COMMENTO AL D.LGS. 129 DEL 2024 DI ATTUAZIONE DEL REGOLAMENTO UE SUI MERCATI DELLE CRIPTO-ATTIVITA'. LE NOVITA' SUL VERSANTE PENALISTICO E AMMINISTRATIVO PUNITIVO*

di
Jacopo Della Torre e Gabriele Ponteprino

(*Professore associato di Diritto processuale penale, Università di Genova; Assegnista di ricerca in Diritto penale, Università di Genova*)

1. Con il d.lgs. 5.9.2024 n. 129 il Governo ha inteso adeguare l'ordinamento italiano al Regolamento 1114/2023/UE, relativo ai mercati delle cripto-attività (c.d. MiCA)[1]. Trattasi, come noto, di un intervento che si colloca nel più generale contesto delle misure approvate dall'Unione in materia di finanza digitale[2]. Un ambito, quest'ultimo,

* Il presente elaborato si inserisce nell'ambito del progetto "*PRIN 2022 PNRR – Progetto: CRYPTOSAFE (Towards a safe seizure and confiscation of crypto-assets in criminal proceedings)*". Codice progetto P2022HW85A; CUP D53D23022280001. *Principal Investigator*: Prof. Jacopo Della Torre.
Pur essendo il frutto di una riflessione congiunta, Jacopo Della Torre ha redatto i parr. 1, 2, 3, 5.1 e 6, mentre Gabriele Ponteprino i parr. 4, 4.1 e 5.

[1] Per un'analisi di più ampio spettro del Regolamento MiCA, nella già cospicua bibliografia, si rimanda alle collettanee a cura di M. Nicotra, F. Sarzana di S. Ippolito e M. Simbula, *Il Micar. Guida al regolamento europeo sui mercati delle cripto*, Milano 2023 e di S. Capaccioli, M.T. Giordano, *Crypto-asset: Regolamento MiCA e DLT pilot regime*, Milano 2023; R. Razzante, *Il panorama delle regole UE su blockchain e crypto asset*, in *Notariato* 2023, 579 ss.; I. Avagna, *Regolamentazione delle cripto-attività: lo scenario comunitario*, in *Amm. & Fin.* 2024, 1 ss.; A. Ciaccia, *Cripto attività: stabilite nuove regole per chi emette e più tutele per chi investe*, in www.ipsoa.it, 14.9.2024; A. Pantaleo, *Crypto attività: qual è il procedimento autorizzativo dei prestatori di servizi*, in www.ipsoa.it, 20.7.2023.

[2] Ci riferiamo al *Digital Finance Package* proposto dalla Commissione europea il 24 settembre al 2020, al fine di «stimolare la competitività e l'innovazione europee nel settore finanziario, creando le basi perché l'Europa possa definire le norme in questo settore a livello mondiale» (cfr. il Comunicato Stampa della Commissione Europea del 24.9.2020, in www.ec.europa.eu/commission). Esso prevede l'implementazione delle «strategie per la finanza digitale e per i pagamenti al dettaglio», nonché una serie di «proposte legislative sulle cripto-attività e la resilienza digitale». Tra quelle recentemente approvate segnaliamo: il Regolamento 2554/2022/UE, relativo alla resilienza operativa digitale per il settore finanziario (c.d. DORA); il Regolamento 858/2022/UE (relativo a un

avente dimensione globale e in continuo sviluppo, ma ancora scarsamente regolato[3]. Difatti, se in particolare per quanto concerne il contrasto al *money laundering* e al finanziamento del terrorismo il legislatore dell'Unione, così come quello interno, si erano già da tempo dimostrati particolarmente sensibili[4], per contro, le modalità di emissione, di offerta al pubblico, di negoziazione e la prestazione di servizi per le cripto-attività non erano finora oggetto di una specifica disciplina.

Il vuoto normativo risultava, tuttavia, intollerabile, non solo per i rischi che ciò determinava a livello di stabilità finanziaria dei Paesi membri, dato l'enorme flusso di asset virtuali scambiati ogni giorno[5], ma anche da una prospettiva più strettamente penalistica.

Ciò risulta chiaro se solo si considera che la peculiare fisionomia delle transazioni di valori basate sulla tecnologia del c.d. "registro-distribuito" (c.d. *blockchain*)[6] –

regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito); la Direttiva 2022/2556/UE (che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario) ed appunto il MiCAR. Per un'analisi complessiva del *Digital Finance Package*: C.M. Stiefmüller, *Analysis of the EU Digital Finance package – A New Finance Watch Report*, in www.finance-watch.org, 18.10.2021.

[3] Sul ricorrente accostamento tra le cripto-attività e le corse all'oro del vecchio *West*, v., tra gli altri, F. Consulich, *Nella* wunderkammer *del legislatore penale contemporaneo: monete virtuali che causano danni reali*, in *DPP* 2022, 153, che denunciava una vera e propria «latitanza della legge».

[4] Cfr., al riguardo, il § 2. Che questo settore rimanga una priorità è dimostrato dalla recente approvazione del nuovo *AML Package*, pubblicato sulla G.U. dell'Unione il 19.6.2024, e destinato a divenire completamente operativo il 10.7.2029 è composto dalla VI Direttiva antiriciclaggio (Direttiva 2024/1640/UE), dal Regolamento antiriciclaggio (il Regolamento 1624/2024/UE, c.d. *single rulebook*, relativo alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo) e dal Regolamento *AMLA* (Regolamento 1620/2024/UE), che istituisce l'Autorità per la lotta al riciclaggio e al finanziamento del terrorismo. Per una visione d'insieme, v. R. Razzante, *Antiriciclaggio: in arrivo Sesta direttiva e codice unico europeo*, in www.ipsoa.it, 1.2.2024; M. Da Rold, *Strategia antiriciclaggio e rischio penale per gli intermediari di criptomonete*, in *questa Rivista*, 14.6.2024, nonché, *amplius*, G. Soana, *The anti money laundering regulation of crypto-assets in Europe*, Milano 2024.

[5] Stando alle più recenti statistiche, nel novembre 2024 il mercato globale delle criptovalute ha raggiunto un valore superiore a tremila miliardi di dollari (*https://www.ilsole24ore.com/art/criptovalute-italia-64percento-un-anno-ecco-regole-consigli-e-rischi-AGdeSUTB?refresh_ce=1*).

[6] Art. 3, co 1, n. 2 del MiCAR, ove tale concetto viene definito come «un archivio di informazioni in cui sono registrate le operazioni e che è condiviso da una serie di nodi di rete DLT ed è sincronizzato tra di essi, mediante l'utilizzo di un meccanismo di consenso». Come giustamente insiste G. Soana, *op. cit.*, 62 s., la peculiarità principale che caratterizza le cripto-attività è quella di poter operare in modo potenzialmente *decentralizzato*, venendo cioè scambiate sulla rete senza la necessaria presenza di intermediari come le banche, a cui venga affidato il compito di controllare la validità delle transazioni (e, in particolare, la mancata "doppia spesa" delle somme). Ciò è reso possibile dal fatto che sono direttamente gli operatori della rete (in particolare i c.d. "minatori") a validare le stesse: essi, tramite l'applicazione di determinati algoritmi del consenso, verificano che i vari passaggi di valore siano coerenti con i precedenti blocchi della catena di transazioni, assicurando così affidabilità all'intero sistema. Ed è proprio da questa prospettiva che si coglie il senso del termine "*blockchain*", cioè l'infrastruttura tecnologica chiave del mondo in esame, che rappresenta, per l'appunto, una catena di

caratterizzate da un carattere tendenzialmente pseudo-anonimo[7], nonché dalla capacità di muovere, in un brevissimo arco di tempo, grandi somme da una parte all'altra del globo, evitando le reti di controllo degli intermediari finanziari tradizionali – le rende particolarmente appetibili per i *bad actors*[8], con un conseguente grave pericolo di moltiplicazione degli episodi di «criminalità finanziaria»[9] e non solo[10]. Del resto, onde dimostrare tale assunto, è sufficiente ricordare che, secondo le stime più accreditate, dal 2021 in poi la quantità di asset di questo tipo legate a traffici illeciti avrebbe sempre superato i 20 miliardi di dollari all'anno[11]. Quel che è peggio è che stime come queste vanno lette fortemente al ribasso: infatti, le stesse prendono in esame soltanto le transazioni che coinvolgono i "portafogli digitali"[12] di cui è già

blocchi di spese via via compiute. Per una completa disamina dell'apparato tecnologico sottostante le cripto-attività cfr. N. Furneaux, *Investigating Cryptocurrencies. Understanding, extracting, and analyzing blockchain evidence*, Chichester 2018, 1 ss.

[7] Sebbene le transazioni di molte cripto-valute, tra cui *in primis* il *bitcoin*, siano liberamente osservabili da chiunque in rete, esse sono, però, coperte da un velo di anonimato, giacché ogni transazione è identificata solamente da una stringa di numeri e lettere (c.d. *hash*), senza che compaia il nominativo del titolare dell'indirizzo di invio e di destinazione del denaro virtuale. Ciò non rende, tuttavia, tali transazioni totalmente anonime: infatti, come accenneremo in seguito, tramite diverse tecniche investigative (sia tradizionali, sia *ad hoc*), si può cercare di risalire alle generalità di coloro che svolgono le transazioni, de-anonimizzandole. Su tali aspetti, v. D. Carlisle, *The Crypto Launderers. Crime and Cryptocurrencies from the Dark Web to DeFi and Beyond*, Chichester 2024, 39 ss.

[8] A ben vedere, tali strumenti hanno esaudito quello che era da sempre un sogno dei gruppi criminali: essi consentono di effettuare pagamenti digitali, pressoché istantanei, in tutto il mondo, senza passare per gli intermediari finanziari ordinari. Senza contare che le criptovalute consentono di ovviare anche ad alcuni dei maggiori inconvenienti che caratterizzano il denaro contante: quali, per l'appunto, la sua fisicità e la possibilità di identificare, a certe condizioni, le singole banconote utilizzate.

[9] Cfr. Regolamento 1114/2023/UE, Considerando 5.

[10] Per una recente panoramica delle plurime fattispecie di reato che possono avere a oggetto cripto-attività, cfr., il Report di Europol, *Cryptocurrencies: tracing the evolution of Criminal finances*, in *www.europol.europa.eu*, dove si specifica che «*the criminal use of cryptocurrency is no longer primarily confined to cybercrime activities, but now relates to all types of crime that require the transmission of monetary value*». Nella dottrina italiana, v. M. Naddeo, *Criptovalute: profili di rilevanza penale*, in *PenaleDP* 2022; N. Mainieri, N. Di Gabriele, *Utilizzi a scopi illeciti delle criptovalute: recenti profili giurisprudenziali e normativi italiani ed internazionali e riferimento al mercato degli NFT*, in *Giur. pen. web* 6/2022, 1 ss.; M. Fazio, *Reati di riciclaggio e operazioni in criptovalute*, in *DPenCont-Riv. trim.* 2/2022, 160 ss.; R.M. Vadalà, *La disciplina penale degli usi ed abusi delle valute virtuali*, in *Riv. dir. internet* 2020, 397 ss.

[11] È quanto emerge dalle stime di *Chainalysis*, secondo cui nel solo 2023 gli *asset* legati a traffici illeciti avrebbero un valore (sempre stimato al ribasso) di ben 24.2 miliardi di dollari. Cfr. il Report di *Chainalysis*, *Crypto Crime Trends: Illicit Activity Down as Scamming and Stolen Funds Fall, But Ransomware and Darknet Markets See Growth*, in *www.chainalysis.com*, 18.1.2024.

[12] È opportuno ricordare che per "spendere" (scambiare) le cripto-attività è indispensabile avere un "portafoglio virtuale" (c.d. *wallet*), cioè uno strumento che contiene le chiavi che consentono a livello tecnico la transazione. Le transazioni si basano, più in particolare, su un sistema di "criptografia asimmetrica", il quale necessità di due diverse tipologie di "chiavi": c'è una "chiave pubblica", che serve per generare gli indirizzi dove ricevere le criptovalute e per crittografare i dati della transazione, e una "chiave privata", che ha la funzione di autorizzare

riconosciuta l'appartenenza ad attori criminali, di modo che vi è una grande "cifra oscura" di flussi criminosi, che non vengono neppure prese in considerazione dai più analitici report del settore.

In questo contesto, le finalità perseguite dal MiCAR sono chiare: introdurre una disciplina uniforme, volta, tanto a favorire lo sviluppo della finanza digitale, in modo conforme a una concorrenza leale, quanto a proteggere i detentori di *crypto-assets* e a garantire la stabilità del mercato. Si tratta di scopi perseguiti, innanzitutto, ponendo in capo degli operatori del settore una dettagliata serie di obblighi, il cui mancato rispetto deve essere prontamente sanzionato dalle Autorità competenti[13].

La stessa filosofia di fondo caratterizza le disposizioni contenute nel d.lgs. 129/2024[14], che si compone di 48 articoli suddivisi in 6 titoli, attraverso cui viene data attuazione alle parti del MiCAR non direttamente applicabili sul territorio nazionale.

In estrema sintesi:

i) il titolo I (artt. 1 e 2) individua l'oggetto e alcune definizioni, rinviando – per il resto – a quelle contenute nel TUF, nel TUB e nel Regolamento MiCA;

ii) il titolo II (artt. 3-10) individua la Consob e la Banca di Italia quali autorità nazionali titolari di poteri di vigilanza, di indagine e sanzionatori, deputate, tra l'altro, nell'ambito delle rispettive competenze[15], a emanare le disposizioni attuative del medesimo decreto e del Regolamento UE.

iii) il titolo III prevede una serie di disposizioni speciali applicabili nei confronti degli emittenti dei *token* collegati ad attività (Capo I, artt. 19-25)[16] e dei prestatori di servizi per le cripto attività (Capo II, artt. 26-29);

---

la spesa (possiamo paragonarla a un PIN bancario). Sul punto, cfr. la chiara spiegazione tecnica di G. Soana, *op. cit.*, 41 ss.

[13] M.T. Paracampo, *I prestatori di servizi per le cripto-attività. Tra mifidizzazione della MICA e tokenizzazione della Mifid*, Torino 2023, 143 ss. Nitido l'affresco di A. Galimberti, *Cripto, finisce l'era dell'anonimato e del nero (e forse anche quella dei crac)*, in www.ilsole24ore.com, 7.9.2024 secondo cui, con l'avvento del MiCAR, «il mondo delle criptovalute e dei *crypto-assets* entra definitivamente nell'età adulta, quella che dovrebbe evitare il ripetersi di cavalcate speculative, crac miliardari e miriadi di sprovveduti investitori scottati da evitabili, facili appetiti».

[14] Per ripercorrere le novità introdotte dal d.lgs. 129, si rimanda a: F. Sarzana di S. Ippolito, M. Nicotra, *Intelligenza artificiale, blockchain e criptovalute*, Milano 2024, 136 ss.; G. Lemme, *Criptovalute e riciclaggio: un rapporto troppo facile*, in *Dialoghi di diritto dell'economia* 2024, 1 ss.; U. Piattelli, S. Caruso e G. Rulli, *Cripto-attività e MiCAR: riflessioni sul decreto di adeguamento*, in www.dirittobancario.it, 17.9.2024.

[15] Per la ripartizione delle quali si veda la *Nota di sintesi Consob/Banca d'Italia. Riparto di competenze tra Consob e Banca d'Italia nell'applicazione di MiCAR*, in www.consob.it, 29.10.2024.

[16] Trattasi degli *asset-referenced token*, di seguito ART, che – a norma dell'art. 3 co. 1 n. 6 – vengono definiti come «un tipo di cripto-attività che non è un *token* di moneta elettronica e che mira a mantenere un valore stabile facendo riferimento a un altro valore o diritto o a una combinazione dei due, comprese una o più valute ufficiali».

iv) il titolo IV, su cui ci soffermeremo nel prosieguo, è invece quello dedicato alle sanzioni, di natura penale (art. 30) ed amministrativa (artt. 31-36) applicabili nei confronti degli operatori sul mercato delle cripto-attività (persone fisiche e persone giuridiche) che contravvengono agli obblighi autorizzativi, di trasparenza e di controllo prescritti dal Regolamento e dai decreti attuativi o che pongono in essere condotte manipolatorie del mercato;

v) da ultimo, il titolo V e il titolo VI prevedono, rispettivamente, alcune disposizioni di coordinamento (artt. 38-44), nonché transitorie e finali (artt. 45-48).

Tanto premesso, prima di procedere a una disamina delle novità più strettamente penalistiche introdotte dal d.lgs. 129/2024, è opportuno fornire un quadro del sistema in cui tali norme si collocano, così da meglio definire il loro orizzonte applicativo.

2. Il primo dato su cui va concentrata l'attenzione è che l'approvazione del Regolamento MiCA rappresenta, a livello europeo, solo un tassello di un percorso evolutivo ben più ampio che ha interessato il settore delle cripto-attività[17].

A tale riguardo, può in questa sede solo osservarsi come un ruolo propulsivo cruciale sia stato assunto dal Gruppo di Azione Finanziaria Internazionale (GAFI), cioè la principale organizzazione intergovernativa che si occupa di sviluppare *standard* globali in materia di integrità finanziaria, contrasto al riciclaggio, al finanziamento al terrorismo e alla proliferazione di armi di distruzione di massa. Come noto, siffatta autorità, sulla scia di indicazioni provenienti tanto da istituzioni statunitensi[18], quanto europee[19], ha elaborato un primo *report* sulle *virtual currencies* già nel 2014[20], seguito da una *guidance* nel 2015[21], con i quali veniva sostanzialmente auspicato un intervento normativo volto a dettare delle prime regole in tema di criptovalute, il cui mercato è esploso a livello globale a seguito del grande successo avuto dal *Bitcoin* nel primo quinquennio degli anni Dieci del Duemila[22].

