

ANTICIPAZIONI

GIORGIO ARDIZZONE

I profili sanzionatori del Regolamento MiCA*

Il contributo si sofferma sugli obblighi sanzionatori previsti dal Regolamento UE 2023/1114 del 31 maggio 2023, volti sostanzialmente a equiparare il regime punitivo in vigore per gli strumenti finanziari tradizionali anche all'offerta al pubblico, alla negoziazione e alla prestazione di servizi relativi alle cripto-attività. In particolare, dopo aver fornito una panoramica della tipologia di sanzioni amministrative che gli Stati Membri hanno l'obbligo di introdurre, vengono prese in considerazione le norme relative agli abusi di mercato, costruite sulla falsariga del MAR II ma rimodellate in considerazione delle peculiarità dell'oggetto materiale della condotta. Successivamente, sono oggetto di analisi le ulteriori previsioni sanzionatorie – tra cui spiccano la nuova incriminazione dell'abusivismo e l'illecito amministrativo di mancata collaborazione con l'Autorità di Vigilanza – che pure potrebbero creare frizioni con alcuni diritti costituzionalmente garantiti, come il *nemo tenetur se detegere*. Da ultimo, ci si sofferma sulla potestà sanzionatoria dell'ABE, analizzando più da vicino le sanzioni amministrative pecuniarie e le penalità di mora irrogabili direttamente dall'Autorità di vigilanza europea.

The MiCAR Sanctioning Profiles.

*The paper focuses on the sanctioning obligations set out in EU Regulation 2023/1114 of May 31, 2023, which essentially aims at equating the sanctioning regime applicable to traditional financial instruments also to the public offering, trading and provision of services related to crypto-assets. In particular, after providing an overview of the type of administrative sanctions that Member States are obliged to introduce, the paper considers the provisions regarding market abuse, which are structured along the lines of MAR II, but redesigned to take into account the specificities of the material object of the conduct. Next, it analyzes the additional sanctioning provisions – among which the new financial abuse incrimination and the administrative offence of non-cooperation with the supervisory authority stand out – which may also cause friction with some constitutionally guaranteed rights, such as *nemo tenetur se detegere*. Finally, turning to the EBA's sanctioning power, a closer look is taken at the administrative fines and periodic penalty payments that can be imposed directly by the Authority.*

SOMMARIO: 1. Uno sguardo d'insieme. – 2. Gli abusi di mercato. – 2.1. Gli illeciti amministrativi introdotti dal d.lgs. 129/2024. – 3. L'abusivismo. – 4. Gli altri obblighi punitivi. – 5. Le misure di vigilanza dell'ABE. – 6. Conclusioni.

1. *Uno sguardo d'insieme.* In tempi recenti, l'Unione europea ha dedicato crescente attenzione al tema della finanza digitale, al fine di colmare vuoti di tutela creati dall'avvento delle nuove tecnologie, sia nella prospettiva del contrasto al riciclaggio e al finanziamento al terrorismo¹ che relativamente

* Il lavoro è destinato al volume *Le cripto-attività – Bitcoin e altri asset digitali alla prova della regolamentazione europea*, a cura di A. Nuzzo, in corso di pubblicazione. Si ringraziano l'Editore e i Curatori

all'emissione, offerta al pubblico, negoziazione e prestazione di servizi di cd. cripto-attività. Con riferimento a quest'ultima esigenza, è stato quindi adottato il Regolamento UE 2023/1114 (cd. MiCAR), volto proprio a garantire l'integrità di tale mercato e tutelare i detentori di *crypto-assets*². A tal fine, dopo aver stabilito un fitto reticolo di obblighi gravanti sugli attori del mercato digitale, il legislatore europeo ha poi imposto agli Stati Membri di sanzionarne la violazione, sulla base di una tecnica normativa già sperimentata soprattutto in tema di *market abuse*. Lo stesso atto di diritto derivato prevede poi delle penalità di mora e ulteriori sanzioni irrogabili direttamente dall'Autorità Bancaria Europea a emittenti di *token* cd. *significativi*, ossia, in sintesi, caratterizzati da un rischio più elevato e quindi gravati da ulteriori obblighi prudenziali³.

Il contributo si propone quindi di analizzare più da vicino gli obblighi punitivi imposti dal MiCAR e le sanzioni introdotte dal d.lgs. 129/2024, che ha recentemente adeguato l'ordinamento nazionale alla normativa europea.

Come dunque si è accennato, con una discutibile tecnica legislativa, l'art. 111, primo paragrafo, del Regolamento MiCA ha imposto agli Stati Membri, fatte salve le norme penali, di prevedere sanzioni amministrative a presidio di svariati obblighi posti da numerosi articoli dell'atto di diritto derivato, ivi elencati secondo il noto metodo del rinvio⁴. La norma citata suddivide le violazioni da

per averne cortesemente autorizzato la pubblicazione in questa Rivista.

¹ In relazione a questi profili, v. per tutti SOANA, *The anti money laundering regulation of crypto-assets in Europe*, Padova, 2024 e BASILE, *Crypto Assets e responsabilità penale*, in *Reati in materia bancaria e finanziaria* a cura di Consulich, in *Trattato teorico-pratico di diritto penale*, diretto da Palazzo-Paliero-Pelissero, Torino, 2024, 461 ss.

² Per uno sguardo più generale al Regolamento e, in particolare, per un inquadramento delle nozioni di cripto-attività e diverse tipologie di *token*, si rinvia ai volumi collettanei a cura di NICOTRA-SARZANA DI S. IPPOLITO-SIMBULA, *Il MiCAR*, Milano 2023; CAPACCIOLI-GIORDANO, *Crypto-asset: Regolamento MiCA e DLT Pilot Regime*, Milano, 2023.

³ V. *infra*, par. 5.

⁴ Si riporta per comodità il testo dell'art. 111, primo paragrafo, MiCAR: «Fatti salvi le sanzioni penali, [...] gli Stati membri, conformemente al diritto nazionale, provvedono affinché le autorità competenti abbiano il potere di adottare le sanzioni amministrative e altre misure amministrative adeguate in relazione almeno alle violazioni seguenti:

- a) violazioni degli articoli da 4 a 14;
- b) violazioni degli articoli 16, 17, 19, 22, 23, 25, degli articoli da 27 a 41 e degli articoli 46 e 47;
- c) violazioni degli articoli da 48 a 51, degli articoli 53, 54 e 55;
- d) violazioni degli articoli 59, 60, 64 e degli articoli da 65 a 83;
- e) violazioni degli articoli da 88 a 92;

assoggettare a sanzione in sei diverse categorie: le prime tre sono relative all'offerta al pubblico, rispettivamente, di *utility token*, *asset-referenced token* e *token* di moneta elettronica; la quarta riguarda la prestazione di servizi per le cripto-attività; le ultime due si occupano, infine, degli abusi di mercato e dell'obbligo di collaborazione a fronte di attività ispettive dell'autorità di vigilanza competente.

Agli artt. 111 e ss. è previsto un nucleo comune di disposizioni, relative ai metodi di calcolo della sanzione, alla possibilità di proporre impugnazione, alla pubblicazione del provvedimento che irroga la misura e alla segnalazione degli illeciti all'ESMA e all'ABE da parte dell'autorità nazionale competente, ossia Consob o Banca d'Italia. Ogni gruppo di illeciti così individuato ha invece uno statuto leggermente differenziato quanto a contenuto e ad ammontare della sanzione irrogabile, come prescritto dai paragrafi successivi dell'art. 111, che impongono di prevedere un trattamento sanzionatorio più incisivo per le condotte connotate da maggiore offensività per l'integrità del mercato unico a giudizio del legislatore europeo.

Così, in particolare, per tutte le violazioni diverse da quelle riguardanti gli abusi di mercato, si stabilisce che l'autorità di vigilanza competente possa pubblicare una dichiarazione contenente la descrizione della condotta antidoverosa e il suo autore nonché irrogare una sanzione amministrativa pecuniaria che può arrivare, nel caso di persone giuridiche, fino al 3%, 5% o 12,5% del fatturato a seconda che l'illecito riguardi, rispettivamente, l'offerta al pubblico di un *utility token*, la prestazione di un servizio per le cripto-attività, ovvero l'offerta al pubblico di un *token* di moneta elettronica o collegato ad altra attività. Peraltro, in deroga a tali percentuali, il massimo della sanzione può comunque arrivare al doppio del profitto realizzato o delle perdite evitate in conseguenza della violazione. Per le persone fisiche, è altresì prevista la sanzione amministrativa accessoria dell'interdizione temporanea dalla possibilità di prestare servizi per i *crypto-assets*.

In aggiunta a tali misure, laddove sia stato commesso un abuso di mercato, sono previste poi la sospensione o revoca dell'autorizzazione per la persona

f) l'omessa collaborazione o il mancato seguito dato nell'ambito di un'indagine, un'ispezione o una richiesta di cui all'articolo 94, paragrafo 3».

giuridica responsabile, la confisca del profitto e l'interdizione temporanea anche alla negoziazione per conto proprio, oltre a importi massimi molto più elevati per la sanzione pecuniaria⁵.

Per quanto riguarda invece le norme comuni a ciascuna categoria di illeciti, l'art. 112 fissa criteri per la scelta e quantificazione delle misure uguali per ciascuna violazione: in particolare, tra gli altri, si deve tener conto del "grado di responsabilità" dell'autore della violazione, del suo carattere doloso o colposo e delle misure adottate *ex post* per evitarne il ripetersi⁶. Contro tali sanzioni è ammessa impugnazione dinanzi a un organo giurisdizionale interno a ciascun Stato Membro⁷. Inoltre, ai sensi dell'art. 114 del Regolamento, la decisione di irrogare il provvedimento è pubblicata a cura dell'Autorità di vigilanza competente, che ha altresì l'obbligo di informare l'ESMA e l'EBA. Da

⁵ Cfr. art. 111, par. 5, MiCAR, che in caso di commissione di un illecito di abuso di mercato richiede che le Autorità competenti degli Stati Membri possano imporre le seguenti misure: «[...] a) una dichiarazione pubblica indicante la persona fisica o giuridica responsabile e la natura della violazione; b) un'ingiunzione diretta alla persona fisica o giuridica responsabile di porre termine al comportamento che costituisce la violazione e di astenersi da ripeterlo; c) la restituzione dei profitti realizzati o delle perdite evitate grazie alla violazione, nella misura in cui possono essere determinati; d) la revoca o la sospensione dell'autorizzazione di un prestatore di servizi per le cripto-attività; e) l'interdizione temporanea di qualsiasi membro dell'organo di amministrazione del prestatore di servizi per le cripto-attività o di qualsiasi altra persona fisica ritenuta responsabile della violazione dall'esercizio di funzioni di gestione nei prestatori di servizi per le cripto-attività; f) in caso di ripetute violazioni dell'articolo 89, 90, 91 o 92, l'interdizione per almeno 10 anni di qualsiasi membro dell'organo di amministrazione del prestatore di servizi per le cripto-attività o di qualsiasi altra persona fisica ritenuta responsabile della violazione dall'esercizio di funzioni di gestione in un prestatore di servizi per le cripto-attività; g) l'interdizione temporanea dalla negoziazione per conto proprio di qualsiasi membro dell'organo di amministrazione di un prestatore di servizi per le cripto-attività o di qualsiasi altra persona fisica ritenuta responsabile della violazione; h) sanzioni amministrative pecuniarie massime di importo pari almeno al triplo dell'ammontare dei profitti realizzati o delle perdite evitate grazie alla violazione, se questi possono essere determinati, anche se supera gli importi massimi stabiliti alla lettera i) o j), a seconda dei casi; i) in caso di persone fisiche, sanzioni amministrative pecuniarie massime pari almeno a 1 000 000 EUR per violazioni dell'articolo 88 e a 5 000 000 EUR per violazioni degli articoli da 89 a 92 o, negli Stati membri la cui valuta ufficiale non è l'euro, al corrispondente valore nella valuta ufficiale al 29 giugno 2023; j) in caso di persone giuridiche, sanzioni amministrative pecuniarie massime pari almeno a 2 500 000 EUR per violazioni dell'articolo 88 e a 15 000 000 EUR per violazioni degli articoli da 89 a 92, o al 2 % per violazioni dell'articolo 88 e al 15 % per violazioni degli articoli da 89 a 92 del fatturato totale annuo della persona giuridica in base agli ultimi bilanci disponibili approvati dall'organo di amministrazione o, negli Stati membri la cui valuta ufficiale non è l'euro, al corrispondente valore nella valuta ufficiale al 29 giugno 2023 [...]». Per una panoramica generale, v. anche BENCINI-FANFANI, *Supervisory e enforcement nel quadro regolamentare MiCA*, in *Crypto-asset: Regolamento MiCA e DLT Pilot Regime*, cit., 293 ss.

