LA TUTELA PENALE DEL MERCATO DELLE CRIPTOATTIVITÀ. TRA PUNTI FERMI E INCERTEZZE

di Gabriele Ponteprino
(*Dottore di ricerca in diritto penale, Università di Genova*)

A fronte dei noti rischi criminogeni derivanti dall'impiego delle criptoattività, la relazione ripercorre sinteticamente gli sviluppi legislativi e giurisprudenziali in ambito penalistico. Il quadro che emerge, in via di progressiva definizione, presenta non irrilevanti profili di criticità sul piano della tenuta dei fondamentali principi garantistici previsti dalla Costituzione.
The paper examines the main legislative and judicial developments concerning the criminal law implications of crypto-assets. The emerging framework, progressively shaped through statutory intervention and judicial interpretation, raises significant concerns regarding the preservation of the fundamental guarantees of criminal law.

Criptoattività, criptovalute, riciclaggio, abusi di mercato
Crypto-assets, crypto-currencies, money laundering, market abuse

Sommario: 1. Premessa. – 2. L'evoluzione normativa: un processo in costante evoluzione. – 3. Gli sviluppi della giurisprudenza in materia di abusivismo finanziario. – 4. La disciplina sanzionatoria del MiCAR: il nuovo delitto di abusivismo in criptoattività. – 5. Il sistema amministrativo punitivo. – 5.1. … qualche spunto critico sul ricorso alla via amministrativa.

1. In questa relazione intendo fornire un sintetico quadro delle novità introdotte sul versante del diritto penale sostanziale per fare fronte ai diffusi rischi di un impiego criminogeno di criptovalute e, più in generale, di criptoattività.

Da un lato, la giurisprudenza nazionale ha fatto ricorso a figure delittuose già esistenti, declinandole in contesti del tutto nuovi, operazione che ha reso necessarie inevitabili forzature ermeneutiche di dubbia compatibilità con il dato legale. Dall'altro lato, le scelte attuate dal legislatore interno sul versante penale e sul versante amministrativo-punitivo sono volte, nel complesso, a recepire – talora supinamente – le prescrizioni di diritto eurounitario.

È venuto così a delinearsi un quadro normativo orientato a una forte anticipazione della tutela, che pone non pochi dubbi di compatibilità con i fondamentali presidi garantistici vigenti in materia penale[1].

* Il presente lavoro è inserito nell'ambito del progetto CRYPTOSAFE (Towards a Safe Seizure and Confiscation of Crypto-Assets in Criminal Proceedings), Project Code P2022HW85A, CUP D53D23022280001 e costituisce la versione aggiornata e arricchita di note dell'intervento tenuto al Convegno finale del PRIN 2022 PNRR CRYPTOSAFE svoltosi presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Genova il 12 febbraio 2026.

[1] Più ampi rilievi sul punto in: J. Della Torre, *Cripto-attività e giustizia penale*, Padova 2026; G. Soana, *The anti-*

Di seguito, ripercorrerò cursoriamente le principali tappe di un'evoluzione siffatta, tentando di mettere in luce le maggiori criticità di tale disciplina sul piano operativo e della tenuta dei principi di garanzia vigenti in materia penale.

2. Con l'inaspettata esplosione, negli anni Duemiladieci, del mercato delle criptovalute – *in primis* del bitcoin – e il crescente ricorso alla tecnologia *blockchain* si è registrato un *fisiologico* vuoto normativo. Il protrarsi – per lungo tempo e a ogni latitudine – di tale condizione di latitanza della legge ha ineluttabilmente favorito incontrollabili «cavalcate speculative e crac miliardari» con gravi pregiudizi a danno di «miriadi di sprovveduti investitori»[2].

Calzante è dunque il parallelismo con il vecchio *west*, la sfrenata corsa all'ora e gli assalti alle diligenze da parte di spregiudicati banditi[3]. Il carattere pseudo-anonimo, la rapidità di circolazione, la collocazione al di fuori dei tradizionali circuiti finanziari e la tendenziale mancanza di un'autorità centrale deputata al controllo del mercato hanno infatti reso le valute virtuali entità opache e spesso inafferrabili. La naturale conseguenza è stata un loro frequente impiego criminogeno, come dimostrano autorevoli *Report* di settore[4], dalla consultazione dei quali emerge che le criptovalute rappresentano un formidabile strumento di riciclaggio e autoriciclaggio di proventi delittuosi[5], senza considerare il loro utilizzo in operazioni sul *dark web* o in altre

money laundering regulation of crypto-assets in Europe, Milano 2024; R.M. Vadalà, *La fattispecie penale tra economia digitale e diritto europeo*, Torino 2025; A. Gullo, G. Ardizzone, *Profili penalistici delle criptovalute*, in www.lalegislazionepenale.eu, 23.5.2026.

[2] A. Galimberti, *Cripto, finisce l'era dell'anonimato e del nero (e forse anche quella dei crac)*, in *www.ilsole24ore.com*, 7.9.2024.

[3] Metafora coniata da 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 *GC* 2022, 929 ss.

[4] Il rinvio è al *Report* del 2025 di Chainalysis, *The 2025 Crypto Crime Report. The rising role of cryptocurrency in all forms of crime and how its transparency is creating unique opportunities for investigation*, in *www.chainalysis.com*, 15.1.2025, stando al quale nel 2024 gli *asset* legati a traffici illeciti avrebbero un valore di oltre 51 miliardi di dollari.

