

SPUNTI IN TEMA DI CRIPTO-ATTIVITÀ E PROCEDIMENTO PENALE*

di Jacopo della Torre

*(Professore associato di Diritto processuale penale,
Università degli Studi di Genova)*

Sommario: 1. Premessa. – 2. L'impiego delle criptovalute per finalità illecite. – 3. La reazione normativa sovranazionale e interna. – 4. *Blockchain* e operazioni di contrasto. – 5. Il c.d. “*follow the crypto*”: una nuova realtà investigativa... orfana di regole. – 6. Il sequestro delle “monete virtuali”: premesse e spunti comparati. – 7. Segue. L'incerto panorama italiano. – 8. Conclusioni.

1. La diffusione delle cripto-attività¹ rappresenta uno dei fenomeni più rivoluzionari degli ultimi anni. Sull'onda del successo avuto dal *Bitcoin* dopo la sua creazione nel 2008², in breve tempo si è assistito allo sviluppo di un enorme mercato globale del settore, fortemente eterogeneo e in continua ascesa, capace di movimentare, ogni giorno, valori per centinaia di miliardi di dollari³.

* Il contributo costituisce la rielaborazione, con l'aggiunta di note, dell'intervento svolto il 27 settembre 2024 nell'ambito del convegno su *Indagini e prove nella società digitale*, tenutosi presso l'Università di Trento ed è destinato alla pubblicazione nel volume dei relativi atti, curato da G. Di Paolo e da L. Pressacco. Il lavoro si inserisce, inoltre, nell'ambito del progetto, finanziato dall'Unione Europea, “PRIN 2022 PNRR: CRYPTOSAFE (*Towards a safe seizure and confiscation of crypto-assets in criminal proceedings*)”. Codice progetto P2022HW85A; CUP D53D23022280001.

¹ Le cripto-attività costituiscono una categoria omnicomprendente, capace di inglobare in sé qualunque «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» (art. 3 co.1 n. 5 reg. 1114/2023/UE, relativo ai mercati delle cripto-attività – c.d. Regolamento MiCA, per una analisi del quale si rimanda a M. Nicotra, F. Sarzana di S. Ippolito, M. Simbula (a cura di), *Il Micar. Guida al regolamento europeo sui mercati delle cripto*, Milano 2023 e S. Capaccioli e M.T. Giordano, *Crypto-asset: Regolamento MiCA e DLT pilot regime*, Milano 2023).

² L'idea del *Bitcoin* è stata presentata al pubblico il 31 ottobre 2008, mediante la pubblicazione di un *white paper* (reperibile a questo link <https://bitcoin.org/bitcoin.pdf>) da parte di un individuo o di un gruppo, identificatosi con lo pseudonimo di “Satoshi Nakamoto”. Il momento non è casuale: si tratta del periodo in cui era scoppiata la grande crisi finanziaria globale, dovuta al fallimento di grandi banche americane come la *Lehman Brothers*. La crisi del 2007-2008 è stata vista come la dimostrazione del fallimento della politica finanziaria globale, basata sugli intermediari bancari tradizionali. Essa ha favorito il lancio di un nuovo mezzo di pagamento digitale, per l'appunto, il *Bitcoin*, pensato per essere “decentralizzato”, cioè, scambiato sulla rete *web* senza la necessaria presenza di intermediari, a cui affidare il compito di controllare la validità delle transazioni (e, in particolare, la mancata “doppia spesa” delle somme).

³ Nel secondo decennio degli anni Duemila, le monete virtuali hanno progressivamente iniziato a diffondersi in tutto il mondo: oggi giorno se ne contano ormai più di 9.000 tipologie con una capitalizzazione complessiva di mercato di oltre tre trilioni di dollari. Per rendersi conto delle peculiarità del fenomeno in esame basti prendere

Tuttavia, come era stato preconizzato già nell'ambito del movimento di pensiero c.d. "cypherpunk", che ha costituito il retroterra culturale per la creazione del fenomeno in esame⁴, gli *asset* virtuali hanno ben presto attirato l'attenzione, non solo dei comuni risparmiatori, degli istituti bancari e delle autorità governative, ma anche della criminalità⁵. È, d'altra parte, un dato oramai accertato che i *bad actors* abbiano repentinamente iniziato a sfruttare le potenzialità del nuovo "oro digitale", al fine di incrementare i loro profitti. Al riguardo, è sufficiente menzionare il celebre caso *Silk Road*, cioè il primo "darknet market"⁶ ad aver impiegato il *Bitcoin* come moneta di scambio, che dalla sua creazione nel 2011, sino alla chiusura nel 2013 da parte dell'FBI, ha gestito vendite di beni illeciti di ogni tipo per centinaia di milioni di dollari⁷.