⁶ Cfr. art. 112, primo paragrafo, MiCAR.

⁷ Così l'art. 113 del Reg. UE 2023/1114.

ultimo, è espressamente previsto che si applichi la tutela in materia di *whistleblowing* al segnalante di una delle violazioni indicate dal MiCAR⁸.

Già sulla base di questa breve rassegna si può agevolmente concludere nel senso della natura sostanzialmente penale delle sanzioni previste dagli Stati Membri nell'adeguamento delle loro legislazioni al Regolamento europeo⁹. È noto infatti che da tempo la stessa Corte di Giustizia adotta un approccio sostanziale nel valutare la natura di una sanzione, mutuato dall'esperienza della Corte di Stasburgo che, a partire dalla nota pronuncia *Engel c. Paesi Bassi*¹⁰, applica le garanzie della Convenzione anche agli illeciti formalmente amministrativi ma che abbiano una intrinseca finalità punitiva¹¹. Occorrerà, dunque, valutare la compatibilità delle sanzioni "amministrative" introdotte nel nostro ordinamento almeno con le tutele previste dalla CEDU¹².

⁸ V. infatti l'art. 116 MiCAR, che rinvia alla Direttiva UE n. 2019/1937, recentemente recepita in Italia con il d.l. 24/2023, che ha modificato la disciplina del *whistleblowing*. Sul punto, v. da ultimo COSSU-VALLI, *Il "whistleblowing": dalla Direttiva 1937/2019 al Decreto Legislativo 24/2023*, in *www.federalismi.it*, 26 luglio 2023, 155 ss. Più in generale sulla disciplina nella prospettiva penalistica, v. DELLA BELLA-ZORZETTO (a cura di), *Whistleblowing e prevenzione dell'illegalità - Atti del I Convegno annuale del Dipartimento di Scienze giuridiche "Cesare Beccaria" - Milano, 18-19 novembre 2019*, Milano, 2020.

⁹ In relazione proprio alle sanzioni introdotte con il d.lgs. 129/2024, ne sostengono la natura sostanzialmente penale anche DELLA TORRE-PONTEPRINO, *Commento al D.lgs. 129 del 2024 di attuazione del Regolamento UE sui mercati delle crypto-attività. Le novità sul versante penalistico e amministrativo punitivo*, in *Leg. pen.*, 18 febbraio 2025, 35. *Amplius* v. par. 2.1 e 4.

¹⁰ Corte EDU, 8 giugno 1976, ricorso n. 5100/71, *Engel e a. c. Paesi Bassi*.

¹¹ Per un'analisi dettagliata della centralità del criterio dello scopo della sanzione nel definire la materia penale v. per tutti FR. MAZZACUVA, *Le pene nascoste. Topografia delle sanzioni punitive e modulazione dello statuto garantistico*, Torino, 2017, 26 ss. Più in generale sul concetto di materia penale, v. anche MASERA, *La nozione costituzionale di materia penale*, Torino, 2018 e i diversi lavori nel volume a cura di DONINI-FOFFANI, *La materia penale tra diritto nazionale ed europeo*, Torino, 2018. Più di recente, v. anche CAVALIERE, *Osservazioni intorno al concetto di "materia penale", tra Costituzione e CEDU*, in *questa Rivista*, 2023, 1 ss.; MANACORDA, *Materia penale*, in *Studi in onore di Carlo Enrico Paliero*, a cura di Piergallini-Mannozi-Sotis-Perini-Scoletta-Consulich, Milano, 2023, 1669 ss. Peraltro, in tal modo, il Legislatore europeo aggira i limiti sulla competenza penale dell'UE: etichettando come "amministrativa" una sanzione che arriva a milioni di euro e con chiara finalità punitiva, finisce per adottare una misura equivalente a (se non maggiormente temibile di) una sanzione penale in assenza della necessaria base giuridica. Relativamente all'azione europea nell'ambito penale, v. da ultimo i contributi nel volume a cura di A. M. Maugeri-Sicurella-Siracusano-Vagliasindi-Scalia-Lucifora, *Diritto penale dell'Unione Europea e nell'Unione Europea. Studi in onore di Giovanni Grasso*, Pisa, 2023 e, con specifico riguardo ai problemi che possono porre le "opzioni punitive" comunitarie, GULLO, *Deflazione e obblighi di penalizzazione di fonte UE*, in *Dir. pen. cont.*, 2016, 10 ss.; BERNARDI, *Il costo "di sistema" delle opzioni europee sulle sanzioni punitive*, in *Riv. it. dir. proc. pen.*, 2018, 557 ss.

¹² Sulle sanzioni amministrative già presenti in ambito finanziario, in relazione alla loro agevole riconduzione nell'alveo della materia penale, v. per tutti DONINI, *Il nodo gordiano della vigilanza bancaria*.

Infatti, è bene fin da subito precisare che il d.lgs. 5 settembre 2024, n. 129 ha innovato la disciplina interna su tale versante, predisponendo un fitto reticolo di illeciti amministrativi modellati direttamente sulle norme del Regolamento (artt. 31-39) e una nuova fattispecie sanzionatoria *ad hoc* per l'abusivismo (art. 30).

Così cursoriamente delineato il quadro d'insieme delle sanzioni imposte dal Regolamento MiCA, è opportuno dunque volgere lo sguardo direttamente agli obblighi che l'atto di diritto derivato intende presidiare tramite tale apparato di *enforcement*. In questa prospettiva, emerge la chiara volontà del Legislatore europeo di fornire all'offerta e alla negoziazione di crypto-attività una tutela sostanzialmente coincidente con quella relativa all'offerta e alla negoziazione di strumenti finanziari, pur con le necessarie differenze imposte dalla particolarità dell'oggetto materiale delle condotte¹³. Per questa ragione, anche in virtù dei numerosi obblighi la cui violazione costituisce un illecito da sanzionare *ex artt.* 111 del Regolamento citato, ci si concentrerà dapprima sulle norme relative agli abusi di mercato, mutate dalla normativa sui prodotti finanziari con i dovuti adattamenti¹⁴; successivamente, si prenderanno in rassegna altri obblighi la cui violazione è stata sanzionata ai sensi del MiCAR, che pure ricalcano alcuni illeciti presenti nel TUF a tutela del risparmio, come appunto l'abusivismo, o a presidio del corretto svolgimento della funzione di vigilanza, come l'omessa collaborazione con la Consob o Banca d'Italia, peraltro di recente oggetto di una sentenza manipolativa di accoglimento della Corte costituzionale per contrasto con il principio del *nemo tenetur se detegere*¹⁵. Da ultimo, verranno prese in considerazione le sanzioni pecuniarie e le

Aspetti problematici del rapporto tra sanzioni penali e amministrative, in *Riv. trim. dir. pen. econ.*, 2023, 23 ss.

¹³ Non sfugge che, a differenza di quanto avvenuto con MAD II e con il Regolamento n. 596/2014, manca in quest'ambito quella «opzione netta a favore della sanzione criminale, reputata indispensabile a fronte della dimostrata inadeguatezza delle sanzioni amministrative, tanto sul versante preventivo quanto su quello repressivo» (MUCCIARELLI, *Mercato finanziario e tutela penale*, in *Reati in materia bancaria e finanziaria* a cura di Consulich, cit., 117). Non a caso, il d.lgs. 129/2024, come si vedrà, ha introdotto una sola nuova norma incriminatrice, lasciando agli illeciti amministrativi il compito di presidiare gran parte delle condotte offensive aventi ad oggetto i *crypto-assets*. Nondimeno, la tipizzazione delle condotte vietate pare avere seguito la medesima tecnica normativa.

¹⁴ Negli stessi termini, M. MAUGERI, *Crypto-attività e abusi di mercato*, in *Il Mulino - Osservatorio del diritto civile e commerciale*, 2022, 425.

¹⁵ Cfr. Corte cost., 13 aprile 2021, n. 84; v. Per i dovuti riferimenti bibliografici, v. *infra*, par. 4.

penalità di mora irrogabili direttamente dall'ABE che, pur essendo formalmente "amministrative" per espressa disposizione dell'atto di diritto derivato¹⁶, hanno una esplicita funzione punitiva.

2. *Gli abusi di mercato.* L'art. 2, paragrafo 4, MiCAR esclude dal suo ambito di applicazione le cripto-attività qualificabili come strumenti finanziari. Di conseguenza, sulla base della qualificazione o meno del *crypto-asset* come strumento finanziario, ci si trova di fronte a due diversi e paralleli tipi di tutela: il primo comprende le diverse norme sanzionatorie, amministrative e penali, contenute all'interno del TUF e che si applicano laddove la cripto-attività rientri nella definizione fornita dall'art. 1, secondo comma, del testo unico citato; il secondo è invece comprensivo delle norme sanzionatorie *ex d.lgs.* 129/2024, introdotte in adeguamento della nuova disciplina europea che, è bene subito precisare, non contemplano sanzioni penali per gli abusi di mercato.

Tale tutela ha perciò carattere residuale: si applica unicamente laddove la rappresentazione digitale di un valore o diritto emesso mediante tecnologia DLT non sia suscettibile di essere qualificata come strumento finanziario. A questo proposito, il d.l. n. 25 del 17 marzo 2023 (cd. "Decreto Fintech"), recependo le indicazioni fornite dal Regolamento Pilota¹⁷, aveva già modificato l'art. 1 del TUF prima dell'entrata in vigore del MiCAR, precisando che possono essere strumenti finanziari anche quelli "*emessi mediante tecnologia a registro distribuito*"¹⁸.

Occorre dunque intendersi su quali siano i casi in cui le cripto-attività possano essere così qualificate, operazione invero non semplice e sulla quale non vi è

¹⁶ V. art. 133, par. 2, Reg. UE 2023/1114.

¹⁷ Si tratta del Regolamento UE 2022/858 che ha modificato l'art. 4 della MiFiD II, ricomprendendo nel novero degli strumenti finanziari anche quelli «emessi, registrati, trasferiti e stoccati mediante tecnologia DLT».