[5] Si rimanda alla monografia di G.J. Sicignano, *Bitcoin e riciclaggio*, Torino, 2019; M. Giuca, *Criptovalute e diritto penale nella prevenzione e repressione del riciclaggio*, in *DPenCont-Riv. trim.* 1/2021, 151 ss. Segnalo incidentalmente che il contrasto al riciclaggio per mezzo di criptovalute costituisce una assoluta priorità a livello europeo: lo dimostra il recente *AML Package* (approvato il 19.6.2024 e destinato a divenire completamente operativo entro il 2029), che si compone della VI Direttiva antiriciclaggio (Dir. 2024/1640/UE), del Regolamento antiriciclaggio (Reg. 1624/2024/UE, c.d. *single rulebook)* e del Regolamento AMLA (Reg. 1620/2024/UE), che istituisce l'Autorità per la lotta al riciclaggio e al finanziamento del terrorismo. La l. 13.6.2025 n. 91 (la legge di delegazione europea) ha delegato il Governo all'attuazione degli atti che compongono l'*AML Package*. Sul punto, J. Della Torre, *Cripto-attività e giustizia penale*, cit., 225; R. Razzante, *Antiriciclaggio: in arrivo Sesta direttiva e codice unico europeo*, in *www.ipsoa.it*, 1.2.2024; V. Capuano, *AML Package: prime considerazioni sui profili*

attività illecite[6].

Alla luce di questo allarmante quadro, molto si è discusso intorno alla possibilità di ricomprendere le valute virtuali entro categorie giuridiche note, così da assicurare una qualche tutela avverso il loro patologico utilizzo[7].

D'altro canto, dinnanzi all'esponenziale crescita del mercato cripto valutario, il vuoto normativo è stato via via colmato a partire dal 2017, prendendo le mosse dal settore dell'antiriciclaggio. È in tale contesto che il legislatore italiano, con una inusuale solerzia, ha introdotto – per mezzo del d.lgs. 25.5.2017 n. 90 – una prima embrionale definizione del concetto di valuta virtuale[8], poi precisata ulteriormente dal d.lgs. 4.10.2019[9] e, infine, sostituita dal riferimento alle cripto-attività (d.lgs. 27.12.2024 n. 204), nozione generica in cui sono ricompresi i diversi modelli oggi osservabili sul mercato che utilizzano la tecnologia a registro distribuito[10]. In questo modo, gli obblighi AML previsti dal 21.11.2007 n. 231 sono stati progressivamente estesi ai prestatori di servizi di criptoattività (*exchangers* e *wallet providers*).

---

sostanziali e formali della nuova disciplina antiriciclaggio dell'UE, in *Riv. reg. mer.* 2024, 501 ss.; I. Borrello, *Il nuovo ordinamento antiriciclaggio europeo*, in *Giorn. dir. amm.* 1/2025, 47 ss.

[6] Sui rischi delittuosi legati all'impiego di cripto-attività, si veda anche il recente *Avviso ai consumatori rivolto da EBA (Autorità bancaria europea), ESMA (Autorità europea degli strumenti finanziari e dei mercati) ed EIOPA (Autorità europea delle assicurazioni e delle pensioni aziendali o professionali),* pubblicato il 6.10.2025 in *www.eiopa.europa.eu*. Per una panoramica dei possibili reati realizzabili mediante il ricorso a criptovalute, si legga il Report di *Europol, Cryptocurrencies: tracing the evolution of Criminal finances*, in *www.europol.europa.eu*, 26.1.2022. In dottrina, v. A. Rosato, *Profili penali delle criptovalute*, Pisa 2021; M. Naddeo, *Criptovalute: profili di rilevanza penale*, in *PenaleDP* 2022; L. Picotti, *Profili penali del Cyberlaundering: le nuove tecniche di riciclaggio*, in *RivTrim-DPenEc.* 2018, 1121 ss.

[7] A. Frattolillo, *Giurisprudenza domestica in materia di criptovalute*, in *Contratti* 2024, 56 ss.

[8] Si veda l'art. 1, co. 2, lett. *qq* del d.lgs. n. 90/2017, che definisce come tale la «rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'Autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente».

[9] Cfr. G.P. Accini, *Cybersecurity e criptovalute. Profili di rilevanza penale dopo la Quinta Direttiva*, in *SP* 15.5.2020; con particolare riguardo all'adattamento dei presidi antiriciclaggio all'evoluzione del mercato delle criptovalute, M. Croce, *Cyberlaundering e valute virtuali. La lotta al riciclaggio nell'era della distributed economy*, in *SP* 27.4.2021. Da ricordare, inoltre, che l'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».

[10] Cfr. P. Carrière, *Cripto-attività quali rappresentazioni "originarie" o "derivative". Profili di diritto societario e dei mercati finanziari*, in *Tokenizzazione di azioni e azioni tokens-Quaderni Giuridici Consob,* a cura di P. Carrière, N. De Luca, M. De Mari, G. Gasparri, T.N. Poli (a cura di), 25.1.2023, 49.

3. Se dunque il legislatore nazionale e quello eurounitario hanno da tempo provveduto a delineare un quadro normativo (sia pur in costante evoluzione) volto a prevenire e reprimere i fenomeni di riciclaggio per mezzo del ricorso a criptovalute, prima dell'entrata in vigore del Regolamento MICA (il Reg. n. 1114/2023/UE, sui mercati delle cripto-attività) e del relativo decreto di recepimento (il d.lgs. n. 129/2024), non vie era alcuna disciplina che regolamentasse le modalità di emissione, di offerta al pubblico, di negoziazione e la prestazione di servizi per le criptoattività.

