

## PROFILI PENALISTICI DELLE CRIPTOVALUTE\*

di Antonio Gullo e Giorgio Ardizzone

(Professore Ordinario di Diritto Penale, Università LUISS Guido Carli;  
Dottorando di ricerca in Diritto Penale, Università Unitelma Sapienza-IUSS Pavia)

Sommario: 1. Criptovalute e responsabilità penale: un'introduzione. – 2. Autoriciclaggio e criptovalute. – 3. Le ipotesi di abusivismo. – 3.1. La normativa applicabile all'offerta abusiva di criptovalute dopo il d.lgs. 129/2024. – 4. Gli abusi di mercato e l'illecito di ostacolo. – 5. Riflessioni conclusive.

1. L'innovazione digitale che ha caratterizzato il mercato dei capitali negli ultimi anni ha aperto scenari inediti anche nella circolazione del valore, imponendo al diritto penale di confrontarsi con lo sviluppo di servizi e prodotti nuovi, come le criptovalute. La caratteristica principale che accomuna i diversi tipi di valute virtuali (e le altre cripto-attività, di cui le prime costituiscono una *species*<sup>1</sup>) è quella di essere emesse e scambiate tramite l'utilizzo della tecnologia *blockchain*, fondata cioè su un registro distribuito in cui gli stessi partecipanti al sistema validano e si fanno garanti delle operazioni, in assenza di un'autorità centrale<sup>2</sup>.

La nascita di tale fenomeno si fa convenzionalmente risalire al 2009, con la creazione del *Bitcoin*, la più nota criptovaluta generata tramite un processo cd. di *mining* digitale in assenza di un emittente centrale e il cui valore dipende unicamente dall'incontro tra domanda e offerta. Tali proprietà non sono necessariamente comuni a ogni valuta virtuale: alcune basano il loro valore sull'andamento di una valuta ufficiale (come *Tether*, che replica 1:1 il valore del dollaro) o su un paniere di beni (è il

---

\* Il presente contributo è frutto della riflessione e del lavoro congiunto dei due Autori. Tuttavia, il paragrafo 2 è attribuibile ad A. Gullo, mentre il paragrafo 4 è attribuibile a G. Ardizzone. I paragrafi 1, 3, 3.1 e 5 sono riferibili a entrambi.

<sup>1</sup> Anche nell'ambito disciplina privatistica, già prima della regolazione europea era in verità sorto un dibattito circa la qualificazione di tali strumenti: v. F. Annunziata, *Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings*, in *Bocconi Legal Studies Research Paper No. 2636561* 2019, 3 ss.; R. Lener, *Criptoattività e cripto valute alla luce degli ultimi orientamenti comunitari*, in *GC* 2023, 376 ss.

<sup>2</sup> Sul funzionamento di tale tecnologia con riferimento alle criptovalute, in prospettiva penalistica, già L. Picotti, *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, in *RTDPE* 2018, 600 ss.

caso del progetto *Libra* di Facebook, poi non andato in porto, che si proponeva di introdurre una nuova moneta privata il cui valore sarebbe stato garantito da una riserva di attività reali a basso rischio e alta liquidità, come depositi bancari e titoli di Stato a breve termine).

Queste ultime, cd. *stablecoins*, oltre ad avere un emittente centrale, si caratterizzano quindi per un tasso di volatilità meno elevato ma, per i rischi che possono porre alla stabilità finanziaria e alla sovranità monetaria degli Stati, sono state oggetto di una disciplina *ad hoc* nel Regolamento MiCA, che distingue a seconda che la criptovaluta sia agganciata unicamente al valore di una moneta fiat (cd. *E-Money Token* o *EMT*) o a un *asset* reale o combinazione di beni, comprese altre valute ufficiali (cd. *Asset-Referenced Token* o *ART*)<sup>3</sup>. I “gettoni” non inquadrabili in nessuna di queste due definizioni possono, a determinate condizioni, rientrare nella categoria residuale di *token* diversi dagli *EMT* e *ART*, con conseguenze pure rilevanti sul versante sanzionatorio.

Ora, dal 2009, la diffusione e l'utilizzo di tali strumenti si è notevolmente diffusa: un rapporto del 2023 dell'*FCA* stima che ne esistano oggi oltre 20,000<sup>4</sup>. L'impiego di criptovalute sul mercato dei capitali, inteso sia come strumento di raccolta del risparmio nell'ambito delle cd. *Initial Coin Offerings* (in sintesi, operazioni poste in essere al fine di raccolta di capitali ove una società, invece di emettere strumenti finanziari tradizionali, si finanzia emettendo una criptovaluta<sup>5</sup>), sia come spinta alla creazione di piattaforme *ad hoc* per lo scambio di *token*, ha dunque fatto sorgere una domanda di tutela dei consumatori e degli investitori alla quale la recente regolamentazione ha cercato di dare risposta. Anche al di fuori del mercato mobiliare, la diffusione di simili strumenti ha imposto la necessità di gestire determinati rischi che, sul versante penalistico, possono essere declinati vuoi come tutela contro le frodi e falsificazione di mezzi di pagamento diversi dal contante (almeno laddove la

---

<sup>3</sup> Per questa tassonomia ripresa dal Regolamento MiCA, si rinvia a F. Annunziata, *La disciplina europea del mercato delle cripto-attività*, in *RS* 2023, 935 ss.; Id., *Tassonomia delle cripto-attività e mercato dei capitali. Primi spunti per un confronto USA-UE*, in *GC* 2024, 905 ss.; R. Piselli, *Le cripto-attività. Le tipiche e le altre*, in *Le cripto-attività. La legislazione europea a disciplina del nuovo mercato*, a cura di A. Nuzzo, Roma 2025, 17 ss.

<sup>4</sup> Si veda il rapporto dell'Autorità di Vigilanza inglese sui mercati disponibile a questo link: <https://www.fca.org.uk/investsmart/crypto-basics?>

<sup>5</sup> Si tratta peraltro di una prassi diffusa da tempo, tanto che già nel 2017 ESMA aveva pubblicato un documento sottolineandone i rischi per gli investitori: [https://www.esma.europa.eu/sites/default/files/library/esma71-99-649\\_press\\_release\\_ico\\_statements.pdf](https://www.esma.europa.eu/sites/default/files/library/esma71-99-649_press_release_ico_statements.pdf). Per riferimenti più puntuali alla disciplina di settore, si veda C. Sandei, *L'offerta iniziale di cripto-attività*, Torino 2022 e, nella manualistica, F. Annunziata, *La disciplina del mercato dei capitali*, Torino 2023, 512 s.

criptovaluta sia utilizzata come mezzo di pagamento), vuoi come bisogno di garantire la tracciabilità dei flussi finanziari in ottica di prevenzione dei delitti di riciclaggio in senso lato, considerata anche la peculiarità della citata tecnologia a registro distribuito<sup>6</sup>.

Sono dunque numerose le fattispecie criminose, rilevanti dal nostro angolo visuale, suscettibili di avere come oggetto materiale una valuta virtuale. Prima di concentrare l'attenzione sui temi che si sono imposti con maggior frequenza nella prassi, conviene allora fornire uno schizzo dei diversi ambiti in cui tali *token* possono venire in rilievo, seguendo l'evoluzione normativa degli ultimi anni.

Una prima categoria sulla quale concentrare l'attenzione riguarda figure tradizionali, il cui oggetto materiale può occasionalmente riguardare le criptovalute e la cui possibile applicazione dipende dall'interpretazione data agli elementi in questione. Il riferimento è, ad esempio, ai delitti di furto o appropriazione indebita: nella prima ipotesi, la rilevanza dell'impossessamento al fine di trarre profitto di una valuta virtuale o delle chiavi crittografiche di un portafoglio digitale dipende dalla lettura del concetto di "cosa mobile", esteso dalla più recente giurisprudenza di legittimità nel senso di farvi rientrare, come noto, anche i *file* presenti su computer o *smartphone*<sup>7</sup>. Si tratta di un percorso ermeneutico non condivisibile che traveste da interpretazione estensiva quella che, a ben vedere, è una vera e propria analogia *in malam partem*, come tale vietata<sup>8</sup>. D'altronde, non solo nella manualistica si evidenzia come la "corporeità" sia una delle note distintive del concetto di cosa<sup>9</sup> ma il legislatore

---

<sup>6</sup> Per un approfondimento sul tema, anche con riferimento specifico al funzionamento della tecnologia *blockchain*, cfr. G. Soana, *The anti money laundering regulation of crypto-assets in Europe*, Padova 2024.

<sup>7</sup> Il riferimento è a Cass. 7.11.2019 (dep. 10.4.2020) n. 11959 con note di N. Pisani, *La nozione di "cosa mobile" agli effetti penali e i files informatici: il significato letterale come argine all'applicazione analogica delle norme penali*, in *DPP* 2020, 651 ss.; A. Scarcella, *Dato informatico, nozione penale di cosa mobile ed appropriazione indebita*, in *CP* 2021, 556 ss.; C. Pagella, *La Cassazione sulla riconducibilità dei file al concetto di "cosa mobile" oggetto di appropriazione indebita: un caso di analogia in malam partem?*, in [www.sistemapenale.it](http://www.sistemapenale.it), 4.3.2021. Per la ricostruzione dei diversi orientamenti sul punto, v. anche C. Colucci, *I dati informatici come "cosa mobile" oggetto di furto o appropriazione indebita*, in *Cybercrime*, a cura di A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Milano 2023, 877 ss. spec. 881 ss.

<sup>8</sup> Concorde anche L. Picotti, *Diritto penale, tecnologie informatiche ed intelligenza artificiale: uno sguardo d'insieme*, in *Cybercrime*, a cura di A. Cadoppi, S. Canestrari, A. Manna, M. Papa, cit., 62, che afferma, riferendosi all'aggravante di cui al comma 3 dell'art. 640-ter Cp (che menziona il "furto o indebito utilizzo dell'identità digitale"), che «il "furto di dati" appare essere una nozione atecnica sul piano giuridico, non essendovi alcuna sottrazione di "cosa" mobile». Dava per scontato che non potesse essere oggetto di furto il *software* o altro programma del computer in virtù della atipicità della «sottrazione-impossessamento di entità incorporali» già F. Sgubbi, voce *Patrimonio (reati contro il)*, in *ED*, XXXII, Milano 1982, 368 ss., spec. 370.

<sup>9</sup> L'orientamento in verità è sempre stato pacifico in dottrina: v. già C. Pedrazzi, voce *Appropriazione indebita*, in *ED*, II, Milano 1958, 840, per cui: «Cosa è soltanto il bene materiale, corporeo [...]. Non sono cose, invece, i beni

si è sempre mostrato consapevole della diversità tra le due realtà qui in esame, tenuto conto che, ove ha ritenuto, ha proceduto espressamente ad ampliare l'ambito oggettivo di applicazione del furto – con l'equiparazione dell'energia elettrica alla *res* – o ha inserito apposite fattispecie calibrate sulle nuove realtà tecnologiche, come avvenuto in materia di danneggiamento<sup>10</sup>. Nondimeno, la giurisprudenza ha altresì ritenuto configurabile il delitto di appropriazione indebita di *Bitcoin* in quanto «costituito da dati informatici», confermando così l'approccio espansivo sopra richiamato<sup>11</sup>. Rimane il fatto che si è in presenza di un orientamento in fase di consolidamento nel panorama applicativo, del quale occorre dunque attendere l'evoluzione.

Da queste ipotesi vanno invece tenute distinte altre fattispecie, come l'estorsione – specialmente se attuata tramite le modalità informatiche descritte dal terzo comma dell'art. 629 Cp – in cui può accadere che venga richiesto un “riscatto” in *Bitcoin* o altra valuta virtuale. In questi casi tuttavia l'elemento costitutivo del profitto non pone problemi riguardo la possibilità di includere al suo interno pagamenti effettuati secondo le modalità sopra richiamate. Trattandosi di fenomeni che possono solo

---

immateriali: un nome, un'idea, un'invenzione, un'opera letteraria o musicale non sono oggetti idonei di appropriazione».

Nella manualistica tale concetto è reso con l'espressione che individua le cose in “*res corporales o quae tangi possunt*”: cfr. C. Giordanengo, *Delitti contro il patrimonio*, in F. Antolisei, *Manuale di diritto penale. Parte Speciale, I*, Milano 2016, 381; G. Fiandaca, E. Musco, *Diritto penale. Parte speciale, II*, Bologna 2023, 28. V. anche le argomentazioni di F. Mantovani, voce *Furto*, in *DigDPen*, Torino 1991, 366 ss., per cui la «fisicità della cosa resta [...] requisito imprescindibile per salvaguardare l'“omogeneità” della categoria dei delitti patrimoniali e la tassatività degli stessi». Si tratta dunque di una scelta ermeneutica in forte tensione con il divieto di analogia, volta in sostanza ad “aggiungere”, nella descrizione del fatto tipico, un oggetto materiale non previsto poiché difficilmente riconducibile al significato letterale dell'elemento nel quale lo si vorrebbe sussumere. Denunciava questo metodo di «interpretazione additiva» volto ad aggirare il divieto di analogia, seppur in relazione ad altre fattispecie, già G. Contento, *Interpretazione estensiva e analogia*, in *Le discrasie tra dottrina e giurisprudenza in diritto penale*, a cura di A.M. Stile, Napoli 1991, 15.

<sup>10</sup> Anche prima dell'introduzione dell'art. 635-bis Cp una parte della giurisprudenza era peraltro ricorsa a una interpretazione “estensiva”, forzando il dato normativo: cfr. Pret. di Torino 23.10.1989, in *DirInf* 1990, 620; T. Firenze 27.1.1986, in *DirInformInf*, 1986, 962, con nota critica di L. Picotti, *La rilevanza penale degli atti di “sabotaggio” ad impianti di elaborazione di dati*. Ancora prima, cfr. T. Torino 12.12.1983, in *DirAut*, 1986, 513 che ha ritenuto integrata la violenza sulle cose per il delitto di esercizio arbitrario delle proprie ragioni in virtù del «danneggiamento di un programma per elaboratore». Anche Cass. S.U. 9.10.1996 (dep. 13.12.1996) n. 1282 ha ritenuto che vi fosse continuità normativa tra il delitto di cui all'art. 635 Cp e il nuovo danneggiamento informatico, valutando dunque corretta la precedente interpretazione della giurisprudenza di merito. Critico da subito in dottrina era anche A. Lanzi, *Sviluppo e prospettive nella disciplina dei computer crimes*, in *IP* 1992, 527 ss. Per una ricostruzione oggi di tale evoluzione, v. pure A. Cappellini, *I delitti contro l'integrità dei dati, dei programmi e dei sistemi informatici*, in *Cybercrime*, a cura di A. Cadoppi, S. Canestrari, A. Manna, M. Papa, cit., 809 ss., spec. 815 ss.