In questa sede, mi occuperò del complesso rapporto tra giustizia penale e cripto-attività da tre prospettive. In prima battuta, fornirò un quadro di come esse vengano oggi utilizzate per eterogenee finalità illecite (§ 2). In secondo luogo, analizzerò la reazione che, sul piano sovranazionale e interno, è stata finora intrapresa per far fronte a questa problematica (§ 3). La terza parte avrà, invece, un *focus* prettamente processualpenalistico. Da un lato, mi soffermerò sull'importanza che per le autorità di *law enforcement* riveste l'impiego di *software* di analisi della *blockchain*⁸, al fine di seguire i flussi di transazioni e di de-anonimizzarle (§ 5). Da un altro lato, affronterò

quale esempio la criptovaluta \$TRUMP, lanciata dal Presidente Trump in occasione del suo secondo insediamento, il cui prezzo è cresciuto in pochi giorni del 45.000%, movimentando un mercato di oltre 10 miliardi di dollari (cfr., al riguardo, <https://www.reuters.com/technology/trumps-new-crypto-token-jumps-ahead-his-inauguration-2025-01-20/>).

⁴ Mi riferisco al *The Crypto Anarchist Manifesto*, in <https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html>.

⁵ Per un'analisi diacronica del fenomeno, cfr. D. Carlisle, *The Crypto Launderers. Crime and Cryptocurrencies from the Dark Web to DeFi and Beyond*, Chichester 2024 e G. Soana, *The Anti Money Laundering Regulation of Crypto-Assets in Europe*, Milano 2024.

⁶ Con tale locuzione si fa riferimento a mercati sviluppati su pagine nel *dark web*, cioè su siti raggiungibili solo mediante l'impiego di *software* o protocolli d'accesso specifici come *Tor* o *I2P*, dove le criptovalute vengono spesso utilizzate come mezzo di offuscamento per acquistare droga, armi, documenti falsi (e così via). Per un'analisi del fenomeno, cfr. ECMDDA - Europol, *Drugs and the darknet. Perspectives for enforcement, research and policy*, The Hague 2017, 16 ss.

⁷ Per un'ampia trattazione di tale caso, recentemente tornato agli onori delle cronache, in ragione del fatto che il Presidente Trump ha graziato il creatore di *Silk Road*, si veda il volume di D. Carlisle, *op. cit.*, 6 ss.

⁸ La *blockchain* rappresenta l'infrastruttura tecnologica di base del mondo delle cripto-attività. Per un'agevole spiegazione sul punto, cfr. N. Furneaux, *Investigating Cryptocurrencies. Understanding, extracting, and analyzing blockchain evidence*, Chichester 2018, 1 ss. e G. Soana, *The Anti Money Laundering*, cit., 29 ss., v. anche sub § 4. Tale concetto ha, oramai, diverse definizioni normative, tra cui è sufficiente qui menzionare l'art. 3 co.1 n. 2 MiCAR, il quale si riferisce a «un archivio di informazioni in cui sono registrate le operazioni e che è condiviso da una serie di nodi di rete DLT ed è sincronizzato tra di essi, mediante l'utilizzo di un meccanismo di consenso».

le delicate problematiche giuridiche e applicative che sorgono nel caso in cui si renda necessario sequestrare i beni in esame (§§ 6-7).

La consapevolezza della complessità che caratterizza i procedimenti penali in cui vengono in rilievo cripto-valute costituirà lo spunto per le conclusioni (§ 8), nelle quali avanza alcune proposte utili per una migliore regolazione del fenomeno, concernenti, tanto il piano interno, quanto quello sovranazionale.