Il perdurante silenzio della legge non ha fatto che alimentare incertezze in merito all'inafferrabile natura delle criptovalute. Si tratta di strumenti refrattari ad un'univoca collocazione giuridica, che, a seconda del contesto, possono assolvere le funzioni più disparate: da una parte, esse si prestano a soddisfare esigenze di pagamento – venendo parzialmente assimilate alla moneta *fiat* –, dall'altra, è ipotizzabile un loro impiego con finalità di investimento, laddove siano ricomprese in determinati schemi contrattuali[11].

Ed ecco, allora, che la giurisprudenza si è presto interrogata in merito alla riconducibilità delle *cryptocurrencies* nel novero degli strumenti o dei prodotti finanziari. Da un tale inquadramento dipende, infatti, l'assoggettamento dei prestatori di servizi agli adempimenti autorizzativi previsti dal TUF (il d.lgs. 24.2.1998 n. 58), la cui inottemperanza integra, tra l'altro, gli estremi del delitto di abusivismo finanziario cui all'art. 166 TUF[12].

A questo proposito, nonostante alcune pronunce (e delibere Consob) qualificassero le criptovalute come strumenti finanziari[13], l'orientamento prevalente riteneva invece che, a determinate condizioni, esse andassero ricomprese nell'onnivora categoria dei prodotti finanziari (cfr. art. 1, comma 1, lett. u, T.U.F.)[14]. Di conseguenza, al cospetto di

[11] Sull'attitudine ambivalente delle criptovalute, M. De Mari, G. Gasparri, T.N. Poli, *Introduzione: DLT e cripto-attività*, in *Tokenizzazione*, cit., 24.

[12] La questione viene affrontata, tra gli altri, da: 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 ss.; 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* 21.9.2021, 55 s.; volendo, G. Ponteprino, *Autoriciclaggio e (in)sussistenza del reato presupposto. il riflesso dell'incerta evoluzione normativa in materia di criptoattività*, in *DPP* 2026, 77 ss.

[13] Cfr. Trib. Verona 24.1.2017 n. 195, commentata da M. Passeretta, *Bitcoin: il leading case italiano*, in *BBTC* 2017, 471 ss.; Consob, Delibera n. 20346 del 21.3.2018, in *www.consob.it*; Consob, Delibera n. 20693 del 14.11.2018, *ivi*; Consob, Delibera n. 20536 del 25.7.2017, *ivi.* Nella giurisprudenza di legittimità: Cass. 17.9.2020 n. 26807, in *www.onelegale.wolterskluwer.it*, che invero si limitava ad affermare che, nel caso di specie, la vendita di *bitcoin* veniva reclamizzata «come una vera e propria proposta di investimento», senza però chiarire se le criptovalute fossero veri e propri strumenti finanziari. Incidentalmente, Cass. 29.5.2025 n. 20138, in *www.onelegale.wolterskluwer.it.*

[14] Cass. 30.11.2021 n. 44337, commentata da A. Quattrocchi, *La natura proteiforme delle criptovalute al crocevia*

operazioni poste in essere violando la disciplina del TUF, avrebbe dovuto concludersi per la sussistenza del delitto previsto dall'art. 166 co. 1 lett. *c*, che incrimina chiunque, senza la necessaria abilitazione, «offre fuori sede, ovvero promuove o colloca mediante tecniche di comunicazione a distanza» sia gli «strumenti finanziari o i servizi o attività di investimento» sia appunto i «prodotti finanziari».

In una prospettiva siffatta, a rilevare erano unicamente la pubblicità e la finanziarietà della proposta di investimento, elementi che si ricavano guardando alla causa concreta del negozio. Ragione per cui, qualora fosse emerso che l'operazione *sub judice* aveva comportato «a) un impiego di capitali, riconducibile generalmente al danaro o, più in generale, a un capitale proprio che può corrispondere anche a una valuta virtuale, b) una aspettativa di rendimento, e c) un rischio proprio dell'attività prescelta, direttamente correlato all'impiego di capitali», ci saremmo trovati dinnanzi a un investimento di natura finanziaria, soggetto alla disciplina del TUF. Le criptovalute avrebbero, pertanto, dovuto essere considerate alla stregua di prodotti finanziari e la relativa attività di reclamizzazione avrebbe costituito una proposta di investimento soggetta agli obblighi informativi di cui all'art. 91 TUF, la cui dolosa omissione è riportabile nell'orizzonte applicativo dell'art. 166 TUF[15].

L'uso del tempo passato non è casuale.

Difatti, dal recepimento nell'ordinamento interno della nuova e più ampia definizione di strumento finanziario fornita dal Regolamento (UE) n. 858/2022 – che a sua volta è intervenuto sulla Direttiva 2014/65 (c.d. Mifid II) – è scaturita una modifica dell'art. 1 comma 2 del TUF[16], tesa a includere nel catalogo degli strumenti finanziari

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.*

[15] Cfr. Cass. 30.11.2021 n. 44337, cit.; Cass. 26.10.2022 n. 44378, cit. Un approccio teso a valorizzare le concrete modalità di svolgimento della singola operazione piuttosto che l'intrinseca natura delle criptovalute viene adottato anche dalla Consob, la quale, negli ultimi anni, in forza dei poteri attribuitele 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*, riconoscendo la loro natura finanziaria ogniqualvolta «implichino l'impiego di capitale, la promessa/aspettativa di rendimento e l'assunzione di un rischio direttamente connesso e correlato all'impiego di capitale». *Ex plurimis*: Consob, Delibera n. 23008 del 14.2.2024, in *www.consob.it*.