---

[17] Per una dettagliata analisi diacronica di tale evoluzione, v. G. Soana, *op. cit.*, 69 ss.

[18] Cfr., al riguardo, D. Carlisle, *op. cit.*, 30 s., il quale ricostruisce il ruolo sul punto avuto dall'*US Treasury Department's Financial Crimes Enforcement Network* (c.d. *FinCEN*).

[19] Non va, del resto, dimenticato che già la Banca Centrale Europea (BCE) aveva avuto occasione di mettere in guardia gli Stati membri dai possibili rischi di distorsione del mercato connessi all'impiego di una moneta virtuale completamente decentralizzata e gestita da soggetti privati. Cfr., ad esempio, ECB, *Virtual Currency Schemes*, 2012; ECB, *Virtual Currency Schemes – A further analysis*, 2015.

[20] GAFI, *Report "Virtual Currencies Key Definitions and Potential AML/CFT Risks"*, 2014.

[21] GAFI, *Guidance for a Risk-Based Approach to Virtual Currencies*, 2015

[22] Il fenomeno in esame, pur essendosi sviluppato esponenzialmente a partire dal 2008 in poi, ha radici ben più risalenti, rintracciabili in un movimento di pensiero, denominato *Cypherpunk*, sviluppatosi negli Stati Uniti già negli anni Ottanta del Novecento, il quale aveva tra i suoi obiettivi primari quello di sfruttare la rivoluzione

Pur trattandosi di atti aventi natura non vincolante (*soft law*), i provvedimenti adottati dal GAFI hanno rappresentato, sin da allora, il "modello" seguito dal legislatore europeo nell'approntare una regolamentazione della materia. Onde rendersi conto di ciò, è sufficiente considerare come il primo atto volto a disciplinare compiutamente questo settore – ovverosia la Quinta Direttiva antiriciclaggio (Direttiva 2018/843/UE) [23] – rappresenti, in sostanza, una replica aggiornata dei contenuti e delle indicazioni provenienti dal predetto organismo internazionale[24]. Pur non essendo questa la sede per un'analisi dettagliata del provvedimento eurounitario da ultimo citato [25], preme qui rilevare come esso abbia inaugurato una prima, importante, fase di reazione sovranazionale nei confronti del fenomeno della criminalità avente ad oggetto le criptovalute[26]. Da questa prospettiva, la principale strategia impiegata è stata quella di rafforzare l'insieme dei presidi antiriciclaggio, adeguandoli, per quanto possibile, al mondo delle monete virtuali[27]. Nella disciplina in materia è stata, infatti, individuata la chiave di volta per intercettare i flussi di transazioni illecite che hanno a oggetto tali beni. Si considerino, ad esempio, le norme che hanno obbligato a rispettare i tradizionali vincoli antiriciclaggio gli *exchanges*, cioè, quegli operatori che svolgono il ruolo cruciale di cambiavalute tra denaro FIAT e valute elettroniche e/o viceversa. Così facendo, il legislatore ha perseguito l'idea per cui, attribuendo degli obblighi di controllo a tali organi, si sarebbe riusciti a

tecnologica in atto per favorire lo sviluppo di forme di: a) comunicazioni criptate; b) transazioni economiche anonime; c) piattaforme dove pubblicare atti governativi coperti da segreto. Tuttavia, la svolta si è avuta solo nel 2008 con la creazione del *Bitcoin* da parte di "Satoshi Nakamoto" (si tratta di uno pseudonimo). Il momento non è casuale: si tratta del periodo in cui era scoppiata la grande crisi finanziaria globale, dovuta al fallimento di grandi banche americane come la Lehman Brothers. La crisi del 2007-2008 è stata vista come la dimostrazione del fallimento della politica finanziaria globale, basata sugli intermediari bancari tradizionali. Essa ha favorito il lancio di un nuovo mezzo di pagamento digitale, per l'appunto il *Bitcoin*, il quale ha portato poi negli anni successivi a un successo globale l'intero mondo delle cripto-attività.

[23] Invero, un primo tentativo si ebbe già con Direttiva 2015/849/UE (cd. IV Direttiva antiriciclaggio), la quale, però, non assoggettava gli operatori del settore delle criptovalute agli obblighi previsti dalla normativa in tema di antiriciclaggio: cfr. G.P. Accini, Cybersecurity *e criptovalute. Profili di rilevanza penale dopo la Quinta Direttiva*, in *SP* 15.5.2020.

[24] Cfr. G. Soana, *op. cit.*, 124 ss.

[25] Si vedano G.P. Accini, *op.cit.*; R.M. Vadalà, *op. cit.*

[26] Così A. Di Giorgio, *NFT e antiriciclaggio, ecco le regole e il loro impatto sulle piattaforme di scambio dei* token, in *www.agendadigitale.eu*, 21.12.2022; A. Conso, L. Martinotti, *Antiriciclaggio e criptovalute: le anticipazioni alla V Direttiva AML*, in *www.dirittobancario.it*, 26.4.2018.

[27] Come sottolinea G. Soana, *Obblighi di prevenzione del riciclaggio e criptoattività. Interventi legislativi ed opportunità regolamentari*, in *ODCC* 2022, fascicolo speciale, 472, «le criptovalute [...] nel bypassare la necessità per gli utenti di avvalersi di intermediari negli scambi di valore digitale, intaccano la premessa fattuale su cui è basata la normativa antiriciclaggio - per scambiare valore online è necessario avvalersi di un intermediario – diminuendone fortemente la cogenza concreta».

intercettare i flussi criminali; e ciò dato l'ovvio interesse dei criminali nel convertire le criptovalute in denaro avente corso legale.

Va osservato, al riguardo, come le suddette indicazioni provenienti dal livello eurounitario siano state prontamente recepite sul versante nazionale. Ciò è avvenuto dapprima con il d.lgs. 90/2017 – che ha individuato tra i soggetti obbligati ai fini antiriciclaggio tutti i prestatori di servizi di conversione di valute virtuali in valute aventi corso forzoso – e, in seguito, con il d.lgs. 125/2019, di attuazione della Quinta Direttiva antiriciclaggio[28]. Quest'ultimo, in particolare, si è spinto – per una volta – ben oltre il contenuto degli atti sovranazionali: esso non si è limitato, infatti, a modificare nuovamente la definizione di valuta virtuale, ma ha anche lodevolmente esteso gli obblighi in esame, oltreché ai «prestatori di servizi di portafoglio digitale», pure ai «prestatori di servizio all'utilizzo di valute virtuali», intesi come tutti coloro che prestano «servizi di emissione, collocamento, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, negoziazione, intermediazione delle valute»[29].

Epperò, nonostante gli sforzi profusi a livello europeo e nazionale, deve darsi conto del fatto che siffatta prima serie di norme non era di certo sufficiente a contenere i rischi criminogeni degli strumenti in esame. Sfruttando la rapida evoluzione che caratterizza il settore delle cripto-attività, i *bad actors* hanno, invero, ben presto sviluppato varie strategie idonee ad aggirare i presidi di tutela approntati dal legislatore in materia di antiriciclaggio. Da un lato, si considerino, a mero titolo esemplificativo, l'implementazione di strumenti sempre più sofisticati volti ad offuscare le transazioni e farle apparire "lecite" (tanto sotto forma di *mixers*[30], quanto di creazione di criptovalute incentrate sulla *privacy*[31]), l'impiego di prestanome o, ancora, l'utilizzo di cambiavalute collocati in giurisdizioni non conformi con gli

[28] Un terzo *step* chiave si è avuto con il Decreto del Ministero dell'Economia e delle Finanze 13.1.2022, il quale, attuando quanto previsto dal d.lgs. 125/2019, aveva esteso l'obbligo di iscrizione, in una sezione speciale del registro dell'Organismo Agenti e Mediatori, anche ai prestatori di servizio all'utilizzo di valute virtuali, obbligandoli a trasmettere periodicamente informazioni sulle operazioni eseguite e attribuendo degli specifici poteri di controllo alla Guardia di Finanza.

[29] Art. 1, co. 1, lett. *f* del d.lgs. 4.10.2019 n. 125.

[30] Trattasi di strumenti che consentono agli utenti di oscurare la cronologia delle proprie transazioni, aggregando un certo numero di trasferimenti e quindi mischiando l'origine e la destinazione dei pagamenti effettuati: cfr. A. Jakubenko, e altri, *Anonymization Technologies of Cryptocurrency Transactions as Money Laundering Instrument*, in *KnE Social Sciences*, 2018, 48.

[31] Si pensi a *Dash* o al *Monero*.

obblighi *AML*[32]. Da un altro lato, si pensi al fatto che non solo i comuni cittadini[33], ma anche i principali prestatori di servizio del settore hanno finito per essere al centro di un numero sempre maggiore di gravi attacchi *hacker* da parte di organizzazioni criminose[34], interessate a impossessarsi, mediante mezzi fraudolenti, di enormi somme di denaro degli investitori. Si collocano, del resto, su questa scia, i fallimenti di grandi *exchanges* come "FTX"[35] o di *stablecoins* come "Terra Luna"[36], i quali hanno causato perdite su scala globale per miliardi di dollari, minacciando così a cascata la stabilità dell'intero mercato finanziario.

A fronte di tali problematiche, è stata inaugurata quella che è stata giustamente definita la "seconda era" nell'ambito della disciplina europea del fenomeno delle cripto-attività[37], volta a intercettare – almeno in parte – la profonda evoluzione che ha interessato il mercato delle cripto-attività a seguito della nascita di *Ethereum*[38] e delle altre migliaia di *altcoins*[39], peraltro alquanto eterogenee tra loro, che sono andate a sommarsi al *Bitcoin*. Pure in tale frangente, un ruolo di prim'ordine è stato assunto dal GAFI che, già tra il 2018 e il 2019[40], ha elaborato una serie di linee guida, dando avvio a una nuova macro-ondata regolativa imperniata, non solo sul contrasto al fenomeno del riciclaggio, ma, più in generale, sull'individuazione di obblighi di trasparenza e di informativa per l'emissione e l'offerta al pubblico di cripto-attività, nonché una migliore vigilanza sui *service provider* e, ancora, una più adeguata protezione del mercato e degli investitori.

Ed è così che si è giunti all'approvazione del Regolamento MiCA, al quale si affianca, come accennato, un più articolato pacchetto di misure approvate dalle istituzioni

[32] Per un'ampia panoramica di tali strategie elusive, cfr. il report della società Elliptic, *Preventing Financial Crime in Cryptoassets*, Edition 2024, in *www.elliptic.com*.
[33] Per i privati, una delle minacce principali è costituita dai c.d. attacchi *ransomware*, cioè forme di estorsioni virtuali tramite virus informatici, in cui il riscatto viene chiesto, molte volte, proprio in criptovalute. V., al riguardo, D. Carlisle, *op. cit.*, 97 ss.
[34] Merita di essere ricordato, al riguardo, il celeberrimo attacco *hacker* compiuto nei confronti di Mt. Gox nel 2011, all'epoca il più grande *exchange* di Bitcoin, che ne ha favorito il fallimento pochi anni dopo.
[35] *https://www.milanofinanza.it/news/crack-ftx-la-lettera-dei-debitori-spiega-il-perche-del-fallimento-quando-si-perdeva-traccia-del-denaro-202304101315271156*.
[36] *https://youngplatform.com/blog/news/riassunto-disastro-terra-luna/*.
[37] Cfr. G. Soana, *op. cit.*, 134 ss.
[38] Ethereum è una *blockchain* lanciata nel 2014 da Vitalilk Buterin: C. Dannen, *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*, New York, 2017.
[39] Con tale espressione si allude generalmente a tutte le criptovalute alternative al *Bitcoin*.
[40] GAFI, *Report to the G20 Finance Ministers and Central Bank Governors*, 2018; GAFI, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, 2019.

europee tra il 2023 e il 2024[41], al fine di offrire un quadro armonizzato più completo per i mercati delle «cripto-attività» nell'Unione europea «non ancora coperti da atti legislativi dell'Unione in materia di servizi finanziari»[42]. Per quanto qui rileva, va segnalato che il principale tassello della disciplina UE in materia, che fa il paio con il MiCAR, è rappresentato dal Regolamento 1113/2023/UE, riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività (c.d. *Transfer of Funds Regulation recast – TFR*), il quale ha esteso ai prestatori di servizi di cripto-attività tutti gli obblighi antiriciclaggio che ricadono sugli intermediari finanziari[43], e ha modificato le definizioni di cripto-attività e dei prestatori di servizi per le cripto-attività presenti nella Direttiva 2015/849/UE (la IV Direttiva antiriciclaggio), uniformandole a quelle fornite dal MiCAR[44].

[41] Ci si riferisce al: *i*) Regolamento 1113/2023/UE; *ii*) Regolamento 1624/2024/UE; *iii*) Direttiva 2024/1260/UE.

[42] Considerando n. 5.

[43] Non è questa la sede per esaminare le fattispecie delittuose applicabili nei confronti dei prestatoti di servizi per le cripto-attività. Si rimanda, nell'ormai ampia bibliografia, a: G.J. Sicignano, *Bitcoin e riciclaggio*, Torino 2019; Id., *231 e criptovalute. La responsabilità da reato dell'ente nel riciclaggio mediante monete virtuali*, Milano 2021; A. Rosato, *Profili penali delle criptovalute*, in *Quaderni di CRST (Centro Ricerca Sicurezza e Terrorismo)* 2021; M. Naddeo, *op. cit.*; Id., *Nuove frontiere del risparmio. Bit Coin Exchange e rischio penale*, in *DPP* 2019, 99 ss.; G.P. Accinni, *op. cit*., 209 ss.; R.M. Vadalà, *Criptovalute e cyberlaundering: novità antiriciclaggio nell'attesa del recepimento della Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale*, in *SP* 6.5.2020; S. Vitale, *Riciclaggio e prevedibilità della risposta penale: interpretazioni giurisprudenziali dubbie e soluzioni* de iure condendo, in *RivTrim-DPenEc.* 2021, 639 ss.; G. Diotallevi, *Riciclaggio, autoriciclaggio (...ed altro ancora) nel tempo della moneta virtuale e della cybersicurezza*, in *QG* 9.10.2024, 1 ss.; L. Picotti, *Profili penali del Cyberlaundering: le nuove tecniche di riciclaggio*, in *RivTrim-DPenEc.* 2018, 1121 ss.

[44] Per quanto concerne l'adeguamento del diritto interno a tali prescrizioni, è attualmente al vaglio delle Camere lo schema di decreto legislativo approvato in via preliminare dal Consiglio dei ministri il 29.10.2024 (Atto del governo n. 227. Schema di decreto legislativo recante adeguamento della normativa nazionale alle disposizioni del Regolamento 1113/2023/UE, 11.7.2024, reperibile in *www.camera.it*, che interviene, tra l'altro, sul d.lgs. 21.11.2007 n. 231 (c.d. decreto antiriciclaggio), assoggettando i prestatori di servizi per le cripto-attività al regime di controllo e sanzionatorio degli intermediari bancari e finanziari, nell'ottica di un complessivo rafforzamento degli strumenti di contrasto al riciclaggio con riguardo ai *crypto-assets*. L'idea di fondo è quella di avvalersi dei soggetti che operano professionalmente sulle piattaforme di cripto-attività – su tutti, *exchange* e *wallet* provider –, imponendo loro più articolati obblighi di identificazione della clientela, così da ridurre l'opacità del sistema e, con essa, la potenzialità offensiva connaturata all'utilizzo di criptovalute. Un'opzione del genere è per molti versi obbligata: l'impiego della tecnologia a registro distribuito (DLT) rende obiettivamente imprescindibile la collaborazione dei prestatori di servizi di cripto-attività, che non di rado costituiscono il principale punto di contatto attraverso cui le persone accedono al mondo virtuale, divenendo – pertanto – logicamente i primi interlocutori degli organi statuali ed europei deputati alla lotta «al riciclaggio di denaro sporco» e al contrasto di altre attività illecite. A quanto emerge da una cursoria lettura dello Schema di decreto, non è previsto l'inserimento di nuove figure delittuose: i «prestatori di servizi per le cripto-attività» – categoria in cui, a seguito delle modifiche, rientreranno sia i prestatori di servizi relativi all'utilizzo di valuta virtuale, sia i prestatori di servizi di portafoglio digitale, potranno eventualmente essere chiamati a rispondere ai sensi dell'art. 55 del d.lgs. 231/2007.

Vale la pena di precisare che il cambio di prospettiva adottato dalle istituzioni europee dopo l'approvazione del MiCAR emerge proprio da un'analisi di tipo linguistico-lessicale[45]. Onde descrivere il fenomeno che qui ci occupa, il GAFI, nel primo *report* del 2014, aveva impiegato l'espressione «*virtual currencies*»[46], all'evidenza parametrata sulla tipologia di mercato di criptovalute allora esistente, costituito principalmente dal *Bitcoin*[47]. Ben presto, però, ci si è resi conto che la presenza di ulteriori strumenti aveva reso tale locuzione inadeguata, incapace di ricomprendere tutte quelle nuove operazioni realizzabili sfruttando la tecnologia *blockchain*. Si è passati, così, all'impiego di locuzioni più generali, come quella di «*virtual asset*»[48], fino a coniare, con l'approvazione del Regolamento MiCA, un'espressione omnicomprensiva, quale, per l'appunto, quella di «*crypto-asset*», ovverosia «la 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»[49].

---

[45] Insiste giustamente sul punto G. Soana, *op. cit*., 134 ss.

[46] Definita come «*a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction*» (GAFI, *Report "Virtual Currencies. Key definitions and potential AML/CFT risks"*, cit.). Al riguardo, si precisa altresì che «*virtual currency is distinguished from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status*».