<sup>11</sup> Così infatti Cass. 20.3.2025 (dep. 29.5.2025) n. 20138. V. pure J. Della Torre, *Cripto-attività e giustizia penale*, Padova 2026, 183, critico rispetto a tale impostazione proprio per l'assenza di una «consistenza tangibile» di tali strumenti, che ritiene al più configurabile, ricorrendone i presupposti, il delitto di cui all'art. 640-ter Cp.

occasionalmente riguardare questi particolari strumenti e che comunque non sembrano porre particolari problemi interpretativi, non saranno oggetto di ulteriore approfondimento.

Spostando invece l'attenzione sui menzionati delitti di riciclaggio, conviene subito ricordare che la prima definizione di valuta virtuale è stata introdotta nel d.lgs. 21.11.2007 n. 231 in attuazione della IV Direttiva estendendo altresì agli *exchanger* gli obblighi previsti dal citato testo unico (ossia, coloro che prestano il servizio di conversione di criptovalute in monete fiat o viceversa)<sup>12</sup>. In particolare, l'art. 1 co. 2 lett. q del menzionato decreto definiva la valuta virtuale come «la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente». A questa definizione, che qualificava come unica finalità del *token* quella di essere utilizzato «come mezzo di scambio», il d.lgs. 4.10.2019 n. 125 – sempre in attuazione della successiva Direttiva AML – ha aggiunto anche la «finalità di investimento», estendendo al contempo gli obblighi antiriciclaggio anche ai *wallet providers*, ossia i soggetti che offrono servizi di cambio o di gestione e salvaguardia delle chiavi crittografiche necessarie per accedere al portafoglio virtuale su cui le criptovalute sono custodite<sup>13</sup>. Anticipando dunque temi che verranno approfonditi in seguito, appare già importante segnalare come la prima definizione legale di tali strumenti, almeno per come modificata nel 2019, contemplava due diverse finalità alternative per le quali le valute virtuali potevano essere acquistate, ossia il “mezzo di scambio” e “la finalità di investimento”. La precisazione è rilevante sia per la configurabilità, ad esempio, dell'autoriciclaggio, che presuppone l'impiego dei proventi criminosi in attività economiche, finanziarie, imprenditoriali o speculative, sia per la possibile integrazione dell'abusivismo finanziario *ex art.* 166 TUF, che dal 2017 ha come oggetto materiale i “prodotti finanziari”<sup>14</sup>. È dunque significativo che il

---

<sup>12</sup> Per una più puntuale rassegna degli obblighi gravanti su tali soggetti all'indomani delle modifiche normative citate, v. G.P. Accinni, *Profili di rilevanza penale delle “criptovalute” (nella riforma della disciplina antiriciclaggio del 2017)*, in *AP* 2018, 20 ss. Più in generale sull'evoluzione della normativa di settore con specifico riferimento ai *crypto-asset*, v. J. Della Torre, *op. cit.*, 162 ss.

<sup>13</sup> Su tale estensione, v. pure G.P. Accinni, *Cybersecurity e criptovalute. Profili di rilevanza penale dopo la quinta direttiva*, in *www.sistemapenale.it* 15.5.2020, 223; M. Croce, *Cyberlaundering e valute virtuali. La lotta al riciclaggio nell'era della distributed economy*, in *www.sistemapenale.it*, 27.4.2021, 134 e 145 ss.; M. Giuca, *Criptovalute e diritto penale nella prevenzione e repressione del riciclaggio*, in *DPenCont* 2021, 161 ss.

<sup>14</sup> V. *infra*, par. 2 e 3.

d.lgs. 231/2007 annoverasse anche la finalità di investimento tra i possibili utilizzi delle valute virtuali.

Il panorama legislativo ha però, come noto, subito un'evoluzione negli ultimi anni. In particolare, il d.lgs. 8.11.2021 n. 184, in attuazione della Dir. 2019/713/UE relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, ha introdotto una nuova definizione di valuta virtuale valida agli effetti della legge penale. Oggi, tale strumento è definito come «una rappresentazione di valore digitale che non è emess[o] o garantit[o] da una banca centrale o da un ente pubblico, non è legat[o] necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettat[o] da persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferit[o], memorizzat[o] e scambiato elettronicamente»<sup>15</sup>. Come dunque si può notare, scompare il riferimento all'utilizzo per finalità di investimento. Di recente, al fine di recepire le indicazioni del pacchetto di regolamentazione europeo relativo alle cripto-attività, il d.lgs. 27.12.2024 n. 204 ha poi abrogato la precedente definizione contenuta nel d.lgs. 231/2007, lasciando in vigore solo quella prevista dal decreto citato relativo alla tutela contro le frodi e le falsificazioni di mezzi di pagamento diversi dal contante. Lo stesso d.lgs. n. 204 ha invece inserito una nuova lettera *m-bis*, che definisce per rinvio al Regolamento MiCA la più ampia nozione di «cripto-attività», ossia qualsiasi «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»<sup>16</sup>. Nella definizione di valuta virtuale oggi in vigore agli effetti della legge penale, manca quindi il riferimento alla possibile funzione di investimento delle criptovalute.

Tornando al d.lgs. 184/2021, è poi necessario soffermare l'attenzione sul delitto di indebito utilizzo e falsificazione di strumenti di pagamento diversi dal contante *ex art. 493-ter Cp* e sulla nuova aggravante prevista per il delitto di frode informatica. Con riferimento alla prima fattispecie, è bene sin da subito precisare che la valuta virtuale, almeno nella sistematica del decreto, è trattata come una *species* degli strumenti di pagamento, definiti come «dispositivo, oggetto o record protetto immateriale o materiale, o una loro combinazione, diverso dalla moneta a corso legale, che, da solo

---

<sup>15</sup> A commento v. G.J. Sicignano, *Recenti innovazioni in tema di frodi e falsificazioni di strumenti di pagamento diversi dai contanti*, in *www.sistemapenale.it*, 9.9.2022, 7 ss.

<sup>16</sup> Sul cambiamento nella strategia di definizione già nella proposta di Regolamento MiCA, v. G. Soana, *Obblighi di prevenzione del riciclaggio e cripto-attività. Interventi regolativi ed opportunità regolamentari*, in *Il Mulino - Rivisteweb* 2022, 473 ss.

o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali». La norma citata punisce dunque chi, al fine di trarne profitto per sé o per altri, utilizza indebitamente o falsifica anche criptovalute, nonché chi «possiede, cede o acquisisce tali strumenti o documenti di provenienza illecita o comunque falsificati o alterati», o ordini di pagamento prodotti con essi. Nondimeno, è pure stato osservato in dottrina come tale delitto sia di difficile applicazione nei casi in cui il suo oggetto materiale sia riferito alle valute virtuali, almeno con riferimento alle prime due tipologie di condotte: a causa infatti dell'utilizzo della tecnologia a registro distribuito cui si è accennato, appare arduo immaginare una falsificazione di *Bitcoin* o altri *token* simili, e ciò sembra del resto confermato dall'assenza di giurisprudenza relativa a casi di questo tenore<sup>17</sup>. Piuttosto, sembrerebbe maggiormente ipotizzabile l'indebito utilizzo, almeno laddove sia posto in essere dal soggetto detentore delle chiavi crittografiche in assenza del consenso del titolare del portafoglio digitale.

Per quanto riguarda invece la frode informatica, come si è accennato il decreto citato ha introdotto una nuova aggravante a effetto speciale integrata laddove l'alterazione o l'intervento senza diritto su un sistema informatico produca un trasferimento di «denaro, di valore monetario o di valuta virtuale». La norma non sembra porre particolari difficoltà interpretative e comunque equipara il trasferimento di criptovalute a quello di denaro sostanzialmente in qualsiasi forma<sup>18</sup>. Appare poi appena il caso di notare come, anche in questo caso, la prassi non sembri restituire riscontri in punto di sua applicazione.

Spostandoci al di fuori del codice penale, va invece sottolineato come la giurisprudenza abbia fatto larga applicazione del menzionato art. 166 TUF, relativo

---

<sup>17</sup> Così G.J. Sicignano, *op. cit.*, 20 s., che ritiene non configurabile anche l'indebito utilizzo poiché difetterebbe l'intestazione formale del portafogli digitale. V. pure J. Della Torre, *op. cit.*, 178, ad avviso del quale la rilevanza applicativa della disposizione sarebbe infatti confinata alla terza tipologia di condotta incriminata relativa al possesso o all'acquisizione di crypto-attività di provenienza illecita. Cfr. anche R.M. Vadalà, *La fattispecie penale tra economia digitale e diritto europeo*, Torino 2025, 181, che ritiene comunque fondata la scelta d'incriminazione poiché terrebbe «in conto la varietà delle soluzioni tecniche che possono essere riferibili, in particolare in una prospettiva evolutiva non preventivabile, allo stesso variegato universo dei *virtual assets*».

<sup>18</sup> V. però anche J. Della Torre, *op. cit.*, 182 s., che ritiene la nuova disposizione idonea ad «abbracciare una serie di fenomeni criminosi particolarmente insidiosi», quali le ipotesi in cui «le criptovalute vengono acquisite tramite attività di *hacking* o tecniche di *phishing* rivolte contro i singoli utenti o fornitori di servizi». Lo stesso Autore (184 ss.) giudica peraltro non condivisibile aver previsto in queste ipotesi una mera circostanza aggravante soggetta al giudizio di bilanciamento, che lascia peraltro irrisolta la ricostruzione dei rapporti con la fattispecie di cui all'art. 493-ter Cp. *Amplius* sui rapporti con quest'ultima fattispecie, cfr. anche R.M. Vadalà, *La fattispecie penale*, cit., 219 ss.

all'abusivismo finanziario, nelle ipotesi di offerta al pubblico di criptovalute senza rispettare le regole di condotta poste dal testo unico citato circa la promozione o il collocamento a distanza di prodotti finanziari<sup>19</sup>. In questo caso, vengono in rilievo le definizioni tecniche previste dalla legislazione di settore, peraltro recentemente oggetto di un nuovo innesto a opera del d.lgs. 5.9.2024 n. 129 in attuazione del già richiamato Regolamento MiCA che, tra l'altro, ha inserito un nuovo delitto di abusivismo relativo specificamente alle cripto-attività<sup>20</sup>. Si tratta dunque di comprendere se il delitto previsto dal TUF possa conservare oggi una sua sfera di operatività dopo la recente modifica normativa e se, come si è accennato, le valute virtuali possano ancora essere qualificate come "prodotti finanziari".

Lo stesso decreto legislativo da ultimo citato ha poi previsto una corposa serie di illeciti amministrativi punitivi, modellati *in toto* su fattispecie penali già esistenti e che sanzionano, tra le altre cose, gli abusi di mercato aventi ad oggetto cripto-attività e le condotte di ostacolo a Banca d'Italia o Consob poste in essere dagli emittenti di valute virtuali o CASP (ossia, prestatori di servizi per le cripto-attività) che, ai sensi del Regolamento MiCA, sono oggi soggetti a vigilanza<sup>21</sup>.

Sempre nell'ambito della legislazione complementare, vanno poi menzionate alcune norme del TUB, relative all'abusiva attività di emissione di moneta elettronica (art. 131-bis TUB) e abusiva attività finanziaria (art. 132 TUB), delle quali il Tribunale di Milano ha fatto applicazione nel caso cd. *OneCoin*<sup>22</sup>. Si trattava di una *Initial Coin Offering* con finalità fraudolente, ossia un'operazione posta in essere al fine di raccolta di capitali ove una società, invece di emettere strumenti finanziari tradizionali, si finanziava emettendo una cripto-valuta presentata come particolarmente redditizia agli investitori. Nondimeno, l'applicazione delle fattispecie citate desta qualche perplessità, considerata la differenza, anche a livello normativo, tra moneta elettronica e criptovaluta, nonché l'assenza di un'attività consistente nella concessione di finanziamenti al pubblico senza autorizzazione capace di integrare il delitto di abusivismo previsto dal TUB<sup>23</sup>. È infatti recente la sentenza della Corte d'Appello di

---

<sup>19</sup> V. *infra*, par. 3.

<sup>20</sup> Su cui v. già le osservazioni di J. Della Torre, G. Pontepino, *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](http://www.lalegislazionepenale.eu) 18.2.2025, 16 ss.; R.M. Vadalà, *Abusivismo in cripto-attività: dubbi sulle tecniche di tipizzazione del diritto penale "permeabile"*, in *DPP* 2025, 1088 ss.

<sup>21</sup> Cfr. J. Della Torre, G. Pontepino, *op. cit.*, 25 ss.; G. Ardizzone, *I profili sanzionatori del Regolamento MiCA*, in *AP* 2025, 19 ss.

<sup>22</sup> T. Milano 5.4.2023, n. 5116.

<sup>23</sup> Si può infatti notare la differenza tra la definizione di moneta elettronica *ex art. 1, co. 2, lett. h-ter TUB*,

Milano che ha ritenuto infondate entrambe le contestazioni proprio sulla base dei rilievi qui in sintesi richiamati<sup>24</sup>, restando dunque i delitti in questione di difficile configurazione in quest'ambito.

Da ultimo, le valute virtuali hanno acquistato rilevanza con l'entrata in vigore del decreto legislativo di recepimento della Dir. 2024/1226/UE, relativa alle sanzioni per la violazione delle misure restrittive adottate dall'Unione<sup>25</sup>. Sono state infatti previste nuove fattispecie criminose volte a intercettare i comportamenti di chi, tra le altre cose, mette a disposizione fondi od omette di congelare diversi *asset* di cui il soggetto destinatario della misura è titolare. Le norme di nuova introduzione, all'interno dell'ampia definizione di "fondi", richiamano anche le cripto-attività disciplinate dal Regolamento MiCA, attribuendo così rilevanza penale anche a simili comportamenti qualora abbiano oggetto valute virtuali<sup>26</sup>.

Si è visto dunque come il panorama normativo sia particolarmente frastagliato, con numerose fattispecie o famiglie di reato che possono venire in rilievo tenuto conto del loro oggetto materiale, e stratificato, considerato l'ingente numero di provvedimenti normativi europei e nazionali che hanno tentato di regolare il fenomeno negli ultimi anni. Prendendo dunque spunto dalle questioni che più si sono imposte nella prassi applicativa, il contributo avrà ad oggetto tre diversi profili di indagine.

In particolare, il primo riguarda la rilevanza delle criptovalute in relazione al delitto di autoriciclaggio: l'attenzione si concentrerà sulla possibile qualificazione di attività finanziaria o speculativa della condotta di acquisto dei *token* e sull'integrazione dell'ostacolo all'identificazione della provenienza criminosa dei fondi utilizzati. Ci si soffermerà poi, come si è accennato, sul dibattito che ha interessato il delitto di abusivismo finanziario *ex art.* 166 TUF e sulla nuova fattispecie introdotta con il d.lgs. 129/2024. Infine, si tratterà brevemente delle nuove figure di abusi di mercato e dell'illecito di ostacolo che, pur avendo qualifica formalmente amministrativa, è

---

anch'essa di derivazione europea, con quella relativa agli effetti della legge penale delle valute virtuali o dei *crypto-assets* ai sensi del Regolamento MiCA. Anche per F. Di Vizio, *Moderni abusivismi e criptovalute. Tra il mito della completa disintermediazione e la realtà dei nuovi intermediari*, in *Discrimen*, 2022, 34 s. i due delitti non sembrano prospettabili, almeno in astratto, posto che, da un lato, gli «operatori professionali in valute virtuali non erogano finanziamenti», non risultando così violata la riserva di attività di cui all'art. 106 TUB e, dall'altro, «l'assenza di valore legale delle valute virtuali preclude la configurabilità delle fattispecie di abusivismo di cui gli artt. 131-bis e 131-ter TUB».