2. Per rendersi conto del ruolo che le cripto-attività rivestono per l'economia criminale è utile esaminare i *report* elaborati in materia dalle numerose società di *blockchain analytics* oramai esistenti⁹.

Le stime maggiormente accreditate, a questo riguardo, sono quelle sviluppate dall'azienda americana *Chainalysis*, la quale produce uno dei *software* privati di tracciamento dei flussi di cripto-attività più utilizzati tanto all'estero, quanto in Italia. Ebbene, secondo le indagini compiute da questa società, dal 2021 in poi la quantità di *crypto-asset* frutto di traffici illeciti avrebbe sempre superato, su scala globale, i 25 miliardi di dollari. Per la precisione, la somma sarebbe stata nel 2021 di 26,5 miliardi, nel 2022 di 54,3, nel 2023 di 46,1, mentre nel 2024 di 51,3¹⁰. E se è vero che si tratta di una fetta di transazioni molto più bassa se comparata alla grandezza complessiva del mercato in questione rispetto a quanto accadeva in passato¹¹, è altrettanto vero che i dati appena riportati sono fortemente sottostimati¹². Si afferma un tanto, non solo perché gli stessi escludono i profitti provenienti «*from non-crypto-native crime, such as traditional drug trafficking and other crimes in which crypto may be used as a means of payment or laundering*»¹³, ma anche in ragione del fatto che essi prendono in esame soltanto gli scambi di cui è già riconosciuta la riconducibilità ad attori criminali. Dal che se ne ricava come vi sia una grande “cifra oscura” di flussi illeciti di cripto-attività,

⁹ Tra i quali, v. *Chainalysis*, *The 2024 Crypto Crime Report*, reperibile in <https://go.chainalysis.com/crypto-crime-2024.html>; *Elliptic*, *Typologies Report 2024. Preventing Financial Crime in Cryptoassets*, reperibile in <https://www.elliptic.co/resources/elliptic-typologies-report-2024>; TRM, *Global Crypto Policy Review & Outlook 2023/24*, <https://www.trmlabs.com/eoy-policy-report-2023-24>.

¹⁰ I dati sono tratti da *Chainalysis*, *Illicit Volumes Portend Record Year as On-Chain Crime Becomes Increasingly Diverse and Professionalized*, reperibile in <https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/>.

¹¹ Cfr. D. Carlisle, *op. cit.*, 195, il quale ricorda che – secondo i dati di *Elliptic* – nel 2012 almeno un terzo di tutte le transazioni *Bitcoin* erano legate ad attività illecite.

¹² Lo rileva giustamente ancora D. Carlisle, *op. cit.*, 195.

¹³ Cfr. *Chainalysis*, *Illicit Volumes*, cit.

non analizzata neppure dai più avanzati *report* del settore.

Un ulteriore aspetto da prendere in considerazione è costituito dal fatto che i dati in materia dimostrano come il flusso di *asset* criminosi si muove, in particolare, verso alcune giurisdizioni, tra cui spiccano gli Stati Uniti, la Russia, la Cina e diversi ordinamenti europei, come il Regno Unito e la Francia¹⁴. Ma anche l'Italia è coinvolta massicciamente nel fenomeno: onde rendersi conto di ciò, è, d'altra parte, sufficiente ricordare come Chainalysis abbia identificato, nel corso del tempo, centinaia di milioni di dollari di attività illecite in cripto-attività riconducibili al nostro Paese¹⁵. E quel che è peggio è che vi sono plurimi esempi concreti di come finanche le mafie (italiane e straniere) stiano sfruttano le cripto-attività nei loro traffici¹⁶.

Detto ciò, va subito precisato che, a differenza di quanto si potrebbe pensare a primo acchito, l'uso criminale delle criptovalute non è limitato a specifiche tipologie di reati, ma copre oramai qualsivoglia genere delittuoso connesso alla trasmissione di un valore monetario¹⁷. Non a caso, già alla fine del 2021, Europol aveva affermato esplicitamente che «*the criminal use of cryptocurrency is no longer primarily confined to cybercrime activities, but now relates to all types of crime*»¹⁸.