[47] Pure il legislatore italiano ha seguito tale impostazione: v. art. 2, co. 1, lett. *qq* del d.lgs. 21.11.2007 n. 231; art. 1, co. 2, lett. *qq* del d.lgs. 25.5.2017 n. 90, ove si fa riferimento alla «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»; art. 1, lett. *d* del d.lgs. 8.11.2021 n. 184, stabilisce che «agli effetti della legge penale», il concetto di «valuta virtuale» sia inteso come «una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è legata necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettata da persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferita, memorizzata e scambiata elettronicamente».

[48] Ovverosia, una «*digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations*» (GAFI, *Glossary: Virtual Asset*, all'indirizzo https://www.fatf-gafi.org/glossary/u-z/). In termini non dissimili si esprime pure la Direttiva 2018/843/UE, ove la «*virtual currency*» è definita come «*a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored, and traded electronically*».

[49] Art. 3 co.1 n. 5. Cfr. D. Masi, *Le criptoattività: proposte di qualificazione giuridica e primi approcci regolatori*, in

Ciò detto, occorre sottolineare come la nuova regolamentazione approntata a livello europeo abbia importanti riflessi pure sul versante penalistico e amministrativo-punitivo. L'esperienza maturata a seguito dei plurimi *crack* finanziari di grossi operatori del settore delle cripto-attività degli ultimi anni, a cui si è fatto cenno, ha, invero, dimostrato che la mancanza di norme chiare e puntuali in materia risultava pericolosa anche per i rischi che ciò determinava a livello «di abuso di mercato e di criminalità finanziaria»[50]. Di talché, era evidentemente necessario correre ai ripari, non solo cercando di gettare le basi per una migliore regolazione generale del mercato delle cripto-attività, ma anche mediante la strutturazione di un adeguato apparato repressivo, volto a presidiarne l'effettivo rispetto nella prassi delle sue linee portanti.

Come avremo modo di vedere meglio in seguito, quanto ai mezzi di realizzazione di un tale apparato, l'art. 111 del Regolamento MiCA, a differenza di quanto è avvenuto in altri settori[51] – ha, tuttavia, scelto di lasciare ai singoli ordinamenti ampi margine di manovra, essendo loro demandata la valutazione in merito all'opportunità di fare ricorso o meno allo strumento del diritto penale sostanziale. Il legislatore europeo si è, più in particolare, limitato a prescrivere ai singoli Stati membri l'adozione di «sanzioni amministrative e altre misure amministrative adeguate» a reprimere una serie di violazioni, individuate mediante un puntuale rinvio a specifiche disposizioni regolamentari, fissando l'ammontare minimo delle stesse. Allo stesso tempo, però, la normativa europea ha espressamente fatto salva la possibilità, da parte dei singoli Paesi, di impiegare lo strumento penalistico, allorquando lo stesso fosse considerato necessario. Ebbene, come meglio vedremo nel prosieguo della trattazione, facendo propria tale linea operativa di fondo, ispirata da una condivisibile logica di *extrema ratio* dello *ius terribile*, il nostro ordinamento, con il d.lgs. 5.9.2024 n. 129, si è limitato a introdurre una singola fattispecie delittuosa che reprime talune ipotesi di mancato rispetto della disciplina autorizzativa prescritta dal MiCAR, privilegiando, per il resto, almeno sulla carta, la strada dell'illecito amministrativo.

3. Così brevemente inquadrato il contesto nel quale si inserisce il MiCAR e il relativo decreto legislativo di adeguamento, occorre ora richiamare alcune definizioni

Banca Impresa Società 2021, 241 ss.; P. Carriere, *Il fenomeno delle cripto-attività* (crypto-assets) *in una prospettiva societaria*, in *Banca Impresa Società* 2020, 461 ss.

[50] Considerando n. 4 del MiCAR.

[51] Si pensi alla disciplina sul mercato mobiliare, ove il legislatore euro-unitario ha notoriamente imposto pregnanti obblighi di tutela penale (specie in relazione alla punibilità degli abusi di mercato).

contenute in detti provvedimenti, necessarie onde poter apprezzare compiutamente i risvolti sul versante penalistico.

Al riguardo, si è già detto come il Regolamento assuma a proprio cardine la nozione di «cripto-attività». All'interno di questa macrocategoria, invero, è possibile distinguere quelle cripto-attività qualificabili come strumenti finanziari (così definiti nella Direttiva 2014/65/UE), rispetto alle quali l'Unione europea ha già approntato una disciplina *ad hoc* (*Markets in Financial Instruments Directive*)[52], e quelle che non lo sono. È solamente con riguardo a queste ultime che il MiCAR è destinato a trovare applicazione[53].

Più in dettaglio, la normativa in esame individua tre differenti tipologie di cripto-attività, le quali sono soggette a discipline autorizzative diversificate, in ragione dei differenti rischi che esse comportano[54]. Il principale fattore di rischio valorizzato a livello europeo si basa, in particolare, sul fatto che il singolo *asset* di riferimento stabilizzi o meno il proprio valore con riguardo ad altri valori pre-individuati[55]. Il che non può stupire tenuto conto dei gravi rischi per la finanza globale, messi in rilievo a più voci negli ultimi anni, determinati dalle cosiddette *stablecoins*[56].

Nella prima classe sono annoverati i cd. «*token* di moneta elettronica» (*e-money token* – EMT), i quali mirano a «mantenere un valore stabile facendo riferimento al valore di una valuta ufficiale [come l'euro o il dollaro]»[57]. Al pari di qualunque altra "moneta elettronica"[58], essi sono equiparabili a dei surrogati elettronici di valute e banconote "analogiche" e, dunque, possono essere impiegati, ad esempio, per effettuare pagamenti[59].

Il secondo tipo di cripto-attività viene identificato nei cd. «*token* collegati ad attività» (*asset-referenced token* – ART), che mirano a «mantenere un valore stabile facendo riferimento a un altro valore o diritto o a una combinazione dei due, comprese

[52] Considerando n. 3.
[53] Considerando n. 4. Cfr. M. Cian, *La nozione di criptoattività nella prospettiva del MiCAR. Dallo strumento finanziario al* token*, e ritorno*, in *Osservatorio del diritto civile e commerciale* 2022, 60.
[54] Considerando n. 18.
[55] E. Franza, *La Regolamentazione dei* Cripto-Asset. *MiCA un primo passo*, in www.dirittobancario.it, 13.9.2024.
[56] K. Duan, A. Urquhart, *The instability of stablecoins*, in *Finance Research Letters*, 2023, 52, 1 ss.
[57] Art. 3 co. 1 n. 7.
[58] Definita dall'art. 2 co. 1 n. 2 della Direttiva 2009/110/CE come «il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso dietro ricevimento di fondi per effettuare operazioni di pagamento ai sensi dell'articolo 4, punto 5), della Direttiva 2007/64/CE e che sia accettato da persone fisiche o giuridiche diverse dall'emittente di moneta elettronica».
[59] M. Cian, *op. cit.*, 66.

una o più valute ufficiali»[60]. Anch'essi, invero, possono assolvere le funzioni di mezzo di pagamento per l'acquisto di beni e servizi, atteso il loro ancoraggio a un paniere di valute e/o di attività[61].

Infine, in una terza categoria, avente carattere residuale, vengono ricondotte tutte quelle cripto-attività – cd. *other than* – diverse da EMT e ART, quali, ad esempio, gli «*utility token*», strumenti destinati «unicamente a fornire l'accesso a un bene o a un servizio prestato dal suo emittente»[62].

Il secondo concetto di base della disciplina è quello di «prestatore di servizi per le cripto-attività»[63] (*Crypto-Assets Service Providers* – CASP).

Il Regolamento circoscrive tale locuzione a «una persona giuridica o altra impresa la cui occupazione o attività consiste nella prestazione di uno o più servizi per le cripto-attività ai clienti su base professionale e che è autorizzata a prestare servizi per le cripto-attività conformemente all'art. 59» del MiCAR. In linea generale, può trattarsi tanto di un soggetto che opera tradizionalmente nel settore delle cripto – quale un *wallet service provider* o un cambiavalute –, quanto di una diversa impresa che presta un servizio di investimento avente ad oggetto cripto-attività[64]. A ben vedere, siamo al cospetto di un *genus* molto ampio, all'interno del quale è possibile distinguere diverse *species*. I primi commentatori[65] hanno individuato, difatti, tre diverse categorie, a seconda del regime di accesso al mercato: *i*) «prestatori su richiesta», i quali sono sottoposti a una procedura autorizzativa "ordinaria" per operare nel settore, prevista agli artt. 59 ss. del MiCAR; *ii*) «prestatori di diritto europeo», richiamati all'art. 60 del MiCAR, che, potendo già usufruire di una sorta di «passaporto europeo»[66] conseguito ai sensi di un'altra normativa in materia finanziaria, sono esenti dall'ordinaria procedura di autorizzazione; *iii*) «prestatori di diritto nazionale», cioè soggetti che, ai sensi dell'art. 143 del Regolamento, godono di un regime di esenzione temporanea ed eventualmente di una procedura di autorizzazione semplificata.

Così fornite alcune definizioni di base, deve da subito darsi conto di una delle principali ombre della disciplina di nuovo conio, costituita dalla difficoltà

[60] Art. 3 co. 1 n. 6.
[61] F. Ciraolo, *La disciplina degli* e-money tokens *tra proposta di Regolamento MiCA e normativa sui servizi di pagamento. Problematiche regolatorie e possibili soluzioni*, in *Riv. reg. merc*. 2022, 251 s.
[62] Art. 3 co. 1 n. 9.
[63] Art. 3 co. 1 n. 15.
[64] S.L. Furnari, *La finanza decentralizzata: cripto-attività, protocolli, questioni giuridiche aperte*, Roma 2023, 94.
[65] M.T. Paracampo, *op. cit.*, 19 ss.
[66] M.T. Paracampo, *op. cit.*, 19.

nell'individuare con precisione l'ambito applicativo del MiCAR e del relativo decreto legislativo di adeguamento.

Al riguardo, va anzitutto osservato come il legislatore europeo abbia adottato un approccio «in negativo»[67], orientato, cioè, a un criterio di residualità e imperniato sul principio di neutralità tecnologica. In breve: devono ritenersi disciplinate dal MiCAR solamente quelle cripto-attività non rientranti nella vigente legislazione dell'UE in materia di mercati e servizi finanziari, indipendentemente dalla tecnologia utilizzata per la loro emissione o il loro trasferimento. Un tanto emerge, in maniera inequivoca, dalla lettura del considerando n. 9, ove vengono esplicitamente escluse dalla sfera di operatività del Regolamento tutte quelle cripto-attività «qualificabili come strumenti finanziari quali definiti dalla Direttiva 2014/65/UE, quelle qualificabili come depositi quali definiti dalla Direttiva 2014/49/UE del Parlamento europeo e del Consiglio, compresi i depositi strutturati quali definiti dalla Direttiva 2014/65/UE, quelle qualificabili come fondi quali definiti dalla direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, eccetto ove siano qualificabili come *token* di moneta elettronica». Lo stesso art. 2, rubricato «ambito di applicazione», si premura di individuare una serie di ipotesi in cui il Regolamento non è destinato ad operare, tra le quali vengono menzionate proprio le cripto-attività che rientrano nella nozione di "strumento finanziario".

L'adozione di una siffatta strategia ha, però, sollevato prevedibili voci critiche in letteratura[68] (e non solo[69]), attesa la difficoltà, in concreto, nello stabilire se la singola fattispecie di volta in volta considerata debba essere qualificata prevalentemente come strumento finanziario, ovvero come cripto-attività[70]. Tutto ciò assume un significativo

[67] M.T. Paracampo, *op. cit.*, 6.

[68] Si vedano, al riguardo, le censure mosse da F. Annunziata, *Verso una disciplina europea delle cripto-attività. Riflessioni a margine della recente proposta della Commissione UE*, in *www.dirittobancario.it*, 15.10.2020; F. Mattassoglio, *Le proposte europee in tema di* crypto-assets *e* DLT. *Prime prove di regolazione del mondo* crypto *o tentativo di* tokenizzazione *del mercato finanziario (ignorando bitcoin)?*, in *Riv. dir. banc.* 2021, 413; M. T. Paracampo, *La consulenza su cripto-attività nella proposta di regolamento europeo MICA tra presunte equivalenze e distonie normative con Mifid 2*, in *Dir. banca e merc. fin.* 2022, 229. Nella letteratura straniera, v. P. Maume, *The Regulation on Markets in Crypto-Assets (MiCAR): Landmark Codification, or First Step of Many, or Both?*, in *ECFR* 2023, 255 s.

[69] BCE, *Parere del 19 febbraio 2021 su una proposta di regolamento del Parlamento europeo e del Consiglio relativo ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937*, 19.2.2021; CESE, *Parere su: «Proposta di regolamento del Parlamento europeo e del Consiglio relativo ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937»*, 24.2.2021.

[70] Come vedremo meglio *sub* par. 4.1, di tale difficoltà era pienamente consapevole lo stesso legislatore europeo, il quale, «al fine di garantire una chiara distinzione tra, da un lato, le cripto-attività disciplinate dal presente regolamento e, dall'altro, gli strumenti finanziari», affida all'ESMA l'onere di emanare orientamenti sui criteri e

rilievo pratico se solo si pensi al quesito circa la necessità di applicare il Regolamento MiCA alle criptovalute in senso proprio, quali *Bitcoin* e simili[71]. L'incertezza, in termini di qualificazione giuridica, che da sempre aleggia attorno a queste figure, infatti, rende assai sfumata la tradizionale distinzione tra strumento finanziario e strumento di pagamento[72], con tutto ciò che ne consegue sul versante regolatorio.

A ogni modo, vari argomenti sembrano tendenzialmente escludere la riconducibilità dei *bitcoin* rispetto alle procedure autorizzative regolate dal MiCAR[73]. In effetti, le criptomonete, pur rientrando nell'ampia definizione di cripto-attività e potendo astrattamente assolvere a funzioni di pagamento o di investimento (*payment tokens*)[74], non paiono incasellabili in alcuno dei tre gruppi appena richiamati (EMT, ART e *other than*). Esse, per un verso, non sono ancorate ad alcun bene o moneta ufficiale di riferimento (*unbacked crypto-asset*), di talché non possono essere ricondotte nella categoria degli *stablecoins*[75], e, per altro verso, non possono essere assimilate neppure agli *utility tokens*, non assolvendo a una funzione di utilità o di godimento.

Ma vi è di più. Dal punto di vista letterale, l'art. 4, co. 3, lett. *b* del Regolamento ricomprende, tra le esenzioni dalla pubblicazione del *white paper* contenente tutta una serie di informazioni chiave dell'emittente di un *asset* virtuale[76], il caso della «cripto-

sulle condizioni per la qualificazione delle cripto-attività come strumenti finanziari.

[71] Ai sensi del considerando n. 10 e dell'art. 2, co. 3 del MiCAR devono, invece, ritenersi esclusi dal suo ambito di applicazione i "Token Non Fungibili" (c.d. *NFT*), ai quali, al limite, potrà essere applicata la disciplina in materia di strumenti finanziari, sempre che rientrino in tale categoria. Cfr. P. Carrière, *Il Regolamento MICA e il* rebus *NFT*, in www.dirittobancario.it, 20.4.2022.

[72] Cfr., sul tema, M. Semeraro, *Moneta legale, moneta virtuale e rilevanza dei conflitti*, in *Riv. di diritto bancario* 2019, 237 ss.; G. Greco, *Valute virtuali e valute complementari, tra sviluppo tecnologico e in-certezze regolamentari*, in *Riv. di diritto bancario* 2019, 61 ss.; P. Carrière, *Le "criptovalute" sotto la luce delle nostrane categorie giuridiche di "strumenti finanziari", "valori mobiliari" e "prodotti finanziari"; tra tradizione e innovazione*, *Riv. di diritto bancario* 2019, 117 ss.

[73] In questo senso pare orientata la dottrina maggioritaria, v. F. Ciraolo, *op. cit.*, 252; R. Lener, L. Furnari, *Cripto-attività: prime riflessioni sulla proposta della commissione europea. Nasce una nuova disciplina dei servizi finanziari crittografati?*, in www.dirittobancario.it, 9.10.2020; M. Mari, *Le cripto-attività nella disciplina MiCAr e la finanziarietà delle "cripto-attività non finanziarie"*, in www.dirittobancario.it, 13.12.2023; F. Mattassoglio, *Le proposte europee in tema di* crypto-assets *e* DLT, cit., 417, 420 s., 453 ss.; M. Nicotra, *L'ingresso dei prestatori di servizi: autorizzazione, requisiti e distinzioni*, in *Il Micar. Guida al regolamento europeo sui mercati delle cripto*, cit., 93; F. Sarzana di S. Ippolito, Token *collegati ad attività ed* e-money token: *il futuro delle* stable-coin, in *Il Micar. Guida al regolamento europeo sui mercati delle cripto*, cit., 60.

[74] F. Ciraolo, *op. cit.*, 252.

[75] F. Mattassoglio, *Le proposte europee in tema di* crypto-assets *e* DLT, cit., 417, nota n. 13.

[76] Considerando n. 24: «un *White Paper* sulle cripto-attività dovrebbe contenere informazioni di carattere generale sull'emittente, sull'offerente o sulla persona che chiede l'ammissione alla negoziazione, sul progetto da realizzare con i capitali raccolti, sull'offerta al pubblico di cripto-attività o sulla loro ammissione alla

attività [...] creata automaticamente a titolo di ricompensa per il mantenimento del registro distribuito o la convalida delle operazioni»[77]. Parimenti, il considerando n. 22 stabilisce che «qualora le cripto-attività non abbiano un emittente identificabile», come avviene nel caso dei *bitcoin*, «esse non dovrebbero rientrare nell'ambito di applicazione dei titoli II, III o IV del [...] regolamento».