¹⁸ Appare appena il caso di precisare che l'aggiunta del Legislatore, ampliando lo spettro dell'oggetto materiale delle condotte, ha generato una nuova incriminazione, nonché, al contempo, un'estensione dei fatti suscettibili di ricadere nel perimetro applicativo dei diversi illeciti amministrativi previsti dal TUF. Prima di tale modifica, infatti, non era possibile qualificare i *crypto-assets* come strumenti finanziari in senso stretto, con conseguente inapplicabilità delle norme sanzionatorie aventi tale oggetto materiale.

unicità di vedute¹⁹ ma che ha importanti ricadute per il penalista poiché, come si è accennato, dall'inquadramento o meno del *crypto-assets* come strumento finanziario dipende la rilevanza penale della condotta di abuso di mercato. A tal proposito, il paragrafo 5 dell'art. 2 del Regolamento conferisce all'ESMA la facoltà di elaborare orientamenti «sulle condizioni e sui criteri per la qualificazione delle cripto-attività come strumenti finanziari». La norma, in punto di legalità, desta qualche perplessità, proprio per i possibili riflessi sul versante penalistico. Tale potere definitorio affidato a un'Autorità amministrativa europea rischia in effetti di non risultare pienamente conforme al principio di riserva di legge in materia penale, essendo difficile argomentare sul piano della natura esclusivamente tecnica dell'integrazione²⁰. Si tratta infatti di precisazioni non meramente interpretative ma suscettibili di modificare sensibilmente – e, ci sembra, in modo imprevedibile – il perimetro delle norme penali: se si rientra nell'ambito applicativo del TUF, la condotta abusiva potrà integrare tanto il delitto di abuso di informazione privilegiata o manipolazione di mercato quanto i corrispondenti illeciti amministrativi²¹; al contrario, la sola tutela MiCAR, come si è accennato, imponeva di

¹⁹ V. per tutti ANNUNZIATA, *La disciplina del mercato dei capitali*, Torino, 2023, 517 ss.; ID., *Tassonomia delle cripto-attività e mercato dei capitali. Primi spunti per un confronto USA-UE*, in *Giur. comm.*, 2024, 5, 915 ss.

²⁰ Ha già sollevato dubbi sul rispetto del principio di legalità da parte della disciplina europea in materia finanziaria proprio in ragione dell'integrazione del precetto da parte di Autorità amministrative svincolate dalla rappresentatività popolare, DONINI, *Il nodo gordiano della vigilanza bancaria*, cit., 35 ss. e spec. 70, anche con la dovuta bibliografia in merito al rapporto tra democrazia e autorità dipendenti. Non si tratta però di una tecnica nuova: a titolo esemplificativo, l'art. 7 par. 5 MAR II permetteva all'ESMA di pubblicare un elenco indicativo di informazioni che avessero carattere privilegiato ai fini della sussistenza dell'*insider trading*. Nella stessa prospettiva in relazione alla manipolazione di mercato, anche PALIERO, *Nuove prospettive degli abusi di mercato?*, in *La crisi finanziaria: banche, regolatori, sanzioni*, Milano, 2010, 69 ss., che già criticava la scelta di affidare alla regolamentazione secondaria di settore la "esemplificazione" («in realtà, *definizione*») di possibili condotte manipolative e di prassi di mercato ammesse, reputandola in contrasto con i «fondamenti costituzionali». Critico sul punto anche MUCCIARELLI, sub *Art. 185 T.U.F.*, in *Il Testo Unico della Finanza* a cura di Fratini-Gasparri, Milano, 2012, 2408 s.

²¹ Sul doppio binario in materia, si rinvia per tutti a TRIPODI, *Ne bis in idem europeo e doppi binari punitivi. Profili di sostenibilità del cumulo sanzionatorio nel quadro dell'ordinamento multilivello*, Torino, 2022. Per quanto riguarda le fattispecie penali di abuso di informazione privilegiata e manipolazione di mercato, limitandoci ai contributi monografici, cfr. PREZIOSI, *La manipolazione del mercato*, Bari, 2008; CONSULICH, *La giustizia e il mercato. Miti e realtà di una tutela penale dell'investimento mobiliare*, Milano, 2010, 193 ss.; AMATI, *Abusi di mercato e sistema penale*, Torino, 2012, 67 ss. e 171 ss.; TRIPODI, *Informazioni privilegiate e statuto penale del mercato finanziario*, Padova, 2012, 71 ss.; F. D'ALESSANDRO, *Regolatori del mercato, enforcement e sistema penale*, Torino, 2014, 101 ss. GUIDI,

prevedere unicamente sanzioni amministrative punitive, senza esigere di replicare lo schema del doppio binario, che in effetti non è stato riproposto dal d.lgs. 129/2024.

Nondimeno, la costruzione di tali illeciti è innegabilmente avvenuta sulla falsariga di quanto già previsto nel MAR II.

In particolare, così come previsto nel Regolamento UE n. 596/2014, il divieto di *insider trading* – comprensivo anche delle condotte di *tipping* e *tuyautage* – poggia sulla nozione di informazione privilegiata²². Eppure, vi sono profili di differenza rispetto alla normativa MAR II a causa della particolare natura delle cripto-attività e che meritano quindi di essere analizzati più da vicino. Dal punto di vista contenutistico, in particolare, è già stato evidenziato come sia stato ampliato il novero di soggetti che l'informazione può riguardare: non più i soli emittenti, ma anche gli offerenti e coloro che chiedono l'ammissione alla negoziazione di un'attività digitale²³. Tale estensione si giustifica sulla base della peculiarità del mercato digitale rispetto alla negoziazione di strumenti finanziari tradizionali: trattandosi di prodotti emessi tramite tecnologia a registro distribuito, è facile che entrino in contatto con conoscenze privilegiate attori come i *miners* e i *wallet providers*, estranei alla negoziazione dei prodotti finanziari diversi dai *token*, che diventano così possibili soggetti attivi dell'illecito²⁴. L'art. 89, par. 5, lett. c) del Regolamento prevede infatti che il divieto di *insider trading* gravi anche su chi, in relazione al suo ruolo nella tecnologia DLT, venga a conoscenza dell'informazione privilegiata.

Per quanto riguarda invece i profili oggettivi, il MiCAR si limita a riprodurre l'art. 7 MAR II. In particolare, viene definita privilegiata l'informazione che,

Abuso di informazioni privilegiate, Torino, 2024.

²² Su cui v. TRIPODI, *Informazioni privilegiate e statuto penale del mercato finanziario*, cit., 221 ss.; D'ALESSANDRO, *Regolatori del mercato, enforcement e sistema penale*, cit., 113 ss. e, più di recente, CONSULICH-MUCCIARELLI, *Informazione e tutela penale dei mercati finanziari nello specchio della normativa euromunitaria sui mercati finanziari*, in *Le Società*, 2016, 179 ss.; AMATI, *L'abuso o comunicazione illecita di informazioni privilegiate*, in *Reati in materia bancaria e finanziaria* a cura di Consulich, cit., 166 ss.; GUIDI, *Abuso di informazioni privilegiate*, cit., 221 ss. Nella manualistica, cfr. SEMINARA, *Diritto penale commerciale. Vol. III*, Torino, 2018, 58 ss.

²³ Cfr. M. MAUGERI, *Cripto-attività e abusi di mercato*, cit., p. 418. Sul punto, v. anche BENCINI-FANFANI, *Prevenzione degli abusi di mercato relativi alle criptoattività*, in *Crypto-asset: Regolamento MiCA e DLT Pilot Regime*, cit., 252 ss.; MIRODDI, *Tutela dell'integrità del mercato: le regole per prevenire gli abusi di mercato*, in *Il MiCAR*, cit., 102.

²⁴ Così anche la stessa ESMA, *Initial coin offerings and crypto-assets*, 9 gennaio 2019, par. 20 ss., 9 s.

se resa pubblica, «potrebbe avere un effetto significativo» sui prezzi non di strumenti finanziari ma di cripto-attività²⁵. Allo stesso modo, viene specificato che per tale nozione si intende l'informazione su cui (non un investitore ragionevole ma) un «possessore di cripto-attività ragionevole» baserebbe le proprie scelte di investimento.

Tale differenza semantica, secondo alcuni, non è casuale. Come infatti è stato osservato, a differenza degli strumenti finanziari tradizionali, è possibile che il rendimento di un *token* non sia agganciato al valore reale di alcun bene ma si «esaurisca nella sola dimensione digitale»²⁶. Ciò è vero, in particolare, per gli *utility token*, il cui prezzo può in taluni casi prescindere dallo stato di salute dell'impresa emittente ed è, per definizione, svincolato da altro valore o diritto. Ora, seguendo il paradigma dell'investitore ragionevole, si è soliti ritenere che l'informazione privilegiata debba essere oggettiva, attendibile e soprattutto capace di segnalare che il prezzo di mercato del titolo sia più basso o più alto del suo valore reale, di modo che un investitore professionale, secondo logica, sia portato a negoziare gli strumenti finanziari sovrastimati o sottostimati, lucrando la differenza²⁷. Se dunque tale è il parametro, almeno con riferimento agli *utility token*, si dovrebbero ritenere privilegiate tutte le informazioni idonee a determinare gli investitori digitali a negoziare cripto-attività anche se non incidono su alcun valore reale, comprese quelle che riguardano andamenti speculativi o irrazionali del mercato²⁸. In altri termini, se è vero che il «possessore ragionevole di cripto-attività» si comporta come l'investitore ragionevole, le peculiarità dei *crypto-assets* permettono di basare la propria (logica) decisione di negoziare tali strumenti digitali anche su informazioni che non avrebbero tale effetto con riferimento ai titoli tradizionali, così estendendo la portata della nozione di informazione privilegiata e, conseguentemente,

²⁵ V. però M. MAUGERI, *Cripto-attività e abusi di mercato*, cit., p. 419 che ritiene ci siano particolari differenze, soprattutto in relazione alla significatività di informazioni esterne all'emittente. Cfr. anche CONSULICH, *Il nastro di Möbius. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso di mercato*, in *Banca, borsa, titoli di credito*, 2018, 207 ss. che pure da tempo avvertiva come la figura dell'investitore ragionevole sarebbe diventata anacronistica con le nuove tecnologie.

²⁶ Così anche M. MAUGERI, *Cripto-attività e abusi di mercato*, cit., 429.

²⁷ V. nella manualistica SEMINARA, *Diritto penale commerciale*, cit., 62. Per una critica alla nozione di investitore ragionevole, v. già TRIPODI, *Informazioni privilegiate*, cit., 259 ss. e, in relazione allo specifico ambito delle cripto-attività, DELLA TORRE-PONTEPRINO, *Commento al D.lgs. 129 del 2024*, cit., 29.

²⁸ Questa è la posizione di M. MAUGERI, *Cripto-attività e abusi di mercato*, cit., 432 e nota 82.

gli obblighi di comunicazione a essa connessi e il perimetro applicativo delle relative fattispecie sanzionatorie.

Per quanto riguarda, invece, il divieto di manipolazione di mercato, non si registrano particolari scostamenti rispetto alla disciplina introdotta con MAR II con riferimento agli strumenti finanziari. Piuttosto, l'esigenza di estendere tale normativa è data dalla relativa facilità con cui è possibile porre in essere condotte di manipolazione operativa "tradizionale"²⁹ su piattaforme di negoziazione DLT e dall'emersione di pratiche nuove proprie dell'ecosistema digitale³⁰.