<sup>24</sup> App. Milano 13.6.2024, n. 1879.

<sup>25</sup> Cfr. le modifiche al codice penale introdotte dal d.lgs. 30.12.2025 n. 211, entrato in vigore il 24.1.2026.

<sup>26</sup> Così infatti l'art. 2 co.1 lett. c n. 8 d.lgs. 211/2025 citato, che ricalca il testo della Dir. 2024/1226/UE. Cfr. sul punto anche J. Della Torre, *op. cit.*, 150 ss.

agevole ricondurre nell'alveo della nozione di "materia penale" cui la Corte EDU ci ha ormai abituato, considerato l'elevato livello di afflittività delle sanzioni e la loro pacifica finalità punitiva<sup>27</sup>.

2. Conviene dunque iniziare con un'analisi più approfondita dei temi sopra accennati relativi al delitto di autoriciclaggio. Innanzi tutto, occorre sottolineare come non sorga qui un problema interpretativo con riferimento all'oggetto materiale previsto dalla norma: se infatti per il furto si pongono le questioni evidenziate in punto di nozione di "cosa mobile", la criptovaluta sembra poter rientrare pacificamente nel concetto di "altra utilità" contemplato dalla fattispecie<sup>28</sup>. Piuttosto, i problemi maggiori affrontati dalla giurisprudenza, come pure si è accennato, hanno riguardato la qualificazione dell'acquisto di valuta virtuale come impiego in attività finanziaria o speculativa e l'integrazione dell'ostacolo tramite lo sfruttamento della tecnologia *blockchain* che, come verrà approfondito, può effettivamente garantire l'anonimato dell'operazione.

Relativamente alla prima questione, è utile partire sottolineando come la Corte di Cassazione abbia dapprima qualificato come finanziaria l'attività di utilizzo di un servizio di cambiavalute, in un caso concreto avente ad oggetto un intermediario professionale<sup>29</sup>. L'ipotesi con cui la Suprema Corte si è confrontata non poneva all'epoca particolari problemi, poiché l'attività professionale di cambiavalute, originariamente richiamata dall'art. 106 TUB, è tendenzialmente ricondotta alla nozione di attività finanziaria insieme alla concessione di finanziamenti e alla

---

<sup>27</sup> Già dalla sentenza della C. eur. GC, 21.2.1984, *Öztürk c. Germania* è stato infatti ben chiaro il centrale ruolo della funzione dell'illecito tra i cd. *Engel criteria* per definire i contorni della materia penale convenzionale; profilo colto a suo tempo già da C.E. Paliero, "Materia penale" e illecito amministrativo secondo la Corte Europea dei Diritti dell'Uomo: una questione "classica" a una svolta radicale", in *RIDPP* 1985, 894 ss. Per una ricostruzione più recente, limitandoci ai contributi monografici, cfr. Fr. Mazzacupa, *Le pene nascoste. Topografia delle sanzioni punitive e modulazione dello statuto garantistico*, Torino 2017, 26 ss.; L. Masera, *La nozione costituzionale di materia penale*, Torino 2018, 57 ss. e 211 ss.

<sup>28</sup> Nello stesso senso anche E. Basile, *Crypto assets e responsabilità penale*, in *Reati in materia bancaria e finanziaria* a cura di F. Consulich, in *Trattato teorico-pratico di diritto penale*, diretto da F. Palazzo, C.E. Paliero, M. Pelissero, Torino 2024, 462. Del resto, la sostituzione a "denaro e valori" di "denaro, beni e altra utilità", operata già con la riforma del riciclaggio del 1990, permette di ricomprendere ogni «entità patrimonialmente apprezzabile»: cfr. G. Pecorella, *Circolazione del denaro e riciclaggio*, in *RIDPP* 1991, 1227. Secondo J. Della Torre, *op. cit.*, 230, le criptovalute potrebbero anche rientrare nella nozione di "beni", anche se l'Autore ritiene non potrebbe comunque negarsi, in via residuale, la loro riconduzione alla clausola di chiusura rappresentata dalle "altre utilità".

<sup>29</sup> Cass. 7.10.2021 (dep. 25.1.2022) n. 2868, con note di G. Soana, *Autoriciclaggio mediante criptovalute*, in *DirInt* 2022, 40 ss. e G.J. Sicignano, *L'utilizzo di moneta virtuale a scopo di autoriciclaggio*, in *DPP* 2022, 1096 ss.

prestazione di servizi di pagamento<sup>30</sup>. Occorre segnalare, sotto questo profilo, che nonostante il d.lgs. 231/2007 inquadrasse gli *exchanger* tra gli operatori *non* finanziari prima delle modifiche attuative del Regolamento MiCA, il previgente comma 8-*bis* dell'art. 17-*bis* d.lgs. 13.8.2010 n. 141 parificava tale attività a quella dei cambiavalute tradizionali, imponendo l'obbligo di iscrizione in una sezione speciale di un apposito registro disciplinato dal TUB avente ad oggetto gli "agenti in attività finanziaria" e mediatori creditizi. Oggi, a seguito del d.lgs. 129/2024, sono invece soggetti alla disciplina per i prestatori di servizi per le cripto-attività ai sensi del MiCAR, rimanendo incerto il loro inquadramento nell'ambito delle attività aventi natura finanziaria.

Perplessità ancora maggiori possono poi sorgere dal riconoscere tale carattere alle operazioni di mero acquisto diretto o tra privati di valute virtuali, tema che impone di confrontarsi direttamente con la natura di tali strumenti, piuttosto che guardare all'attività posta in essere.

In questi casi, risulta in effetti più arduo inquadrare tali condotte nell'ambito di un'attività finanziaria, anche perché nella normativa settoriale relativa all'antiriciclaggio è stata abrogata la definizione che faceva riferimento alla finalità di investimento quale utilizzo della criptovaluta e, nell'unica definizione legale vigente agli effetti della legge penale, difetta tale richiamo. Nondimeno, va segnalato che un'interpretazione di questo tenore risulta possibile mutuando gli approdi cui la giurisprudenza è giunta in materia di abusivismo, qualificando le valute virtuali come prodotti finanziari<sup>31</sup>. Anticipando sin d'ora temi che verranno di seguito approfonditi, si può infatti già affermare che l'attività finanziaria dovrebbe comprendere unicamente quelle operazioni che comportino: i) l'impiego di capitali; ii) una aspettativa di rendimento; iii) un rischio correlato alla remunerazione del capitale investito<sup>32</sup>. Si tratta di caratteristiche che possono effettivamente ricorrere specialmente quando si acquistano criptovalute connotate da un alto tasso di volatilità (come i *Bitcoin*); e in effetti, come appena ricordato, la giurisprudenza in materia di abusivismo è granitica nel qualificare simili valute come "prodotti finanziari", *genus* di cui fanno parte gli strumenti finanziari e ogni altro «investimento di natura finanziaria»<sup>33</sup>.

---

<sup>30</sup> Conclude nel senso che non esista dubbio sulla natura finanziaria dell'attività di cambiavalute anche G.J. Sicignano, *ult. op. cit.*, 1102, differenziando però, ai fini del riciclaggio, l'ipotesi di trasferimento di proventi illeciti per finalità di investimento in criptovalute da quella di mero acquisto di valuta virtuale.

<sup>31</sup> Si veda la giurisprudenza citata *infra*, par. 3.

<sup>32</sup> F. Annunziata, *La disciplina del mercato dei capitali*, cit., 376; R. Costi, *Il mercato mobiliare*, Torino 2024, 11 ss.

<sup>33</sup> Si tratta della definizione fornita dall'art. 1 co. 1 lett. u, TUF.

Va tuttavia precisato come la finalità di investimento non riesca da sola a restituire l'utilità di questi particolari *token*, che possono anche essere impiegati come mezzo di scambio<sup>34</sup>. Inoltre, non pare corretto accogliere una soluzione che faccia leva unicamente sulle motivazioni soggettive dell'agente. Più convincente risulta quindi l'interpretazione, oggi maggioritaria anche in giurisprudenza, che qualifica l'acquisto di valute virtuali come attività speculativa<sup>35</sup>. Si tratta infatti, come pure è stato notato in dottrina<sup>36</sup>, di una linea ermeneutica maggiormente coerente sia con il fenomeno delle criptovalute sia con l'indirizzo estensivo che la Corte di Cassazione ha adottato nell'interpretazione della locuzione richiamata, suscettibile di farvi ricomprendere anche il gioco d'azzardo<sup>37</sup>. Nonostante dunque alcune voci contrarie, scettiche sulla possibile natura speculativa della mera attività di sostituzione di denaro con valute virtuali<sup>38</sup>, va dunque sottolineato come l'interpretazione assolutamente pacifica in seno alla Corte di legittimità sia quella di qualificare come tale anche solo l'attività di cambio, facendo leva sia sulla già richiamata elevata volatilità del valore di tali strumenti, sia sulla lettura estensiva consolidata di "attività speculativa".

Piuttosto, quali scenari futuribili, occorre prospettare l'eventualità di acquisto di *E-Money Token* o *Asset-Referenced Token*, ossia *stablecoins* che, pur essendo emesse tramite tecnologia DLT, sono caratterizzate, per quel che qui interessa, dall'aver un valore stabile, poiché ancorato a un sottostante reale o a una moneta fiat. In questi casi, sembra venir meno l'intento di ricavare profitto o il rischio di perdite che può invece connotare le attività di investimento in altri tipi criptovalute, escludendo di

---

<sup>34</sup> Come pure si vedrà, si consideri già da ora che la disciplina di settore esclude che possano essere considerati strumenti finanziari gli strumenti di pagamento e si è tendenzialmente concordi nel ritenere che essi non possano nemmeno essere inquadrabili come prodotti finanziari: cfr. R. Costi, *op. cit.*, 10. Dalla polifunzionalità della valuta virtuale deriva dunque il dibattito sul tema, che inevitabilmente si riflette anche sulle categorie penalistiche.

<sup>35</sup> Cfr. Cass. 7.7.2022 (dep. 13.7.2022) n. 27023; Cass. 28.10.2022 (dep. 20.1.2023) n. 2585. Non prende posizione esplicita sul tema ma ritiene comunque astrattamente configurabile il delitto in caso di acquisto di criptovalute, Cass. 31.5.2023 (dep. 30.6.2023) n. 28279.

<sup>36</sup> G. Soana, *Criptoriciclaggio: un orientamento che si consolida*, in *DirInt* 2022, 753 s., che pure fa riferimento, da un lato, all'elevata volatilità di alcune criptovalute come il *Bitcoin*, che ne renderebbe impossibile l'utilizzo come mezzo di scambio e, dall'altro, alla presa di posizione delle istituzioni europee che pure hanno smesso di riferirsi a tali strumenti come "valute" adottando, nelle definizioni positive, il più neutro termine "asset".

<sup>37</sup> Cass. 19.6.2019 (dep. 14.10.2019) n. 42052; Cass. 27.6.2023 (dep. 14.7.2023) n. 30642. Sul punto, con osservazioni però critiche sul richiamato indirizzo, volendo A. Gullo, *La disciplina antiriciclaggio nel codice penale: gli artt. 648-bis, 648-ter e 648-ter.1*, in *Reati in materia bancaria e finanziaria* a cura di F. Consulich, cit., 400 s.

<sup>38</sup> M. Naddeo, *Nuove frontiere del risparmio, Bitcoin exchange e rischio penale*, in *DPP* 2019, 107; G. J. Sicignano, *L'utilizzo di moneta virtuale*, cit., 103.

conseguenza anche la possibilità di qualificare l'operazione come finanziaria o speculativa ai fini dell'autoriciclaggio<sup>39</sup>.

Con riferimento alla seconda problematica, ossia l'integrazione dell'estremo dell'ostacolo, l'indirizzo del tutto prevalente in giurisprudenza è quello di considerare le valute virtuali in sé come strumenti concretamente idonei a rendere più difficoltosa l'identificazione della provenienza delittuosa dei fondi utilizzati<sup>40</sup>. Tale sostanziale presunzione, correttamente avversata in dottrina<sup>41</sup>, trova le sue ragioni nel particolare funzionamento della tecnologia *blockchain*. Il sistema su cui si basa il funzionamento del registro distribuito – cd. *permissionless* – permette infatti di ricostruire la tracciabilità dell'operazione (è possibile cioè seguire il flusso di denaro utilizzato per la compravendita, in ipotesi, di *Bitcoin*) ma garantisce un alto grado di anonimato perché assicura la dissimulazione del beneficiario, non consentendo di risalire all'identità del soggetto che ha effettuato l'acquisto. Sulla base di questi elementi di fatto, c'è anche chi ha sottolineato come la norma faccia riferimento all'ostacolo riferito all'identificazione del provento criminoso e non al soggetto che pone in essere la condotta: dalla pseudonimia del titolare del portafoglio digitale non potrebbe dunque conseguire l'integrazione della fattispecie criminosa, posta la sicura

---

<sup>39</sup> A conclusioni simili giungeva già G. Soana, *Criporiciclaggio*, cit., 755 s. Anche E. Basile, *op. cit.*, 463 riconosce il possibile carattere speculativo dell'acquisto di criptovalute, anche se ritiene di potervi rinvenire altresì carattere "economico" sulla base della «economicità di un valore spendibile come mezzo di pagamento» e sull'assoggettamento a «tassazione dei proventi ricavati dal possesso di cripto-attività». L'orientamento non convince fino in fondo, restando preferibile inquadrare nell'ambito delle attività "economiche" solamente quelle aventi le caratteristiche descritte dall'art. 2082 Cc.

<sup>40</sup> Cfr. soprattutto Cass. 28.10.2022 n. 2585, cit., che fa leva sul «potenziale alto grado di anonimato, senza previsione di alcun controllo sulla provenienza del denaro convertito in moneta virtuale» e sull'«uso del *dark* e *deep web*», che consentirebbe, «anche attraverso l'utilizzo di tecniche crittografate, un elevato livello di riservatezza, con sostanziale impossibilità di individuare sia l'utente che l'oggetto delle compravendite virtuali»; Cass. 7.7.2022 n. 27023, cit., che richiama poi le stesse modalità d'acquisto delle criptovalute, che si presterebbero «ad agevolare condotte illecite, in quanto [...] è possibile garantire un alto grado di anonimato (sistema cd. *permissionless*), senza previsione di alcun controllo sull'ingresso di nuovi "nodi" e sulla provenienza del denaro convertito (si è anche sottolineato come sia ormai noto il vasto numero di criptovalute utilizzate nel *dark web*, proprio per le loro peculiari caratteristiche, e che alcune di esse, attraverso l'uso di tecniche crittografiche avanzate, garantiscono un elevato livello di *privacy* sia in relazione alla persona dell'utente sia in relazione all'oggetto delle compravendite)». Con riferimento alla nozione di ostacolo, sia nuovamente consentito il rinvio, anche per la dovuta bibliografia, a A. Gullo, *op. cit.*, 401 ss.