Alla luce di ciò, le uniche disposizioni del MiCAR rispetto alle quali sembrerebbe residuare uno spazio di applicabilità per i *bitcoin* e simili parrebbero quelle in materia di prestatori di servizi per le cripto-attività, qualora essi abbiano ad oggetto tali criptovalute[78].

4. Come si è avuto modo di anticipare, l'apparato sanzionatorio delineato dal d.lgs. 129/2024, sulla scia della fonte europea di riferimento, viene indubbiamente a colmare un vuoto di tutela. La sottoposizione degli operatori del settore a un rigoroso regime autorizzativo e di controllo, che impone loro il rispetto di plurimi requisiti organizzativi, professionali e di onorabilità – primo fra tutti la mancata condanna per reati nell'ambito del riciclaggio o del finanziamento del terrorismo – mira a salvaguardare il funzionamento del mercato, la libera e leale concorrenza ed il patrimonio degli investitori in *crypto-assets*. Mediante la previsione degli illeciti penali e amministrativi che analizzeremo nel prosieguo, il legislatore ha cercato, insomma, di reprimere sul nascere eventuali patologie del sistema, arginando i rischi di perpetrazione di frodi, manipolazioni, abusi ed altre attività illecite, che hanno minato e minano tutt'oggi la stabilità e la crescita del mercato delle cripto-attività.

Entrando più nel dettaglio nella parte della disciplina che rileva in questa sede, l'unica disposizione del d.lgs. 129/2024 avente immediata ricaduta in materia penalistica in senso stretto è l'art. 30, che introduce il reato di abusivismo legato a operazione di cripto-attività. Come emerge dalla lettura dell'art. 19 co. 2 lett. *g* n. 7 della legge di delegazione europea 2022-2023 (l. 21.2.2024 n. 15), la sua tipizzazione risponde alla necessità di prevedere «sanzioni penali efficaci, proporzionate e dissuasive nei confronti di chiunque emetta, offra al pubblico o chieda l'ammissione

negoziazione, sui diritti e sugli obblighi connessi alle cripto-attività, sulla tecnologia sottostante utilizzata per tali cripto-attività e sui relativi rischi».

[77] Con la definizione si fa, evidentemente, riferimento alla procedura di "*mining*" (ovvero di estrazione) delle nuove criptovalute, denominata *proof of work*, su cui ancora oggi si basa il *bitcoin*.

[78] Così si ricava dal considerando n. 22. Si veda, sul punto, F. Ciraolo, *op.cit.*, 252, nota n. 20, ove l'A. esemplifica richiamando il caso di una piattaforma di *exchange* che operi anche su *bitcoin*, consentendo la custodia e lo scambio di tale criptovaluta.

alla negoziazione di cripto-attività disciplinate dal Regolamento (UE) 2023/1114 in mancanza dei requisiti e delle autorizzazioni ivi previsti nonché di chiunque svolga servizi disciplinati dal medesimo Regolamento (UE) in mancanza delle autorizzazioni ivi previste».

Siamo, evidentemente, al cospetto di una "disposizione a più fattispecie", in cui si criminalizzano quattro diverse tipologie di esercizio abusivo di attività connesse al mercato dei *crypto-assets*, tutte punite con la reclusione da sei mesi a quattro anni e con la multa da 2066 a 10.329 euro. Si noti, peraltro, che la forbice edittale è analoga a quella prevista per i delitti di abusivismo bancario di cui agli artt. 131 ss. del TUB e leggermente meno severa rispetto a quella dell'abusivismo finanziario di cui all'art. 166 del TUF (il d.lgs. 24.2.1998 n. 58), ove la pena irrogabile va da uno a sei anni di reclusione.

Procediamo con ordine:

i) il delitto di cui alla lett. *a* dell'art. 1 reprime l'offerta al pubblico e la richiesta e l'ottenimento dell'ammissione alla negoziazione di *token* collegati ad attività da parte di un emittente che non abbia ricevuto l'autorizzazione di cui all'art. 16 co. 1 lett. *a* del MiCAR. A norma dell'art. 11 del d.lgs. 129, il procedimento di concessione e revoca di una autorizzazione siffatta è di competenza della Banca d'Italia, d'intesa con la Consob, cui spetta l'onere di verificare la sussistenza dei requisiti e delle condizioni indicate dall'art. 21 del MiCAR;

ii) alla lett. *b* viene invece punito il prestatore di servizi per le cripto-attività che operi sul mercato in mancanza dell'autorizzazione di cui all'art. 59 del Regolamento MiCA, che viene concessa dalla Consob, d'intesa con la Banca d'Italia, all'esito della complessa procedura di cui all'art. 63 del MiCAR;

iii) la fattispecie di cui alla lett. *c* sanziona, ancora, chiunque emetta *token* di moneta elettronica in violazione delle prescrizioni dell'art. 48 del MiCAR, che richiedono all'emittente il possesso dell'autorizzazione quale ente creditizio o istituto di moneta elettronica;

iv) da ultimo, alla lett. *d* è punito chi offre al pubblico o chiede e ottiene l'ammissione alla negoziazione di *token* di moneta elettronica in assenza del consenso scritto dell'emittente.

Segnaliamo incidentalmente che, nell'originario Schema di decreto legislativo predisposto dal Dipartimento del Tesoro per la consultazione pubblica[79], la fattispecie

[79] Dipartimento del Tesoro, *Schema di decreto legislativo per l'adeguamento della normativa nazionale alle*

in commento si componeva anche di un secondo comma che disponeva l'applicabilità del reato di abusiva emissione di moneta elettronica *ex* art. 131 *bis* TUB nei confronti di chi emetta indebitamente moneta elettronica ovvero di chi la offra al pubblico in assenza di previo assenso dell'emittente. Nella versione definitiva del decreto, il capoverso è tuttavia stato eliminato e sostituito dalle previsioni *sub* iii e *sub* iv. Il correttivo non ha alcun impatto a livello penalistico[80], posta l'identità dei soggetti incriminabili e della cornice edittale.

Un dato è, peraltro, certo: la decisione di introdurre una figura delittuosa *ad hoc* è perfettamente in linea con la strategia adottata dal legislatore di costruire un *corpus* normativo unitario, che regolamenti il mercato delle cripto-attività non finanziarie.

Detto ciò, non sfuggirà come, a livello strutturale, la fattispecie di cui all'art. 30 in commento presenta evidenti tratti di affinità con gli altri delitti di abusivismo previsti dal TUB e dal TUF.

Essa designa un reato di pericolo presunto[81] di carattere pluri-offensivo, che si pone quale presidio di tutela anticipata del buon funzionamento e dell'integrità del mercato, ma salvaguarda altresì l'interesse individuale dei privati a trattare soltanto con soggetti affidabili, in modo da favorire un «ordinato e sereno svolgimento» delle proprie operazioni nel settore delle cripto-attività[82]. Questi interessi, a ben vedere, restano «sullo sfondo dell'incriminazione», quasi fossero «astratti obiettivi di tutela», che non

---

disposizioni del regolamento (UE) 2023/1114, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937 – Allegato I, in www.dt.mef.gov.it.

[80] Non a caso nel *dossier* relativo all'Atto del Governo n. 172. *Adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2023/1114, relativo ai mercati delle cripto-attività*, 11.7.2024, consultabile sul portale www.documenti.camera.it, viene ribadito che «la determinazione della cornice edittale prevista in caso di abusiva prestazione delle attività» di emissione e di offerta al pubblico di *token* di moneta elettronica «è la medesima prevista dagli articoli 131 e 131-bis del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo n. 385 del 1993, che puniscono, rispettivamente, le condotte di abusiva attività bancaria e di abusiva emissione di moneta elettronica». In argomento, M. Misiti, *"Monete virtuali" e valute virtuali: distinzioni linguistiche e ricadute penalistiche sulla fattispecie di abusiva emissione di moneta elettronica*, in *PenaleDP* 29.11.2024.

[81] Nello stesso senso, ma in relazione all'abusivismo finanziario, la granitica giurisprudenza. A titolo esemplificativo, si vedano: Cass. 9.12.2024 n. 45014, in www.onelegale.wolterskluwert.it; Cass. 22.10.2020 n. 37528, in *CEDCass.*, m. 280109; Cass. 16.1.2015 n. 25160, m. 265299. In senso analogo, la prevalente dottrina: v. per tutti: S. Seminara, *Diritto penale commerciale. Vol. II, Il diritto penale del mercato mobiliare,* Torino 2018, 23; S. Preziosi, *Modelli di sviluppo economico e diritto penale*, in *RTrim-DPenEc.* 2020, 671 ss.

[82] Cfr. in riferimento al delitto di cui all'art. 166 TUF, M. Bencini, L. Fanfani, S. Pelizzari e V. Todini, *Profili penali della tutela del risparmio. Truffa, abusi di mercato e gestione patrimoniale*, Milano 2021, 118. Peraltro, l'assenza di autorizzazione configura, di norma, un tradimento dell'affidamento riposto dal privato che intenda operare con cripto-attività nei confronti dei professionisti a cui si rivolge. Sul punto, F. Di Vizio, *Moderni abusivismi e criptovalute. Tra il mito della completa disintermediazione e la realtà di nuovi intermediari*, in *Discrimen* 19.4.2022, 41.

contribuiscono in alcun modo alla selezione delle condotte penalmente rilevanti[83]. Vale allora quanto già rilevato in relazione all'art. 166 TUF: anche il delitto in parola tutela, in via immediata, una mera funzione, ossia il meccanismo di regolazione e controllo del mercato delle cripto-attività. Il legislatore ha, infatti, ritenuto l'esercizio non autorizzato delle attività professionali ivi richiamate di per sé idoneo a pregiudicare la trasparenza del sistema, in quanto preclude alle autorità competenti di esercitare i propri poteri di vigilanza[84]. Il che comporta l'ingresso sul mercato di soggetti che operano in maniera abusiva, essendosi deliberatamente sottratti alla selezione preventiva e al rigoroso sistema di verifica imposto dal MiCAR.

Il delitto di cui all'art. 30 assume, dunque, una forte valenza preventiva e l'anticipazione della tutela è giustificata, nella prospettiva del legislatore, dall'importanza degli interessi da proteggere, dal loro carattere diffuso e dalla loro potenziale estensione: tangibile è, infatti, il rischio che il mancato rispetto delle "regole del gioco" – ora divenuto estremamente formalizzato – conduca ad una «vittimizzazione di massa» di risparmiatori ed investitori in *crypto-assets*, finendo con il pregiudicare la tenuta stessa del mercato[85].

In un contesto siffatto, il ricorso a fattispecie di danno[86] rischia di dimostrarsi inadeguato, in quanto – per dirla con le parole di un illustre studioso – esse *entrano in gioco* «nel momento in cui i buoi sono ormai fuggiti dalla stalla», talvolta producendo effetti deflagranti[87].

---

[83] Così F. Consulich, *Il diritto penale nell'età del cripto-oro. Gli elementi normativi della fattispecie di abusivismo finanziario tra monete virtuali e investimenti reali*, in *GComm.* 2021, 933. Molto si è scritto intorno ai problemi di tenuta del sistema che comporta la tutela penale delle funzioni. Cfr. G. Losappio, *La tutela penale delle funzioni. Una proposta di rivisitazione metodologica*, in *Scritti in onore di Alfonso M. Stile*, Napoli 2013, 691 ss., nonché G. De Francesco, *Interessi collettivi e tutela penale. Funzioni e programmi di disciplina dell'attuale complessità sociale*, in *Studi in onore di Giorgio Marinucci*, I, Milano 2006, 929 ss.

[84] Siamo al cospetto di un «reato omissivo mediante commissione», poiché l'inosservanza dell'obbligo di richiedere l'autorizzazione integra gli estremi del tipo in tanto in quanto essa «si traduca nella violazione della condotta positiva, per la cui produzione quell'obbligo [...] era prescritto». In proposito, M. Mantovani, *L'esercizio di un'attività non autorizzata. Profili penali*, Torino 2003, 144.

[85] D'obbligo è il parallelismo con i mercati finanziari, coi relativi tracolli, fallimenti e scandali e con le perdite di milioni di investitori e risparmiatori: in questo come in quel contesto, siamo di fronte a fenomeni di vittimizzazione di massa. Nitidamente, M. Donini, *Sicurezza e diritto penale. La sicurezza come orizzonte totalizzante del diritto penale*, a cura di M. Donini, M. Pavarini, *Sicurezza e diritto penale*, Bologna 2011, 21. Concetti poi ripresi e sviluppati in E. Amati, *Abusi di mercato e sistema penale*, Torino 2012, 35.

[86] Trattasi di una tutela aggiuntiva rispetto a quella offerta dai tradizionali reati contro il patrimonio, *in primis* la truffa, la cui integrazione non è di certo preclusa dalla sussistenza del delitto di abusivismo. Cfr. A. Rossi, *L'esperienza giurisprudenziale del diritto penale economico nel tempo della crisi*, in *RIDPP* 2014, 627 ss.

[87] Davvero efficace la metafora di T. Padovani, *Diritto penale della prevenzione e mercato finanziario*, in *RIDPP* 1995, 644 s., il quale giustamente rileva come le «regole del gioco debbano essere presidiate da sanzione [...], così

Volendo tracciare l'*identikit* dei soggetti attivi, sebbene la fattispecie descritta dall'art. 30 integri un reato comune, che in astratto può essere commesso da *chiunque*, appare tuttavia chiaro che le attività subordinate all'ottenimento dell'autorizzazione non richiesta o negata – emissione di *token* e prestazione di servizi relativi a cripto-attività – saranno realizzabili in via pressoché esclusiva da strutture meta-individuali. L'assunto trova conferma nel Regolamento MiCA, nel quale i prestatori di servizi per cripto-attività vengono identificati in «persone giuridiche o altr[e] impres[e]»; anche gli emittenti di *token* collegati ad attività sono necessariamente imprese o persone giuridiche (cfr. art. 16 MiCAR), mentre gli emittenti di *token* di moneta elettronica devono essere autorizzati quali «enti creditizi o istituti di monete elettronica».

Ebbene, appurata la natura complessa di tali organismi, suscita qualche perplessità la mancata inclusione della fattispecie in parola nel novero dei delitti presupposto per la responsabilità amministrativa degli enti da reato *ex* d.lgs. 231/2001. Chiamate a rispondere saranno, allora, solo le persone fisiche che operano all'interno di tali organizzazioni complesse e, per lo più, coloro i quali ricoprono una posizione di vertice. Questa scelta – a nostro avviso davvero discutibile – è non di meno coerente con quella operata in relazione ai delitti di abusivismo bancario e finanziario, che per l'appunto non compaiono nel catalogo 231[88].

4.1. Detto ciò, va rilevato che la fattispecie di cui all'art. 30 d.lgs. 129/2024 è destinata a trovare applicazione nelle ipotesi di abusivismo relative a cripto-attività soggette al regime MiCAR. È pertanto inevitabile che i suaccennati problemi relativi all'individuazione dell'ambito operativo del Regolamento siano destinati a riflettersi sulla definizione dei margini di tipicità del reato in esame, con ovvie ricadute in punto di prevedibilità e certezza del diritto[89].

---

da garantire una repressione utile e non meramente simbolica», neutralizzando tempestivamente le «situazioni disfunzionali». Più in generale, sulla necessità di anticipare la soglia dell'intervento penale (e sanzionatorio in senso lato) con riguardo alla criminalità economica e finanziaria, si veda il pur risalente saggio di D. Pulitanò, *L'anticipazione dell'intervento penale in economia*, in AA.VV., *Diritto penale, diritto di prevenzione e processo penale nella disciplina del mercato finanziario. Atti del IV congresso nazionale di diritto penale*, Torino 1996, 10.

[88] Critici sull'esclusione del reato di cui all'art. 166 TUF dal *sistema 231*, B. Albertini, L. Franzetti, *La fattispecie di abusivismo tra consulenti finanziari autonomi e consulenti finanziari abilitati all'offerta fuori sede*, in *SOC* 2023, 343 ss.; M. Bencini, L. Fanfani, S. Pelizzari e V. Todini, *op. cit.*, 287 s. In precedenza, E. Montani, *Il reato di abusivismo: art. 166 tuf*, in *Reati in materia economica*, a cura di A. Alessandri, *Trattato teorico pratico di diritto penale*, diretto da F. Palazzo, C.E. Paliero, VIII, Torino 2017, 232 ss.

[89] Come infatti osserva N. Recchia, *I reati bancari. La tutela del corretto svolgimento dell'attività di intermediazione*, in *Reati in materia bancaria e finanziaria*, a cura di F. Consulich, *Trattato teorico pratico di diritto penale*, diretto da F. Palazzo, C.E. Paliero e M. Pelissero, Torino 2024, 17 «il rinvio a puntuali, ma

In particolare, è lecito pronosticare l'insorgenza di alcune criticità nella definizione dei rapporti con il delitto di abusivismo finanziario *ex* art. 166 TUF[90]. La questione è intimamente connessa alla possibilità di riconoscere ai *crypto-assets* la natura di strumenti finanziari e di assoggettare i professionisti operanti con le cripto-attività agli adempimenti previsti dal TUF per gli "intermediari finanziari"[91]. Sino al recente passato, andava sicuramente escluso che le criptovalute potessero, di per sé, rientrare in siffatta categoria, in quanto non ricomprese nell'elenco tassativo dell'Allegato I Sezione C cui rimanda l'art. 1 co. 2 del TUF.

Malgrado ciò, in giurisprudenza si è progressivamente consolidato un orientamento che, al sussistere di determinate condizioni, include le cripto-valute nell'onnivora categoria dei prodotti finanziari (art. 1 co. 1 lett. *u* TUF)[92], riconoscendo l'integrazione del reato di cui all'art. 166 co. 1 *lett.* c del TUF al cospetto di condotte poste in essere in mancanza degli adempimenti autorizzativi richiesti dal TUF[93].