[16] Segnatamente, l'art. 1 comma 2 stabilisce che «per strumento finanziario si intende qualsiasi strumento riportato nella Sezione C dell'Allegato I, compresi gli strumenti emessi mediante tecnologia a registro distribuito. Gli strumenti di pagamento non sono strumenti finanziari». Cfr. le modifiche introdotte dal d.l. 30.3.2023 n. 25, convertito nella l. 10.5.2023 n. 52.

anche quelli emessi mediante tecnologia a registro distribuito che non siano strumenti di pagamento e, dunque, talune tipologie di cripto-attività[17].

Specularmente, l'art. 2, par. 2 del MiCAR esclude l'operatività di quest'ultimo regolamento innanzi a 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»[18].

Si tratta di un quadro assai complesso, destinato a porre non pochi problemi interpretativi. Sebbene infatti il legislatore abbia preso atto delle variegate e proteiforme fisionomia delle criptoattività – che rende francamente inipotizzabile una loro riduzione a denominatore comune – residuano tuttavia notevoli difficoltà nello stabilire se un certo *assets* possa ritenersi uno strumento finanziario – soggetto alla normativa TUF (ed agli obblighi autorizzativi la cui violazione integra gli estremi dell'art. 166) – o se rientri piuttosto nell'ambito MiCAR (ed agli obblighi autorizzativi la cui violazione integra gli estremi del neo-introdotto delitto di abusivismo in cripto-attività di cui all'art. 30 del d.lgs. 129/2024)[19].

4. Consideriamo ora più da vicino il sistema di sanzioni penali e amministrative introdotto dal d.lgs. 129/2024, che, come noto, è posto a presidio del rispetto degli obblighi di trasparenza e informazione dettati dal MiCAR con riguardo all'emissione, all'offerta al pubblico e alla negoziazione di criptoattività diverse dagli strumenti finanziari. Il precipuo scopo di una tale disciplina – che parzialmente ricalca quella del TUF – è garantire un'adeguata protezione e vigilanza di un mercato in costante

[17] Come già ipotizzato F. Consulich, *Nella* wunderkammer, cit., 158.

[18] Sui problemi derivanti dall'introduzione di siffatta disciplina: I. D'Ambrosio, *La regolamentazione delle cripto-attività tra Decreto Fintech e regolamento MiCA*, in *Riv. dir. banc.* 2024, 812 ss.; L. Di Stefano, A. Di Giorgio, R. Ferretti, Criptovalute e moneta elettronica: tra distinzioni necessarie e rilevanza penale, in *Riv. dir. banc*. 2024; sia consentito inoltre il rinvio a: J. Della Torre, G. Ponteprino, *Commento al d.lgs. 129 del 2024 di attuazione del regolamento UE sui mercati delle cripto-attività. Le novità sul versante penalistico e amministrativo punitivo*, in www.lalegislazionepenale.eu, 18.2.2025, 35 ss.

[19] Sulla di natura finanziaria o meno delle criptoattività: F. Annunziata, *Cripto-attività e strumenti finanziari: le Linee guida dell'ESMA*, in *Riv. dir. banc.* 8.1.2025; M. Cian, *Noterelle su finanziarietà e non finanziarietà nei "crypto-assets": la Suprema Corte sulla natura del servizio di "exchange",* in *BBTC* 2023, 1 ss. A fronte di tale problematico inquadramento, anche il MiCAR, al Considerando 14, auspicava l'emanazione di «orientamenti sui criteri e sulle condizioni per la qualificazione delle cripto-attività come strumenti finanziari». A ciò ha in effetti provveduto l'ESMA, con l'elaborazione delle *Guidelines on the conditions and criteria for the qualification of cryptoassets as financial instruments* del 17.12.2024 (consultabili, nella versione italiana, su *www.esma.europa.eu*), che non hanno tuttavia fugato criticità e incertezze.

crescita, tutelare la libera e leale concorrenza e quindi anche il patrimonio degli investitori.

Sul versante repressivo, il legislatore italiano ha optato per un limitatissimo ricorso al diritto penale, privilegiando l'illecito amministrativo punitivo, che – in contesti ad elevata complessità tecnica – risulta «più graduabile ed efficace» rispetto allo *ius terribile*[20]. Il d.lgs. 129/2024 si è infatti limitato a introdurre, all'art. 30, una nuova figura delittuosa – meglio, una fattispecie a più norme – in cui vengono punite, con la reclusione da sei mesi a quattro anni (oltreché la multa)[21], talune forme di abusivismo relative ai *token* collegati ad attività e ai *token* di moneta elettronica – come l'emissione, l'offerta al pubblico, la richiesta e l'ottenimento dell'ammissione alla negoziazione non autorizzate – nonché l'abusiva prestazione di servizi in relazione a tutte le tipologie di cripto-attività rientranti nel MiCAR.

Siamo al cospetto di reati di pericolo presunto[22], che realizzano una notevole anticipazione della soglia del penalmente rilevante, in quanto sono posti a presidio di una mera funzione, ossia il meccanismo di regolazione e controllo del mercato delle criptoattività. In via mediata, poi, essi tutelano anche il patrimonio dei privati investitori, che potrebbero essere potenzialmente pregiudicati dall'azione di professionisti che si sottraggano deliberatamente al severo regime autorizzativo dettato dal MiCAR.