A tal proposito, replicando lo stesso schema dell'art. 16 del Regolamento UE n. 596/2014, l'art. 92 MiCAR impone determinati obblighi di *compliance* tecnica volti a prevenire e individuare condotte anomale sui mercati digitali, accompagnate dall'obbligo di segnalazione dell'abuso all'Autorità competente. In particolare, è affidato nuovamente all'ESMA il compito di elaborare norme tecniche volte a specificare i dispositivi o i sistemi da implementare a tal fine. L'unica differenza di rilievo rispetto alla tutela MAR II riguarda ancora una volta il soggetto tenuto all'adempimento. Infatti, in relazione agli strumenti finanziari "classici" tale obbligo poteva gravare unicamente sul gestore del mercato o della sede di negoziazione. È però possibile, tramite la tecnologia a registro distribuito, scambiare *crypto-assets* su piattaforme DLT «decentralizzate», ossia in assenza di un'autorità "centrale" garante delle operazioni. Per questo motivo, il Regolamento impone l'obbligo di individuare e comunicare gli abusi di mercato non al gestore della piattaforma di negoziazione – che potrebbe anche non esserci – ma a «chiunque predisponga o esegua a titolo professionale operazioni in crypto-attività». I destinatari dell'obbligo so-

²⁹ Con riferimento alla nozione di manipolazione operativa/informativa, anche per la dovuta bibliografia sul punto, v. per tutti D'ALESSANDRO, *La manipolazione del mercato*, in *I reati in materia bancaria e finanziaria* a cura di Consulich, cit., 203 ss. e 207 ss.

³⁰ M. MAUGERI, *Cripto-attività e abusi di mercato*, cit., p. 421. Sulle peculiarità dei mercati DLT in ordine alla tutela del corretto funzionamento del mercato dei capitali, v. anche TAGLIAMONTE, *L'integrità dei mercati delle crypto-attività, tra vecchie e nuove tutele*, in *Il Mulino - Osservatorio del diritto civile e commerciale*, 2022, 381 ss. Per le nuove pratiche manipolative nell'odierno funzionamento dei mercati finanziari, v. CONSULICH, *Il nastro di Möbius*, cit., 201 ss.; ID., *Intelligenza artificiale e mercati finanziari*, in Consulich (a cura di), *Reati in materia bancaria e finanziaria*, cit., 255 ss.; TRIPODI, *Abusi di mercato e trading algoritmico*, in *Il diritto nell'era digitale*, a cura di Giordano-Panzarola-Police-Preziosi-Proto, Milano, 2022, 745 ss.

no dunque da ricercarsi sulla base della professionalità dell'attività svolta: è vero infatti che la maggioranza delle operazioni sono svolte per il tramite dei cd. *wallet providers*, primi soggetti obbligati ai sensi dell'art. 92 MiCAR, che detengono le chiavi crittografiche dei clienti al fine di effettuare gli scambi dei valori digitali. Nondimeno, desta qualche perplessità obbligare tali gestori a denunciare i loro clienti in caso rilevino "qualsiasi ragionevole sospetto" di condotte abusive.

Appare evidente, all'esito di questa breve rassegna, che il Legislatore europeo abbia in ogni modo cercato di equiparare la tutela dei mercati finanziari tradizionali a quella dei mercati digitali, almeno con riferimento agli abusi di mercato. Eppure, in virtù della limitata competenza dell'Unione in materia penale³¹, MiCAR non può che imporre agli Stati Membri di adottare sanzioni amministrative (anche se, come si è visto, sostanzialmente punitive).

2.1. *Gli illeciti amministrativi introdotti dal d.lgs. 129/2024.* La scelta del Legislatore nazionale, come si è accennato, è stata dunque quella di non andare oltre quanto richiesto e introdurre – in relazione a questa categoria di condotte – solo illeciti amministrativi. È bene in primo luogo precisare nuovamente che il perimetro applicativo di tali fattispecie non si sovrappone in alcun modo a quelle previste dal TUF e si distingue in virtù dell'oggetto materiale della condotta, che *non* deve essere uno strumento finanziario.

Relativamente agli abusi in senso stretto, l'art. 33 del decreto citato prevede quindi la sanzione amministrativa pecuniaria da cinquemila a cinque milioni di euro per tutte le condotte di *insider trading* – comprese il *tipping* e il *tuyau-tage* – e per la manipolazione di mercato, rinviando *in toto* agli artt. 89, 90 e 91 del Regolamento. È poi previsto che la suddetta sanzione debba essere elevata fino al triplo laddove il profitto ottenuto – che deve essere determinabile – sia superiore al massimo edittale. Inoltre, sempre tramite la tecnica del rinvio all'art. 111 MiCAR, è data facoltà alla Consob di irrogare determinate sanzioni accessorie: dichiarazione pubblica indicante l'autore della violazione,

³¹ Per un inquadramento generale, v. nella manualistica MARINUCCI-DOLCINI-GATTA, *Manuale di diritto penale. Parte generale*, Milano, 2023, 52 ss., nonché i diversi contributi contenuti nel volume a cura di GRANDI, *I volti attuali del diritto penale europeo*, Ferrara, 2021.

restituzione dei profitti o delle perdite evitate, revoca o sospensione dell'autorizzazione a operare come prestatore di servizi per cripto-attività, interdizione dall'esercizio di funzioni di gestione nei prestatori di tali servizi da sei mesi a tre anni, nonché dalla negoziazione per conto proprio fino a tre anni³².

Per le medesime violazioni, l'art. 34 del decreto prevede la responsabilità della persona giuridica nel cui interesse o vantaggio sono commessi gli illeciti, ricalcando l'art. 187-*quinquies* del TUF. La norma ripropone infatti i medesimi meccanismi di imputazione di cui al d.lgs. 231/2001, al quale espressamente rinvia. Perché dunque possa essere irrogata la sanzione pecuniaria fino a quindici milioni di euro – o, laddove il profitto sia superiore, quindici per cento del fatturato totale annuo –, occorrerà la sussistenza anche della cd. colpa d'organizzazione, al contrario delle altre sanzioni amministrative, pure previste dal decreto, per le quali l'ente continua a rispondere in via oggettiva³³. Appare appena il caso di notare come tutte le sanzioni così introdotte risultino di pari importo a quelle previste dal TUF per i medesimi comportamenti aventi ad oggetto gli strumenti finanziari tradizionali³⁴. L'unica differenza so-

³² Cfr. art. 32, commi 3 e 4, e 36, comma 3, d.lgs. 129/2024.

³³ Sulla struttura di tale illecito dell'ente, non essendo qui possibile riportare la sterminata bibliografia sul punto, si rinvia per tutti a MONGILLO, *La colpa d'organizzazione: enigma ed essenza della responsabilità "da reato" degli enti*, in *Cass. pen.*, 2023, 4, 704 ss. e, nella manualistica, LATTANZI-SEVERINO (a cura di), *Responsabilità da reato degli enti*, Torino, 2020. Va in ogni caso sottolineato come tale scelta di imputazione dell'illecito alla persona giuridica costituisca una prassi virtuosa seguita dal Legislatore, inaugurata proprio con l'art. 187-*quinquies* del TUF per le sanzioni amministrative e oggi replicata, in parte, per le misure punitive in ambito fiscale: cfr. d.lgs. 128/2015 come modificato dai d.lgs. 221/2023 e 108/2024 in tema di *Tax Control Framework*. Sul tema, v. ALLENA, *Il regime di adempimento collaborativo nella recente riforma tributaria*, in *Dir. Prat. Trib. Int.*, 2024, 2, 434 ss.; MARINO, *La nuova cooperative compliance: profili generali*, in *La riforma fiscale, diritti e procedimenti*, a cura di Giovannini, Pisa, 2024, vol. I, 185 ss., nonché, in prospettiva penalistica, CONSULICH, *La collaborazione pubblico-privato nello specchio della colpa d'organizzazione: il caso del Tax Control Framework*, in *Riv. Dir. Trib.*, 2024, 5 ss. La scelta legislativa impone infatti di non irrogare sanzioni all'ente che si è dotato di un assetto organizzativo adeguato a prevenire la commissione di illeciti al suo interno, permettendo così di premiare la società *compliant* e, conseguentemente, spostare il baricentro della risposta statuale dalla repressione alla prevenzione. Nel senso proprio dell'auspicabilità di una *compliance* "integrata" (e, cioè, non solo penalistica), v. per tutti SEVERINO, *Fiscalità e competitività ai tempi del PNRR*, in *Rass. Trib.*, 2022, pp. 461 ss. Per un quadro più generale della filosofia della *compliance* nel sistema sanzionatorio degli enti collettivi, v. per tutti SEVERINO, *La responsabilità dell'ente ex d.lgs. n. 231 del 2001: profili sanzionatori e logiche premiali*, in *La pena, ancora: fra attualità e tradizione. Studi in onore di Emilio Dolcini*, a cura di Paliero-Viganò-Basile-Gatta, Milano, 2018, vol. 2, 1101 ss.

³⁴ Su cui v. per tutti TRIPODI, *Gli illeciti amministrativi in tema di abusi di mercato*, in *Reati in materia bancaria e finanziaria* a cura di Consulich, cit., 275 ss.

stanziale sta nella irrilevanza penale della condotta. Tale disparità di trattamento si candida dunque a ulteriore argomento a sostegno della illegittimità del doppio binario³⁵: la sua mancata riproposizione sembra infatti suscettibile di integrare un profilo di irragionevolezza *ex art. 3 Cost.* per il sistema punitivo del TUF, risultando complesso argomentare circa il maggior disvalore di comportamenti aventi ad oggetto strumenti finanziari piuttosto che *crypto-assets*; non a caso, le cornici edittali dei relativi illeciti amministrativi sono le medesime.

Per quanto riguarda gli altri obblighi cui si è dato attuazione, l'art. 32 d.lgs. 129/2024 sanziona la mancata comunicazione al pubblico di informazioni privilegiate e la mancata predisposizione di sistemi di individuazione e rilevazione degli abusi di mercato, rinviando rispettivamente agli artt. 88 e 92 MiCAR e ai relativi atti delegati e di attuazione. Sempre seguendo la falsariga del TUF, è previsto che le sanzioni siano irrogabili nei confronti delle persone giuridiche senza necessità di ulteriori condizioni; al contrario, perché possano essere inflitte anche alle persone fisiche è necessario che siano integrati i presupposti specificati dall'art. 36, primo comma, del decreto citato, modellato sull'art. 190-*bis* del TUF³⁶.

In particolare, è previsto che possano esserne destinatari tanto i soggetti apicali quanto il «personale» delle società responsabili degli illeciti al ricorrere di due condizioni cumulative: a) la violazione deve essere «conseguenza» del mancato rispetto «dei doveri propri o dell'organo di appartenenza»; b) la condotta deve aver inciso «in modo rilevante sulla complessiva organizzazione

³⁵ V. *supra*, nota 21.

³⁶ Si riporta per comodità il testo dell'art. 36, primo comma, d.lgs. 129/2024: «Fermo restando quanto previsto per le società e gli enti nei confronti dei quali sono accertate le violazioni, le sanzioni e le altre misure amministrative indicate dagli articoli 31, commi 1, lettera b), e 3, 32, commi 1, lettera b), 2, lettera b), e 4, e 35, comma 1, lettera b), del presente decreto si applicano nei confronti dei soggetti che svolgono funzioni di amministrazione, direzione o controllo e del personale delle società e degli enti nei confronti dei quali sono accertate le violazioni, 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». Sulla norma «gemella» prevista dal TUF, che ripropone le medesime condizioni per applicare le sanzioni amministrative diverse da quelle in materia di *market abuse* alle persone fisiche, v. BONETTI, sub *Art. 190-bis T.U.F.*, in *Commentario Breve al Testo unico della finanza* a cura di Calandra Buonauro, Padova, 2020, 1359 ss.

o sui profili di rischio aziendali, ovvero 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»³⁷.