Segnatamente, esso incrimina chiunque, senza la necessaria abilitazione, «offre fuori sede, ovvero promuove o colloca mediante tecniche di comunicazione a distanza, prodotti finanziari o strumenti finanziari o servizi o attività di investimento». Trattasi di una fattispecie a «selettività debole», in quanto il richiamo alla aperta e atecnica nozione di "prodotto finanziario" priva il precetto di un pregnante «attributo di determinatezza»[94]. A rilevare sono unicamente la pubblicità dell'investimento proposto e la sua finanziarietà, che si ricava dalla disamina della causa concreta del negozio[95]. Laddove emergesse che l'operazione di movimentazione di *crypto-assets*

sovrabbondanti, elementi normativi, definitori» non facilita «l'intellegibilità della fattispecie richiesta dalla garanzia costituzionale in materia penale della tassatività/determinatezza».

[90] Profilo già sottolineato in un primo commento "a caldo" da L. Di Stefano, A. Di Giorgio e R. Ferretti, *Criptovalute e moneta elettronica: tra distinzioni necessarie e rilevanza penale*, in www.dirittobancario.it, 3.9.2024.

[91] Il tema è sviluppato da F. Di Vizio, *op. cit.*, 1 ss.

[92] Si definiscono come tali «gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria». Questo inquadramento – molto discusso in dottrina – viene sostenuto da E. Girino, *Criptovalute: un problema di legalità funzionale*, in *Riv. dir. banc.* 2018, 55 ss.

[93] Cfr. Cass. 17.9.2020 n. 26807, in *CEDCass.*, m. 279590, commentata da R.M. Vadalà, *La dimensione finanziaria delle valute virtuali. Profili assiologici di tutela penale*, in *GI* 2021, 2224 ss.; F. Dalaiti, *Cripto-valute e abusivismo finanziario: cripto-analogia o interpretazione estensiva?*, in *SP* 21.1.2021; Cass. 30.11.2021 n. 44337, commentata da A. Quattrocchi, *La natura proteiforme delle criptovalute al crocevia della tutela penale del mercato finanziario*, in *GI* 2022, 1213 ss.; G. Mentasti, *Per la Cassazione la finalità di investimento del bitcoin rende configurabile l'abusivismo finanziario*, in www.altalex.com, 14.12.2021; Cass. 26.10.2022 n. 44378, in *CEDCass.*, m. 284124, con nota di R. Razzante, *Le cripto attività come prodotti finanziari*, in *Riv. it. ant.* 2022, 42 ss.; Cass. 14.9.2023 n. 37767, in www.onelegale.wolterskluwer.it; Cass. 19.7.2024 n. 29649, *ivi.* Per una schematica ricognizione, A. Frattolillo, *Giurisprudenza domestica in materia di criptovalute*, in *I Contratti* 2024, 56 ss.

[94] F. Dalaiti, *op. cit.*, 57.

[95] A. Quattrocchi, *op. cit.*, 1216.

avesse comportato «a) un impiego di capitali, riconducibile [...] al danaro o, più in generale, a un capitale proprio che può corrispondere anche a una valuta virtuale, b) una aspettativa di rendimento, e c) un rischio proprio dell'attività prescelta, direttamente correlato all'impiego di capitali», saremmo al cospetto di un investimento di natura finanziaria. La valuta virtuale andrebbe, allora, ricompresa tra i prodotti finanziari, mentre l'attività di reclamizzazione concretizzerebbe una proposta di investimento, soggetta «agli obblighi la cui omissione integra il reato di cui all'art. 166 TUF»[96].

L'impostazione seguita dalla Cassazione è in linea con quella della Consob, che, negli ultimi anni, esercitando i poteri conferitegli dall'art. 7 *octies* TUF, ha emesso una pluralità di provvedimenti sospensivi e inibitori nei confronti di piattaforme *web* che offrono abusivamente investimenti in *crypto-assets* (in particolare le *Initial Coin Offers*), riconoscendone la natura finanziaria laddove essi «implichino l'impiego di capitale, la promessa/aspettativa di rendimento e l'assunzione di un rischio direttamente connesso e correlato all'impiego di capitale»[97].

Quest'ultimo indirizzo era andato incontro alle critiche di una parte della dottrina, secondo cui l'affermazione della responsabilità *ex* art. 166 co. 1 lett. *c* era frutto di una forzatura interpretativa ai limiti dell'analogia *in malam partem* in contrasto con l'assetto normativo allora vigente. Il d.lgs. 231/2007 qualificava, infatti, le principali figure operanti nel settore delle cripto-attività – *exchanges e i wallet providers* – come "operatori di valuta virtuale"; costoro venivano equiparati ai cambiavalute ed erano, pertanto, soggetti all'obbligo di iscrizione nel relativo registro: ragione per cui, in caso di esercizio abusivo dell'attività, avrebbero dovuto essere piuttosto chiamati a rispondere per l'illecito amministrativo di cui all'art. 17 *bis* co. 5 del d.lgs. 13.8.2010 n. 141, in quanto fattispecie speciale rispetto all'art. 166 TUF[98].

A nostro parere, queste obiezioni non coglievano pienamente nel segno. Come noto, alcune criptovalute hanno natura proteiforme e possono assolvere a molteplici funzioni, non sempre determinabili *a priori*, tra cui anche quella di strumento di

[96] Cfr. Cass. 26.10.2022 n. 44378, cit.; Cass. 30.11.2021 n. 44337, cit., la quale nitidamente afferma che il *bitcoin* rappresenterebbe «un prodotto finanziario qualora acquistato con finalità d'investimento: la valuta virtuale, quando assume la funzione, e cioè la causa concreta, di strumento d'investimento e, quindi, di prodotto finanziario, va disciplinato con le norme in tema di intermediazione finanziaria».

[97] A mero titolo esemplificativo cfr. Delibera n. 23008 del 14.2.2024, in www.consob.it; Delibera n. 2289 del 15.11.2023, in www.consob.it, nelle quali viene dato «Ordine, ai sensi dell'art. 7-octies, comma 1, lett. b), del D. lgs. n. 58/1998 di porre termine alla violazione dell'art. 18 del Tuf».

[98] Di questo avviso F. Dalaiti, *op. cit.*, 60; M. Guastadisegni, *Criptovaluta e prodotto finanziario: l'eterno ritorno della causa negoziale*, in *Danno & resp.* 2022, 492 ss.

investimento. Sicché, non va escluso che esse – in ragione delle peculiarità dell'operazione di volta in volta considerata – siano riportabili nel novero dei prodotti finanziari[99]. Si prendano, ad esempio, i *bitcoin*: di norma, si tratta di un mezzo di pagamento su base volontaria; il discorso cambia quando il loro acquisto venga pubblicamente reclamizzato come una vera e propria proposta di investimento in un'attività rischiosa e con ampie prospettive di guadagno[100]: in casi del genere, appare pienamente corretto applicare la disciplina del TUF[101].

Ora, il quadro normativo è parzialmente mutato, senza però fugare ogni criticità.

Da un lato, con il Regolamento 858/2022/UE (relativo a un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito) il legislatore euro-unitario è intervenuto sulla definizione di "strumento finanziario" fornita dalla Direttiva 2014/65 (c.d. Mifid II)[102]; di conseguenza, il d.l. 30.3.2023 n. 25 (convertito con modificazioni nella l. 10.5.2023 n. 52), nell'adeguare la disciplina nazionale, ha modificato, tra l'altro, l'art. 1 co. 2 del TUF, il quale oggi annovera tra gli strumenti finanziari anche quelli emessi mediante tecnologia a registro distribuito e, dunque, talune tipologie di cripto-attività[103].

Da un altro lato, l'art. 2 par. 2 del MiCAR esclude espressamente l'operatività di tale *corpus* normativo al cospetto di cripto-attività qualificabili come strumenti finanziari, mentre l'art. 36 del d.lgs. 129/2024 stabilisce che «la disciplina del TUF avente ad oggetto i prodotti finanziari non si applica alle cripto-attività che rientrano nell'ambito di applicazione MiCAR».

Alla luce di ciò, si può ben dire che il diritto positivo ha quantomeno preso atto dell'esistenza di svariate tipologie di cripto-attività, con caratteristiche e funzioni differenti, da cui consegue l'applicazione di un diverso regime. Ed ecco allora che appare evidentemente semplicistico affermare che le condotte di abusivismo sinora riportate nell'alveo dell'art. 166 TUF rileveranno sempre oggi ai sensi del neo

[99] Cfr. A. Quattrocchi, *op. cit*., 1216; F. Consulich, *Nella* wunderkammer, cit., 155. Tuttavia, a detta di M. Guastadisegni, *op. cit.*, 492 ss., «la criptovaluta non è un prodotto finanziario. Lo è [...] il contratto che l'abbia in oggetto, come cosa incorporale da scambiare (e valore virtuale da trasferire), allorché preveda specifiche clausole di oggettivazione della funzione d'investimento. Solo in quest'ultimo ed eccezionale caso, pertanto, potrà applicarsi la disciplina legislativa della sollecitazione all'investimento, tra cui, in particolare, le norme concernenti sia le condizioni dell'offerta al pubblico (art. 94-*bis* TUF) sia la riserva dell'attività di offerta fuori sede (art. 30 TUF) o a distanza (art. 32 TUF), sussistendo l'imprescindibile presupposto: il prodotto finanziario».
[100] È il caso affrontato, in sede cautelare, da: Cass. 17.9.2020 n. 26807, cit.
[101] F. Di Vizio, *op. cit.*, 50.
[102] Cfr. l'art. 18 del Regolamento MiCA.
[103] Soluzione caldeggiata da F. Consulich, *Nella* wunderkammer, cit., 158.

introdotto art. 30 d.lgs. 129/2024. L'art. 30 – lo abbiamo visto – criminalizza talune forme di abusivismo relative ai *token* collegati ad attività e ai *token* di moneta elettronica che, di norma, assolvono a una funzione di pagamento, nonché la prestazione di servizi non autorizzata relativa a tutte le tipologie di cripto-attività rientranti nel MiCAR. Al cospetto, invece, di *crypto-assets* aventi in sé natura di strumento finanziario o sottostanti a un contratto di tipo finanziario dovrebbe, invece, continuare ad applicarsi la disciplina del TUF ed eventuali violazioni della riserva di attività potranno comportare l'integrazione del reato di cui all'art. 166.

Se ciò è vero, lo è altrettanto il fatto che non risulta comunque sempre agevole comprendere se un *crypto-assets* vada o meno qualificato come strumento finanziario[104]: le incertezze appaiono palesi se consideriamo che è lo stesso MiCAR ad imporre a chi chieda l'ammissione alla negoziazione o ai gestori di piattaforme di negoziazione di cripto-attività diverse dai *token* collegati ad attività o dai *token* di moneta elettronica la presentazione dei motivi per cui tali cripto-attività non andrebbero escluse dall'ambito del Regolamento, magari perché "strumenti finanziari" (cfr. art. 8 par. 4). Oneri similari ricadono anche sugli emittenti di *token* collegati ad attività, che sono tenuti a presentare, a corredo della domanda di autorizzazione, un parere giuridico secondo cui il prodotto in oggetto non è, tra l'altro, uno strumento finanziario (cfr. art. 18 par. 2 lett. *e* sub *i*)[105].

Di questi problemi definitori è, peraltro, anche in questo caso al corrente lo stesso legislatore euro-unitario: il considerando 14 del MiCAR ha ravvisato, infatti, l'opportunità di rimettere all' *European Securities and Markets Authority* l'emanazione di «orientamenti sui criteri e sulle condizioni per la qualificazione delle cripto-attività come strumenti finanziari», così da assicurare una «chiara distinzione tra, da un lato, le cripto-attività disciplinate dal presente Regolamento e, dall'altro, gli strumenti finanziari»[106]. Le *Guidelines on the conditions and criteria for the qualification of*

[104] Sull'assetto venutosi a delineare con l'entrata in vigore del MiCAR: M. De Mari, *Le cripto-attività nella disciplina MiCAr e la finanziarietà delle "cripto-attività non finanziarie"*, in *www.dirittobancario.it,* 13.12.2023.
[105] In proposito, L. Di Stefano, A. Di Giorgio e R. Ferretti, *op. cit.*, cit.
[106] Tali orientamenti dovrebbero inoltre consentire «una migliore comprensione dei casi in cui le cripto-attività che sono altrimenti considerate uniche e non fungibili con altre cripto-attività potrebbero essere qualificabili come strumenti finanziari». Nella stessa direzione, si prevede che, «al fine di promuovere un approccio comune alla classificazione delle cripto-attività, l'ABE, l'ESMA e l'Autorità europea di vigilanza (Autorità europea delle assicurazioni e delle pensioni aziendali e professionali) (EIOPA), istituita dal regolamento (UE) n. 1094/2010 del Parlamento europeo e del Consiglio ("autorità europee di vigilanza" o "AEV"), dovrebbero promuovere discussioni su tale classificazione. Le autorità competenti dovrebbero poter chiedere alle AEV pareri sulla classificazione delle cripto-attività, comprese le classificazioni proposte dagli offerenti o dalle persone che chiedono l'ammissione alla negoziazione. Gli offerenti o le persone che chiedono l'ammissione alla negoziazione

cryptoassets as financial instruments sono state, in effetti, pubblicate dall'ESMA nel *Final Report* dello scorso 17.12.2024[107] e – a una cursoria analisi – ci sembra che possa trattarsi di un valido strumento nelle mani degli addetti ai lavori per valutare la natura finanziaria di un certo *crypto-assets*, pur nella consapevolezza che una tale operazione qualificatoria, siccome prodotto di attività interpretativa, sconta un più o meno evidente margine di aleatorietà.

Alla luce di quanto osservato – e in attesa di conoscere i primi sviluppi prasseologici sul punto – il rischio di un'erronea o imprevedibile qualificazione delle cripto-attività quali strumenti finanziari o meno sembra, in ogni caso, non trascurabile, con ovvie ricadute a livello penalistico, se non altro in ragione della diversa cornice edittale prevista dal nuovo delitto di cui art. 30 del d.lgs. 129/2024 e da quello di cui all'art. 166 TUF.

5. Come abbiamo avuto modo di anticipare, il nuovo delitto di abusivismo rappresenta solo uno dei presidi sanzionatori introdotti dal provvedimento in commento.

In attuazione dell'art. 111 del MiCAR, il legislatore nazionale ha, invero, affiancato alla nuova fattispecie penalistica una serie di illeciti amministrativi (artt. 31-36)[108], il cui accertamento spetta, nell'ambito delle rispettive competenze, alla Consob e alla Banca di Italia; organi, quest'ultimi, tenuti a seguire il procedimento sanzionatorio previsto dall'art. 195 del TUF, salvo il caso in cui vengano in rilievo i *token* di moneta elettronica, al cospetto dei quali si applica la procedura indicata dall'art. 195 TUB (art. 37).

I destinatari di tali sanzioni sono innanzitutto società ed enti rispetto a cui sia stata accertata la violazione – abbiamo del resto già sottolineato il carattere meta-individuale di emittenti e prestatori di cripto-attività – e solo in seconda battuta le

---

sono i principali responsabili della corretta classificazione delle cripto-attività, che potrebbe essere contestata dalle autorità competenti, sia prima della data di pubblicazione dell'offerta sia in qualsiasi momento successivo». Qualora la classificazione di una cripto-attività sembri non essere coerente con il presente regolamento o con altri pertinenti atti legislativi dell'Unione in materia di servizi finanziari, le AEV dovrebbero avvalersi dei poteri loro conferiti dai regolamenti (UE) n. 1093/2010, (UE) n. 1094/2010 e (UE) n. 1095/2010 al fine di garantire un approccio uniforme e coerente a tale classificazione»: cons. n. 14 del MiCAR.

[107] Consultabili al seguente link: *https://www.esma.europa.eu/sites/default/files/2024-12/ESMA75453128700-1323_Final_Report_Guidelines_on_the_conditions_and_criteria_for_the_qualification_of_CAs_as_FIs.pdf*.

[108] Si veda l'analisi di U. Piatelli, S. Caruso e G. Rulli, *Cripto-attività e MiCAR: riflessioni sul decreto di adeguamento*, in *www.dirittobancario.it*, 17.9.2024; A Messina, *Cripto attività: previste sanzioni amministrative e penali per operatori e management*, in *www.ipsoa.it*, 25.6.2024.

persone fisiche. Esse si applicano, più in particolare, «nei confronti dei soggetti che svolgono funzioni di amministrazione, direzione o controllo e del personale delle società e degli enti nei confronti dei quali sono accertate le violazioni», unicamente quando queste ultime sono conseguenza del mancato rispetto «di doveri propri o dell'organo di appartenenza e la condotta ha inciso in modo rilevante sulla complessiva organizzazione o sui profili di rischio aziendale, ovvero ha provocato un grave pregiudizio per la tutela dei possessori di cripto-attività o per la tutela della stabilità finanziaria, l'integrità dei mercati finanziari e il regolare funzionamento del sistema dei pagamenti» (cfr. art. 36 par. 1).

Di seguito analizzeremo il contenuto delle singole figure di illecito amministrativo che, in forza dell'art. 3 co. 1 l. 24.11.1981 n. 689[109], possono essere punite sia a titolo di dolo – ipotesi a nostro avviso *fisiologica* – sia a titolo di colpa.

L'art. 31 si apre con la clausola di riserva «salvo che il fatto costituisca reato» e punisce, in via amministrativa, l'inosservanza delle disposizioni richiamate dall'art. 111 par. 1 lett. *a, b, c, d* del Regolamento MiCA, dei relativi atti delegati e delle disposizioni attuative adottate da Banca d'Italia e Consob.