<sup>41</sup> Riconosce la possibile idoneità dissimulativa delle operazioni in *crypto-assets* ma critica l'automatismo cui giunge la giurisprudenza, E. Basile, *op. cit.*, 465. Cfr. però anche J. Della Torre, *op. cit.*, 231 s., che pure richiama alcune condotte («frazionamento sistematico delle transazioni; impiego di *mixer* o *tumblers* e il ricorso a protocolli *second layers*») idonee di per sé a «ritardare l'attività investigativa», per cui almeno laddove la rete o il *token* siano «concepiti sin dall'origine per assicurare un elevato grado di opacità [...] l'idoneità dissimulativa delle operazioni sarebbe *in re ipsa*».

tracciabilità dell'operazione<sup>42</sup>. E ciò sarebbe tanto più imperativo con riferimento all'art. 648-ter.1 Cp, in cui è espressamente prevista, come noto, una clausola rafforzata, relativamente all'ostacolo, rispetto agli altri delitti di riciclaggio. Altri adottano invece una soluzione mediana, distinguendo opportunamente l'ipotesi di acquisto diretto da quella in cui l'agente si rivolga a un *exchanger* o cambiavalute centralizzato: in questi casi, infatti, l'intermediario ha l'obbligo di verificare l'identità del proprio cliente, e sarebbe quindi necessario un *quid pluris* di insidiosità per ritenere integrata l'idoneità della condotta al nascondimento della provenienza illecita del bene investito, come l'utilizzo di un'identità falsa<sup>43</sup>.

Per concludere dunque su questo primo profilo, si può affermare che la giurisprudenza è oggi pacifica nel qualificare l'acquisto di criptovalute come attività speculativa e nel ritenere *in re ipsa* integrato l'ostacolo. Nondimeno, qualche perplessità può sorgere in relazione al tipo di valuta virtuale che si intende acquistare (venendo meno il carattere speculativo dell'operazione ove l'attività abbia ad oggetto i cd. *stablecoins*) e sulla effettiva capacità di occultamento nei casi in cui ci si rivolga a un intermediario autorizzato in assenza di ulteriori accorgimenti volti a mascherare la propria identità.

3. Venendo dunque al secondo tema che ci si propone di affrontare, conviene anche qui partire dal dato per cui, come si è accennato, la giurisprudenza è consolidata nel qualificare l'attività di offerta al pubblico di valute virtuali in assenza di autorizzazione come abusivismo finanziario ex art. 166 co.1 lett. c TUF, che punisce l'attività di offerta fuori sede ovvero promozione o collocazione a distanza di prodotti finanziari, strumenti finanziari e servizi o attività di investimento<sup>44</sup>. La questione attiene quindi alla qualificazione delle criptovalute come "prodotti finanziari" e, in considerazione delle novità normative di recente introduzione dopo l'entrata in vigore del

---

<sup>42</sup> V. in particolare G.J. Sicignano, *L'utilizzo di moneta virtuale*, cit., 1100 s. *Contra*, R.M. Vadala, *La fattispecie penale*, cit., 280, secondo la quale «la scissione tra provenienza oggettiva e soggettiva, con assegnazione all'art. 648-bis c.p. solo della prima, non ha un fondamento legale».

<sup>43</sup> Così G. Soana, *Criptoriciclaggio*, cit., 756 s.

<sup>44</sup> Si confronta per prima con la questione Cass. 17.9.2020 (dep. 25.9.2020) n. 26807, annotata da M. Arbotti, *La vendita "on line" di moneta virtuale "Bitcoin" pubblicizzata quale forma di investimento per i risparmiatori è attività soggetta agli adempimenti previsti dalla normativa in materia di strumenti finanziari*, in [www.dirittodiinternet.it](http://www.dirittodiinternet.it) 8.1.2021; R.M. Vadala, *La dimensione finanziaria delle valute virtuali. Profili assiologici di tutela penale*, in *GI 2021*, 2255 ss. e 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. La soluzione accolta è stata poi ripresa, *ex multis*, da Cass. 10.11.2021 (dep. 30.11.2021) n. 44337; Cass. 17.5.2023 (dep. 14.9.2023) n. 37767; Cass. 16.5.2024 (dep. 19.7.2024) n. 29649; Cass. 3.6.2025 (dep. 17.6.2025) n. 22651.

Regolamento MiCA, appare opportuno ricostruire in sintesi il dibattito formatosi sul punto prima del d.lgs. 129/2024.

Occorre dunque partire dalle definizioni presenti nel TUF di “strumenti” e “prodotti” finanziari, alle quali occorre riconoscere funzione integrativa del precetto penale<sup>45</sup>. L’art. 1, co. 2, del TUF definisce i primi attraverso il rinvio a un catalogo tendenzialmente chiuso, riportato in un’apposita Sezione di un Allegato al Testo Unico. La norma chiarisce poi, grazie alle modifiche effettuate con il d.l. 17.3.2023 n. 25, in attuazione del cd. Regolamento Pilota, che possono essere strumenti finanziari anche quelli «emessi tramite tecnologia a registro distribuito». Da tale dato normativo, si può quindi ricavare un’importante indicazione: la qualifica non dipende cioè dal mezzo tecnologico utilizzato ma piuttosto dalla possibilità di ricondurre il *token* a uno degli elementi tassativamente indicati nel catalogo cui il TUF rinvia. Si tratta poi di una nozione valida in tutta l’UE: l’elenco citato è infatti fortemente influenzato dalla disciplina recata da MiFID e MiFID II, il cui tratto comune sta nella «idoneità dello strumento a formare oggetto di negoziazione sul mercato dei capitali»<sup>46</sup>. Ne deriva che anche la criptovaluta può essere qualificata come “strumento finanziario”, a condizione che sia riconducibile a una di tali categorie *tassative* normativamente individuate. Per quel che rileva ai nostri fini, la giurisprudenza in tema di abusivismo ha finora escluso tale qualificazione anche se, come si vedrà a breve, la disciplina MiCAR lascia ancora aperta questa possibilità. Va tuttavia sottolineato come la stessa norma del TUF richiamata disponga chiaramente che «gli strumenti di pagamento non sono strumenti finanziari». Considerata dunque sia la previgente definizione contenuta nel d.lgs. 231/2007, sia soprattutto quella tuttora valida agli effetti della legge penale che inquadra le valute virtuali come *species* del più ampio *genus* di strumenti di pagamento diversi dal contante, appare in effetti arduo ricondurre tale tipologia di *token* agli strumenti finanziari, almeno per quanto attiene ai profili penalistici.

---

<sup>45</sup> Così anche F. Consulich, *Nella wunderkammer del legislatore penale contemporaneo: monete virtuali che causano danni reali*, in *DPP* 2022, 157. Tale tecnica normativa è del resto coerente con l’approccio del legislatore in questo settore: come notava già C. Pedrazzi, voce *Mercati finanziari (disciplina penale)*, in *DigDPen.*, Torino 1993, 657: «la sanzione repressiva interviene a sostegno di un’organizzazione pubblicistica dei mercati stessi, che senza vincolare l’iniziativa degli operatori la incanala in un quadro istituzionale volto a prevenire disfunzioni patologiche e a salvaguardare gli interessi in gioco. Poiché ovviamente tale organizzazione attinge le proprie strutture in massima parte dal diritto amministrativo, residua alla disciplina penale una funzione accessoria e servente, di sottolineatura e rafforzamento». Su tale funzione del diritto penale oggi in questo settore, v. anche le riflessioni di F. Mucciarelli, *Supervisione finanziaria e sistema sanzionatorio: la prospettiva penalistica*, in *RS* 2023, 164 ss.

<sup>46</sup> Cit. da F. Annunziata, *La disciplina del mercato dei capitali*, cit., 98.

Un discorso parzialmente diverso vale invece per la nozione di “prodotti finanziari”, che comprende, come si è accennato, sia gli strumenti finanziari sia ogni altro «investimento di natura finanziaria». A differenza della prima definizione, tale qualifica ha carattere unicamente nazionale e non trova riscontro nella disciplina europea. Nell’ambito del mercato mobiliare, è funzionale a estendere gli obblighi previsti dagli artt. 91 ss. TUF in materia di offerta al pubblico e raccolta del risparmio, con la finalità di fornire una tutela agli investitori più ad ampio spettro di quella imposta a livello unionale, che ha ad oggetto solo gli strumenti che ricadono nell’ambito di applicazione del Regolamento Prospetto<sup>47</sup>. Trattandosi dunque di una nozione “aperta”, la giurisprudenza ha individuato quegli “indici di finanziarietà” cui si è accennato prima, che devono ricorrere congiuntamente affinché un qualsiasi prodotto possa qualificarsi come “finanziario” e far scattare di conseguenza gli obblighi a tutela dell’investitore a cui presidio è posta la fattispecie di abusivismo<sup>48</sup>. Se dunque si può tendenzialmente escludere che la criptovaluta rientri, agli effetti della legge penale, nella nozione di “strumento finanziario”, la giurisprudenza è invece consolidata nel riconoscere la sussistenza del delitto di abusivismo in caso di offerte al pubblico di valute virtuali in assenza delle prescritte autorizzazioni, qualificando tali *token* come prodotti finanziari. Tale indirizzo interpretativo fa in realtà leva soprattutto sulle *modalità* dell’offerta, per cui occorrerebbe l’adempimento degli obblighi citati ogniqualvolta la vendita di *Bitcoin* o strumenti simili venga presentata come una proposta di investimento, tramite la pubblicizzazione di informazioni volte a far aderire i risparmiatori all’iniziativa e la prospettazione di guadagni futuri. A ben vedere, dunque, la Corte di Cassazione non si è concentrata tanto sulla natura intrinseca, sul modo d’essere delle criptovalute, quanto piuttosto sulla loro funzione nel caso concreto, ossia sulla causa reale per cui sono offerte facendo appello al

---

<sup>47</sup> R. Costi, *op. cit.*, 11.

<sup>48</sup> In particolare, si rammenta qui come l’investimento abbia natura finanziaria quando comporta: i) l’impiego di capitale; ii) una aspettativa di rendimento; iii) un rischio correlato alla remunerazione del capitale investito. Nella dottrina civilistica, contrario a ritenere le criptovalute prodotti finanziari era già F. Annunziata, *Tassonomia delle cripto-attività*, cit., 924. Critica tale classificazione anche G. Schneider, *Le cripto-attività quali prodotti finanziari: il fine giustifica i mezzi?*, in *GC* 2023, 971, che ritiene come «non siano conformi al requisito del “rendimento” finanziario operazioni in cui la redditività si manifesti per effetto del mutamento dell’oggetto dell’investimento e, pertanto, dell’aumento del valore del bene in sé nel corso del tempo», dovendo il rendimento piuttosto costituire «elemento intrinseco dell’operazione stessa direttamente derivante dall’instaurazione di un rapporto con un soggetto terzo – l’offerente – e dalla sua etero-gestione». In relazione alla funzione di investimento per i profili penali legati all’abusivismo, v. anche R.M. Vadalà, *La funzione d’investimento e le valute virtuali: scenari di repressione penale*, in *DirInt* 2022, 119 ss.

pubblico risparmio<sup>49</sup>. In dottrina, c'è chi ha fatto notare come una simile operazione rischiasse di distaccarsi troppo dai dati legali allora esistenti (la definizione di valuta virtuale essenzialmente come mezzo di scambio e la qualifica di *exchanger* e *wallet providers* come operatori *non* finanziari all'interno del d.lgs. 231/2007)<sup>50</sup>. L'opinione maggioritaria, anche in questa ipotesi, si è comunque conformata alla conclusione raggiunta in seno alla Corte di legittimità sottolineando come, da un lato, la nozione "ampia" di prodotto finanziario impedisse di invocare un ricorso all'analogia *in malam partem* e, dall'altro, come le classificazioni contenute in un preciso *corpus* normativo (nel caso in questione, antiriciclaggio) avessero valore, per così dire, settoriale, potendo venire in rilievo unicamente nell'ambito del «perimetro del testo di legge che le cont[engono]»<sup>51</sup>.

Ad ogni modo, l'entrata in vigore del Regolamento MiCA e il nuovo d.lgs. 129/2024 impongono di confrontarci con l'evoluzione che ha caratterizzato il settore. In particolare, in attuazione della normativa europea, è recentemente entrato in vigore un nuovo delitto di abusivismo, che sanziona la violazione di alcuni obblighi contenuti nel MiCAR. La norma di nuova introduzione punisce infatti quattro diverse condotte:

a) l'offerta al pubblico o l'ammissione alla negoziazione di un *ART* in assenza dell'autorizzazione (art. 30 co. 1 lett. a d.lgs. 129/2024). La norma riguarda dunque quella particolare categoria di *stablecoins* il cui valore è agganciato a un paniere di beni o a un diverso *asset* reale, come ad esempio *Pax Gold*, collegato a quello dell'oro<sup>52</sup>. La

---

<sup>49</sup> Coglie tale profilo, in chiave critica, anche M. Guastadisegni, *Criptovaluta e prodotto finanziario: l'eterno ritorno della causa negoziale*, in *Danno e resp.* 2022, 506. Nel senso comunque che si dovrebbe guardare alla funzione che la criptovaluta assolve nel caso concreto piuttosto alle modalità di presentazione dell'offerta, M. Cian, *Noterelle su finanziarietà e non finanziarietà nei crypto-assets: la Suprema Corte sulla natura del servizio di exchange*, in *BBTC* 2023, 6. Sostanzialmente dello stesso avviso anche R. Compostella, L. Cipriani, *Reimpiego in bitcoin di denaro proveniente da reato e autoriciclaggio: una soluzione (troppo) semplice per una realtà (molto) complessa*, in *BBTC* 2024, 196, che ritengono che la qualificazione del *token* come prodotto finanziario «non potrà che dipendere, di volta in volta, dalla funzione svolta dalla valuta virtuale e dallo specifico ambito di riferimento». Nella dottrina penalistica, sembra dirsi favorevole a una lettura simile F. Dalaiti, *Cripto-valute e abusivismo finanziario: cripto-analogia o interpretazione estensiva*, in *www.sistemapenale.it* 21.9.2021, 63 s., che ritiene doversi «sondare la reale natura dell'offerta e le effettive intenzioni che muovono l'acquirente», escludendo così ogni automatismo.

<sup>50</sup> Così N. Recchia, *La tutela del corretto svolgimento dell'attività di intermediazione*, in *I reati in materia bancaria e finanziaria*, a cura di F. Consulich, cit., 34.