In ottemperanza alle indicazioni eurounitarie, il legislatore italiano ha ravvisato la necessità di neutralizzare in radice le «situazioni disfunzionali»[23]. Esso ha dunque

---

[20] Su pregi e limiti del ricorso al diritto amministrativo punitivo, con particolare riguardo alla tutela dei mercati finanziari: A. Tripodi, *Gli illeciti amministrativi in tema di abusi di mercato*, in *Reati in materia bancaria e finanziaria*, a cura di A. Alessandri, *Trattato teorico pratico di diritto penale*, diretto da F. Palazzo, C.E. Paliero, VIII, Torino 2017, 232 ss.; 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, 12 ss. In precedenza, la questione è stata tematizzata da: C.E. Paliero, *La sanzione amministrativa come moderno strumento di lotta alla criminalità economica*, in *RivTrim-DPenEc.* 1993, 1027 ss.

[21] La cornice edittale è analoga a quella prevista per il delitto di abusivismo bancario *ex* artt. 131 ss. TUB e leggermente meno elevata rispetto a quella del reato di abusivismo finanziario di cui all'art. 166 del TUF, ove la pena va da uno a sei anni di reclusione.

[22] Così, in relazione al similare art. 166 TUF, la granitica giurisprudenza e la prevalente dottrina: Cfr. Cass. 23.5.2025 n. 23654; Cass. 9.12.2024 n. 45014, in *www.onelegale.wolterskluwer.it*; 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.

[23] Sulla necessità di anticipare la tutela penale al cospetto di insidiose forme di criminalità economica, v. già 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, nonché T. Padovani, *Diritto penale della prevenzione e mercato finanziario*, in *RIDPP* 1995, 644 s., a detta del quale il ricorso alle tradizionali fattispecie di danno (come il furto o la truffa) si rivelerebbe in tali contesti

ritenuto che l'abusivo esercizio di attività professionali richiamate a mezzo dei plurimi rinvii contenuti nell'art. 30 d.lgs. 129/2024 (condotte miste attive e omissive, ove al mancato rispetto degli obblighi ai quali è subordinata la concessione dell'autorizzazione per l'esercizio di una certa attività segue il suo effettivo svolgimento)[24] sia di per sé idoneo a compromettere la trasparenza e l'integrità del sistema, poiché pregiudica il regolare svolgimento delle operazioni e la fiducia dei privati investitori.

Del resto, la prospettiva accolta da MiCAR è quella di un controllo decentrato, che fa ricadere sui professionisti del settore una serie di obblighi comunicativi, autorizzativi e di controllo[25], nel complesso volti a prevenire la perpetrazione di possibili illeciti (manipolazioni di mercato, abuso e comunicazione illecita di informazioni privilegiati e così via).

La formulazione del delitto in parola, al pari di quella degli altri illeciti amministrativi punitivi tipizzati dal d.lgs. 129/2024, si distingue per un ampissimo impiego della tecnica del rinvio alla disciplina MiCAR, agli atti delegati, nonché alle norme tecniche di regolamentazione e attuazione elaborate dalle autorità di settore[26]. Una recente dottrina ha ricondotto siffatto fenomeno normativo alla categoria del «diritto penale permeabile», nella quale vengono ricomprese quelle tipologie delittuose che «in virtù del ricorso alle tecniche del rinvio e degli elementi normativi, sono "penetrat[e]" da concetti derivanti da discipline specialistiche anche di fonte sovranazionale»[27]. Questo genere di reati è insomma avvinto da un indissolubile legame con la disciplina extra-penale di riferimento, che contribuisce in maniera essenziale a definire i contenuti del precetto, al punto inficiare la sua stessa

---

del tutto inefficace, in quanto esse vengono in rilievo «nel momento in cui i buoi sono ormai fuggiti dalla stalla», producendo effetti spesso deflagranti.

[24] Analogamente all'art. 166 TUF, anche il delitto di cui all'art. 30 d.lgs. 129/2024 configura un reato omissivo mediante commissione, poiché il mancato rispetto dell'obbligo di richiedere l'autorizzazione all'organo competente integra gli estremi del tipo in tanto in quanto «si traduca nella violazione della condotta positiva, per la cui produzione quell'obbligo [...] era prescritto». Cfr. M. Mantovani, *L'esercizio di un'attività non autorizzata. Profili penali*, Torino 2003, 144.

[25] È del resto logico che in un settore in costante sviluppo, prima che legislatore e le competenti autorità di vigilanza, siano i gestori del mercato a poter assumere un ruolo chiave nella prevenzione dei possibili illeciti, innanzitutto predisponendo e aggiornando costantemente i *compliance programs*. Cfr. F. Consulich, *Manipolazione del mercato e declino del sistema finanziario*, cit., 18.

[26] 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.

[27] Il pensiero corre all'innovativa ricostruzione di R.M. Vadalà, *La fattispecie penale tra economia digitale e diritto europeo*, cit., 66.

«autonomia concettuale»[28]. In definitiva, si tratta, di norme penali in bianco, a cui va riconosciuta una funzione meramente sanzionatoria: tali fattispecie sono infatti sprovviste di un autonomo contenuto di disvalore, che può essere ricavato soltanto dalle norme regolative del mercato delle criptoattività[29].

Conscio che le implicazioni critiche derivanti dall'utilizzo di questa tecnica normativa (esattamente analoga a quella adottata nel contesto dei mercati finanziari) meriterebbero ben altro approfondimento, in questa relazione mi limito a sottolineare:

i) i rischi sul piano della tenuta del principio di legalità e le delicate questioni di diritto successorio che potrebbero derivare da – invero assai probabili – interpolazioni del Regolamento MiCA o degli atti delegati, destinate a incidere, in forza dei rinvii contenuti nell'art. 30, sulla delimitazione del perimetro operativo del tipo delittuoso;

ii) il *vulnus* recato alla conoscibilità e all'accessibilità della legge penale[30], che risulta di difficile lettura per gli stessi professionisti del settore, finendo con l'alimentare incertezze in un settore già di per sé caratterizzato da elevatissima complessità tecnica.

iii) la debolissima offensività del reato previsto dall'art. 30 d.lgs. 129/2024, che – come visto – punisce condotte prodromiche alla realizzazione di possibili abusi, criminalizzando il mancato rispetto delle prescrizioni MiCAR volte a salvaguardare la regolarità e la trasparenza del mercato delle criptoattività.