3. *L'abusivismo*. Si è accennato che il Regolamento europeo imponeva in realtà di prevedere numerosissime sanzioni amministrative, volte a presidiare quasi ogni adempimento imposto agli attori del mercato digitale e andando ben oltre il mero divieto di abusi di mercato. Tale costellazione di illeciti, costruiti già nel MiCAR, come pure si è accennato, con la tecnica del rinvio, tende a punire le irregolarità nei diversi momenti di negoziazione e offerta delle cripto-attività, differenziandosi per la tipologia di *token*. In particolare, non potendosi qui fornire una elencazione esaustiva di tutti gli obblighi oggi presidiati da sanzioni amministrative *ad hoc*, verranno prese in considerazione le sole violazioni maggiormente rilevanti.

In primo luogo, è imposto di sanzionare l'offerta al pubblico senza autorizzazione e la prestazione non autorizzata di servizi per le cripto-attività³⁸. Nondimeno, con riferimento a questi specifici obblighi, non avrebbe sorpreso se il nostro Paese si fosse avvalso della facoltà prevista dal paragrafo 1, secondo comma, dell'art. 111 MiCAR, comunicando alla Commissione che tale condotta costituiva già reato nel nostro ordinamento.

L'art. 166, lett. a) e c), del TUF prevedeva infatti già sanzioni penali per chi, senza esservi abilitato, svolge servizi o attività di investimento ovvero offre fuori sede, «promuove o colloca mediante tecniche di comunicazione a distanza, prodotti finanziari o strumenti finanziari o servizi o attività di investi-

³⁷ Pare qui il caso di ricordare l'insegnamento recente di DONINI, *Il nodo gordiano della vigilanza bancaria*, cit., 38 ss. e nota 9 che fa notare come una simile tecnica legislativa (che fa discendere la conseguenza sanzionatoria da un parametro elastico come "l'incisione rilevante sui profili di rischio aziendale" della propria condotta) sia incompatibile con il principio di legalità. Lo statuto convenzionale (e costituzionale) di tali illeciti è perciò particolarmente problematico, anche considerata la loro pacifica appartenenza alla materia penale.

³⁸ V. art. 111, primo paragrafo, lett. a), b), c) e d) del MiCAR. Sui profili dell'offerta al pubblico nella proposta di regolamento, v. FRIGENI, *Il mercato primario delle cripto-attività. Offerta al pubblico e regime di trasparenza nella Proposta di Regolamento MiCA*, in *Il Mulino - Osservatorio del diritto civile e commerciale*, 2022, 23 ss.

mento»³⁹.

Si è visto infatti come solo grazie alle modifiche introdotte in attuazione del Regolamento pilota sia possibile qualificare come “strumenti finanziari” i *crypto-assets*; al contrario, era invece già possibile ritenere che questi ricadessero nel perimetro applicativo delle sole norme aventi ad oggetto materiale i “prodotti finanziari”, la cui definizione è più ampia, ricomprendendo anche ogni altra forma di investimento diversa dagli strumenti finanziari⁴⁰. In questo senso, invero, si era espressa parte della dottrina, nonché un orientamento giurisprudenziale che aveva ritenuto applicabile la fattispecie di abusivismo anche all’offerta al pubblico senza autorizzazione di criptovalute⁴¹.

La Corte di Cassazione sembrava infatti propendere per l’applicabilità della

³⁹ Sul delitto di abusivismo, anche con i dovuti riferimenti bibliografici, v. SEMINARA, *Diritto penale commerciale*, cit., 22 ss. e, proprio con riferimento alle crypto-attività, NADDEO, *Nuove frontiere del risparmio, bitcoin exchange e rischio penale*, in *Dir. pen. proc.*, 2019, 104; RECCHIA, *La tutela del corretto svolgimento dell’attività di intermediazione*, in *Reati in materia bancaria e finanziaria* a cura di Consulich, cit., 31 ss.; CONSULICH, *Il diritto penale nell’età del crypto-oro. Gli elementi normativi della fattispecie di abusivismo finanziario tra monete virtuali e investimenti reali*, in *Giur. comm.*, 2022, 928 ss. Appare appena il caso di precisare che, come recentemente riconosciuto anche in giurisprudenza, non poteva invece applicarsi il delitto di emissione abusiva di moneta elettronica ex art. 131-bis TUB, stante la diversa definizione normativa di crypto-valuta: cfr. Corte d’Appello di Milano, Sez. II pen., 13 giugno 2024, n. 1879.

⁴⁰ Cfr. art. 1, comma 1, lett. u) TUF, per cui sono “prodotti finanziari”: «gli strumenti finanziari e ogni altra forma di investimento di natura finanziaria». Sulla tale possibile qualificazione delle crypto-attività, v. ex multis ANNUNZIATA, *Verso una disciplina europea delle cryptoattività: riflessioni a margine della recente proposta della Commissione UE*, in www.diritto bancario.it, 15 ottobre 2020; SIRENA, *La tutela del consumatore nella commercializzazione a distanza delle crypto-attività*, in *Il Mulino - Osservatorio del diritto civile e commerciale*, 2022, 319 s.; M. PALAZZO, *Blockchain e crypto-attività*, in *Il diritto nell’era digitale* a cura di Giordano-Panzarola-Police-Preziosi-Proto, cit., 213 ss.; LENER, *Cryptoattività e crypto valute alla luce degli ultimi orientamenti comunitari*, in *Giur. comm.*, 2023, 376 ss. e, in ambito fiscale, da ultimo PIERRO, *L’origine europea della nozione di crypto-attività e la scelta del Legislatore nazionale*, in *Cor. trib.*, 2024, 4, 382 ss.

⁴¹ Questo è infatti il ragionamento seguito da CONSULICH, *Nella wunderkammer del legislatore penale contemporaneo: monete virtuali che causano danni reali*, in *Dir. pen. proc.*, 2022, 157 che non ha ritenuto integrasse gli estremi di una analogia *in malam partem* la sussistenza del delitto di abusivismo per chi offre senza autorizzazione su un social network delle criptovalute. Sostanzialmente concordi sul punto, anche QUATTROCCHI, *La natura proteiforme delle criptovalute al crocevia della tutela penale del mercato finanziario*, in *Giur. it.*, 2022, 1217; VADALÀ, *La dimensione finanziaria delle valute virtuali. Profili assiologici di tutela penale*, in *Giur. it.*, 2021, 2231. Cfr. Cass., Sez. II, 25 settembre 2020, n. 26807 e Cass., Sez. II, 10 novembre 2021, n. 44337, con nota di CIAN, *Noterelle su finanziarità e non finanziarità nei crypto-assets: la Cassazione sulla natura del servizio di exchange*, in *Banca, borsa, titoli di credito*, 2023, 3 ss e di GUASTADISEGNI, *Crypto-valuta e prodotto finanziario: l’eterno ritorno della causa negoziale*, in *Danno e Resp.*, 2022, 494 ss.; Cass., Sez. II, 22 novembre 2022, n. 44378, con notazioni di ERRICO, *Sequestro preventivo di criptovalute*, in *Giur. it.*, 2024, 435 ss.

disciplina, ritenendo che, laddove l'offerta al pubblico di tali valori fosse presentata come una effettiva proposta di investimento, si rientrerebbe nell'ambito di operatività degli artt. 91 ss. del TUF. Per tale ragione, sarebbe stata quindi già configurabile la fattispecie citata in caso di offerta al pubblico di *token* di moneta elettronica o collegati ad altra attività senza autorizzazione⁴². Inoltre, come si è accennato, c'è chi ha precisato come tale conclusione non si ponesse in contrasto con il divieto di analogia *in malam partem*, essendo possibile far rientrare i *crypto-assets* nel campo semantico dei "prodotti finanziari", oggetto materiale dell'incriminazione⁴³.

Il d.lgs. 129/2024 ha invece sconfessato *in toto* tale approccio. In primo luogo, l'art. 39 del decreto ha 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. Anche con riferimento ai prodotti finanziari, viene quindi esclusa l'applicabilità delle norme del TUF, rendendo così non più configurabile la fattispecie prevista all'art. 166 citato.

Per evitare vuoti di tutela e adeguare l'ordinamento interno agli obblighi imposti dalla normativa euro-unionale, è stata quindi introdotta una fattispecie di abusivismo *ad hoc*, che punisce con la reclusione da sei mesi a quattro anni e con la multa da 2.066 a 10.329 euro diverse violazioni del Regolamento. In particolare, è punita l'offerta al pubblico o l'ottenimento dell'ammissione alla negoziazione di *token* collegati ad altra attività in violazione dell'art. 16 MiCAR; la prestazione di servizi per le cripto-attività in violazione dell'art. 59; l'emissione di *token* di moneta elettronica ovvero la loro offerta o ammissio-

⁴² Cfr. Cass., Sez. II, 25 settembre 2020, n. 26807, cit.; Cass., Sez. II, 10 novembre 2021, n. 44337, cit.; Cass., Sez. II, 22 novembre 2022, n. 44378, cit.

⁴³ Cfr. note 40 e 41. Contrario a questa impostazione era invece, nella dottrina civilistica, ANNUNZIATA, *Tassonomia delle cripto-attività*, cit., 924, che riteneva contraddittorio già prima del d.lgs. 129/2024 qualificare i *token* come prodotti finanziari *ex TUF*, con evidenti conseguenze sul piano penalistico. Sul punto, v. anche i rilievi di RECCHIA, *La tutela del corretto svolgimento dell'attività di intermediazione*, cit., 33 s. che acutamente osserva come dalla preesistente definizione normativa di criptovaluta come mezzo di scambio per l'acquisto di beni o servizi *ex art. 1, comma 2, lett. qq), d.lgs. 231/2007* avrebbe dovuto conseguire l'impossibilità per l'organo giudicante di qualificarle alla stregua di strumenti di investimento e quindi prodotti finanziari *ex TUF*. Nonostante infatti tale conclusione sia possibile per la formulazione normativa di tale ultima definizione, per l'A. non ci si sarebbe dovuti allontanare dall'unico dato legale (allora) esistente nella normativa antiriciclaggio, anche per l'elevato tecnicismo della materia che avrebbe dovuto condurre a fare affidamento proprio sugli elementi normativi.

ne alla negoziazione in violazione dell'art. 48 del Regolamento⁴⁴.

Si tratta di un modello di tutela che ricalca le diverse fattispecie di abusivismo previste nel nostro ordinamento⁴⁵, la cui costruzione poggia sullo svolgimento dell'attività riservata in assenza della prescritta autorizzazione, a tutela in primo luogo della funzione svolta dalle Autorità di Vigilanza⁴⁶. La differenza nella delimitazione del fatto tipico sta piuttosto nel rinvio espresso alle norme di diritto europeo, tecnica legislativa invero criticabile soprattutto per le norme formalmente penali⁴⁷.

Quanto ai profili di diritto intertemporale, la nuova fattispecie costituisce *lex mitior* per le condotte che si era prima abbastanza concordi nel sussumere nel delitto di cui all'art. 166 citato, che prevede la pena della reclusione fino a otto anni.

