «*Mercati centralizzati, decentralizzati. Prospettive di inquadramento della DeFi nell'attuale orizzonte MiFID*», in *Osservatorio del diritto civile e commerciale*, fasc. speciale, Il Mulino, (settembre 2022): 42 e ss.
- TRAUTMAN L. J. «*The FTX Crypto Debacle: Largest Fraud Since Madoff?*» *SSRN Electronic Journal*, 2022. https://doi.org/10.2139/ssrn.4290093.
- TROIANO V., MOTRONI R. «*La MiFID II: Rapporti con la clientela - regole di governance - mercati*». Cedam, 2016.
- U.S. SECURITIES AND EXCHANGE COMMISSION. «*SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities*». https://www.sec.gov/news/press-release/2017-131.
- UNITED STATES: FINANCIAL CRISIS INQUIRY COMMISSION. «*The Financial Crisis Inquiry Report: Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States*». U.S. Government Printing Office, 25 febbraio 2011. https://www.govinfo.gov/app/details/GPO-FCIC.
- URBANI A. «*Verso la centralizzazione della supervisione antiriciclaggio?*», in *Rivista trimestrale di diritto dell'economia*, fasc. suppl. al n. 1 (2022): 172 e ss.
- US SECURITY EXCHANGE COMMISSION. «*Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*», Release n. 81207, 25 luglio 2017
- VALSANIA M. «*Ftx, scoppia il caso delle donazioni bipartisan: soldi ai politici Usa per regole più blande*», 28 febbraio 2023, Il Sole 24 Ore.
- VAN DER LINDEN T., SHIRAZI T. «*Markets in Crypto-Assets Regulation: Does It Provide Legal Certainty and Increase Adoption of Crypto-Assets?*», in *Financial Innovation* 9, fasc. 1 (10 gennaio 2023): 22. https://doi.org/10.1186/s40854-022-00432-8.
- VAN VALKENBURGH P. «*There's No Such Thing as a Decentralized Exchange*», in *Coin Center* The Block (3 ottobre 2020).
- VENTORUZZO M. «*Abusi di mercato, sanzioni Consob e diritti umani: il caso Grande Stevens e altri c. Italia*», in *rivista delle società*, 2014, 693 e ss.
- Vezzoso S. «*FinTech, access to data, and the role of competition policy*», in Competition and Innovation, 30 gennaio 2018, https://deliverypdf.ssrn.com/delivery.php?ID=294114121126074117025031101118086070063055032019074004085073104009029007070020109007042057100123047057125069095099123022025010126016017086082004067088091084030097002033082004005082017107068092011095007122086110.

- VEZZOSO S. «*Fintech, Access to Data, and the Role of Competition Policy*». SSRN Scholarly Paper. Rochester, NY, 22 gennaio 2018. https://doi.org/10.2139/ssrn.3106594.
- VICARI A. «*Il white paper nella proposta di regolamento sulle cripto-attività (MiCAR)*» osservatorio del diritto civile e commerciale, fasc. speciale (settembre 2022): 249 e ss.
- WALCH A.. «*Committee on Banking, Housing, and Urban Affairs Cryptocurrencies: What Are They Good For?*» Responses to Questions for the Record UNITED STATES SENATE COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS, 27 luglio 2021.
- WRIGHT I. «*Cos'è il token FTX (FTT)? Prezzo, storia e come acquistarlo*», https://coinkickoff.com/it/ftx-token-ftt/.
- ZETZSCHE D. A, ANNUNZIATA F., ARNER D. W., BUCKLEY R. P. «*The Markets in Crypto-Assets Regulation (MiCA) and the EU Digital Finance Strategy*», in *Capital Markets Law Journal* 16, fasc. 2 (20 luglio 2021): 203–25. https://doi.org/10.1093/cmlj/kmab005.
- ZETZSCHE D. A., ARNER D.W., BUCKLEY R. P. «*Decentralized Finance*», in *Journal of Financial Regulation* 6, fasc. 2 (20 settembre 2020): 172–203. https://doi.org/10.1093/jfr/fjaa010.
- ZETZSCHE D. A., ARNER D.W., BUCKLEY R. P. «*The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*». SSRN Scholarly Paper. Rochester, NY, 13 agosto 2017. https://doi.org/10.2139/ssrn.3018214.
- ZETZSCHE D. A., ARNER D.W., BUCKLEY R. P., BARBERIS J. N. «*From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*». SSRN Scholarly Paper. Rochester, NY, 28 aprile 2017. https://doi.org/10.2139/ssrn.2959925.
- ZETZSCHE D. A., ARNER D.W., BUCKLEY R. P., Föhr L. «*The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*». SSRN Scholarly Paper. Rochester, NY, 24 luglio 2018. https://doi.org/10.2139/ssrn.3072298.
- Zoppini A. «*La concorrenza tra ordinamenti giuridici*», in Vol. 68. *Percorsi*. Laterza, 2004.