Trattasi di un'ampissima serie di violazioni riguardanti la disciplina a) delle cripto-attività c.d. *other than*; b) quella dei *token* collegati ad attività; c) quella dei *token* di moneta elettronica e, infine, d) quella relativa al regime dei prestatori di servizio per cripto-attività. Oltre alla sanzione pecuniaria, aumentata sino al doppio laddove il vantaggio ottenuto superi i massimi edittali di cui al co. 1, le autorità competenti hanno facoltà di disporre ulteriori misure a carattere *lato sensu* sanzionatorio e, segnatamente, una dichiarazione pubblica indicante responsabile e tipologia di violazione, nonché un'ingiunzione diretta alla persona fisica o giuridica responsabile di porre termine al comportamento che costituisce la violazione e di astenersi da ripeterlo.

L'art. 32 punisce, invece, le violazioni nella comunicazione al pubblico di informazioni privilegiate *ex* art. 87 del MiCAR poste in essere da emittenti, offerenti e persone che chiedono l'ammissione alla negoziazione di cripto-attività, nonché l'inottemperanza agli obblighi relativi alla prevenzione e individuazione degli abusi di mercato evocati dall'art. 92 del Regolamento. Al pari di quanto disposto dall'art. 30,

[109] Per un inquadramento della disciplina generale dell'illecito amministrativo e dello statuto di garanzie che presidiano la sua operatività, basti il rinvio all'affresco recentemente tracciato da: C.E. Paliero, *Nascita ed evoluzione del sistema sanzionatorio amministrativo in Italia*, in *Le sanzioni amministrative. Quaderno 29 SSM*, Roma 2023, 17 ss.

anche qui viene prescritto un aumento di pena se il vantaggio conseguito è più alto del massimo edittale; a ciò si aggiungono le misure accessorie irrogabili dalla Consob: dichiarazione pubblica, ingiunzione di porre fine alla condotta illecita, restituzione dei profitti realizzati o delle perdite evitate grazie alla violazione, revoca o sospensione dell'autorizzazione a prestare servizi per le cripto-attività.

Ancora, gli artt. 33 e 34 puniscono, rispettivamente, persone fisiche ed enti per l'abuso di informazioni privilegiate (l'*insider trading*), per la comunicazione illecita di informazione privilegiate (il *tipping*) e per la manipolazione del mercato. È lo stesso MiCAR a precisare in cosa consistano le singole condotte indebite: le definizioni fornite risultano nella sostanza sovrapponibili a quelle contenute nel Regolamento MAR (Regolamento 596/2014/UE), che si riflettono sulla perimetrazione degli illeciti amministrativi tipizzati dal TUF agli artt. 187 *bis* e 187 *ter* e, per quanto concerne la responsabilità di enti e società, all'art. 187 *ter.1*.

L'art. 89 del MiCAR descrive l'abuso di informazioni privilegiate come l'acquisto, la cessione, l'annullamento o la modifica di un ordine di cripto-attività – per conto proprio o di terzi – effettuato utilizzando informazioni privilegiate, ossia informazioni che non sono state rese pubbliche e che – laddove divulgate – «potrebbero avere un effetto significativo sui prezzi di tali cripto-attività o sul prezzo di una cripto-attività collegata»[110]. Abuso e tentativo di abuso di informazioni privilegiate sono puniti in egual misura: l'equiparazione è ricavabile dal disposto del par. 2 dell'art. 89 del MiCAR, cui rimanda l'art. 33 del d.lgs. in commento, che – come ormai è noto – si limita a fare generico riferimento «alla violazione del divieto di abuso di informazioni privilegiate di cui all'art. 89»[111]. La parificazione dei limiti tra tentativo e consumazione (come del resto quella tra ipotesi colpose e ipotesi dolose) suscita, invero, perplessità, a maggior ragione se guardiamo alla notevole (e forse eccessiva) asprezza delle sanzioni

[110] Cfr. art. 87 del Regolamento MiCA. Sulla nozione di "informazione privilegiata" prevista dal TUF, in sostanza sovrapponibile a quella qui esaminata: F. D'Alessandro, *Regolatori del mercato, enforcement e sistema penale*, Torino 2014, 113 ss.; F. Mucciarelli, *Gli abusi di mercato riformati e le persistenti criticità di una tormentata disciplina*, in *DPC* 10.10.2018; Id., *Mercato finanziario e tutela penale*, in *questa Rivista*, 13.2.2024, 14 ss.; S. Seminara, Disclose or abstain? *La nozione di informazione privilegiata tra obblighi di comunicazione al pubblico e divieti di insider trading: riflessioni sulla determinatezza delle fattispecie sanzionatorie*, in *BBTC* 2008, 331 ss.; S. Giavazzi, *L'abuso di informazioni privilegiate*, in *Diritto e procedura penale delle società*, a cura di G. Canzio, L. Luparia Donati, Milano 2022, 775 ss.

[111] Al contrario, il comma finale dell'art. 187 *bis* del TUF – che sanziona in via amministrativa abuso e comunicazione illecita di informazioni privilegiate – prevede espressamente che «per le fattispecie previste dal presente articolo il tentativo è equiparato alla consumazione». Cfr. F. D'Alessandro, *op. cit.*, 156.

amministrative irrogabili, che – per le persone fisiche – toccano il massimo edittale di 5 milioni di euro.

Comunque sia, nel divieto di abuso di informazioni privilegiate sanzionato dall'art. 22 rientrano anche la raccomandazione e l'induzione a un'altra persona basate sull'informazione privilegiata (il *tuyautage)*[112], mentre colui che si avvale di tali sollecitazioni è punito solo quando «sa o dovrebbe sapere» che esse si fondano su informazioni privilegiate. Il par. 5 dell'art. 89 del MiCAR elenca i possessori di informazioni privilegiate nei confronti dei quali opera il divieto di abuso (ad esempio «il membro di organi di amministrazione, direzione o vigilanza dell'emittente, dell'offerente o della persona che chiede l'ammissione alla negoziazione» o colui che possegga l'informazione perché coinvolto in attività illecite, il c.d. *insider criminale*). Divieto che si estende anche all'*insider secondario*, ossia il soggetto che, sebbene privo di una qualifica che lo ponga in condizione di «vantaggio informativo»[113], entra comunque in possesso di informazioni privilegiate e «sa o dovrebbe sapere di trovarsi» al loro cospetto.

La seconda delle condotte incriminate dall'art. 33 del d.lgs. 129/2024 è il divieto di *tipping*: nessuno in possesso di informazioni privilegiate può divulgarle a terzi, salva l'ipotesi in cui la diffusione avvenga nell'ambito «del normale esercizio di un'attività lavorativa, di una professione o di una funzione» (art. 90 MiCAR)[114]. Il divieto di comunicazione illecita è finalizzato a preservare la riservatezza delle informazioni prima che esse vengano divulgate, in modo da scongiurare il rischio che i destinatari della comunicazione illecita si collochino in una posizione di indebito vantaggio sul mercato delle cripto-attività[115]. A norma del par. 2 dell'art. 90 del MiCAR è, altresì, illecita «la divulgazione a terzi delle raccomandazioni o induzioni [...]» quando la persona che le divulga «sa o dovrebbe sapere che esse si basa[no] su informazioni privilegiate».

A questo riguardo, ci siano consentite due brevi osservazioni.

---

[112] Come ben spiegato da E. Amati, *Abusi di mercato e sistema penale*, Torino 2012, 154, l'introduzione di una fattispecie *ad hoc* è giustificata dal fatto che «la raccomandazione e l'induzione non presuppongono la trasmissione della notizia».

[113] Sulla figura dell'*insider secondario*, M. Gambardella, *Condotte economiche e responsabilità penale*, Torino 2018, 324 ss.

[114] Da sottolineare che l'art. 90 del Regolamento MiCA ricalca, in larga parte, il contenuto dell'art. 10 del Regolamento MAR.

[115] Cfr. M. Bencini, L. Fanfani, S. Pelizzari e V. Todini, *op. cit.*, 209 s.

Per quanto concerne lo sfuggente concetto di "normalità", esso va declinato alla luce del ruolo ricoperto dal soggetto agente: sicché la comunicazione sarà da ritenersi lecita allorché rientri nel fisiologico esercizio dell'attività dell'*insider*, rivelandosi funzionale allo svolgimento delle proprie tipiche mansioni[116].

Sotto altro profilo, il reiterato impiego della locuzione "dovrebbe sapere" attribuisce espressa rilevanza alle condotte colpose dell'*insider secondario*, nonché a quelle di chi si avvalga o divulghi raccomandazioni o induzioni aventi ad oggetto informazioni privilegiate[117]. Orbene, riteniamo che l'individuazione del contenuto della pretesa doverosa il cui mancato rispetto da luogo al rimprovero per colpa (l'*Anlass*)[118] possa rivelarsi alquanto problematica. In assenza di più specifiche indicazioni normative, l'interprete è infatti chiamato a valutare se le condizioni in cui versava l'agente fossero tali da potergli permettere di sapere – laddove avesse agito secondo diligenza – di disporre di informazioni privilegiate (nel caso dell'*insider secondario*) o di raccomandazioni o induzioni basate su informazioni privilegiate. Sin troppo evidente il rischio che simili valutazioni finiscano con l'essere fondate sul mero intuito.

Infine, l'ultima condotta menzionata dall'art. 33 è quella di manipolazione del mercato, che – anche in questo caso – viene definita facendo rinvio al MiCAR, e precisamente all'art. 90. Esso ripropone la dicotomia impiegata dall'art. 12 del Regolamento 596/2014/UE (il Regolamento MAR)[119] nel descrivere le condotte di manipolazione del mercato finanziario: così, il par. 2 introduce un elenco tassativo di attività qualificate come manipolatorie, tutte caratterizzate da una innata connotazione fraudolenta.

Si tratta del contegno di chi: a) salvo che per motivi legittimi – concluda un'operazione, collochi un ordine, o ponga in essere un'altra condotta che fornisca (o sia suscettibile di fornire) informazioni false o fuorvianti relative a offerta, domanda e prezzo delle cripto-attività ovvero ne fissi il prezzo a un livello anormale o artificiale[120];

---

[116] Si richiama l'interpretazione consolidatasi con riguardo alle fattispecie del TUF. Cfr. S. Giavazzi, *op. cit.*, 749.
[117] In proposito, F. Mucciarelli, *Gli illeciti amministrativi degli artt. 187 bis, 187 ter e 187 ter.1 TUF dopo la riforma all'insegna della tecnica del rinvio*, in *SOC* 2019, 578 ss.
[118] Sul concetto di *Anlass*, imprescindibile la teorizzazione di G. Forti, *Colpa ed evento nel diritto penale*, Milano 1990, 251; più di recente: F. Giunta, *Culpa, Culpae*, in *Discrimen* 4.6.2019, 15; M. Caputo, *Colpa penale del medico e sicurezza delle cure*, Torino 2017, 116; da ultimo, L. Carraro, *Spazi teorici di autoresponsabilità e colpa "stradale" nell'investimento di un pedone: rigidità giurisprudenziale e prospettazioni dogmatiche*, in *AP* 2/2023, 17.
[119] Su cui F. Consulich, *Manipolazione dei mercati e diritto eurounitario*, in *SOC* 2016, 207 ss.
[120] Quanto alla misurazione delle soglie di "anomalia" e "anormalità", sembra che si debba far riferimento al prezzo che avrebbe avuto il *crypto-asset* in assenza del fattore perturbativo. Valutazione agevole a livello teorico, ma che sul piano pratico, appare realisticamente complessa. Cfr., sempre in relazione alla materia dei mercati finanziari, F. Mucciarelli, *Gli illeciti amministrativi*, cit., 578.

b) concluda un'operazione o ponga in essere un'altra attività che incida o possa incidere sul prezzo di una o più cripto-attività, attuata mediante l'utilizzo di uno strumento fittizio o di un altro tipo di inganno od espediente; c) diffonda informazioni false o fuorvianti relative a offerta, domanda e prezzo delle cripto-attività.

Il successivo par. 3 elenca, invece, una serie di comportamenti da considerare «tra l'altro» come manipolazione del mercato tra cui, ad esempio, «l'acquisizione di una posizione dominante sull'offerta o sulla domanda di una cripto-attività, che abbia o possa avere l'effetto di fissare, direttamente o indirettamente, i prezzi di acquisto o di vendita oppure crei, o possa creare, altre condizioni commerciali inique». Si tratta di un catalogo aperto e meramente esemplificativo di condotte, di per sé sprovviste di un'intrinseca componente decettiva, ma che – ove declinate in peculiari contesti e poste in essere con particolari modalità – danno luogo a una manipolazione del mercato[121].

L'illecito amministrativo in commento è integrato anche da contegni realizzati in forma colposa: paradigmatica, in proposito, l'ipotesi di cui alla lett. *c* del par. 2 dell'art. 90 MiCAR, che attribuisce rilievo alla manipolazione commessa diffondendo informazioni «che forniscano, o è probabile che forniscano, segnali falsi o fuorvianti in merito all'offerta, alla domanda o al prezzo di una o più cripto-attività», non solo quando l'agente sappia, ma anche quando avrebbe dovuto sapere, della falsità e della nota fuorviante del dato trasmesso.

Tralasciando il terzo comma dell'art. 33, che si limita a rinviare alla disciplina contenuta nei co. 2 e co. 3 dell'art. 32 (relativi all'aggravamento di pena laddove i vantaggi conseguiti dall'agente superino i massimi edittali e alle misure amministrative accessorie irrogabili dalla Consob), vale la pena soffermarsi sul disposto del co. 2, il quale esclude l'assoggettamento alla sanzione amministrativa qualora l'autore di una condotta di manipolazione del mercato dimostri di aver agito «per motivi legittimi».

Riempire di significato tale locuzione risulta piuttosto difficoltoso. È vero: la norma è parzialmente sovrapponibile al co. 4 dell'art. 187 *ter* TUF, ma in quel contesto, si parla di «aver agito per motivi legittimi *e* in conformità alle prassi ammesse nel mercato»[122].

[121] Riteniamo che possa tornare utile – in ragione di tratti di somiglianza tra la disciplina in commento e quella enucleata dal TUF – la lettura delle notazioni critiche espresse da: F. Mucciarelli, *Gli illeciti amministrativi*, cit., 578 ss.; Id., *Gli abusi*, cit.; F. Consulich, Market manipulation *e legislazione cosmetica*, in *SOC* 2019, 558; S. Preziosi, *Nuova disciplina della manipolazione di mercato e bene giuridico tutelato*, in *AP* 1/2021, 1 ss.

[122] Previsione che si ritrova al co. 1 *bis* dell'art. 185 TUF, che punisce il delitto di manipolazione del mercato, escludendo la punibilità di chi «ha commesso il fatto per il tramite di ordini di compravendita o operazioni effettuate per motivi legittimi e in conformità a prassi di mercato ammesse, ai sensi dell'articolo 13 del

Il rimando alle prassi di settore, che sono oggetto di disciplina nell'ambito del mercato mobiliare, rende senza dubbio più agevole definire statuto giuridico e dimensione operativa dell'art. 187 *ter* co. 4: esso designerebbe una scriminante, più precisamente una «causa di giustificazione di origine prasseologico-consuetudinaria», che assume efficacia in tanto in quanto le prassi vengano riconosciute dalla Consob[123].

Nel contesto in esame, invece, il riferimento ai motivi legittimi assume le sembianze di una vera e propria «delega in bianco a qualsiasi motivazione giuridica incompatibile con la finalità di manipolazione»[124]. Il MiCAR – giova ribadirlo, primo *corpus* normativo euro-unitario deputato alla regolazione del mercato dei *crypto-assets* – menziona solo incidentalmente le prassi relative a cripto-attività, ma non regola in alcun modo modalità e requisiti per il loro riconoscimento. È quindi all'evidenza problematico comprendere quando si sia di fronte a un contegno che, pur alterando il fisiologico andamento degli scambi, vada ritenuto lecito e quando invece siano integrati gli estremi della manipolazione punibile. Pure in questo caso, il pericolo è che la valutazione venga condotta su base intuitiva, con naturali pregiudizi in punto di prevedibilità e certezza. È però possibile ipotizzare che, in un futuro non remoto, il legislatore europeo provvederà a introdurre una disciplina sulle condizioni di ammissibilità e sulle procedure di riconoscimento delle prassi di settore, proprio come accade in ambito MAR[125].

Soffermandoci ancora per un attimo sulla materia degli abusi di mercato, ma sotto il profilo della responsabilità amministrativa dell'ente, va registrato che l'art. 34 del d.lgs. in commento prevede un regime di imputazione costruito sulla falsariga di

Regolamento (UE) n. 596/2014».

[123] Non è questa chiaramente la sede per indagare la discussa natura giuridica del co. 4 dell'art. 187 *ter* TUF. Propende per il suo valore scriminante, con tutto con ciò che ne consegue in punto di disciplina: F. Consulich, *Lo statuto penale delle scriminanti. Principio di legalità e cause di giustificazione. Necessità e limiti*, Torino 2018, 340 ss., secondo cui il principale ostacolo a un inquadramento siffatto sarebbe costituito dalla «disponibilità del potere di giustificare» le condotte in capo alla stessa autorità deputata a punirle amministrativamente. La giustificazione non sarebbe – come accade di norma – preesistente, ma sorgerebbe «dall'attività dell'applicatore del diritto». Saremmo, quindi, al cospetto di una scriminante «topica» – in quanto riferita a specifiche tipologie comportamentali ammesse dall'autorità competente – e circolare, poiché la Consob, da un lato, provvede «all'*enforcement* delle norme punitive» e, dall'altro, può giustificarle. Dello stesso avviso, F. Mucciarelli, *Gli abusi*, cit., 15. *Contra*, ad esempio, S. Preziosi, *La manipolazione del mercato nella cornice dell'ordinamento comunitario e del diritto penale italiano*, Bari 2008, 119, che lo riconduce nel novero delle cause di esclusione della tipicità. Sulla questione v. A. Gargani, *Commento agli artt. 187-bis – 187 septies Testo unico in materia di intermediazione finanziaria, inseriti dall'art. 9, co. 2, lett. a), l. 62/2005 (Legge comunitaria 2004),* in *LP* 2006, 108.