Da una prospettiva economica, si è già accennato come le cripto-attività abbiano favorito il repentino sviluppo di veri e propri mercati criminali – presenti nel *dark web*¹⁹, ma anche su *social network* come *Telegram*²⁰ – in cui si vendono droga, armi, materiale pedopornografico, documenti falsi o rubati, fino ad arrivare alla possibilità di assoldare *killer* e a organizzare il traffico di esseri umani.

¹⁴ Cfr. Chainalysis, *270 Service Deposit Addresses Drive 55% of Money Laundering in Cryptocurrency*, reperibile in <https://www.chainalysis.com/blog/cryptocurrency-money-laundering-2021/>.

¹⁵ Si veda, in proposito, N. Buonanno, *Attività criminali basate sulle criptovalute: ultimi trend e modalità di tracciamento*, in www.cybesecitalia.events, 6.

¹⁶ Cfr. A. Anselmi, *Onion routing, cripto-valute e crimine organizzato*, Pisa 2019, nonché A. Nicaso (et. al.), *The Dark-Web Side of Mafias. Appalti, crypto e cybercrime. Le mafie adesso, più invisibili e potenti*, Milano 2024.

¹⁷ Al riguardo, cfr. N. Furneaux, *There's No Such Thing as Crypto Crime. An Investigative Handbook*, Chichester 2025, 67 ss.

¹⁸ Europol, *Cryptocurrencies: tracing the evolution of criminal finances*, dicembre 2021, reperibile in europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances.

¹⁹ Al riguardo, va detto che le autorità giudiziarie americane ed europee hanno compiuto, nell'ultimo decennio, una lotta senza quartiere ai c.d. *darknet market*, costellata di grandi successi: pensiamo, ad esempio, all'eliminazione da parte della polizia tedesca del *darknet market Hydra* nel 2022, che gestiva traffici illeciti per miliardi di dollari o, per quanto concerne l'Italia, al c.d. “Berlusconi Market”, smantellato nel 2019 dalla Procura di Brescia. Nondimeno, i dati di Chainalysis provano come tale fenomeno sia ben lungi da essere sradicato: cfr. Chainalysis, *The 2024 Crypto Crime Report*, cit., 90.

²⁰ Cfr. l'articolo ONU: *Telegram è un hotspot per fronti e riciclaggio di criptovalute*, reperibile in <https://www.binance.com/it/square/post/14555538331489>.

Se quanto detto è vero, va, tuttavia, osservato come le fattispecie aventi a oggetto cripto-attività si siano comunque evolute in modo profondo nel corso del tempo.

Da un lato, hanno acquisito sempre maggiore rilievo forme di reati come le truffe *online*, i furti di criptovalute e gli attacchi informatici (i c.d. *ransomware*). Si tratta di illeciti che, oltre a poter destabilizzare il mercato legale²¹, costituiscono una minaccia pure per la sicurezza nazionale, essendo dimostrato come essi siano spesso sviluppati da gruppi di *hacker* supportati da autorità statali, come la Corea del Nord²².

Da un altro lato, è oramai assodato che pure varie organizzazioni terroristiche – tra cui l'ISIS e Al-Qaeda – abbiano effettivamente cominciato a sfruttare le criptovalute per raccogliere fondi e/o comprare armi²³. Risale, ad esempio, alla fine di dicembre del 2024 la notizia della condanna pronunciata da una giuria americana nei confronti di un uomo di Springfield, per aver spedito oltre 185.000 dollari in *asset* virtuali a membri dell'ISIS²⁴.

Ma l'esperienza insegna che il punto d'elezione privilegiato che lega vasti traffici criminali alle cripto-attività è costituito dal riciclaggio²⁵. Tali beni si rivelano, invero, da questo angolo visuale particolarmente problematici già solo per il fatto che – come vedremo meglio in seguito – essi consentono di scambiare, pressoché istantaneamente, flussi di valore da una parte all'altra del globo, senza richiedere l'intervento di una banca o di un altro istituto di investimento tradizionale. Il che significa bypassare, in un solo colpo, i principali soggetti su cui si è da sempre sorretto il sistema contro il *money-laundering*, costruito faticosamente a livello internazionale

²¹ Si pensi a casi celebri come gli attacchi agli *exchange* “FTX” o “Bybit”, oppure a *stablecoins* come “Terra Luna”, i quali hanno causato perdite su scala globale per miliardi di dollari.