5. Come anticipato poc'anzi, accanto al delitto di abusivismo di cui all'art. 30, il d.lgs. 129/2024 ha tipizzato una pluralità di illeciti amministrativi punitivi, il cui riscontro è appannaggio, a seconda delle rispettive competenze, della Consob o della Banca di Italia, che sanzionano – con particolare asprezza – le condotte illecite poste in essere dai soggetti – principalmente società ed enti – che operano quali emittenti o prestatori di servizi in cripto-attività.

In estrema sintesi:

i) l'articolo 31 punisce, «salvo che il fatto costituisca reato», una serie di violazioni riguardanti la disciplina delle cripto-attività *other than*, dei *token* collegati ad attività,

[28] Molto chiaramente anche F. Giunta, *Il diritto penale dell'economia: tecniche normative e prova dei fatti*, in *RivTrim-DPenEc.* 2017, 546 ss. quando rileva che, con riguardo alle fattispecie di abusivismo, la tutela penale viene costruita «sulla sagoma della sua regolamentazione extrapenale, con la conseguenza che quest'ultima finisce per intrecciarsi con l'oggetto della tutela, diventandone parte integrante».

[29] Cfr. ancora R.M. Vadalà, *La fattispecie penale tra economia digitale e diritto europeo*, cit., 66, la quale giustamente osserva che le fattispecie di abusivismo «vivono in un raccordo necessario ed indissolubile con la disciplina extrapenale».

[30] Su cui in generale A. Massaro, *Determinatezza della norma penale e calcolabilità giuridica*, Napoli 2020.

dei *token* di moneta elettronica e, infine, di quella relativa al regime dei prestatori di servizi per cripto-attività. Oltre alla sanzione pecuniaria[31], le autorità competenti hanno facoltà di disporre ulteriori misure a carattere *lato sensu* sanzionatorio, come ad esempio una dichiarazione pubblica indicante il responsabile e la tipologia della violazione, o un'ingiunzione di porre termine o di astenersi dal ripetere il comportamento illecito.

ii) l'art. 32 punisce le violazioni nella comunicazione al pubblico di informazioni privilegiate di cui all'art. 88 MiCAR, nonché l'inottemperanza agli obblighi relativi alla prevenzione e all'individuazione degli abusi di mercato evocati dall'art. 92 MiCAR;

iii) gli artt. 33 e 34 sanzionano, invece, persone fisiche ed enti per l'abuso di informazioni privilegiate, la comunicazione illecita di informazioni privilegiate e la manipolazione del mercato. Le condotte indebite vengono definite dal MiCAR e risultano sostanzialmente sovrapponibili a quelle descritte 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.

iv) infine, l'art. 35 sanziona persone fisiche ed enti che non ottemperino alle richieste od omettano di collaborare con le autorità munite di poteri di sorveglianza e di indagine (come Consob e Banca d'Italia). Anche in ragione della peculiare fisionomia del mercato delle criptoattività, il MiCAR ha infatti costruito un sistema a base collaborativa, orientato a un "controllo di prossimità", tale per cui è in primo luogo compito dei professionisti di settore segnalare «senza indugio» alle autorità competenti le operazioni sospette, che potrebbero dar luogo a possibili abusi.

5.1. Ebbene, dalla schematica ricostruzione del quadro sanzionatorio relativo alla repressione degli illeciti in ambito MiCAR, emerge nitidamente come il legislatore italiano – in assenza di specifici obblighi di criminalizzazione di matrice eurounitaria

[31] Che si distingue per un ampissimo *range edittale*, da euro 30.000 fino a euro 5 milioni. Per una sua applicazione v. ad esempio Consob, Delibera n. 23815 del 8.1.2026. in *www.consob.it*, che ha condannato a «1) una sanzione amministrativa pecuniaria pari a euro 200.000, della quale è contestualmente ingiunto il pagamento; 2) un'ingiunzione di astenersi dal ripetere la violazione; 3) una dichiarazione pubblica indicante la persona fisica responsabile e la natura della violazione - di cui è disposta la pubblicazione sul sito internet dell'Istituto nella sezione dedicata alle "Comunicazioni - Avvisi ai risparmiatori"», un soggetto (noto alle cronache scandalistiche italiane) che – pur non essendo una persona giuridica, come invece richiesto da MiCAR – ha effettuato «una offerta al pubblico di cripto-attività, diverse dai token collegati ad attività o dai token di moneta elettronica, denominati memecoin $CORONA», mancando di ottemperare agli obblighi informativi prescritti dal MiCAR.

– abbia fatto per lo più ricorso all'illecito amministrativo punitivo, attribuendo rilevanza penale unicamente a talune forme di abusivismo.

L'assetto così delineato sembra poter soddisfare le esigenze di efficienza, celerità e dissuasività, particolarmente avvertite dal legislatore UE. Inoltre – ma sul punto s'è già detto – Consob e Banca d'Italia dispongono di un bagaglio di competenze tecniche molto ampio e sono dotate di penetranti poteri di indagini: fattori che indubbiamente agevolano e velocizzano l'attività di accertamento e repressione degli illeciti perpetrati sul mercato delle criptoattività.