[124] Così F. Consulich, *La giustizia e il mercato. Miti e realtà di una tutela penale dell'investimento mobiliare*, Milano 2010, 227.

[125] Sui meccanismi di istituzione delle prassi, F. Mucciarelli, *Gli abusi*, cit., 11 ss.

quello di cui al d.lgs. 231/2001. Anche qui, l'ente risponde qualora la violazione sia commessa nel suo interesse o vantaggio, da soggetti inseriti nella struttura complessa (in ruolo apicale o sotto altrui direzione e vigilanza) e che non agiscono nell'esclusivo interesse proprio o di terzi. Peraltro, l'ultimo comma dell'art. 34 richiama alcune disposizioni del d.lgs. 231/2001 (gli artt. 6, 7, 8 e 12), estendendo il loro raggio di applicazione all'accertamento della responsabilità dell'ente per gli illeciti ivi tipizzati. Nemmeno sotto questo versante siamo di fronte a un'assoluta novità: l'art. 34 costituisce piuttosto una replica dell'art. 187 *ter* TUF, chiaramente destinata ad operare nel contesto MiCAR.

Da ultimo, l'art. 35 del d.lgs. 129 sanziona le persone fisiche e giuridiche che non ottemperino alle richieste od omettano di collaborare con le autorità munite di poteri di sorveglianza e di indagine enucleati dall'art. 94 del MiCAR. Gli operatori professionali sul mercato delle cripto-attività sono, infatti, tenuti a istituire sistemi e procedure volte a prevenire e neutralizzare eventuali abusi di mercato[126]. Su di essi grava inoltre l'obbligo di segnalare «senza indugio» alle autorità competenti le operazioni sospette, che potrebbero, cioè, risolversi in un abuso di mercato. Il presidio introdotto dall'art. 35 è stato concepito come strategico al fine di garantire una fattiva collaborazione tra le istituzioni e i professionisti di settore, il cui contributo risulta utile per ridurre o arginare i pericoli connessi all'acquisto o alla detenzione di cripto-attività, che, come ancora recentemente avvertito dall'ESMA, e nonostante l'entrata in vigore del MiCAR, hanno tutt'oggi natura altamente rischiosa e speculativa[127].

5.1. All'esito della rassegna dei nuovi illeciti amministrativi introdotti dal d.lgs. 129/2024, viene immediatamente in luce un esasperato utilizzo della tecnica del rinvio, per il vero già impiegata nella tipizzazione del delitto di abusivismo di cui all'art. 30. Tutte le disposizioni sanzionatorie (penali o amministrative che siano) richiamano specifiche previsioni del MiCAR e non mancano rimandi agli atti delegati e alle norme tecniche di regolamentazione e attuazione elaborate dalle autorità di settore. Orbene,

[126] In un settore magmatico e in costante evoluzione, prima ancora che legislatore e le competenti autorità di vigilanza, sono i gestori del mercato a dover svolgere un ruolo chiave nella prevenzione di possibili illeciti, innanzitutto predisponendo ed aggiornando costantemente i *compliance programs*. Rileva l'impossibilità, da parte delle autorità pubbliche, di «regolare e monitorare» ogni aspetto del mercato, essendo indispensabile che gli operatori privati contribuiscano alle attività di *enforcement*, F. Consulich, *Manipolazione del mercato e declino del sistema finanziario. Spunti di riflessione a margine del ventesimo anniversario dell'avvio del processo Parmalat*, in *SP* 4.9.2024, 18.

[127] Cfr. ESMA, *Avvertenza sulle cripto-attività*, 13.12.2024, consultabile sul portale www.consob.it.

è facile intuire come il ricorso a tale tecnica normativa renda assai difficoltose la lettura e l'immediata comprensione del testo, in quanto il contenuto del precetto la cui violazione integra gli estremi dell'illecito è ricavabile soltanto mediante una non agevole combinazione tra diversi provvedimenti normativi.

A ciò si aggiunga che eventuali e probabili modifiche del Regolamento o degli atti delegati incideranno, presumibilmente, sulla delimitazione del raggio operativo delle singole fattispecie tipizzate dal d.lgs., dando luogo a incertezze sul piano della tenuta del principio di legalità e a livello di diritto successorio. In ogni caso, un così ampio ricorso alla tecnica del rinvio è destinato ad avere inevitabili ricadute sotto il profilo dell'accessibilità del dato normativo e della prevedibilità delle conseguenze sanzionatorie: il che complica i compiti dell'interprete e crea un non trascurabile *vulnus* agli operatori del mercato, i quali si trovano al cospetto di una disciplina di non immediata fruizione e per molti versi oscura.

A nostro parere, nonostante l'estrema prolissità dell'alternativa proposta, sarebbe stato preferibile procedere a una diretta trasposizione delle disposizioni MiCAR rilevanti, limitando allo stretto necessario il nudo rinvio agli articoli del Regolamento[128].

Apprezzabile è invece la scelta del legislatore euro-unitario di definire gli abusi di mercato commessi in relazione a cripto-attività per mezzo della tecnica casistica, già utilizzata nel contesto del mercato mobiliare[129]. Scelta che consente di individuare con maggior precisione le tipologie di condotte vietate, accrescendo così la determinatezza delle fattispecie punite dal d.lgs. 129/2024.

Va poi sottolineata una divergenza rispetto alla disciplina del TUF: nel reprimere le violazioni in ambito MiCAR, il legislatore ha rinunciato alla costruzione di un doppio binario sanzionatorio[130], relegando l'intervento dello *ius terribile* al solo delitto di abusivismo[131]. Il rischio di sovrapposizioni tra il penale e l'amministrativo viene così

[128] Da condividersi critiche e soluzioni proposte da F. Mucciarelli, *Gli illeciti amministrativi*, cit., 578 ss. a commento degli illeciti tipizzati dal TUF.

[129] Guarda con favore a una simile opzione, improntata a «frammentarietà e sussidiarietà», F. Consulich, *Market manipulation*, cit., 558 ss.

[130] Per uno sguardo di insieme sulla tematica, tra i molti scritti successivi alla sentenza della C.eur., 4.3.2014, *Grande Stevens et al. c. Italia* si rimanda a: F. Viganò, *La Grande Camera della Corte di Strasburgo su* ne bis in idem *e doppio binario sanzionatorio*, in *DPC* 18.11.2016; C. Silva, *Sistema punitivo e concorso apparente di illeciti,* Torino 2018, 33 ss.; F. Consulich, *Il prisma del ne bis in idem nelle mani del giudice eurounitario,* in *DPP* 2018, 949 ss.; M. Scoletta, *Il principio di* ne bis in idem *e i modelli punitivi "a doppio binario",* in *DPenCont-Riv. trim.* 4/2021, 180 ss.; F. Mazzacuva, *Le pene nascoste. Topografia delle sanzioni punitive e modulazione dello statuto garantistico*, Torino 2017, 287 ss.

[131] F. Consulich, *Manipolazione del mercato e declino del sistema finanziario,* cit., 12.

fugato in radice dalla presenza della clausola di riserva a favore del penale prevista in apertura dell'art. 31, autentica fattispecie *omnibus* che sanziona amministrativamente tutte le violazioni degli obblighi autorizzativi e procedurali introdotti dal MiCAR non integranti gli estremi del reato di cui all'art. 30. Se guardiamo alla tipologia di condotte punite dall'una e dall'altra norma, residua, tuttavia, qualche perplessità in merito alla ragionevolezza della scelta attuata dal nostro legislatore di punire solo in via amministrativa l'emissione e l'offerta di *crypto-assets* che non sono *token* di moneta elettronica e *token* collegati ad attività, attribuendo invece rilevanza penale alla prestazione di servizi non autorizzata relativa a tutte le tipologie di cripto-attività poste in essere da persone giuridiche e imprese (art. 59, par. 1 lett. *a* Regolamento MiCA), senza alcuna differenziazione di sorta. Non sembra poi trovare una razionale giustificazione il distinguo operato tra le persone giuridiche e imprese di cui al menzionato art. 59, par. 1 lett. *a* del MiCAR – che, in caso di violazione della riserva di attività, rispondono penalmente – e i soggetti indicati alla lett. *b* – enti creditizi, depositari centrali di titoli, imprese di investimento, gestori del mercato, istituti di moneta elettronica, società di gestione di un OICVM [132] e gestori di un fondo di investimento alternativo – i quali sono responsabili a livello amministrativo ai sensi dell'art. 32 del d.lgs. 129/2024[133].

A ogni modo, le ragioni sottese alla scelta del legislatore di percorrere, a differenza di quanto avviene nel TUF[134], la «rotaia preferenziale» del diritto amministrativo[135] sono molteplici: si va da quelle più spiccatamente economiche – considerati gli elevati costi che produce l'attivazione di due procedure parallele aventi ad oggetto il medesimo fatto storico – a quelle di natura pratica-utilitaristica. L'analisi "dinamica" del sistema delineato dal TUF, da cui la disciplina in commento ha tratto ampio spunto, ha infatti mostrato il maggiore successo riscosso dalla sanzione amministrativa, «più graduabile ed efficace» dello strumento penalistico[136]. Non può

[132] Acronimo di Organismo di investimento collettivo in valori mobiliari.
[133] Sul punto, M. Misiti, *op. cit.*
[134] In quell'ambito, per il vero, è lo stesso legislatore euro-unitario ad imporre il ricorso (anche) a sanzioni penali, principalmente per ragioni promozionali, in quanto l'impiego dello *ius terribile* permette di accrescere la fiducia del pubblico nel mercato mobiliare. Cfr. F. Consulich, *Manipolazione dei mercati*, cit., 204. Sul valore maggiormente stigmatizzante della sanzione penale, si leggano C.E. Paliero, A. Travi, *La sanzione amministrativa. Profili sistematici,* Milano 1988, 22.
[135] F. Consulich, *Manipolazione del mercato e declino del sistema finanziario,* cit., 12.
[136] Sul successo dell'illecito amministrativo punitivo nel perseguimento degli abusi di mercato: A. Tripodi, *Gli illeciti amministrativi in tema di abusi di mercato*, in *Reati in materia bancaria e finanziaria*, cit., 275; F. Consulich, *Manipolazione dei mercati*, cit., 204; ma in passato già C.E. Paliero, *La sanzione amministrativa come moderno strumento di lotta alla criminalità economica*, in *RivTrim-DPenEc.* 1993, 1027 ss.

inoltre trascurarsi il fatto che la Consob dispone di un ampio bagaglio di competenze tecniche e di penetranti poteri di indagine, che rendono evidentemente più agevole l'individuazione e la repressione degli abusi di mercato. Considerazioni, queste, valevoli anche con riguardo al settore delle cripto-attività, nel quale le autorità competenti – nel nostro ordinamento Consob e Banca d'Italia[137] – vedono attribuirsi dal MiCAR un ampio ventaglio di poteri di normazione, di vigilanza e di indagine (cfr. art. 94 del Regolamento).

Va però detto apertamente che l'ideale *self-restraint*, mantenuto dal legislatore interno sul versante del ricorso al mezzo penalistico sostanziale, rischia di celare una sorta di truffa delle etichette, in quanto gli illeciti amministrativi, introdotti dal d.lgs. 129/2024, sembrano avere tutte le caratteristiche per poter essere ricondotti alla nozione euro-convenzionale di *matière pénale*, laddove si faccia applicazione dei ben noti criteri identificati dalla giurisprudenza sovranazionale sin dal celeberrimo caso *Engel*[138]. Si afferma un tanto dal momento che le sanzioni formalmente amministrative di nuovo conio non si limitano a rispondere a finalità repressive e dissuasive, ma hanno, del pari, una severità notevole, che non esitiamo a definire draconiana.

Peraltro, sottolineiamo incidentalmente che la fissazione di elevatissime cornici edittali – sia per le sanzioni irrogabili nei confronti delle persone fisiche, sia per quelle nei confronti degli enti – è accompagnata dalla pressoché totale equiparazione dei limiti di pena a fronte di illeciti evidentemente espressivi di un diverso disvalore: emblematico l'art. 33, che punisce in egual misura l'*insider trading*, la comunicazione illecita di informazioni privilegiate e la manipolazione di mercato[139]. La conformità di un simile assetto al principio di proporzionalità sanzionatoria appare per lo meno dubbia, e ciò tanto a livello estrinseco-ordinale quanto sul piano intrinseco-cardinale[140].

---

[137] Per un'analisi dei procedimenti sanzionatori innanzi a Consob e Banca d'Italia: E. Bindi, A. Pisaneschi e P. Luccarelli, *Le sanzioni della Banca d'Italia e della Consob*, in *GComm.* 2021, 553 ss.

[138] C.eur. GC, 8.6.1976, ric. nn. 5100/71, 5101/71, 5102/71, 5354/72, 5370/72, *Engel e a. c. Paesi Bassi*, su cui diffusamente L. Masera, *La nozione costituzionale di materia penale*, Torino 2018, 25 ss.

[139] Analoghe criticità sono state riscontrate analizzando la disciplina del TUF, ove però la presenza del doppio binario penale-amministrativo e le continue modifiche legislative volte ad innalzare l'entità della risposta repressiva rendono ancor più evidente la complessiva irrazionalità del sistema. Cfr. C. Silva, *La proporzionalità della pena in materia di abusi di mercato. profili problematici di un sindacato diffuso di riequilibrio sanzionatorio*, in *SP* 21.6.2023, 5; V. Napoleoni, *Diritto penale dell'economia*, Milano 2017, 603.

[140] Sullo scrutinio di proporzionalità nel contesto delle sanzioni amministrative, si veda da ultimo C. cost., 6.2.2023 n. 46. In dottrina: F. Viganò, *La proporzionalità della. Profili di diritto penale e costituzionale*, Torino 2021, 86 ss., il quale sottolinea come, in tale contesto, il giudizio di costituzionalità si fondi sul parametro di cui all'art. 3, non avendo (per lo meno sino ad oggi) la Corte ritenuto il principio di rieducazione applicabile agli

Comunque sia, dall'attribuzione della natura "penale" agli illeciti qui esaminati dovrebbe conseguire la necessità di estendere loro l'apparato di garanzie penalistiche costituzionali ed euro-convenzionali: è, in effetti, quanto sta accadendo in relazione agli illeciti amministrativi punitivi in materia di abusi di mercato, ove l'azione congiunta della giurisprudenza euro-unitaria e costituzionale ha via via implementato le tutele nei confronti dei soggetti sottoposti a procedure sanzionatorie innanzi alla Consob e alla Banca di Italia[141] (si pensi al riconoscimento, per mano della Consulta, del diritto al silenzio dell'incolpato nel procedimento di cui all'art. 187 *quinquiesdecies* TUF[142], all'estensione della garanzia della *lex mitior* in relazione agli illeciti amministrativi di cui all'art. 187 *bis* e *ter*[143], o, ancora, all'affermazione del principio di irretroattività della confisca per equivalente *ex* art. 187 *sexies* co. 2[144] e alla sottoposizione allo scrutinio di proporzionalità della confisca amministrativa di cui all'art. 187 *sexies*[145]).

E, tuttavia, nonostante il progressivo accrescimento dei presidi garantistici in relazione all'illecito amministrativo "para-penale"[146], è inevitabile che la decisione di

illeciti amministrativi punitivi. Altresì, F. Mazzacuva, *Il principio di proporzionalità delle sanzioni nei recenti tracciati della giurisprudenza costituzionale: le variazioni sul tema rispetto alla confisca*, in *questa Rivista*, 7.12.2020.

[141] Rimandiamo alla ricognizione di: D. Guidi, *Poteri della Consob ed estensione delle garanzie "penalistiche" al procedimento sanzionatorio amministrativo: verso un nuovo punto di equilibrio*, in *RivTrim-DPenEc.* 2023, 438 ss.; E. Bindi, *L'ampliamento del contraddittorio nel procedimento sanzionatorio Consob: alcuni spunti per rafforzare un percorso già iniziato*, in *SOC* 2023, p. 128 ss.

[142] Cfr. C. cost., 30.4.2021 n. 84, commentata da C. Bonzano, *Matiére pénale e diritto al silenzio: la Consulta mette un punto fermo… o quasi*, in *DPP* 2022, 47 ss. che ha dichiarato l'illegittimità costituzionale dell'art. 187 *quinquiesdecies* TUF «nella parte in cui si applica anche alla persona fisica che si sia rifiutata di fornire alla Banca d'Italia o alla Consob risposte che possano far emergere la sua responsabilità per un illecito passibile di sanzioni amministrative di carattere punitivo, ovvero per un reato». La declaratoria di incostituzionalità è stata preceduta da una pronuncia della Corte di Lussemburgo (sollecitata dalla stessa Consulta) che – anche alla luce della giurisprudenza della Corte EDU – ha confermato l'esistenza del diritto al silenzio, collocandolo «al centro della nozione di equo processo». Cfr. C.G. UE 2.2.2021, C-481/19. Sulla vicenda: G. Lasagni, *La Corte di giustizia riconosce il diritto al silenzio nei procedimenti amministrativi punitivi (e la Corte costituzionale conferma)*, *GComm*. 2021, 1179 ss. Non sfuggirà, peraltro, come problemi di analogo tenore potrebbero sorgere, in particolare, per quanto concerne il sopra menzionato art. 35 del d.lgs. 129 del 2024, il quale sanziona le persone fisiche e giuridiche che non ottemperino alle richieste od omettano di collaborare con le autorità. Nel caso tale fattispecie venga considerata sostanzialmente penale, gli obblighi dalla stessa imposti possono, invero, finire per confliggere proprio con quei pilastri del diritto di difesa penalistico, costituiti dal diritto al silenzio e di non collaborare.