<sup>51</sup> In questo senso si esprime F. Consulich, *Nella wunderkammer*, cit., 155. Concorde con questa linea interpretativa anche A. Quattrocchi, *La natura proteiforme delle criptovalute al crocevia della tutela penale del mercato finanziario*, in *GI* 2022, 1217.

<sup>52</sup> Per una rassegna delle più note valute virtuali, tra cui quella appena citata, e per il loro inquadramento giuridico, si veda M. Lehmann, F. Schinerl, *The Concept of Financial Instruments: Drawing the Borderline between MiFID and MiCAR*, in *EBI Working Paper* n. 171 2024, 29 ss, spec. 33 per quanto attiene a *Pax Gold*.

norma, peraltro, sanziona la sola violazione dell'art. 16 par. 1 lett. a MiCAR, ossia l'offerta o ammissione abusiva effettuata da un ente diverso da quello creditizio – menzionato alla lett. b della disposizione citata –, la cui violazione della normativa di settore integra di conseguenza solo un illecito amministrativo;

b) l'emissione di *EMT* da parte di soggetti diversi da enti creditizi o istituti di moneta elettronica autorizzati (art. 30 co. 1 lett. c d.lgs. 129/2024); e c) l'offerta al pubblico o l'ammissione alla negoziazione di tale strumento in assenza del consenso scritto da parte dell'emittente (art. 30 co. 1 lett. d d.lgs. 129/2024). Con riferimento dunque agli *stablecoins* così qualificabili, poiché aventi come sottostante altra moneta fiat, è punita sia l'offerta abusiva sia la violazione della riserva di attività con riferimento alla loro emissione;

d) la prestazione di servizi per cripto-attività senza autorizzazione (art. 30 co. 1 lett. b d.lgs. 129/2024). L'elenco delle attività che ricadono in tale definizione è simile a quello previsto dal TUF per i servizi di investimento ma contiene alcune specificità dovute alle caratteristiche tecniche dei *token*, come la custodia delle chiavi crittografiche<sup>53</sup>. Anche in questa ipotesi è dunque prevista un'autorizzazione da parte dell'Autorità di Vigilanza competente all'esito di una procedura disciplinata dall'art. 63 MiCAR, sempre volta alla tutela del consumatore/investitore che deve poter fare affidamento sul prestatore di servizi<sup>54</sup>.

Come si può notare, infine, non è sanzionata penalmente la violazione della disciplina di settore relativa all'offerta al pubblico di un *token* diverso da *EMT* o *ART*, per la quale non è richiesta un'autorizzazione ed è sufficiente osservare la normativa sulla redazione di un documento informativo (cd. *White Paper*), che svolge una funzione simile a quella del prospetto per gli strumenti finanziari tradizionali<sup>55</sup>. Appare pure il caso di sottolineare come la pena detentiva prevista per questo delitto sia pari alla metà di quella prevista dall'art. 166 TUF<sup>56</sup>.

---

<sup>53</sup> Cfr. Art. 3 par. 1 punto 16 MiCAR per l'elenco puntuale delle diverse attività ricadenti nella definizione.

<sup>54</sup> Peraltro, l'autorizzazione non è necessaria per enti creditizi, depositari centrali di titoli, imprese di investimento, gestori del mercato, istituti di moneta elettronica e società di gestione di un OICVM (art. 59 par. 1 lett. b MiCAR). La violazione della disciplina di settore da parte di tali enti integrerà di conseguenza solo illecito amministrativo. Coglie tale profilo anche J. Della Torre, *op. cit.*, 207, che ritiene irragionevole tale disparità di trattamento. I gestori di FIA devono invece essere autorizzati ex art. 60 del Regolamento citato.

<sup>55</sup> Piuttosto, sembra rilevante che la notifica del *White Paper* all'Autorità di Vigilanza debba contenere la precisa indicazione del motivo per cui la cripto-attività non è uno strumento finanziario, un *ART* o un *EMT* (art. 8 par. 4 MiCAR), proprio al fine di evitare vuoti di tutela. Tutte le violazioni degli artt. 4-14 del Regolamento (richiamate dall'art. 111 par. 1 lett. a) sono comunque sanzionate in via amministrativa dall'art. 31 d.lgs. 129/2024: cfr. J. Della Torre, G. Pontepino, *op. cit.*, 25 ss.

<sup>56</sup> La norma di nuova introduzione punisce la condotta abusiva con la pena della reclusione da sei mesi a quattro

3.1 Dall'inquadramento di un fatto nell'una o nell'altra fattispecie dipende quindi l'applicazione di un trattamento sanzionatorio notevolmente diverso. Diventa dunque fondamentale comprendere se la nuova disciplina europea, anche per come se ne è data attuazione nell'ordinamento nazionale, consenta di continuare a ritenere le cripto-valute "prodotti finanziari" ovvero se la tutela penale debba rimanere in queste ipotesi appannaggio esclusivo del nuovo delitto di abusivismo di cui all'art. 30 d.lgs. 129/2024.

Ora, in primo luogo, l'art. 2 del MiCAR esclude dal suo ambito di applicazione le cripto-attività (*genus* in cui sono ricomprese anche le criptovalute) che si qualificano come strumenti finanziari. La normativa europea si fonda quindi su una bipartizione: qualora il *token* si qualifichi come strumento finanziario, si applicherà la disciplina MiFID; altrimenti, troverà applicazione, in via residuale, la disciplina MiCAR<sup>57</sup>. Sul piano sanzionatorio, la differenza ha un certo rilievo: le fattispecie a tutela dell'investitore sono infatti più severe nel primo caso, come avviene per le ipotesi di abusi di mercato, che costituiscono delitti solo quando hanno ad oggetto strumenti finanziari. Va poi ricordato che l'approccio europeo si fonda su un principio cd. di *neutralità tecnologica*: è cioè ininfluenza ai fini classificatori l'utilizzo o meno del registro distribuito; ciò che conta è unicamente la possibilità di ricondurre il *token* a una delle categorie che si qualificano come strumenti finanziari. L'operazione, invero, non è semplicissima, anche se sono stati recentemente pubblicati degli Orientamenti dall'ESMA sulle condizioni e criteri per la qualificazione di *crypto-assets* come valori mobiliari o strumenti finanziari di altro tipo<sup>58</sup>.

---

anni, a fronte della forbice edittale uno-otto anni prevista per il delitto del TUF a seguito del generale raddoppio di pena introdotto per numerose disposizioni a seguito dei *crack* finanziari dei primi anni Duemila dall'art. 39 della l. 28 dicembre 2005, n. 262 (su cui, volendo, anche A. Gullo, *Gli interventi sul sistema sanzionatorio*, in *La tutela del risparmio nella riforma dell'ordinamento finanziario* a cura di L. De Angelis, N. Rondinone, Torino 2008, 587 ss.). È appena il caso di notare come non si possa ritenere tacitamente abrogata la norma con riferimento alla fattispecie del TUF sulla scorta di un recente intervento delle Sezioni Unite che ha avuto ad oggetto l'abusiva attività finanziaria ex art. 132 TUB: il "ritorno" alla originaria cornice edittale sei mesi-quattro anni è stato infatti frutto, secondo l'interpretazione dei giudici di legittimità, della integrale riscrittura della norma a opera dell'art. 8 d.lgs. 141/2010. Al contrario, le modifiche del 2017 e del 2022 all'art. 166 TUF, pur avendone allargato il perimetro di operatività, non permettono di giungere alle medesime conclusioni anche per il delitto di abusivismo finanziario. Cfr. Cass. S.U. 23.2.2023 (dep. 27.4.2023) n. 17615, con nota di E. Basile, *Tutela del risparmio e abusivismo finanziario: "lascia o raddoppia"? Per le Sezioni Unite è abrogato l'incremento sanzionatorio del 2005*, in *DPP* 2023, 2730 ss.

<sup>57</sup> V. per tutti F. Annunziata, *La disciplina europea del mercato delle cripto-attività*, cit., 937 ss.

<sup>58</sup> V. gli Orientamenti dell'Autorità europea sulle condizioni e sui criteri per la qualificazione delle cripto-attività come

A livello nazionale, la situazione è complicata ulteriormente dalla nozione di prodotto finanziario, assente nel panorama eurounitario, e al cui interno la giurisprudenza consolidata sussume pacificamente le criptovalute presentate come mezzo di investimento. Il d.lgs. 129/2024, nell'adeguare l'ordinamento interno ha dunque tentato un'opera di coordinamento: oltre alla nuova fattispecie *ad hoc* per l'abusivismo, ha poi avuto cura di precisare che «la disciplina del TUF avente a oggetto i *prodotti finanziari* non si applica alle cripto-attività che rientrano nell'ambito di applicazione» del Regolamento MiCA<sup>59</sup>. Il quadro risulta dunque ulteriormente articolato, e necessita di essere ricostruito come segue.

Qualora la criptovaluta rientri nell'ambito applicativo del MiCAR, e non sia cioè uno strumento finanziario, la nuova norma citata impone di ritenere che questa *non* possa qualificarsi nemmeno alla stregua di prodotto finanziario secondo la definizione esistente a livello nazionale. Ciò rende necessario, di conseguenza, comprendere quali valute virtuali siano soggette a regolamentazione da parte del recente atto di diritto derivato. Un primo punto fermo può essere rappresentato dalle cd. *stablecoins*: tali *token* aventi valore stabile sono infatti qualificabili come *EMT* o *ART* e la loro offerta al pubblico o negoziazione in violazione della disciplina di settore integra il nuovo delitto di abusivismo previsto dall'art. 30 comma 1 lett. *a* o *d* d.lgs. 129/2024. Non si tratta, in questa ipotesi, di un'interpretazione particolarmente ardita: già prima delle modifiche normative, si poteva infatti essere abbastanza d'accordo nel non qualificare tali strumenti come “prodotti finanziari”, considerata l'assenza degli indici di finanziarietà che caratterizza il loro acquisto.

Maggiori problemi sorgono invece con riferimento alle criptovalute suscettibili di essere qualificate come “*token* diversi da un *EMT* o *ART*”, categoria residuale astrattamente suscettibile di ricomprendere anche le valute virtuali non agganciate a valori reali o monete fiat e quindi connotate da un alto tasso di volatilità che si prestano a essere considerate come mezzo di investimento di natura finanziaria. Si tratta, peraltro, del caso che più si è posto nella prassi, in cui l'offerente abusivo prospetta ai

---

strumenti finanziari: [https://www.esma.europa.eu/sites/default/files/2025-03/ESMA75453128700-1323\\_Guidelines\\_on\\_the\\_conditions\\_and\\_criteria\\_for\\_the\\_qualification\\_of\\_CAs\\_as\\_FIs\\_IT.pdf](https://www.esma.europa.eu/sites/default/files/2025-03/ESMA75453128700-1323_Guidelines_on_the_conditions_and_criteria_for_the_qualification_of_CAs_as_FIs_IT.pdf). I chiari riflessi di una simile tecnica sulla tenuta della legalità penale sono del resto già stati oggetto di puntuale analisi: v. D. Notaro, *Autorità indipendenti e norma penale. La crisi del principio di legalità nello Stato policentrico*, Torino 2010, spec. 285 ss.

<sup>59</sup> Così l'art. 39 d.lgs. 129/2024. V. anche C.E. Paliero, *Nuove prospettive degli abusi di mercato?*, in *La crisi finanziaria: banche, regolatori, sanzioni*, Milano 2010, 69 ss., che pure criticava già la scelta di affidare a fonti secondarie il compito di definire in via esemplificativa le condotte manipolative e le prassi di mercato ammesse per la manipolazione di mercato.

risparmiatori l'acquisto di *Bitcoin* o *crypto-assets* simili. In queste ipotesi, occorre comprendere quando e a che condizioni si possa applicare il Regolamento europeo, anche considerato che il nuovo delitto di abusivismo *non* prevede una fattispecie *ad hoc* per l'offerta abusiva al pubblico di tali *token* diversi da *EMT* o *ART*, non essendo prevista in questo caso alcuna autorizzazione.

Sul punto, è bene precisare che il Regolamento MiCA «*non* disciplina le cripto-attività in sé considerate ma il *mercato* di tali cripto-attività»<sup>60</sup>. Ciò significa che, ove manchi un emittente centrale come nel caso del *Bitcoin*, il Regolamento potrà trovare applicazione limitatamente alla parte relativa alla *prestazione di servizi* ma *non* agli obblighi che caratterizzano l'emittente, compresa la normativa per l'offerta al pubblico del *token*. La soluzione è confermata anche dal *Considerando 22* del MiCAR, secondo il quale, in assenza di un emittente identificabile, si potrà applicare unicamente la disciplina prevista in tema di prestazioni di servizi per la cripto-attività, naturalmente ove il servizio abbia ad oggetto tale tipologia di *crypto-asset*<sup>61</sup>.

In tali ipotesi, dunque, il Regolamento MiCA non disciplina l'offerta al pubblico; trattandosi di materia «al di fuori dell'ambito di applicazione» della normativa citata, potrebbe continuare a trovare applicazione l'indirizzo giurisprudenziale che qualifica queste particolari criptovalute come prodotti finanziari ove vengano presentate con modalità tali da rappresentare una proposta di investimento, ampliando la portata applicativa delle norme del TUF. Al contrario, nel caso in cui a essere offerto ai risparmiatori non sia direttamente il *Bitcoin* ma più in generale servizi per le cripto-attività (prestazioni di custodia e amministrazione delle chiavi crittografiche, esecuzioni di ordini, gestione del portafoglio, ecc.) aventi ad oggetto questa tipologia di *token*, si dovrebbe rientrare nuovamente nell'ambito del Regolamento europeo e troverebbe applicazione, se del caso, non il delitto di abusivismo *ex art. 166 TUF* ma il nuovo e meno grave delitto di cui all'art. 30 lett. *b* d.lgs. 129/2024, che punisce la prestazione di servizi per le cripto-attività in assenza della prescritta autorizzazione.

---

<sup>60</sup> Cit. da F. Annunziata, *La disciplina del mercato dei capitali*, cit., 516.

<sup>61</sup> Si riporta qui, per la parte di interesse, il testo del *Considerando*: «Qualora le cripto-attività non abbiano un emittente identificabile, esse non dovrebbero rientrare nell'ambito di applicazione dei titoli II, III o IV del presente regolamento. I prestatori di servizi per le cripto-attività che prestano servizi in relazione a tali cripto-attività dovrebbero tuttavia rientrare nell'ambito di applicazione del presente regolamento». Cfr. anche J. Della Torre, *op. cit.*, 97 s., che pure riconosce come, ad esempio, il *Bitcoin* sia escluso dalle regole relative all'offerta al pubblico e all'ammissione alla negoziazione proprio per «l'assenza di un centro di imputazione giuridicamente responsabile», restando tuttavia applicabile la disciplina di vigilanza e regolazione sui CASP che offrano servizi aventi ad oggetto tale particolare *token*.