Già prima delle modifiche introdotte con il d.lgs. 129/2024, appariva invece

⁴⁴ Per un'analisi della nuova fattispecie, v. anche DELLA TORRE-PONTEPRINO, *Commento al D.lgs. 129 del 2024*, cit., 16 ss.

⁴⁵ V. per tutti RECCHIA, *La tutela del corretto svolgimento dell'attività di intermediazione*, cit., 5 ss. per un'analisi puntuale degli elementi costitutivi delle diverse fattispecie di abusivismo.

⁴⁶ Nel senso che le norme in materia di abusivismo tutelino in via immediata proprio la funzione di vigilanza, anche per ulteriori riferimenti al dibattito sul punto, RECCHIA, *La tutela del corretto svolgimento dell'attività di intermediazione*, cit., 10 s. *Amplius* sul tema, cfr. LOSAPPIO, *Risparmio, funzioni di vigilanza e diritto penale. Lineamenti di un sottosistema*, Bari, 2004, 330 ss.;

⁴⁷ È noto da tempo che in questo settore il quadro giuridico sottostante abbia sempre guidato la penna del Legislatore penale: per tutti v. ALESSANDRI, *Parte generale*, in *Manuale di diritto penale dell'impresa* a cura di Pedrazzi-Alessandri-Foffani-Seminara-Spagnolo, Bologna, 1998, 46. Nondimeno, pare comunque censurabile la scelta di individuare nelle norme europee l'asse portante della tutela penalistica, anche per il *vulnus* evidente al principio di precisione, come del resto sottolineato da molti proprio in relazione a fattispecie simili nel diritto penale dell'economia: cfr. RAMPIONI, *Diritto penale dell'economia e principi informativi del sistema penale*, in *Diritto penale dell'economia*, a cura di Rampioni, Torino, 2024, 14 ss.; in relazione agli abusi di mercato, cfr. MUCCIARELLI, *Gli abusi di mercato riformati e le persistenti criticità di una tormentata disciplina*, in www.dirittopenalecontemporaneo.it, 10 ottobre 2018, 8 ss. e 17; ID., *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, 5, 579; TRIPODI, *Gli illeciti amministrativi in materia di abusi di mercato*, cit., 284 ss.; AMATI, *L'abuso o comunicazione illecita di informazioni privilegiate*, cit., 166; GAMBARDELLA, *Condotte economiche e responsabilità penale*, Torino, 2020, 382; meno critico sull'eterointegrazione delle fonti in questo ambito è invece PREZIOSI, *Modelli di sviluppo economico e diritto penale. Sullo sfondo della crisi pandemica*, in *Riv. trim. dir. pen. econ.*, 2020, 3-4, 689 ss. *Amplius* sul tema, v. PAGLIARO, voce *Legge penale*, in *Enc. Dir.*, XXIII, 1973, 1045 ss. e 1051 s.; MOCCIA, *La promessa non mantenuta. Ruolo e prospettive del principio di determinatezza/tassatività nel sistema penale italiano*, Napoli, 2001, 13 ss. V. pure RECCHIA, *La tutela del corretto svolgimento dell'attività di intermediazione*, cit., 12 per la possibile qualificazione della fattispecie in esame come norma penale in bianco, anche con ulteriori riferimenti bibliografici.

più arduo applicare l'art. 166 lett. a) del TUF, poiché sarebbe stato necessario qualificare la prestazione di servizi per le cripto-attività come “servizi e attività di investimento” ex art. 1, comma 5 del testo unico citato⁴⁸. Dalla definizione fornita dall'art. 3 MiCAR, sembra infatti possibile qualificare in tal senso le attività di consulenza, gestione di portafoglio, ricezione, trasmissione ed esecuzione di ordini di cripto-attività per conto dei clienti. Lo svolgimento di tali attività senza autorizzazione poteva dunque integrare il delitto di abusivismo secondo l'orientamento cui si è accennato, almeno prima delle modifiche legislative di recente introduzione. Per le altre condotte definite dal Regolamento europeo, *in primis* la prestazione dei servizi di custodia e amministrazione – consistenti, sostanzialmente, nella detenzione per conto dei clienti delle chiavi crittografiche – era invece necessario un intervento legislativo *ad hoc*. È pur vero che chi offre tale prestazione difficilmente non svolge poi servizi di ricezione ed esecuzione di ordini. Nondimeno, per anticipare la tutela già al servizio di mera detenzione delle chiavi, come del resto imposto dalla normativa eurounionale, era necessario modificare la disciplina introducendo una nuova fattispecie sanzionatoria, obbligo soddisfatto proprio dall'art. 30 citato che punisce, come si è accennato, anche lo svolgimento di qualsiasi servizio per i *crypto-assets* in violazione della disciplina di settore (e che, relativamente a questa attività, costituisce di conseguenza una nuova incriminazione).

4. *Gli altri obblighi punitivi.* Accanto agli obblighi di autorizzazione, MiCAR imponeva poi di sanzionare la violazione della normativa sul *White Paper*, al fine di assicurare maggiore tutela all'affidamento dei risparmiatori sul documento informativo dell'investimento. Sotto questo profilo, la *ratio* della sanzione ricalca quella del falso in prospetto, naturalmente non applicabile alla disciplina delle cripto-attività⁴⁹.

⁴⁸ Sui servizi di negoziazione e custodia di cripto-attività come disciplinati dalla proposta di Regolamento, v. CIOCCA, *Servizi di negoziazione, custodia e regolamento di cripto-attività*, in *Il Mulino - Osservatorio del diritto civile e commerciale*, 2022, pp. 79 ss. Per la definizione di prestatore di servizi per le cripto-attività, v. anche DELLA TORRE-PONTEPRINO, *Commento al D.lgs. 129 del 2024*, cit., 13 ss.

⁴⁹ Si tratta infatti di documenti aventi disciplina e contenuti diversi: v. VICARI, *Il white paper nella proposta di Regolamento sulle cripto-attività*, in *Il Mulino - Osservatorio del diritto civile e commerciale*, 2022, 249 ss; FRIGENI, *Il mercato primario delle cripto-attività*, cit., pp. 28 s.; PATTI, *L'offerta al pubblico di cripto-attività nel titolo II del Regolamento MiCA*, in *Riv. dir. civ.*, 2024, 1, 97 ss.

Il Legislatore nazionale non ha però profuso particolari sforzi per adeguare in tal senso la disciplina interna. Con una previsione *omnibus*, l'art. 31 del d.lgs. 129/2024 si limita infatti a punire con una sanzione amministrativa pecuniaria da cinquemila a settecentomila euro per le persone fisiche e da trentamila a cinque milioni di euro per le persone giuridiche, salvo che il fatto costituisca reato, ogni «inosservanza delle disposizioni richiamate dall'art. 111, par. 1, lett. a), b), c) e d)» del MiCAR che, come si ricorderà, sono a loro volta costruite per rinvio a numerosissimi articoli del Regolamento relativi all'offerta al pubblico e alla prestazione di servizi per i diversi tipi di *token*⁵⁰. L'unica nota positiva di una norma simile è la presenza della clausola di riserva, che almeno permette di non far sottostare a una doppia sanzione le violazioni degli artt. 16, 48 e 59 del MiCAR, che dovrebbero integrare il nuovo delitto di abusivismo. Anche in questa ipotesi, vale la pena sottolineare come, fermo restando la responsabilità dell'ente, la sanzione possa essere irrogata a una persona fisica solo in presenza delle suindicate condizioni previste dall'art. 36 del d.lgs. 129/2024⁵¹.

Da ultimo, la normativa europea imponeva altresì di sanzionare il mancato adempimento all'obbligo di collaborazione con le Autorità di vigilanza nell'ambito delle investigazioni in materia di abusi di mercato. L'art. 94, par. 3, MiCAR permette infatti a Consob e Banca d'Italia, tra le altre cose, di accedere a qualunque «documento e dato sotto qualsiasi forma», di «richiedere o esigere informazioni da chiunque» e accedere ai locali allo scopo di sequestrare documenti⁵². L'art. 111, par. 1, lett. f) prescriveva dunque di sanzionare l'omessa collaborazione a tali attività.

In realtà, non era necessaria l'introduzione di un'altra norma *ad hoc*: gli artt. 170-*bis* e 187-*quinqüesdecies* TUF e l'art. 2638 c.c. già sanzionano, a vari

Sull'incriminazione del TUF, v. da ultimo LONGARI, *Profili critici del delitto di falso in prospetto*, in *Dir. pen. & giust.*, 2024, 5, 1348 ss.; PERINI, *La tutela penale della corretta e Capitoło II trasparente partecipazione agli emittenti (artt. 169, 172, 173 e 173-bis TUF)* in Consulich, (a cura di), *Reati in materia bancaria e finanziaria*, cit., 138 ss.

⁵⁰ V. nota 4 per il testo. Lamentano l'«esasperato utilizzo della tecnica del rinvio» in relazione a tutti gli illeciti amministrativi anche DELLA TORRE-PONTEPRINO, *Commento al D.lgs. 129 del 2024*, cit., 32 s., per i quali sarebbe stato preferibile trasporre direttamente le norme del Regolamento rilevanti.

⁵¹ V. *supra*, nota 36.

⁵² Cfr. artt. 4 e 15 d.lgs. 129/2024 per i poteri ispettivi conferiti alle autorità di vigilanza in questo settore.

livelli, la mancata cooperazione con le autorità di vigilanza di settore⁵³. Il Legislatore nazionale, dimentico di tali previsioni, ha previsto un nuovo illecito contenuto nell'art. 39 del decreto citato, per cui: «in caso di omessa collaborazione o mancato seguito dato nell'ambito di un'indagine, un'ispezione o una richiesta, incluse quelle di cui all'articolo 94, par. 3» MiCAR «si applica: a) nei confronti delle persone giuridiche, la sanzione amministrativa pecuniaria da euro 30.000 fino a euro 5 milioni, ovvero, se superiore, fino al 10 per cento del fatturato totale annuo; b) nei confronti delle persone fisiche, inclusi gli esponenti aziendali e il personale di cui all'articolo 36 del presente decreto e al ricorrere delle condizioni ivi stabilite, la sanzione amministrativa pecuniaria da euro 5.000 fino a euro 5 milioni».

Confezionare una previsione più problematica sarebbe stato difficile. Partendo dai profili sanzionatori, la formulazione letterale delle misure punitive da irrogare agli enti lascia a desiderare, essendo necessario interpretare la norma nel senso che è possibile applicare una sanzione parametrata al fatturato solo se *il profitto* conseguito per effetto della commissione dell'illecito è superiore al massimo edittale. Per le persone fisiche, manca poi una previsione che permetta in tali ipotesi di elevare l'importo della sanzione, invece previsto nella fattispecie di mancata collaborazione di cui all'art. 187-*quinquiesdecies* TUF.

Ancora, la norma va oltre quanto richiesto dal Regolamento europeo, sanzionando ogni difetto di cooperazione alle richieste delle Autorità di Vigilanza (da leggersi, nell'ambito dei poteri ispettivi conferiti in materia di criptoattività), *incluse* le violazioni contemplate dall'atto di diritto derivato.