[143] Cfr. C. cost. 20.2.2019 n. 63, con nota di M. Scoletta, *Retroattività favorevole e sanzioni amministrative punitive: la svolta, finalmente, della Corte costituzionale*, in *DPC* 2.4.2019.

[144] C. cost. 25.10.2018 n. 223, con nota di F. Consulich, *La materia penale: totem o tabù? Il caso della retroattività in mitius della sanzione amministrativa*, in *DPP* 2019, 467 ss.

[145] C. cost. 10.5.2019 n. 112, con nota di R. Acquaroli, *La confisca e il controllo di proporzionalità: una buona notizia dalla Corte costituzionale*, in *DPP* 2020, 197 ss.

[146] Sul punto rimandiamo alle interessanti osservazioni di V. Manes, *La riconversione garantistica dell'illecito*

seguire la strada amministrativa – di certo più appagante in termini di deflazione della macchina penale e di rapidità – finisca per scontare un'inevitabile diminuzione del livello di tutela dei diritti dei soggetti sottoposti a procedimento e sanzione. Basti pensare che – a oggi – in ambito amministrativo-punitivo non è richiesto il rispetto dello standard di prova dell'al di là di ogni ragionevole dubbio. Secondo l'opinione prevalente, la responsabilità viene, infatti, qui accertata sulla base di regole probatorie più blande, che fanno leva sui fumosi e più elastici concetti di «ragionevole probabilità», di «preponderanza dell'evidenza» o sulla logica del «più probabile che non»[147]. Il che rappresenta un deficit esiziale se è vero che – come ha affermato esplicitamente la Corte europea dei diritti dell'uomo[148] – tale standard probatorio assurge ad essenziale corollario della presunzione d'innocenza, la quale costituisce, a sua volta, «la prima e fondamentale garanzia che il procedimento assicura al cittadino»[149].

Pertanto, una volta preso atto del ruolo di assoluto protagonista assunto dall'illecito amministrativo nella repressione degli abusi di mercato (anche in relazione alle cripto-attività soggette al MiCAR), non può che auspicarsi l'introduzione, per mano del legislatore, di un apparato di salvaguardie di tipo procedimentale *ad hoc*. Queste ultime non devono essere per forza mutuate *in toto* da quelle vigenti in materia penalistica, ma vanno costruite tenendo comunque conto della particolare fisionomia e gravità delle sanzioni irrogabili – che seppur non privano gli individui della libertà personale, possono avere una portata economico e interdittiva di enorme afflittività – dei destinatari di tali sanzioni (principalmente enti e persone giuridiche) e delle peculiarità del sistema in cui esse sono chiamate ad operare[150].

---

para-penale: il concorso mediante omissione dei sindaci nell'illecito amministrativo di manipolazione del mercato ex art. 187 ter Tuf, in *SP* 15.3.2024.

[147] Così F. Consulich, *Manipolazione del mercato e declino del sistema finanziario,* cit., 15, secondo cui il mancato riconoscimento della *BARD* rule costituirebbe, per lo meno sul versante sostanziale, «l'ultimo criterio differenziale, in termini di garanzia, tra sanzioni penali ed amministrative punitive». Nella direzione del riconoscimento del canone dell'oltre ogni ragionevole dubbio nei procedimenti amministrativi di carattere punitivo-afflittivo sembra muoversi una recente sentenza del Consiglio di Stato in materia di Antitrust, la quale – dopo aver ribadito la natura «penale in senso convenzionale delle sanzioni irrogate dall'Autorità indipendente» – ha affermato che «qualora sussista un dubbio nella mente del giudice» in merito all'esistenza degli elementi idonei a dimostrare l'esistenza degli elementi costitutivi che integrano l'infrazione, «esso deve andare a beneficio» del destinatario «della decisione che constata un'infrazione». Cfr. C.st. 9.5.2022 n. 3570, in *www.giustizia-amministrativa.it*.

[148] V., ad esempio, C.eur. 6.12.2022, *Kerimoğlu v. Turkey*, § 67.

[149] Così L. Lucchini, *Elementi di procedura penale*, Firenze 1895, 15.

[150] Ove, come visto, un ruolo chiave – anche sul piano della prevenzione e repressione degli abusi – è riservato alle autorità competenti e all'autoregolamentazione degli operatori del mercato.

6. Come si è cercato di mettere in luce, l'approvazione del MiCAR e il suo recepimento nell'ordinamento italiano, a opera del d.lgs. 129/2024, rappresentano uno snodo importante nella regolamentazione del mercato delle cripto-attività. Benché la normativa di nuovo conio susciti alcune perplessità sul versante della tecnica legislativa adottata, specie con riguardo all'individuazione dell'ambito applicativo, essa si fa comunque nel complesso apprezzare per il tentativo di disciplinare fenomeni complessi e forieri di rischi eccessivi per la stabilità del mercato e per gli investitori.

Per di più, come si è avuto modo di vedere, il nuovo apparato normativo produce effetti positivi anche sul versante della giustizia penale e del diritto amministrativo-punitivo. È ben vero che la tipizzazione di nuove figure di illecito che reprimessero le violazioni del MiCAR costituiva una scelta per molti versi obbligata per il nostro legislatore, il quale era tenuto a conformare la normativa interna alle prescrizioni dell'art. 111 del Regolamento. Nondimeno, è di intuitiva evidenza che la predisposizione di adeguati strumenti sanzionatori risulti un presidio chiave per tutelare il virtuoso funzionamento dell'intero sistema delle cripto-attività delineato in sede euro-unitaria. Solo in questo modo era, infatti, possibile garantire effettività, a monte, all'intera disciplina, riducendo i rischi di condotte patologiche.

Se ciò è vero, alla luce di quanto affermato nei precedenti paragrafi, il giudizio sulla bontà della scelta, operata dal d.lgs. in commento, di ridurre al minimo il ricorso allo *ius terribile* in favore dell'illecito amministrativo punitivo, seppur astrattamente condivisibile, non può, tuttavia, che lasciare il sapore di una parziale occasione perduta. Da una parte, una simile opzione appare coerente con le recenti strategie di contrasto alla criminalità economica e finanziaria, e comporta un indubbio guadagno in termini di efficienza e di celerità; dall'altra, però, i vantaggi sul piano preventivo e punitivo non sembrano oggi accompagnati da un soddisfacente apparato di garanzie operanti nei confronti dei soggetti sottoposti a tali sanzioni, di natura formalmente amministrativa, ma, di fatto, sostanzialmente penali.

Giunti a questo punto, occorre più in generale riconoscere come, tanto il MiCAR, quanto la corposa disciplina antiriciclaggio approvata dall'Unione in questo settore, non possano essere considerati dei punti d'arrivo, ma solo i primi passi di un percorso che deve essere necessariamente più ampio e ambizioso. Onde contrastare in modo efficace i traffici illeciti che abbiano a oggetto cripto-attività è, invero, indispensabile focalizzare l'attenzione su profili ancora oggi non sufficientemente esplorati, come

quelli legati, per un verso, ai rischi specifici determinati dal funzionamento delle tecnologie basate sul registro distribuito [151], e, per un altro, alle peculiarità che caratterizzano le investigazioni in questo settore.

Da tale seconda prospettiva, l'esperienza insegna, infatti, che l'attività di contrasto alla criminalità che abbia a oggetto *cripto-assets*, oltre a presentare il più delle volte una spiccata matrice transazionale (il che, data la volatilità e la rapidità delle transazioni, richiederebbe di predisporre strumenti di cooperazione di polizia e giudiziaria *ad hoc*, in grado di consentire uno scambio di informazioni e di dati estremamente rapido[152]), si fondano sull'impiego incrociato di plurimi atti di indagine tecnologici specifici, particolarmente avanzati[153]. Si allude, sia a forme eterogenee di raccolte massive di dati da fonti aperte (c.d. OSINT) e – in particolare – da *social network* (c.d. SOCMIT), sia – e soprattutto – all'utilizzo di algoritmi di analisi della *blockchain* (c.d. *blockchain analysis*) [154], i quali si sono dimostrati con il tempo ausili essenziali per gli investigatori nel difficile compito di ricostruire le transazioni e di deanonimizzarle.

Ma vi è di più: un altro settore particolarmente delicato, con riferimento al quale ci sono state finora solo timide aperture a livello di disciplina positiva europea[155], è quello dei sequestri e delle confische dei *crypto-assets*[156]. Come è stato messo in luce finanche nell'ambito del Fondo Monetario Internazionale, il fenomeno in esame «*require adjusting some legal requirements and practices (e.g., freezing/seizing orders to be*

[151] Si pensi, ad esempio, ai rischi determinati dal fatto che questi strumenti possono operare in modo del tutto decentralizzato, i quali richiedono di adottare delle strategie di contrasto *ad hoc*. Si veda, al riguardo, G. Soana, *op. cit*., 218 ss. il quale giustamente rileva come negli atti più recenti (e, in particolare, con il regolamento *Travel rule*) il legislatore europeo si stia sempre più rendendo conto di ciò, avendo perché inaugurato una terza fase di regolamentazione del fenomeno in esame.

[152] È questo, del resto, l'auspicio manifestato dagli stessi appartenenti alle forze dell'ordine che quotidianamente sono impegnati nell'attività di contrasto a questo tipo di criminalità: v. V. Giordano, *L'attività della Guardia di Finanza nell'ambito del sistema antiriciclaggio ed il contrasto all'utilizzo dei* cryptoassets *per finalità illecite*, in *Riv. della Guardia di Finanza*, 2022, 512.

[153] Per una panoramica analitica sul punto, v. N. Furneaux, *There's No Such Thing as Crypto Crime. An Investigative Handbook*, Chichester 2025, in particolare 109 ss.

[154] Per un'ampia disamina di tali strumenti, v. D. Carlisle, *op. cit*., 63 s.; A. Balaskas e V.N.L. Franqueira, *Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges*, in *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Glasgow, UK, 2018, pp. 1-8; N. Furneaux, *op. ult. cit*., 125 ss.; G. Soana, *op. cit*., 224 ss.; C. Pelker Alden, C. Brown e R. Tucker, *Using Blockchain Analysis from Investigation to Trial*, in *Department of Justice Journal of Federal Law and Practice*, 2021, 59–100.

[155] Il riferimento va alla direttiva 2024/1260/UE, la quale menziona esplicitamente le cripto-attività nel suo ambito operativo.

[156] Per un'ampia disamina della tematica, cfr. N. Furneaux, *op. cit*., 445 s.

issued by a court)»[157], onde consentire di realizzare un'attività di prevenzione e di repressione efficiente. Ciò si deve al fatto che la procedura volta all'ablazione di questa categoria di beni è caratterizzata da molteplici complessità di ordine tecnico, frutto della loro natura immateriale e volatile[158].

Tutto ciò fa comprendere, da un'ulteriore angolazione, come le forme di criminalità in cui vengano in rilievo *crypto-asset* pongano sfide tanto complesse ai sistemi di giustizia penale contemporanei, da obbligare gli stessi ad assumere un atteggiamento proattivo, teso ad aggiornare progressivamente i propri ecosistemi normativi e operativi onde cercare di affrontarle[159]. Purtroppo, va ammesso come l'ordinamento italiano presenti, per parte sua, ancora vistose criticità a questo riguardo. Se, infatti, per quanto concerne il piano sostanziale, anche grazie al provvedimento in commento, alcuni passi avanti sono stati fatti, sul piano processuale non si possono che denunciare, anzitutto, le gravi lacune che affliggono il codice di rito per quanto concerne i mezzi di ricerca della prova ad alto contenuto tecnologico. Non è un mistero, del resto, come, pur a fronte delle oramai continue censure della dottrina[160],

[157] Così si esprime, testualmente, il report del Fondo monetario internazionale, redatto N. Schwarz (e altri), *Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations*, in *FinTech Notes* No 2021/002.

[158] Si considerino, solo per fare alcuni esempi, le difficoltà nell'individuare e nell'apprendere la chiave privata, necessaria onde poter trasferire i fondi presenti nel *wallet* oggetto di sequestro. Specie nel caso di un *hardware wallet*, poiché la *password* è conservata all'interno di un dispositivo digitale fisico (si pensi a Ledger o Trezor), la sua apprensione presuppone la conoscenza del *pin* di sblocco del predetto *device*. Ma non è tutto. Pure qualora l'autorità inquirente riesca ad ottenere la disponibilità della chiave privata, l'indagato – o un suo complice – potrebbe aver copiato e archiviato (in formato digitale o cartaceo) siffatta *password*, potendo così accedere da remoto al *wallet* e trasferire il "denaro" *ivi* presente. Inoltre, l'utilizzo del cd. *backup recovery seed*, consentendo al titolare del *wallet* di recuperare in ogni momento la disponibilità delle somme, potrebbe eludere il vincolo reale (solo apparente) imposto sul bene. Ed è proprio per fugare l'insieme di questi pericoli che le più avanzate linee guida sviluppatesi in materia a livello internazionale (cfr., ad esempio, iPROCEEDS-2, *Guide on seizing cryptocurrencies,* 23 s. e GAFILAT, *Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Asset,* December 2021, 104) suggeriscono, in linea di principio, di trasferire la somma da congelare su un *wallet* "statale", posto sotto controllo dell'autorità di *law enforcement*. Per una panoramica operativa delle tecniche da seguire per sequestrare efficacemente le cripto-attività, cfr. N. Furneaux, *op. cit*., 445 s.,nonché A. Owen, M. Nizzero e A. Larkin, *Seizing Crypto: When Asset Recovery Goes Digital*, in *www.rusi.org* 13.6.2024.

[159] Cfr., al riguardo, le articolate raccomandazioni approvate nel 2024 da Europol e dal Basel Institute on Governance, *A race against time: Europol – Basel Institute on Governance recommendations on preventing and combating the criminal use of cryptocurrencies*, in *baselgovernance.org*.

[160] In generale, sulla necessità di un intervento legislativo volto a regolamentare queste nuove strumentazioni investigative, v., pur con differenti prospettive di riforma, M. Gialuz, *Premessa*, in *Le nuove intercettazioni. Legge 28 febbraio 2020 n. 7*, in *Dir. di internet* 2020, Supplemento al n. 3, 7; S. Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *CP* 2015, 789 ss.; M. Miraglia, *Il* "Trojan *(non) di Stato": una disciplina da completare*, in *PPG* 2023, 1227 ss.; F. Nicolicchia, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*,

il nostro ordinamento continui a non disciplinare un ampio novero di forme di *digital investigations* oggi essenziali per il contrasto alla criminalità (basti pensare al pedinamento GPS, alle videoriprese investigative, al *virus trojan* impiegato in modalità diversa rispetto alla semplice captazione ambientale o al sequestro di *device*[161]), tra cui vanno annoverati anche gli strumenti sopra menzionati dell'OSINT e della *blockchain analysis*. Per di più, va rilevato come il legislatore nostrano, a differenza di quello di altri Paesi[162], non abbia, finora, dettato neppure previsioni *ad hoc* in materia di sequestri e confische di cripto-attività, facendo così sorgere delicate problematiche applicative[163]. Ed è chiaro che, per evitare che l'arretratezza complessiva del tessuto codicistico sul punto finisca per determinare frutti avvelenati sempre maggiori, tanto per quanto concerne l'efficienza delle indagini, quanto – e soprattutto – per il rispetto dei diritti fondamentali della persona, si rende necessario un netto cambio di passo.

Fenomeni come quello della criminalità sulla *blockchain* dimostrano, insomma, come sia indispensabile aprire al più presto un ambizioso cantiere di riforma dedicato al rapporto tra giustizia penale e nuove tecnologie. Solo così si potrà sperare di stare al passo delle organizzazioni criminali, evitando che continui a concretizzarsi quanto preconizzato, sul finire del secolo scorso, dai più cupi manifesti *Cypherpunk*, ovverosia che uno spettro continui a infestare «*the modern world, the specter of crypto anarchy*»[164].

Milano 2020, *passim*; W. Nocerino, *Il captatore informatico nelle indagini penali interne e transfrontaliere*, Milano 2021, 317 ss.; e, volendo, J. Della Torre, A. Malacarne, *L'utilizzo dei* file di log *per scopi di contrasto alla criminalità: nodi problematici e possibili soluzioni*, in *AP* 3/2023.

[161] È noto, peraltro, come almeno a questo riguardo è stata approvato lo scorso anno dal Senato il ddl 806, sul sequestro di dispositivi, sistemi informatici o memorie digitali. Per un commento, cfr. A. Chelo, *Tanto tuonò che piovve: il nuovo sequestro di dispositivi informatici*, in *PenaleDP* 2024; S. De Flammeis, Le *sfide della prova digitale: sequestri, chat, processo penale telematico e intelligenza artificiale*, in *SP* 7.3.2024; O. Murro, *Lo smartphone come fonte di prova. Dal sequestro del dispositivo all'analisi dei dati*, Milano 2024.

[162] Il Regno Unito, ad esempio, ha adottato un ampio *corpus* normativo sul punto a seguito dell'approvazione dell'*Economic Crime and Corporate Transparency Act* (2023).

[163] Per un quadro di sintesi degli stessi, cfr. M. Antinucci e D. Scampoli, *Il sequestro e la confisca di bitcoin*, in *DPP* 2024, 1083; F. Cajani, *Sequestri di* files *e* Bitcoin: *i riflessi della dematerializzazione di beni e valute sulla disciplina penal-processualistica italiana*, *ivi* 2021, 742; P. Dal Checco, *Sequestro e confisca: tecnica e procedura*, in *Criptoattività, criptovalute e* Bitcoin, a cura di S. Capaccioli, Milano 2021, 329; R. Lupo, *Quale sequestro per le criptovalute?*, in *ilCentuaro* 2020, 50 ss.

[164] *The Crypto Anarchist Manifesto*, in https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html.