Al tempo stesso, il circoscritto impiego dello *ius terribile* costituisce un vantaggio sul piano del rispetto dei principi – spesso dimenticati – di frammentarietà, sussidiarietà ed *extrema ratio* [32].

Si aggiunga inoltre che la scelta attuata dal legislatore italiano di rinunciare alla costruzione di un doppio binario sanzionatorio penale-amministrativo – che invece si rinviene nella, per molti versi similare, disciplina del TUF[33] – consente di evitare qualsiasi duplicazione sanzionatoria, scongiurando in radice ogni possibile violazione del divieto di *bis in idem*[34].

D'altra parte, però, non può farsi a meno di rilevare che il ricorso al diritto amministrativo punitivo in luogo del diritto penale comporti una inevitabile *deminutio* sul piano delle garanzie.

Peraltro, a uno sguardo più attento, dietro l'atteggiamento di *self restraint* serbato dal d.lgs. 129/2024 per quanto concerne il ricorso al diritto penale sostanziale, potrebbe invero celarsi una vera e propria frode delle etichette, dal momento che – a ben vedere – gli illeciti amministrativi *ivi* tipizzati sembrerebbero riportabili entro la nozione euro-convenzionale di *matière pénale*, così come descritta sulla base dei noti *Engel criteria*[35].

---

[32] Sul punto, C.E. Paliero, *Pragmatica e paradigmatica della clausola di* extrema ratio, in *RIDPP* 2018, 1477 ss.

[33] Da ricordare che in quel contesto la scelta è però obbligata, dal momento che – come noto – il legislatore europeo ha imposto una serie di pregnanti obblighi di tutela penale (specie in relazione alla punibilità degli abusi di mercato).

[34] Sulla portata del principio del *ne bis in idem* in ambito eurounitario e convenzionale, si leggano: 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.

[35] Corte EDU, Gr. Chambre, 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.

Difatti, al netto della veste formale attribuita dal legislatore interno, essi prevedono sanzioni pecuniarie e interdittive che possono raggiungere livelli draconiani[36]. È però vero che, stando ai più recenti sviluppi della giurisprudenza EDU, il parametro della gravità della sanzione – il terzo criterio *Engel* – non sembra assumere rilievo dirimente nel riconoscimento o meno della natura penale di un certo illecito[37].

Un peso decisivo avrebbe invece il criterio che guarda alla finalità della sanzione, a cui andrebbe riconosciuta natura "sostanzialmente penale" quando abbia uno scopo afflittivo-punitivo[38]. Una tale condizione parrebbe in effetti soddisfatta dagli illeciti amministrativi di cui agli artt. 31 ss. d.lgs. 129/2024, che hanno una indubbia funzione punitiva, non trattandosi certo di misure aventi carattere preventivo o risarcitorio.

Ora, il riconoscimento della natura sostanzialmente penale di tali disposizioni rappresenterebbe un indubbio guadagno sul piano garanzie nei confronti dei soggetti sottoposti a procedimento e sanzione per il mancato rispetto della disciplina MiCAR.

È quanto sta in effetti accadendo con riguardo alla similare disciplina degli abusivi di mercato, ove la giurisprudenza della Consulta e della Corte EDU – una volta affermata la natura sostanzialmente penale di talune tipologie di illecito amministrativo ivi previste – ha via via provveduto all'applicazione delle garanzie penalistiche operanti a livello Convenzionale.

---

[36] Da sottolineare, inoltre, la discutibile equiparazione delle cornici edittali tra tipologie di illecito amministrativo evidentemente espressive di un diverso disvalore: si pensi all'art. 33 d.lgs. 129/2024 che sanziona in egual misura l'*insider trading*, la comunicazione illecita di informazioni privilegiate e la manipolazione di mercato. Un simile assetto potrebbe rivelarsi foriero di tensioni con il principio di proporzionalità, le cui violazioni – come noto – vengono oggi frequentemente sottoposte a scrutinio da parte della Consulta. Problemi analoghi si registrano con riguardo alla disciplina del TUF: in quel contesto, tuttavia, la previsione del doppio binario sanzionatorio penale-amministrativo e le continue modifiche legislative volte a inasprire la 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; nonché V. Napoleoni, *Diritto penale dell'economia*, Milano 2017, 603.

[37] Se è vero che, stando alla concezione originaria, il parametro della gravità della sanzione rappresentava un autonomo criterio (il terzo) per la valutazione della natura sostanzialmente penale di un determinato illecito, nella più recente giurisprudenza della Corte di Strasburgo, tale modello «risulta implicitamente derogato [...] laddove si sostiene che l'elevata carica di afflittività della misura non depone univocamente nel senso della sua natura punitiva, né è incompatibile con una finalità preventiva». Sul punto, L. Masera, *I criteri Engel alla prova della prassi interna la necessità di maggiore chiarezza sistematica nell'elaborazione della nozione costituzionale di* matière pénale, in *SP* 1.7.2025, 15 ss., il quale precisa che il criterio della gravità della sanzione è stato declassato «ad elemento (non decisivo) da tenere in considerazione insieme ad altri per valutare la natura punitiva dell'illecito, che diventa dunque l'unico criterio per valutare la natura sostanzialmente penale di una misura amministrativa».

[38] *Ibidem.*

Basti pensare: all'estensione, ad opera della Corte costituzionale, del diritto al silenzio dell'incolpato nel procedimento di cui all'art. 187 *quinquiesdecies* TUF [39]; all'affermazione dell'operatività della garanzia della *lex mitior* con riguardo agli illeciti amministrativi di cui all'art. 187 *bis* e *ter* TUF[40]; o, ancora al riconoscimento del principio di irretroattività della confisca per equivalente *ex* art. 187 *sexies* co. 2 TUF[41] e allo scrutinio di proporzionalità cui è stata sottoposta la confisca amministrativa *ex* art. 187 *sexies* TUF[42].