In quest'ultima ipotesi, infatti, sono già numerose le delibere della Consob che ingiungono di porre termine all'offerta abusiva di *servizi* per cripto-attività, tendenzialmente aventi ad oggetto siti *web* che permettono, dietro versamento di denaro, di impartire ordini di acquisto o vendita di valute virtuali<sup>62</sup>. Tali delibere richiamano infatti le norme MiCAR e non TUF, che potrebbero invece trovare applicazione solo ove sia offerta al pubblico direttamente una criptovaluta non rientrante nel perimetro di applicazione delle norme europee (per riportare un caso effettivamente accaduto, l'offerta di *Bitcoin* su *Facebook*) e non un servizio per l'attività di compravendita del *crypto-asset*.

Tirando dunque le fila, e cercando di semplificare il più possibile l'elevato tasso di tecnicismo che connota la materia, a seguito dell'entrata in vigore del d.lgs. 129/2024 la rilevanza penale delle condotte abusive aventi ad oggetto criptovalute sembra potersi ricostruire come segue:

a) ove l'offerta al pubblico abbia ad oggetto uno *stablecoin*, troverà applicazione il nuovo delitto di abusivismo ex art. 30 decreto citato;

b) alla stessa conclusione si deve pervenire ove l'offerta al pubblico abbia ad oggetto non una *valuta* virtuale ma un *servizio* per le cripto-attività, a prescindere dalla natura della criptovaluta, se *stablecoin* o meno;

c) rimane invece possibile l'integrazione dell'art. 166 TUF in caso di condotte che abbiano ad oggetto l'offerta con finalità di investimento di criptovalute non disciplinate dal MiCAR anche solo limitatamente alla materia *de qua*, come ad esempio il *Bitcoin* e altri strumenti per i quali non sia possibile identificare un emittente cui applicare gli obblighi previsti dalla nuova normativa;

d) ove invece tale emittente sia identificabile, e si rientri dunque nuovamente nell'ambito del Regolamento citato, la violazione delle norme relative all'offerta al pubblico come la mancata o incompleta pubblicazione del *White Paper* sarà sanzionata solo in via amministrativa dall'art. 31 d.lgs. 129/2024, che richiama in via mediata le diverse norme relative all'offerta al pubblico di *token* diversi da *EMT* o *ART* (artt. da 4 a 14 MiCAR). Anche questa conclusione sembra suffragata da una recente delibera Consob, che ha infatti fatto riferimento a tali disposizioni per imporre la immediata cessazione dell'offerta abusiva di una criptovaluta rientrante nella definizione di

---

<sup>62</sup> Cfr., *ex multis*, Delibera 12.2.2025 n. 23422, in Bollettino Consob 2.1/25; Delibera 4.3.2025 n. 23455, in Bollettino Consob 3.1/25.

“*token other than*” ma che presentava un emittente centrale offerente cui rivolgere l’ordine<sup>63</sup>.

È chiaro dunque come la razionalità complessiva del sistema riposi, per le criptovalute diverse dagli *stablecoin*, sulla possibilità di individuare un diverso e maggiore disvalore nelle ipotesi di offerta al pubblico di *token* per i quali non sia individuabile un emittente centrale: in questo caso, infatti, dovrebbe trovare applicazione l’art. 166 TUF, che prevede come massimo edittale otto anni di reclusione; ove invece l’emittente sia individuabile, l’offerta abusiva sembrerebbe essere punita solo con un illecito amministrativo che, ancorché severo (fino a settecentomila euro se l’autore della violazione è una persona fisica), non raggiunge certo un grado comparabile di afflittività e stigma.

In verità, non sembra che tra le due ipotesi possa rinvenirsi una diversa offensività tale da poter giustificare una simile disparità di trattamento: non si vede, insomma, perché chi offre abusivamente *Bitcoin* dovrebbe rischiare di andare incontro a una severa pena detentiva mentre chi promette lauti guadagni offrendo in violazione della normativa una altrettanto volatile criptovaluta di propria emissione dovrebbe essere punito solo in via amministrativa.

Nondimeno, l’analisi del quadro normativo, di spiccata complessità anche per la presenza della nozione, tutta italiana, di “prodotto finanziario”, sembrerebbe orientare verso questa soluzione: il richiamato art. 39 d.lgs. 129/2024, nel disporre che «la disciplina del TUF avente a oggetto i prodotti finanziari non si applica alle cripto-attività che rientrano nell’ambito di applicazione» del Regolamento MiCA, lascia supporre che, *a contrario*, ove la valuta virtuale non sia disciplinata dalla normativa europea questa possa qualificarsi come prodotto finanziario; il citato *Considerando* 22 del MiCAR esclude dall’ambito di applicazione della normativa sull’offerta al pubblico i *token* privi di emittente centrale; ed ecco che quest’ultimi possono tornare a integrare l’oggetto materiale del delitto di cui all’art. 166 TUF, con quel che ne consegue in punto di ragionevolezza del diverso (e quindi, sproporzionato<sup>64</sup>) trattamento sanzionatorio.

---

<sup>63</sup> Cfr. Delibera 4.3.2025 n. 23460, in cui l’Autorità di Vigilanza richiama infatti l’art. 4 par. 1 MiCAR e l’art. 94 par. 1 lett. *u* del medesimo Regolamento per la parte in cui permette, «qualora vi sia motivo di presumere che [...] una persona stia offrendo cripto-attività o chiedendo l’ammissione alla negoziazione di cripto-attività diverse dai *token* collegati ad attività o dai *token* di moneta elettronica senza aver notificato un *White Paper* sulle cripto-attività conformemente all’articolo 8, di ordinare la cessazione immediata dell’attività senza preavviso».

<sup>64</sup> Al di là dei profili di proporzionalità cd. *cardinale* (ossia, tra illecito e sanzione in sé), pare qui profilarsi un macroscopico caso di (s)proporzionalità cd. *ordinale*, ossia di incoerenza delle scelte di politica criminale per cui si sono previste sanzioni sensibilmente diverse per fatti dallo stesso disvalore. A prescindere dunque dai recenti passi compiuti dalla Corte Costituzionale circa il progressivo “spogliarsi” dal bisogno di un *tertium*

Deve peraltro evidenziarsi che, in ogni caso, la risposta sanzionatoria che pare delinearci per i *token* senza un emittente centrale risulti affetta da irragionevolezza pure avuto riguardo a quella (da uno a quattro anni) prevista dal decreto legislativo qui in esame per l'offerta al pubblico di *stablecoin* (differenza di trattamento che risiede nella fortemente criticabile scelta del legislatore della tutela del risparmio, nel 2005, di operare un raddoppio "cieco" delle sanzioni penali e una quintuplicazione di quelle amministrative contenuti in taluni corpi normativi, tra cui il testo unico finanziario)<sup>65</sup>.

Va pure sottolineato come la Corte di Cassazione, nella più recente sentenza in cui il tema è venuto in rilievo, abbia continuato a dare per scontato l'integrazione del delitto di abusivismo, senza prendere in considerazione altre possibilità anche a seguito dell'entrata in vigore del d.lgs. 129/2024 e senza interrogarsi sulla eccessività del trattamento sanzionatorio in confronto a quello previsto dall'illecito di cui all'art. 31 del decreto citato<sup>66</sup>. Nonostante dunque si possa avanzare più di un dubbio circa la tenuta complessiva del sistema con riferimento all'offerta abusiva, con finalità di investimento, di criptovalute prive di un emittente centrale, occorre in ogni caso registrare come l'attuale *trend* giurisprudenziale rimanga pressoché invariato.

4. Proseguendo nel solco sin qui tracciato, occorre concentrare da ultimo l'attenzione su alcuni degli illeciti amministrativi punitivi di nuova introduzione, relativi, come si è accennato, agli abusi di mercato aventi ad oggetto criptovalute e all'ostacolo all'Autorità di Vigilanza nel sistema di attuazione del MiCAR. Il punto di partenza, di ordine generale, è la natura "sostanzialmente penale" delle misure previste: la severità delle sanzioni e la finalità repressiva collocano questi illeciti nella *matière pénale* ai sensi dei criteri *Engel*, con tutte le ricadute garantistiche che ne conseguono<sup>67</sup>.

---

*comparationis*, si tratta di profili che potrebbero certamente finire sotto la lente della Consulta. *Amplius* sul tema, v. per tutti F. Viganò, *La proporzionalità della pena*, Torino 2021, spec. 160 ss.

<sup>65</sup> L'art. 6, comma 3, d.lgs. n. 72 del 2015 ha poi ripristinato l'originaria forbice edittale per le sanzioni pecuniarie. Lo stesso articolo aveva poi previsto una problematica disciplina transitoria che negava la retroattività *in mitius*, su cui è dovuta intervenire la Corte costituzionale: cfr. C. Cost., 20.2.2019, n. 63, con nota di M. Scoletta, *Retroattività favorevole e sanzioni amministrative punitive: la svolta, finalmente, della Consulta*, in [www.dirittopenalecontemporaneo.it](http://www.dirittopenalecontemporaneo.it) 2.4.2019.

<sup>66</sup> Cfr. Cass. 25.11.2025 (dep. 12.12.2025) n. 1576.

<sup>67</sup> Si consideri che gli illeciti amministrativi previsti per gli abusi di mercato relativi a *crypto-assets* prevedono, come si vedrà, la medesima sanzione di quelli previsti dal TUF per gli strumenti finanziari, cui la Corte di Strasburgo ha riconosciuto natura sostanzialmente penale già in C. eur., 4.3.2014, *Grande Stevens c. Italia* e che sono ormai parametro di riferimento per la categoria a livello nazionale. Definisce gli artt. 187-bis e 187-ter TUF

Anche all'interno degli illeciti di *market abuse* si ritrova la dicotomia strumento finanziario/*crypto-assets*: solo nel caso (come si è visto, remoto) in cui la criptovaluta fosse inquadrata nella prima categoria, troveranno applicazione le norme sanzionatorie TUF, il cui oggetto materiale è in questo caso confinato ai soli "strumenti" e non anche ai "prodotti" finanziari<sup>68</sup>. Nelle ipotesi dunque in cui la valuta virtuale sia ammessa alla negoziazione in una piattaforma *ad hoc* per lo scambio di *crypto-assets*, verranno in rilievo gli illeciti amministrativi di nuova introduzione, anch'essi previsti dal d.lgs. 129/2024.

La normativa MiCAR replica la struttura portante del MAR, adattandola però all'oggetto digitale<sup>69</sup>. Con riferimento all'*insider trading*, anche in questo caso infatti il sistema poggia sulla nozione di "informazione privilegiata", che deve essere sfruttata in senso lato sul mercato perché sia integrato l'illecito<sup>70</sup>. Nondimeno, vi sono appunto alcune diversità, che si giustificano sulla base delle differenti caratteristiche dei *token* ricadenti nel perimetro del Regolamento MiCA. Da un punto di vista oggettivo, l'informazione potrà riguardare, oltre a emittente, prodotto od ordine impartito da un cliente, anche gli offerenti e coloro che chiedono l'ammissione alla negoziazione<sup>71</sup>. In relazione ai profili soggettivi, già il MAR individuava quali primi destinatari dei divieti

---

come «idealtipo di illecito amministrativo di ultima generazione», A.F. Tripodi, *Gli illeciti amministrativi in materia di abusi di mercato*, in *I reati in materia bancaria e finanziaria*, a cura di F. Consulich, cit., 227. Anche per quanto attiene alle altre sanzioni in materia, v. da ultimo C. Eur., 11.9.2025, *Mereghetti c. Italia* e, in dottrina, M. Donini, *Il nodo gordiano della vigilanza bancaria. Aspetti problematici del rapporto tra sanzioni penali e amministrative*, in *RTDPE* 2023, 23 ss.

<sup>68</sup> Per una ricostruzione dell'oggetto materiale, anche in relazione all'evoluzione circa le sedi di negoziazione rilevanti per l'integrazione del delitto, v. da ultimo D. Guidi, *Abuso di informazioni privilegiate. Modelli di configurazione dell'illecito e prospettive evolutive*, Torino 2024, 168 ss. e, nella manualistica, S. Seminara, *Diritto penale commerciale*, Vol. III, Torino 2022, 59 ss.

<sup>69</sup> Così anche M. Maugeri, *Cripto-attività e abusi di mercato*, in *Il Mulino - Rivisteweb* 2022, 425.

<sup>70</sup> Limitandoci in questa sede all'essenziale, cfr. 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, 333 ss.; A.F. Tripodi, *Informazioni privilegiate e statuto penale del mercato finanziario*, Padova 2012, 221 ss.; F. D'Alessandro, *Regolatori del mercato, enforcement e sistema penale*, Torino 2014, 113 ss.; E. Amati, *L'abuso o comunicazione illecita di informazioni privilegiate*, in *Reati in materia bancaria e finanziaria* a cura di F. Consulich, cit., 166 ss.; D. Guidi, *op. cit.*, 221 ss.

<sup>71</sup> Cfr. art. 87 MiCAR. Preme poi sottolineare che la nozione non fa più riferimento all'investitore ragionevole ma al "possessore di cripto-attività" ragionevole: la differenza non è casuale poiché la decisione di negoziare tali strumenti potrebbe *ragionevolmente* dipendere da informazioni che non incidono su alcun valore reale dell'attività sottostante, ma che, per le peculiarità dei mercati digitali e in particolare degli *utility token*, risultano comunque idonee a orientare la scelta di acquisto o vendita, includendo dunque anche dati di natura puramente speculativa o irrazionale: in questo senso M. Maugeri, *op. cit.*, 429, che ritiene quindi ci sia un ampliamento della nozione di informazione privilegiata con riferimento ai *crypto-assets*. In relazione all'evoluzione della figura dell'investitore ragionevole al cospetto delle nuove tecnologie, v. pure F. Consulich, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso di mercato*, in *BBTC* 2018, 207.

di abuso i membri degli organi di amministrazione o controllo o partecipanti al capitale degli enti che l'informazione può riguardare, ovvero chi ha accesso a tale informazione in ragione dell'esercizio di un'attività lavorativa, professione o funzione o del suo coinvolgimento in attività criminali<sup>72</sup>. MiCAR aggiunge a queste categorie anche coloro che ne vengano a conoscenza a causa del loro ruolo nella tecnologia DLT: si tratta, in primo luogo, dei *miners*, che svolgono la funzione di convalidare le operazioni e che per questo sono tendenzialmente "ricompensati" proprio in valute virtuali. Naturalmente, in quanto prestatori di servizi, rientrano nell'ambito soggettivo di applicazione anche i già citati *wallet providers*, ossia coloro che detengono le chiavi crittografiche dei portafogli digitali dei consumatori<sup>73</sup>.

Principio generale, così come per la regolamentazione in materia di strumenti finanziari, è l'obbligo di divulgazione al pubblico dell'informazione privilegiata e, specularmente, il divieto di abuso.