Quel che più stupisce è poi l'assenza di una clausola di riserva che faccia chiarezza in merito ai rapporti con le altre fattispecie sanzionatorie citate che pure puniscono la mancata collaborazione con Banca d'Italia e Consob⁵⁴. L'unico

⁵³ Per un'analisi degli illeciti citati, v. TRIPODI, *sub Art. 2638 cc., 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 De Nova, Bologna, 2018, 619 ss.; SEMINARA, *Diritto penale commerciale*, Torino, 2018, vol. II, 161 ss.; CORNACCHIA, *L'ostacolo all'Autorità di vigilanza*, in *Reati in materia bancaria e finanziaria*, a cura di Consulich, cit., 327 ss.; GAMBARDILLA, *Condotte economiche e responsabilità penale*, cit., 157 ss.

⁵⁴ Sui rapporti tra le diverse fattispecie, v. da ultimo DONINI, *Il nodo gordiano della vigilanza bancaria*,

modo per evitare una palese sproporzione del trattamento sanzionatorio è dunque quello di espungere dal perimetro applicativo delle suddette norme sanzionatorie – *in primis* quelle penali di cui agli art. 170-*bis* TUF e 2638 c.c. – le condotte poste in essere nell’ambito di un’attività ispettiva riguardante i *crypto-assets*, per le quali dovrebbe quindi applicarsi solo l’art. 39 d.lgs. 129/2024.

Da ultimo, la previsione impone di collaborare anche alla società o persona fisica responsabile della violazione e che, proprio per l’effetto della propria condotta collaborativa, potrebbe vedersi irrogata una sanzione sostanzialmente penale⁵⁵. A questo riguardo, peraltro all’esito di un dialogo con la stessa Corte di Giustizia dell’Unione Europea⁵⁶, la Corte costituzionale ha di recente dichiarato costituzionalmente illegittimo proprio l’art. 187-*quinqüesdecies* del TUF nella parte in cui sanziona anche chi si rifiuta di rispondere nell’ambito di un’audizione di fronte Banca d’Italia o Consob per esercizio del proprio diritto al silenzio. Un’interpretazione costituzionalmente orientata della norma impone dunque di non assoggettare a sanzione la persona che invochi il *nemo tenetur se detegere* per non essere forzata a rendere dichiarazioni autoincriminanti o da cui emerge la propria responsabilità per un illecito amministrativo punitivo, nei limiti in cui si deve ritenere la suddetta condotta

cit., 53 ss.; CORNACCHIA, *L’ostacolo all’Autorità di vigilanza*, cit., 354.

⁵⁵ Sulla problematica, v. 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, 57 ss.; CONFALONIERI, *Il nemo tenetur se detegere nel labirinto delle fonti*, in *Dir. pen. cont. – Riv. trim.*, 2020, 108 ss.; ID., *Il diritto “fondamentale” al silenzio nei procedimenti Consob e Banca d’Italia*, in *Le Società*, 2022, 86 ss.; SFORZA, *Il nemo tenetur se detegere nelle audizioni Consob e Banca d’Italia: uno statuto ancora da costruire*, in *Sist. pen.*, 2022, 83 ss.; CORNACCHIA, *L’ostacolo all’Autorità di vigilanza*, cit., 331 ss. Più in generale sulla questione, già TASSINARI, *Nemo tenetur se detegere. La libertà dalle autoincriminazioni nella struttura del reato*, Bologna, 2012, 381 ss. V. pure PIETROCARLO, *L’ostacolo all’esercizio delle funzioni delle autorità pubbliche di vigilanza: condivisibili conferme e “punti oscuri” nella recente giurisprudenza di Cassazione*, in *Arch. pen. web*, 2023, 3, 15 ss., per cui il mero silenzio non sarebbe rilevante ai fini dell’integrazione del delitto di cui all’art. 2638 c.c.

⁵⁶ Cfr. Corte di Giustizia UE, 2 febbraio 2021, C-489/19, D.B. c. Consob, con commenti di LASAGNI, *La Corte di Giustizia riconosce il diritto al silenzio nei procedimenti amministrativi punitivi (e la Corte costituzionale conferma)*, in *Giur. comm.*, 2021, 1179 ss.; CRIPPA, *Procedimento “formalmente” amministrativo e nemo tenetur se detegere*, in *Riv. it. dir. proc. pen.*, 2021, 762 ss.; SCHIAVONE, *Il diritto al silenzio nello spazio giuridico europeo: osmosi delle garanzie se la sanzione amministrativa è “punitiva”*, in *Dir. pen. proc.*, 2023, 412 ss. A commento della successiva sentenza della Corte cost., 13 aprile 2021, n. 84, v. anche COMPOSTELLA, *Illecito amministrativo punitivo e diritto al silenzio: una pronuncia (non del tutto) a rime obbligate*, in *Banca, borsa, titoli di credito*, 2022, 515 ss.; BONZANO, *Diritto al silenzio e matière pénale*, in *Dir. pen. proc.*, 2022, 47 ss.

coperta dal diritto al silenzio⁵⁷.

5. *Le Misure di Vigilanza dell'ABE*. Completano infine il corredo sanzionatorio del MiCAR le Misure di Vigilanza dell'ABE⁵⁸. A differenza delle sanzioni imposte dall'art. 111 del Regolamento citato, che necessitano l'intervento del Legislatore nazionale per trovare applicazione, le sanzioni amministrative pecuniarie e le penalità di mora di competenza dell'ABE sono previste interamente dalla normativa europea e, come noto, sono direttamente applicabili in tutti gli Stati Membri. Tuttavia, se per le prime è imposto di sanzionare anche le persone fisiche responsabili della violazione, le misure di vigilanza in questione si indirizzano – per la massima parte – verso persone giuridiche.

Tali illeciti sono volti a presidiare l'attività di vigilanza svolta dall'Autorità europea nei confronti degli emittenti di *token* collegati ad attività significativi o *token* di moneta elettronica significativi, ossia che rispettano i requisiti stabiliti, rispettivamente, dagli artt. 43, 44 o 56 e 57 del Regolamento. Tali emittenti, in considerazione dell'impatto del *crypto-asset* sul mercato digitale, sono infatti gravati da ulteriori obblighi prudenziali e di comunicazione nei confronti sia delle Autorità di Vigilanza che dei possessori di tali *token*. Per questo motivo, gli allegati V e VI del MiCAR prevedono una lista di violazioni che le suddette imprese possono porre in essere, al ricorrere delle quali l'Autorità Bancaria Europea può adottare una delle misure previste dall'art. 130 del Regolamento.

In particolare, ai sensi del suddetto articolo, in caso di riscontro di una delle violazioni ivi elencate, l'ABE può, tra le altre cose, ingiungere all'emittente di porre fine alla condotta che costituisce l'irregolarità e adottare sanzioni amministrative pecuniarie o penalità di mora, imporre all'impresa di fornire in-

⁵⁷ Per la verità, vi sono delle controversie sull'estensione del *nemo tenetur* anche alle persone giuridiche e all'accesso ai documenti: v. sul punto AMATI, *Dinamiche evolutive del diritto al silenzio*, cit., 117 ss.; LASAGNI, *La Corte di Giustizia riconosce il diritto al silenzio nei procedimenti amministrativi punitivi*, cit., 1183 ss. Nella giurisprudenza della Corte EDU, v. per tutte Corte EDU, 4 ottobre 2022, app. n. 58342/2015, *De Legé v. Paesi Bassi*, per quanto riguarda tale problematica.

⁵⁸ Per un commento alle misure nella proposta del Regolamento, v. MURINO, *Vigilanza ed enforcement sui mercati delle cryptoattività nella proposta di Regolamento MiCA*, in *Il Mulino - Osservatorio del diritto civile e commerciale*, 2022, 447 ss. Cfr. poi BENCINI-FANFANI, *Supervisory e enforcement nel quadro regolamentare MiCA*, cit., 309 ss.; ALESSI, *Il ruolo delle Autorità competenti: la collaborazione tra ABE, ESMA e Autorità nazionali*, in *Il MiCAR*, cit., 120 ss.

formazioni supplementari, sospendere o vietare l'offerta al pubblico di *token* o la loro negoziazione e, per i *token* collegati ad altra attività, imporre di modificare, sospendere o vietare le comunicazioni di *marketing* e finanche imporre la rimozione di una persona fisica dal consiglio d'amministrazione dell'emittente⁵⁹. Si tratta di uno dei pochi casi in cui la potestà sanzionatoria europea in materia finanziaria ha un effetto diretto su una persona non giuridica, peraltro con una misura certamente afflittiva. I criteri di scelta delle misure sono esplicitati dal paragrafo 3 dell'art. 130 e sono i medesimi in base ai quali è modulato il *quantum* della sanzione amministrativa pecuniaria.

Più nel dettaglio, la gravità della violazione cui rapportare la misura è valutata sulla base della natura dolosa o colposa della violazione, la durata del comportamento antidoveroso, il grado di responsabilità dell'emittente, la sua capacità finanziaria, il suo livello di cooperazione con le autorità di vigilanza, le misure adottate per rimediare alla violazione e le sue conseguenze, in particolare se quest'ultima abbia favorito o agevolato la commissione di un illecito penale finanziario o abbia avuto un impatto particolarmente negativo sugli interessi dei possessori delle cripto-attività. Il limite massimo cui può arrivare la sanzione pecuniaria è pari al doppio del profitto realizzato o delle perdite evitate tramite la commissione dell'illecito o, alternativamente, al 12,5% o 10% del fatturato a seconda che riguardi un *asset-referenced token* o un *token* di moneta elettronica⁶⁰.

La penalità di mora, invece, consiste in un importo da pagare pari al 3% del fatturato per le persone giuridiche o al 2% del reddito medio giornaliero per le persone fisiche per ogni giorno in cui persiste una violazione accertata dall'ABE ovvero per ogni giorno in cui una persona fisica si rifiuta di collaborare con l'autorità di vigilanza nell'esercizio dei suoi poteri ispettivi. In particolare, infatti, è previsto che tale penalità di mora si possa applicare nei confronti di chi si rifiuta di fornire informazioni richieste, di sottoporsi a ispezione in loco o di fornire registrazioni, dati, procedure o altro materiale. Tale meccanismo, simile alle *astreintes*, è rivisto dopo un periodo massimo di sei

⁵⁹ Cfr. art. 130 Reg. UE 2023/1114.

⁶⁰ V. art. 131 Reg. UE 2023/1114.

mesi durante il quale può perdurare la misura⁶¹.

La sanzione amministrativa e la penalità di mora sono irrogate all'esito di un procedimento interno all'ABE. In particolare, allorché vi sia il sospetto di una violazione rilevante ai sensi dell'art. 130 MiCAR, l'Autorità europea nomina un funzionario indipendente – ossia non coinvolto nella vigilanza dell'ente destinatario del procedimento – che, all'esito di una fase istruttoria, formula delle conclusioni sulla base delle quali l'ABE adotta una decisione⁶². Le persone interessate hanno il diritto di essere ascoltate in audizione, anche se l'art. 134 del Regolamento citato delega alla Commissione il compito di specificare le norme procedurali per garantire a pieno il diritto di difesa. Contro la decisione così adottata è ammesso riesame di fronte la Corte di Giustizia⁶³.

È innegabile che tale disciplina sconti alcune criticità. Come si è accennato, infatti, si tratta pacificamente di sanzioni sostanzialmente penali, che vanno ben oltre il mero risarcimento del danno: basti guardare all'entità massima che possono raggiungere le misure *ex artt.* 131 e 132 MiCAR e i loro criteri di scelta, tra cui compare anche il “grado di responsabilità” dell'ente. A tal proposito suona davvero come una *excusatio non petita* l'affermazione contenuta nel paragrafo 2 dell'art. 133, ai sensi del quale tali misure «sono di natura amministrativa». Nonostante tale presa di posizione, appare invero evidente che tanto le sanzioni pecuniarie quanto le penalità di mora⁶⁴ di “amministrativo” abbiano solamente il *nomen*, con tutte le criticità che ne possono derivare in punto di rispetto delle garanzie penalistiche, tanto più che alcune di queste misure hanno come diretti destinatari le persone fisiche.