Malgrado ciò, siffatto lodevole ampliamento dei presidi garantistici al cospetto dell'illecito amministrativo para-penale non consente comunque di colmare quel *gap* rispetto alle tutele riconosciute dall'ordinamento interno all'individuo sottoposto a procedimento e sanzioni "propriamente penali". A questo proposito, mi pare doveroso sottolineare che, in ambito amministrativo-punitivo, non sia a oggi richiesto il rispetto della BARD *rule*: stando all'indirizzo prevalente, infatti, la responsabilità viene accertata sulla base di regole probatorie più blande – che fanno leva sui concetti fumosi

[39] C. cost., 30.4.2021 n. 84, 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». Prima di questa pronuncia era intervenuta la Corte di Lussemburgo (sollecitata dalla stessa Consulta) la quale, richiamando la giurisprudenza della Corte EDU, ha riconosciuto l'esistenza del diritto al silenzio, collocandolo «al centro della nozione di equo processo». Cfr. C.G. UE 2.2.2021, C-481/19. In argomento, G. Lasagni, *La Corte di giustizia riconosce il diritto al silenzio nei procedimenti amministrativi punitivi (e la Corte costituzionale conferma)*, *GComm*. 2021, 1179 ss.; O. Mazza, *Una nuova dimensione per il diritto al silenzio in ambito penale tributario*, in *Rass. Trib.* 2022, 297 ss.; G. Canesechi, *La corte di giustizia sul diritto al silenzio: un primo passo verso il "giusto procedimento" amministrativo punitivo*, in *RIDPP* 2021, 461 ss.

[40] 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; M. Branca, *Anche per le sanzioni amministrative punitive vale il beneficio della 'lex mitior'. Nulla di nuovo per la "doppia pregiudizialità"*, in *GCost* 2019, 841 ss.; in argomento, nell'ampia bibliografia, E. Amati, *L'illecito amministrativo di manipolazione del mercato e le persistenti criticità del doppio binario sanzionatorio*, in *GComm* 2021, 263 ss., nonché V. Nardi, *Retroattività favorevole e sanzioni amministrative "sostanzialmente" penali: un primo passo verso il generale riconoscimento?*, in *AP* 2019, 1 ss.

[41] 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.; G.L. Gatta, *Non sempre "depenalizzazione" equivale a "mitigazione". La Corte costituzionale sull'irretroattività delle sanzioni amministrative "punitive" più sfavorevoli di quelle penali (a proposito della confisca per equivalente per l'insider tading secondario)*, in *DPC* 13.12.2018.

[42] 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.; N. Madia, *La Consulta dichiara la parziale illegittimità costituzionale dell'art. 187-'sexies' del d.lgs. n. 58 del 1998 sia nel testo introdotto dalla l. n. 62 del 2005 sia in quello modificato dal d.lgs. n. 107 del 2018*, in *RIDPP* 2019, 841 ss.

e sfuggenti, come la «ragionevole probabilità», la «preponderanza dell'evidenza» –, o sulla logica della «più probabile che non» propria dell'ordinamento civile[43].

Ebbene, a mio parere, il mancato riconoscimento dell'operare della regola BARD comporta un intollerabile *vulnus* per le garanzie individuali, se è vero che – come affermato esplicitamente dalla CEDU – tale *standard* probatorio rappresenta un essenziale corollario della presunzione d'innocenza, la quale costituisce, a sua volta, «la prima e fondamentale garanzia che il procedimento assicura al cittadino»[44].

Alla luce di tutto quanto osservato, l'auspicio è dunque che il legislatore provveda a una riforma di sistema, aggiornando e integrando la disciplina contenuta nella l. 24.11.1981 n. 689, mediante la predisposizione di un apparato di garanzie sostanziali e procedimentali *ad hoc*, che tenga adeguatamente conto della peculiarità dei contesti presidiati dall'illecito amministrativo punitivo[45].

Auspicio che è presumibilmente destinato ad essere tradito, a fronte della nota ritrosia del decisore politico a impegnarsi in riforme di ampio spettro del comparto sanzionatorio, che sono difficilmente spendibili a livello mediatico e propagandistico e non garantiscono certo un immediato ritorno in termini di maggior consenso. Cionondimeno, il ruolo assoluto protagonista ormai assunto dall'illecito amministrativo punitivo nella repressione degli abusi di mercato – da ultimo nell'ambito delle criptoattività – rende la messa in cantiere di un intervento di ampio spettro non ulteriormente procrastinabile.

[43] Ad avviso di F. Consulich, *Manipolazione del mercato e declino del sistema finanziario,* cit., 15, il mancato riconoscimento della regola probatoria dell'oltre ogni ragionevole dubbio rappresenterebbe (per lo meno a livello sostanziale) «l'ultimo criterio differenziale, in termini di garanzia, tra sanzioni penali ed amministrative punitive».

[44] Cfr. C. eur. 6.12.2022, *Kerimoğlu v. Turkey*, § 67.

[45] Con specifico riguardo all'ambito MiCAR e a quello del mercato finanziario, bisognerebbe, ad esempio, tenere a mente il fatto che le sanzioni amministrative irrogabili – pur non privative della libertà personale – possono avere una portata economico e interdittiva di enorme afflittività, e che i destinatari di tali sanzioni sono principalmente enti e persone giuridiche.