Già la violazione dell'obbligo di *disclosure* è sanzionata, come avviene nel TUF, in via amministrativa<sup>74</sup>. A differenza invece di quanto previsto per gli strumenti finanziari, le condotte di abuso dell'informazione (*trading, tipping e tuyautage*) non integrano alcuna nuova fattispecie di reato, ma il sistema di *enforcement* poggia unicamente su sanzioni pecuniarie e interdittive irrogabili dall'Autorità di Vigilanza, il cui importo è peraltro identico a quello previsto dagli illeciti amministrativi di abuso di mercato previsti dal TUF (sanzione fino a cinque milioni di euro, aumentabile fino al triplo del profitto conseguito, cui possono aggiungersi, tra le altre cose, la revoca o sospensione dell'autorizzazione a operare come prestatore di servizi per cripto-attività e l'interdizione dall'esercizio di funzioni di gestione nei prestatori di tali servizi o dalla negoziazione per conto proprio fino a tre anni)<sup>75</sup>.

Lo stesso può dirsi per l'illecito di manipolazione di mercato, le cui peculiarità sono piuttosto da ricercarsi nelle relative modalità commissive legate alle nuove piattaforme

---

<sup>72</sup> Per un primo commento all'allora nuova nozione eurounitaria, v. F. Consulich, F. Mucciarelli, *Informazione e tutela penale dei mercati finanziari nello specchio della normativa eurounitaria sui mercati finanziari*, in *Le Società* 2016, 179 ss.

<sup>73</sup> Nello stesso senso, M. Maugeri, *op. cit.*, 418.

<sup>74</sup> Cfr. art. 193 TUF in relazione agli obblighi previsti dall'art. 114 e 114-bis del medesimo testo unico e art. 32, comma 1, d.lgs. 129/2024 in relazione all'art. 88 MiCAR. La costruzione di tali norme non brilla per la tecnica normativa utilizzata, profilo in realtà comune ai diversi illeciti amministrativi di settore: v. già 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 *Le Società* 2019, 579.

<sup>75</sup> L'elevata incidenza di simili misure sulle libertà personali è particolarmente evidenziata da F. Viganò, *Garanzie penalistiche e sanzioni amministrative*, in *RIDPP* 2020, 1812.

di negoziazione, il cui carattere decentralizzato favorisce o quantomeno rende più semplice la diffusione di condotte elusive dei meccanismi di controllo, in particolare attraverso l'impiego di algoritmi di *trading* automatizzato o particolari tecniche di *wash trading* e *spoofing* più difficilmente riconducibili a un centro decisionale individuabile <sup>76</sup>. Tale frammentazione dei punti di accesso e la possibile anonimizzazione dei soggetti coinvolti rendono infatti più ardua l'attribuzione soggettiva della condotta manipolativa e hanno imposto un parziale ripensamento degli strumenti di vigilanza, affinché le Autorità possano efficacemente presidiare anche gli spazi digitali non intermediati dai tradizionali operatori finanziari.

Non a caso, l'art. 92 del Regolamento MiCA ha previsto anche in questi casi l'adozione di dispositivi, sistemi e procedure efficaci a prevenire e segnalare tempestivamente le condotte di abuso in capo a «chiunque predisponga o esegua a titolo professionale operazioni in cripto-attività». Da richiamare qui la differenza rispetto al MAR, che impone invece tale obbligo ai gestori della sede di negoziazione: il motivo risiede ancora una volta nel carattere decentralizzato che caratterizza il mercato "cripto" e che dunque rende possibile l'assenza di una simile figura.

Così riassunti in breve i punti salienti della disciplina, sul lato sanzionatorio conviene differenziare la posizione di enti e persone fisiche a seconda che la violazione della disciplina di settore riguardi o meno una condotta di *insider trading* o manipolazione di mercato ovvero si risolva nell'inadempimento dell'obbligo di *disclosure* o mancata adozione dei sistemi di prevenzione e rilevamento degli abusi. Nel primo caso, le sanzioni amministrative citate possono essere irrogate direttamente nei confronti sia delle persone fisiche che degli enti. Questi ultimi, peraltro, ne rispondono secondo i criteri di imputazione di cui al d.lgs. 231/2001: sempre replicando la struttura del TUF, l'art. 34 d.lgs. 129/2024 richiama infatti gli elementi costitutivi della responsabilità da reato affinché la persona giuridica possa essere ritenuta responsabile.

---

<sup>76</sup> In relazione alle nuove tecniche di manipolazione operativa, spesso poste in essere tramite l'IA, v. pure F. Consulich, *Intelligenza artificiale e mercati finanziari*, in *Reati in materia bancaria e finanziaria* a cura di F. Consulich, cit., 259 ss.; A.F. Tripodi, *Abusi di mercato e trading algoritmico*, in *Il diritto nell'era digitale*, a cura di R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto, Milano 2022, 745 ss. A commento della nuova recente aggravante per il delitto di cui all'art. 185 TUF proprio in relazione all'utilizzo di sistemi di intelligenza artificiale, v. F. Mucciarelli, *Intelligenza artificiale e condotte manipolative su strumenti finanziari: una nuova aggravante con effetto attenuante*, in [www.sistemapenale.it](http://www.sistemapenale.it), 17.10.2025, che sottolinea il mancato coordinamento con gli effetti dell'art. 39 l. 28 dicembre 2005 n. 262 in relazione al raddoppio dell'originaria cornice edittale.

Al contrario, per le altre due tipologie di violazione il decreto citato individua quale primo responsabile l'ente; la persona fisica potrà essere sanzionata solo quando ricorrono le condizioni poste dall'art. 36 che, sempre sulla falsariga del TUF, prevede che possano essere ritenuti responsabili i «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, quando l'inosservanza è conseguenza della violazione di doveri propri o dell'organo di appartenenza e la condotta ha inciso in modo rilevante sulla complessiva organizzazione o sui profili di rischio aziendali, 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»<sup>77</sup>.

Questi ultimi criteri di imputazione sono poi validi anche per il nuovo illecito amministrativo di ostacolo alle funzioni dell'Autorità di Vigilanza. La norma si inserisce all'interno di un panorama normativo in verità già particolarmente frammentato: alla fattispecie generale di cui all'art. 2638 Cc, si affiancano infatti anche le due figure sussidiarie di cui agli artt. 170-bis TUF (reato) e 187-*quinquiesdecies* TUF (illecito amministrativo), limitatamente alle condotte relative all'attività di vigilanza di Consob e Banca d'Italia, oltre ad altre norme settoriali che vengono in rilievo con riferimento ad altre Autorità<sup>78</sup>. Ebbene, l'art. 35 d.lgs. 129/2024 punisce l'omessa collaborazione o il mancato seguito dato a indagini, ispezioni o richieste, *incluse* (dice la norma) quelle effettuate ai sensi dell'art. 94 par. 3 Regolamento MiCA, che si riferiscono cioè all'attività ispettiva esercitata in materia di abusi di mercato. In considerazione del dato letterale, che sembrerebbe punire con tale illecito amministrativo *ogni* condotta di omessa collaborazione, tra cui *anche* quelle aventi ad oggetto l'attività di vigilanza sulle cripto-attività, la disposizione citata suscita in effetti qualche perplessità per il mancato coordinamento con le altre fattispecie

---

<sup>77</sup> La norma ricalca l'art. 190-bis TUF, che prevede la medesima regola per la maggior parte delle sanzioni amministrative del sistema finanziario. Peraltro, secondo M. Donini, *Il nodo gordiano della vigilanza bancaria*, cit., 38 s. far dipendere l'illiceità della condotta da criteri così elastici sarebbe incompatibile con il principio di legalità, almeno laddove si valutasse tale regola «secondo i parametri delle norme penali».

<sup>78</sup> Cfr. *ex multis* A.F. Tripodi, sub Art. 2638 c.c., *Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza*, in *Commentario del codice civile Scialoja-Branca-Galgano. Disposizioni penali in materia di società, consorzi e altri enti privati*, a cura di G. De Nova, Bologna, 2018, 619 ss.; L. Cornacchia, *L'ostacolo all'Autorità di vigilanza*, in *Reati in materia bancaria e finanziaria*, a cura di F. Consulich, cit., 327 ss. Nella manualistica, v. pure S. Seminara, *Diritto penale commerciale*, Vol. II, Torino 2021, 168 ss.; A. Rossi, *Illeciti relativi al controllo ed alle funzioni di vigilanza*, in F. Antolisei, *Manuale di diritto penale. Leggi complementari*, I, Milano 2022, 333 ss.; E. Amati, N. Mazzacuva, *Diritto penale dell'economia*, Padova 2023, 142 ss.

summenzionate, in più punti sovrapponibili<sup>79</sup>. Manca infatti – come invece presente nei due illeciti del TUF – una clausola di riserva che faccia chiarezza sul punto. In chiave sistematica, sembra potersi sostenere, in primo luogo, che le norme del testo unico citato non dovrebbero poter trovare applicazione laddove l’oggetto dell’attività di vigilanza riguardi una cripto-attività: la soluzione è infatti da preferirsi sulla base dell’esclusione dall’ambito del MiCAR degli strumenti finanziari e, nell’ordinamento interno, dal d.lgs. 129/2024 dei prodotti finanziari. Qualora dunque l’attività di vigilanza riguardasse tali *token*, dovrebbero trovare applicazione le norme previste dal testo unico della finanza; ove invece si trattasse di un *crypto-asset* (comprese le criptovalute), si applicherebbe invece l’illecito di nuova introduzione.

Piuttosto, problemi maggiori sembrano riguardare il delitto previsto dal codice civile, che prevede anche l’ostacolo come oggetto del dolo specifico o come evento del reato<sup>80</sup>. Ebbene, nelle ipotesi in cui l’“omessa collaborazione” o il “mancato seguito alle indagini o richieste” di Banca d’Italia o Consob fosse posto in essere al fine di ostacolarne l’esercizio delle funzioni o integrasse effettivamente un ostacolo alla loro attività di supervisione, a rigore sembrerebbero integrate entrambe le fattispecie, essendo l’art. 2638 Cc una norma generale, suscettibile di applicarsi a ogni contesto sottoposto a vigilanza. Nondimeno, in queste ipotesi deve ritenersi che il delitto codicistico assorba l’illecito amministrativo, così come – seppur in virtù della clausola di riserva – non si fa concorrere il reato citato con gli altri illeciti di ostacolo previsti dal TUF<sup>81</sup>. In breve, è come se l’art. 35 d.lgs. 129/2024 fosse stato pensato (maldestramente) per assolvere nel settore delle cripto-attività alle funzioni svolte

---

<sup>79</sup> V. anche J. Della Torre, G. Ponteprino, *op. cit.*, 32, che concentrano l’analisi sulle condotte di omessa collaborazione relative alla vigilanza sugli abusi di mercato. Occorre comunque tener presente che l’art. 35 d.lgs. 129/2024, come si è visto, richiama *anche* il mancato seguito a un’indagine relativa a ipotesi di *market abuse* ma non esaurisce in ciò solo la sua portata precettiva, essendo piuttosto suscettibile di ricomprendere anche gli altri ambiti soggetti alla supervisione delle Autorità indipendenti (emissione, offerta al pubblico, prestazione di servizi, ecc.).

<sup>80</sup> Sui contorni di tali definizioni, oltre i riferimenti citati *supra*, nota 78, v. anche A. Alessandri, *Diritto penale e attività economiche*, Bologna 2010, 272, in relazione alla necessaria idoneità decettiva della condotta per la fattispecie a dolo specifico e E. Pietrocarlo, *I “labili” confini del concetto di ostacolo all’esercizio delle funzioni delle autorità pubbliche di vigilanza*, in *RDC* 2021, 540 ss.; L. Foffani, *Società*, in *Commentario breve alle leggi penali complementari*, a cura di F. Palazzo, C.E. Paliero, Padova 2007, 2558 circa la nozione di “ostacolo”. V. pure F. Consulich, *Il caso Antonveneta: abuso di informazioni privilegiate e ostacolo alle funzioni di vigilanza*, in *Casi di diritto penale dell’economia, I. Impresa e mercato (Cirio, Parmalat, Antonveneta, Bnl-Unipol)*, a cura di L. Foffani, D. Castronuovo, Bologna 2015, 164, per il quale l’ostacolo potrebbe anche essere inteso, più che come evento, come aggettivo della stessa condotta tipica.

<sup>81</sup> In ordine al concorso tra le diverse norme, v. anche M. Gambardella, *Condotte economiche e responsabilità penale*, Torino 2020, 166 ss.; M. Donini, *Il nodo gordiano della vigilanza bancaria*, cit., 53 ss.

dall'art. 187-*quinqüesdecies* TUF nel campo finanziario, ponendosi come fattispecie sussidiaria rispetto al più grave delitto di ostacolo. Di conseguenza, anche in assenza della clausola di riserva, sembra comunque potersi pervenire alla conclusione per cui, qualora la medesima condotta integri anche il reato di cui all'art. 2638 Cc, si applicherà solamente quest'ultimo e non il relativo illecito amministrativo<sup>82</sup>.

Un'ultima notazione su questo tema. La previsione impone infatti di collaborare anche alla società o persona fisica responsabile di una precedente violazione e che, proprio per l'effetto della propria condotta collaborativa, potrebbe vedersi irrogata una pena o un'altra sanzione sostanzialmente penale. Sul punto, è noto il dibattito che ha interessato l'art. 187-*quinqüesdecies* del TUF relativamente al diritto al silenzio, che ha condotto a una dichiarazione di parziale illegittimità costituzionale anche a seguito di un intervento della Corte di Giustizia UE<sup>83</sup>. Nonostante dunque ad oggi non siano chiari i confini del *nemo tenetur se detegere* specialmente in queste situazioni<sup>84</sup> (in

---

<sup>82</sup> Secondo J. Della Torre, *op. cit.*, 211, il delitto di cui all'art. 2638 Cc, co. 1, sarebbe invece speciale per specificazione relativamente al connotato fraudolento delle condotte e quindi prevalente sull'illecito amministrativo; al contrario, quest'ultimo dovrebbe prevalere sul delitto di cui all'art. 2638 Cc, co. 2, perché a sua volta speciale in relazione all'oggetto dell'attività di vigilanza, ossia le cripto-attività non finanziarie. Ci sembra, tuttavia, che tale ultimo elemento specializzante sia in realtà presente anche con riferimento al delitto di ostacolo previsto dal primo comma della disposizione codicistica: non si può dunque farlo valere solo in un caso e non nell'altro, via che se percorsa porterebbe però a sostenere la specialità bilaterale tra l'art. 35 d.lgs. 129/2024 e l'art. 2638, primo comma, c.c., con l'indesiderabile conseguenza di far concorrere le due fattispecie. Per evitare un simile effetto, è dunque preferibile ritenere che la condotta di ostacolo rappresenti un *quid pluris* rispetto alla semplice «omessa collaborazione o mancato seguito nell'ambito di un'indagine, ispezione o richiesta», in modo speculare alla «mancata cooperazione» di cui all'art. 187-*quinqüesdecies* TUF relativamente all'attività di vigilanza finanziaria. In tal modo, anche in assenza della clausola di riserva, dovrebbe prevalere il reato per le condotte che cagionino altresì un ostacolo, evitandosi così il concorso formale di illeciti.