In secondo luogo, con riferimento alle penalità di mora indirizzate nei confronti di persone fisiche che si rifiutano di collaborare con l'ABE, si ripropongono i problemi emersi in materia di obbligo di collaborazione con le autorità di vigilanza e *nemo tenetur se detegere*. Nondimeno, pur potendosi

⁶¹ Cfr. art. 132 Reg. UE 2023/1114.

⁶² Cfr. art. 133 MiCAR.

⁶³ V. art. 135 Reg. UE 2023/1114.

⁶⁴ Sulla natura sanzionatoria delle penalità di mora con riferimento al meccanismo simile previsto per la BCE dall'art. 18, par. 7, Reg. UE 1024/2013, v. FELISATTI, *Poteri sanzionatori e principio del ne bis in idem nel meccanismo di vigilanza unico sugli istituti di credito*, in *Riv. trim. dir. pen. econ.*, 2018, 707 ss., nonché TRIPODI, *Ne bis in idem europeo e doppi binari punitivi*, cit., 108, nota 126 e bibliografia ivi citata.

trattare di un *vulnus* a un diritto costituzionalmente garantito, la tutela più immediata contro tali misure – che, si ricorda, costituiscono titolo esecutivo in tutti gli Stati Membri – è il riesame non di fronte un Tribunale interno ma di fronte alla Corte di Giustizia⁶⁵. Peraltro, nonostante le affermazioni di principio del Regolamento per cui è pienamente tutelato il diritto di difesa durante l'*iter* procedimentale, l'effettivo rispetto di tale diritto è di fatto demandato a un atto delegato della Commissione.

Da ultimo, tali sanzioni sono suscettibili di cumularsi con altri eventuali illeciti penali o amministrativi integrati con il medesimo comportamento, con un rischio di violazione del *ne bis in idem*, tanto più alto considerato che l'ABE è tenuta a comunicare le violazioni alle autorità competenti dei Paesi Membri. È pur vero che l'art. 134, par. 11, del Regolamento prevede che l'Autorità Bancaria Europea si astenga dall'imporre sanzioni amministrative o penali di mora quando lo stesso fatto è già stato giudicato con sentenza penale irrevocabile. Nondimeno, tale previsione non neutralizza tutti i rischi: non contempla infatti le ipotesi di litispendenza⁶⁶ né, soprattutto, impone agli Stati Membri di non sanzionare nuovamente la stessa condotta già punita dall'ABE⁶⁷.

⁶⁵ Sulla tutela giurisdizionale avverso le decisioni dell'EBA, v. TORCHIA, *La nuova governance economica dell'Unione europea e l'Unione bancaria*, in *La costituzione dell'Unione bancaria e l'influenza sull'ordinamento italiano*, a cura di Chiti-Santoro, Pisa, 2016, 60 s.

⁶⁶ Peraltro, alle ipotesi di litispendenza viene applicato il principio del *ne bis in idem* solamente dalla giurisprudenza interna e con riferimento ai soli procedimenti formalmente penali: cfr. Cass. pen., Sez. Un., 28 giugno 2005, n. 34655 che ha esteso la portata del principio «alle situazioni di litispendenza, non riconducibili nell'ambito dei conflitti di competenza di cui all'art. 28 c.p.p. [...] sempreché i due processi abbiano ad oggetto il medesimo fatto attribuito alla stessa persona, siano stati instaurati ad iniziativa dello stesso ufficio del pubblico ministero e siano devoluti, anche se in fasi o in gradi diversi, alla cognizione di giudici della stessa sede giudiziaria». Al contrario, costituendo un *minimum standard* nella tutela dei diritti fondamentali, l'ipotesi contemplata dalla Convenzione EDU non si estende ai casi di litispendenza: per costante giurisprudenza della Corte di Strasburgo, l'avvio simultaneo di più procedimenti non viola la portata convenzionale del principio, purché il secondo si arresti una volta che l'altro sia definito con una decisione definitiva. Cfr. *ex multis*, Corte EDU, 24 giugno 2003, ricorso n. 65831/01, *Garaudy c. Francia*; 3 ottobre 2002, ricorso n. 48154/99, *Zigarella c. Italia*; 18 ottobre 2011, ricorso n. 53785/09. Per una critica a tale approccio nella giurisprudenza della Corte di Strasburgo, v. la *dissenting opinion* del giudice Pinto de Albuquerque allegata a Corte EDU, 15 novembre 2016, ricorsi n. 24130/11 e n. 29758/11, *A e B c. Norvegia*, par. 41, nota 112 e, volendo, ARDIZZONE, *The ne bis in idem Principle in the Age of Balancing*, in *European Papers*, vol. 8, 2023, 873 ss.

⁶⁷ Sui cumuli sanzionatori all'interno del meccanismo di vigilanza unico, v. già FELISATTI, *Poteri sanzionatori e principio del ne bis in idem nel meccanismo di vigilanza unico sugli istituti di credito*, cit., 694 ss.; PISANESCHI-BINDI-LUCARELLI, *Le sanzioni della Banca d'Italia e della Consob*, in *Giur. comm.*,

6. *Conclusioni.* Il regime sanzionatorio introdotto dal Regolamento MiCA e implementato dal d.lgs. 129/2024 configura un tentativo di estendere alla regolamentazione delle cripto-attività i principi e gli strumenti repressivi già consolidati nel diritto sanzionatorio “tradizionale” dei mercati finanziari. Nondimeno, l’approccio adottato non è privo di criticità.

In primo luogo, vale la pena evidenziare la rozzezza della tecnica legislativa utilizzata, in ambito tanto europeo quanto nazionale. L’art. 111 del Regolamento imponeva infatti di sanzionare la violazione di un numero estremamente rilevante di disposizioni, richiamate per rinvio; l’art. 31 d.lgs. 129/2024, invece di fare ordine, si è limitato a sua volta a rinviare alla norma europea, senza nemmeno elencare nuovamente gli articoli dell’atto di diritto derivato la cui violazione costituisce illecito amministrativo. L’effetto pratico di un simile rinvio a catena è la difficile intelligibilità del precetto, se non altro per la necessità di individuare di volta in volta la norma del Regolamento che si assume violata. Inoltre, è il caso di sottolineare come l’illecito citato permetta – per lo meno in astratto – di applicare sanzioni draconiane anche in caso di inosservanza di regole di per sé vaghe, come l’obbligo di agire in modo onesto, corretto e professionale per gli offerenti e le persone che chiedono l’ammissione alla negoziazione di cripto-attività diverse dai *token* collegati ad altra attività o di moneta elettronica⁶⁸. Insomma, si sarebbe dovuto recuperare in sede nazionale il *deficit* di tassatività contenuto nelle disposizioni europee, puntualizzando le condotte vietate senza ricorrere alla tecnica del (doppio) rinvio e differenziando le cornici edittali degli illeciti sulla base del loro disvalore, senza parificare sul versante sanzionatorio la violazione di quasi tutte le norme del Regolamento.

Né, a giustificazione di tale pigrizia legislativa, si potrebbe addurre la natura

2021, 553 ss.; DONINI, *Il nodo gordiano della vigilanza bancaria*, cit., 56 ss. V. poi TRIPODI, *Ne bis in idem europeo e doppi binari punitivi*, cit., 67 s. e 106 s. con riferimento alle duplicazioni sanzionatorie per effetto degli illeciti amministrativi previsti nel TUB e nel TUF e diversi da quelli in materia di abusi di mercato, nonché quelli risultanti per effetto di poteri sanzionatori della BCE.

⁶⁸ Cfr. art. 14, par. 1, lett. a) del Regolamento MiCA, richiamato a sua volta dall’art. 111, par. 1, lett. a) a cui rinvia il citato art. 31 d.lgs. 129/2024 che, vale la pena di ricordare, permette l’irrogazione di sanzioni pecuniarie fino a settecentomila euro per le persone fisiche e cinque milioni di euro per quelle giuridiche.

formalmente amministrativa dell'illecito citato: l'inequivocabile vocazione punitiva – nonché il livello elevatissimo di afflittività – avrebbe dovuto imporre ben altra attenzione nella costruzione di un simile impianto sanzionatorio, certamente appartenente alla “*matière pénale*”.

Un secondo elemento di criticità riguarda le sanzioni a presidio dell'obbligo di collaborare con le Autorità di Vigilanza di settore. Si è visto infatti come tale ambito, già popolato da numerosi illeciti di varia natura, sia stato di recente al centro di un dibattito circa il rispetto del *nemo tenetur se detegere*, che ha interessato sia la Corte costituzionale che la Corte di Giustizia⁶⁹. Nondimeno, la scelta è stata quella di inserire un nuovo illecito amministrativo di mancata collaborazione, senza prendere posizione circa la questione del diritto al silenzio e senza regolare il rapporto tra la nuova norma e le fattispecie sanzionatorie già in vigore. Come si è accennato, ci sembra dunque che la soluzione migliore sia di quella di ritagliare uno spazio applicativo autonomo all'illecito di nuovo conio, ritenendo che le condotte poste in essere nell'ambito di un'attività ispettiva riguardante le cripto-attività debbano collocarsi al di fuori dei confini dell'art. 2638 c.c. e delle disposizioni del TUF.

Da ultimo, la stratificazione delle competenze tra autorità nazionali e organismi sovranazionali, come l'ABE e l'ESMA, crea due ulteriori problematiche sul versante sanzionatorio. *In primis*, come pure si è accennato, l'attività normativa posta in essere dall'Autorità indipendente ha delle ricadute dirette per la definizione del perimetro delle fattispecie criminose di abusi di mercato, che risultano tanto più estese quanto più si considerino le cripto-attività strumenti finanziari, con tutte le ricadute in punto di legalità che una simile scelta comporta⁷⁰.

In secondo luogo, la potestà sanzionatoria diretta dell'ABE genera potenziali sovrapposizioni tra procedimenti sanzionatori per il medesimo fatto, con rischi di violazione del *ne bis in idem*. Come si è visto, nonostante la problematica sia ben nota anche in sede europea, il rimedio apprestato dall'art. 134 del Regolamento si rivela inidoneo a scongiurare la duplicazione procedimentale: oltre alle ipotesi di litispendenza, non è infatti precluso agli Stati Membri di

⁶⁹ V. *supra*, par. 4, anche per i riferimenti bibliografici.

⁷⁰ V. *supra*, par. 2.

punire nuovamente il comportamento oggetto della misura punitiva irrogata dall'Autorità Bancaria né il procedimento amministrativo punitivo interno vale a impedire la seconda sanzione dell'ABE⁷¹.

Nonostante dunque il formale adeguamento dell'ordinamento italiano, l'impressione è quella di trovarsi di fronte a un quadro normativo estremamente frammentato, dove la tecnica legislativa utilizzata complica l'intelligibilità di precetti sanzionatori che si innestano su una normativa già di per sé iper-tecnica. Sarebbe stato dunque opportuno assicurare una maggiore coerenza con i principi fondamentali propri di un sistema sanzionatorio moderno e garantista, a prescindere dal *nomen* che si dà agli illeciti di nuova costruzione.

⁷¹ V. *supra*, par. 5.