<sup>83</sup> Il riferimento è a C.G. UE, 2.2.2021, C-489/19, D.B. c. Consob e C. cost., 13.4.2021, n. 84. A commento del caso v., tra gli altri, G.L. Gatta, "Nemo tenetur se detegere" e procedimento amministrativo davanti alla Consob per l'accertamento dell'abuso di informazioni privilegiate: la Cassazione solleva questione di legittimità costituzionale dell'art. 187-*quinqüesdecies* T.U.F., in [www.dirittopenalecontemporaneo.it](http://www.dirittopenalecontemporaneo.it) 27.4.2018; G. Lasagni, *La Corte di Giustizia riconosce il diritto al silenzio nei procedimenti amministrativi punitivi (e la Corte costituzionale conferma)*, in GC 2021, 1179 ss.; E. Basile, *La Corte di Giustizia riconosce il diritto al silenzio nell'ambito dei procedimenti amministrativi "punitivi"*, in [www.sistemapenale.it](http://www.sistemapenale.it) 3.2.2021; C. Bonzano, *Diritto al silenzio e matière pénale*, in DPP 2022, 47 ss.; S. Schiavone, *Il diritto al silenzio nello spazio giuridico europeo: osmosi delle garanzie se la sanzione amministrativa è "punitiva"*, in DPP 2023, 412 ss. Si confronta con la questione, nel più generale ambito del procedimento Consob, anche D. Guidi, *Poteri della Consob ed estensione delle garanzie "penalistiche" al procedimento sanzionatorio amministrativo: verso un nuovo punto di equilibrio?*, in RTDPE 2023, 443 ss.

<sup>84</sup> V. in particolare G. Lasagni, *Banking Supervision and Criminal Investigation*, Cham 2019, 257 ss.; E. Amati, *Dinamiche evolutive del diritto al silenzio. Riflessi sul diritto punitivo e sugli obblighi di collaborazione con le autorità ispettive e di vigilanza*, Torino 2023, 95 ss. e, in relazione al delitto codicistico di ostacolo, 205 ss. Con riferimento alla disposizione in commento, v. pure J. Della Torre, *op. cit.*, 212 s. Si interrogava sulla compatibilità dell'art. 2638 (e 2625) c.c. con il *nemo tenetur*, risolvendo comunque in senso positivo la questione, anche D. Tassinari, *Nemo tenetur se detegere. La libertà dalle autoincriminazioni nella struttura del reato*, Bologna 2012, 374 ss., spec. 382. Anche la giurisprudenza di legittimità pare in effetti orientata in tal senso: cfr. Cass. 8.4.2025

particolare, si discute se il diritto a non collaborare per l'autore della violazione contenga anche un diritto a non consegnare documenti <sup>85</sup>) e posto che il comportamento dell'interessato non potrà consistere in condotte ingiustificatamente dilatorie, come il rifiuto di presentarsi a un'audizione, pare comunque potersi ricavare un insegnamento *minimo* per cui, non potendosi costringere il trasgressore a deporre contro sé stesso, alcune condotte astrattamente sussumibili nell'illecito citato dovrebbero in ogni caso andare esenti da sanzione. È il caso, ad esempio, della persona fisica che, sentita in audizione, si rifiuti di rispondere a una domanda palesemente autoincriminante.

5. Il quadro che emerge da questa rapida ricognizione è dunque quello di un sistema ancora *in fieri*, nel quale la disciplina delle cripto-attività si colloca all'incrocio fra le opposte esigenze di non disincentivare l'innovazione che fa respirare il mercato dei capitali e fornire al contempo una tutela "forte" agli investitori e ai risparmiatori che decidono di acquistare o utilizzare le criptovalute.

Le soluzioni prescelte, tendenzialmente dettate dalla necessità di "inseguire" di volta in volta il progresso tecnologico, hanno portato alla costruzione di una struttura particolarmente stratificata, che l'interprete è chiamato a ricondurre a sistema.

Da questo punto di vista, le questioni affrontate – in particolare per quanto attiene alle offerte abusive di valute virtuali e alle nuove forme di abuso di mercato e all'illecito di ostacolo – mostrano come il diritto penale in questo settore continui a caratterizzarsi come strumento di *enforcement* delle "regole del gioco"<sup>86</sup>, essendo per lo più posto a presidio della disciplina regolatoria sottostante <sup>87</sup>. La linea di

---

(dep. 28.7.2025) n. 27569, concernente tuttavia una ipotesi di mendacio volta a non far emergere la responsabilità penale degli imputati per aggrottaggio. Con riferimento tuttavia al delitto previsto dal primo comma della disposizione, una parte della dottrina ritiene comunque irrilevanti le condotte di mero silenzio, facendo leva sia sulla lettera della norma, che si riferisce a un "occultamento tramite mezzi fraudolenti", sia a un raffronto con la fattispecie di cui al comma 2 dell'art. 2638 Cc: cfr. M. Zannotti, *L'ostacolo all'esercizio delle funzioni di vigilanza* (art. 2638 c.c.), in *I nuovi reati societari: diritto e processo*, a cura di A. Giarda, S. Seminara, Padova 2002, 586; A. Nisco, *L'ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza*, in *RTDPE* 2013, 257 s. Appare comunque il caso di sottolineare come la giurisprudenza sia orientata a riconoscere rilevanza penale al mero silenzio anche in queste ipotesi: cfr. Cass. 20.10.2022 (dep. 7.3.2023) n. 9623 con osservazioni, in relazione alla rilevanza del silenzio, di E. Pietrocarlo, *L'ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza: condivisibili conferme e "punti oscuri" nella recente giurisprudenza di Cassazione*, in *AP* 2023, 15 ss.

<sup>85</sup> V. in particolare C. eur., 4.10.2022, *De Legé v. Paesi Bassi*, che ha posto notevoli limiti sul punto.

<sup>86</sup> L'espressione è naturalmente di C. Pedrazzi, voce *Mercati finanziari (disciplina penale)*, cit., 654. Cfr. anche T. Padovani, *Diritto penale della prevenzione e mercato finanziario*, in *RIDPP* 1995, 638 ss., che riprende tale impostazione in relazione agli abusi di mercato.

<sup>87</sup> Attuali sul punto le considerazioni di F. Bricola, *Profili penali della disciplina del mercato finanziario*, in *Banca*

demarcazione del rischio consentito, il cui superamento integra dunque il reato<sup>88</sup>, risente tuttavia di una opacità di fondo. L'elevatissimo tasso di tecnicismo della materia contribuisce infatti non poco a rendere più sfumato lo stesso confine tra lecito e illecito, o quantomeno l'individuazione di un trattamento sanzionatorio più o meno severo. Emblematico l'esempio dell'abusivismo: la sovrapposizione (apparente) degli artt. 166 TUF e 30 d.lgs. 129/2024 deriva dall'incerto statuto delle criptovalute già sul versante privatistico, riflettendosi l'inquadramento del *token* nell'una o nell'altra categoria direttamente sulla configurabilità della fattispecie. In particolare, si è visto come sia possibile ritenere applicabile la prima norma nei casi in cui l'offerta della valuta virtuale, presentata come mezzo di investimento, fuoriesca dal perimetro applicativo delle norme MiCAR. Ove invece si offra al pubblico uno *stablecoin* senza autorizzazione ovvero si offra la prestazione di servizi per criptovalute, potrà trovare applicazione il meno grave delitto di nuova introduzione, come del resto sembrano testimoniare le prime decisioni della Consob che si sono confrontate con la questione<sup>89</sup>. Se tale soluzione sembra restituire un certo ordine al sistema, non può però sottacersi come l'applicabilità o meno del Regolamento circa le offerte di *crypto-assets* non qualificabili come *stablecoin* (e quindi la possibile qualificazione di tali criptovalute come prodotto finanziario) dipenda dalla possibilità di identificare per esse un emittente, con la censurabile conseguenza per cui dall'esito di tale indagine deriva l'applicazione alternativa del grave delitto previsto dal TUF o di una mera sanzione amministrativa, come sembrano peraltro confermare le recenti decisioni della Consob e della Corte di Cassazione<sup>90</sup>.

Sempre rimanendo nell'ambito della tutela del mercato delle valute virtuali, anche i nuovi illeciti amministrativi punitivi sembrano seguire il medesimo schema, osservabile già dalla tecnica normativa con la quale sono stati redatti. Il massiccio

---

e borsa 1990, 40, che, individuando nel risparmio *ex* 47 Cost. il bene finale tutelato dal delitto di abusivismo bancario, si diceva favorevole a una «proposta diretta a mantenere la trasgressione a pericolo presunto a livello di illecito amministrativo e a costruire, accanto ad essa, una fattispecie caratterizzata dal pericolo concreto, sanzionata penalmente [...]» che contenga elementi ulteriori al mero difetto dell'autorizzazione, quali la mancanza dei suoi «presupposti oggettivi e soggettivi», evitando così un eccessivo arretramento della tutela penale. Nello stesso senso si era espresso A. Fiorella, *Intermediazione del credito e reati bancari (primi riflessi in prospettiva di riforma)*, in *Materiali per una riforma del sistema penale*, Milano 1984, 270 s. Anche per quel che riguarda le criptovalute, la rilevanza penale dell'abusivismo è invece sempre ancorata alla violazione formale della disciplina di settore, e gli stessi illeciti amministrativi, pure per la massima parte così costruiti, raggiungono in ogni caso un livello di afflittività quantomeno comparabile a quello delle sanzioni penali.

<sup>88</sup> Il riferimento è a F. Sgubbi, *Il risparmio come oggetto di tutela penale*, in *GC* 2005, 344.

<sup>89</sup> V. *supra*, par. 3.1.

<sup>90</sup> V. sempre *supra*, note 63 e 66.

ricorso al rinvio al regolamento europeo per l'individuazione del precetto continua a configurarsi, per utilizzare un'espressione di cui si è già fatto uso in materia di sanzioni amministrative per abusi di mercato, come una «pratica diffusa quanto discutibile»<sup>91</sup>, che rende in effetti difficoltosa l'attività di interpretazione. Se non altro, si è condivisibilmente evitata la costruzione di un altro doppio binario, non essendosi replicata in questo settore la stessa duplicazione punitiva ancora vigente in materia di abusi di mercato aventi ad oggetto strumenti finanziari tradizionali<sup>92</sup>. Una simile opzione avrebbe inevitabilmente riprodotto le questioni di compatibilità con il *ne bis in idem* convenzionale, ricreando le tensioni già note nel sistema *market abuse*<sup>93</sup>. A ciò si aggiunga che il legislatore ha comunque introdotto una nuova ipotesi di ostacolo all'Autorità di vigilanza, che si inserisce nella già nutrita selva di illeciti di simile tenore, nel cui ambito potrebbero riproporsi i problemi connessi al *nemo tenetur se detegere*, già affrontati proprio con riferimento all'art. 187-*quinquiesdecies* TUF.

Su questo versante, si continua in effetti a fare uso di sanzioni punitive prive del *nomen* "pena", sottratte al pacchetto di garanzie forti tradizionalmente riservate al penale, virando così su una più comoda tutela amministrativa ma particolarmente temibile per gli attori del mercato mobiliare, perché coniuga elevatissime sanzioni pecuniarie con misure interdittive e meccanismi cd. di *naming and shaming* (ossia, la pubblicazione del provvedimento che accerta la violazione), che possono avere come effetto pratico quello di rendere sostanzialmente impossibile la prosecuzione della propria attività lavorativa<sup>94</sup>. Senza dunque voler aprire un'altra parentesi, sia sufficiente sottolineare come il punto di equilibrio tra efficienza e garanzie in questo particolare frangente sia effettivamente difficile da ricercare<sup>95</sup>.

---

<sup>91</sup> Cit. da F. Mucciarelli, *Gli abusi di mercato riformati e le persistenti criticità di una tormentata disciplina*, in *DPenCont*, 2018, 9. Con riferimento in particolare al nuovo delitto di abusivismo di cui all'art. 30 d.lgs. 129/2024, v. anche R.M. Vadalà, *La fattispecie penale*, cit., 343, secondo la quale un simile rinvio a catena mette «a rischio la conoscibilità del precetto».

<sup>92</sup> Su cui si rinvia per tutti a A.F. Tripodi, *Ne bis in idem europeo e doppi binari punitivi. Profili di sostenibilità del cumulo sanzionatorio nel quadro dell'ordinamento multilivello*, Torino 2022.

<sup>93</sup> Per un riassunto anche delle diverse soluzioni prospettate in dottrina circa il suo superamento, sia consentito il rinvio a A. Gullo, *Materia penale e ne bis in idem: un'introduzione*, in *DPenCont* 2025, 1 ss.

<sup>94</sup> Sottolinea come l'incidenza sul diritto al lavoro quale garantito dall'art. 4 Cost. possa rientrare in una lettura ampia della "libertà personale", F. Mucciarelli, *Sanzioni e attività d'impresa: qualche nota*, in *La pena, ancora fra attualità e tradizione. Studi in onore di Emilio Dolcini*, a cura di C.E. Paliero, F. Viganò, F. Basile, G.L. Gatta, Milano 2018, 1170.

<sup>95</sup> Per un quadro sul punto in relazione anche agli aspetti processuali, v. pure A. Pisaneschi, P. Luccarelli, E. Bindi, *Le sanzioni della Banca d'Italia e della Consob*, in *GC* 2021, 553 ss.

Con riferimento invece al delitto di autoriciclaggio, va comunque osservato che anche in quest'ambito le caratteristiche tecniche delle criptovalute possano incidere sulla valutazione degli elementi costitutivi del reato. La giurisprudenza ha infatti ricondotto l'acquisto di valute virtuali nell'alveo delle attività finanziarie o, più frequentemente, speculative, valorizzando l'elevata volatilità dei *token* e la possibilità di conseguire un rendimento, mentre rimane controversa la sussumibilità degli *stablecoin* in tale nozione, data la sensibilmente minore componente di rischio/rendimento. Analoga attenzione è stata dedicata al profilo dell'ostacolo, che la giurisprudenza ritiene in genere integrato, secondo cadenze criticabili, *in re ipsa* in ragione della pseudonimia tipica delle operazioni su *blockchain*, pur con qualche dubbio nei casi in cui l'acquisto avvenga tramite intermediari soggetti a obblighi di identificazione.

Per concludere, si è visto come la disciplina delle criptovalute costituisca un banco di prova emblematico della capacità del diritto penale di adattarsi a fenomeni tecnologici che è comunque chiamato a regolare facendo uso delle sue categorie tradizionali. Rimanendo dunque sul versante sanzionatorio, dovremo in effetti attendere l'utilizzo che la prassi farà degli strumenti già in vigore, come avvenuto in materia di autoriciclaggio e abusivismo finanziario, e di quelli di nuova introduzione, come gli abusi di mercato, l'illecito di ostacolo e la nuova fattispecie di "cripto-abusivismo", al fine di saggiare correttamente il grado di maturità dell'ordinamento di fronte alle nuove sfide del mercato digitale.