²² Si pensi al ruolo rivestito dal noto “Gruppo Lazarus”: D. Carlisle, *op. cit.*, 97 ss.

²³ In argomento, v. A. Burgess, R. Hamilton e C. Leuprecht, *Terror on the Blockchain: The Emergent Crypto-Crime-Terror Nexus*, in D. Goldbarsht e L. de Koker (a cura di), *Financial Crime, Law and Governance*, Cham 2024, 203 ss.; A. Lavorgna, *Organised Crime Goes Online: Realities and Challenges*, in *Journal of Money Laundering Control* 2015, 153 ss.; G. Milad, S.M.A. Irwin, *The use of crypto-currencies in funding violent jihad*, *ivi* 2016, 407 ss.

²⁴ La notizia si può reperire al seguente link: <https://www.justice.gov/usao-edva/pr/federal-jury-convicts-springfield-man-crypto-financing-scheme-isis>.

²⁵ Il tema è ampiamente studiato dalla letteratura penalistica italiana. A quest'ultimo proposito, basti ricordare il dibattito concernente la natura giuridica delle criptovalute e, di conseguenza, la possibilità di sussumere le “monete 2.0” in una delle diverse declinazioni dell'oggetto materiale del reato di riciclaggio ai sensi dell'art. 648-bis Cp. Cfr., a livello monografico, G.J. Sicignano, *Bitcoin e riciclaggio*, Torino 2019 e G. Soana, *The Anti Money Laundering*, *cit.*, *passim*. Si vedano pure L. Picotti, *Profili penali del Cyberlaundering: le nuove tecniche di riciclaggio*, in *RTrimDPenEc* 2018, 590 ss.; F. Pomes, *Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione*, *DPenCont – Riv. trim.* 2019, 159 ss.; M. Naddeo, *Nuove frontiere del risparmio, Bit Coin Exchange e rischio penale*, in *DPP* 2019, 101 ss.

e interno²⁶. Senza contare che le criptovalute consentono di ovviare anche ad alcuni dei maggiori inconvenienti che caratterizzano il denaro contante, laddove impiegato per questi scopi: quali la sua fisicità e la possibilità di identificare, a certe condizioni, le singole banconote utilizzate.

I criminali hanno poi dimostrato grandi capacità di adattamento al repentino sviluppo del mondo delle cripto-attività. A questo proposito, non va trascurato che se, per lungo tempo, le transazioni illecite di cripto-attività hanno avuto a oggetto soprattutto i *Bitcoin*, oggi la situazione è mutata. I dati, infatti, ci dicono che negli ultimi anni stanno iniziando a essere sempre più sfruttate a questo fine altre tipologie di *asset* virtuali, come le *stablecoins*²⁷. Ancora, vari *report* dimostrano come anche gli ultimi derivati del “mondo cripto” presentino forti rischi. Il riferimento va: a) ai c.d. *Non Fungible Tokens* (NFT), cioè *token* crittografici non replicabili perché registrati in una *blockchain*, quali opere d'arte, video, foto o audio²⁸; b) agli strumenti di finanza decentralizzata²⁹; c) al metaverso³⁰; d) alle forme integrate di portafogli di criptovalute e mezzi di comunicazione criptata.

Si può, in definitiva, ben dire che la galassia delle cripto-attività è, oramai, al centro di uno scontro globale tra *bad actors* e autorità di *law enforcement*. I primi hanno sviluppato strategie sempre più sofisticate per eludere i controlli. Le seconde hanno cercato di rispondere alla minaccia, sia attraverso strumenti economici³¹, sia di tipo normativo (§ 3) e investigativo (§ 4-6).

²⁶ Come sottolinea G. Soana, *Obblighi di prevenzione del riciclaggio e criptoattività. Interventi legislativi ed opportunità regolamentari*, in *Orizzonti del Diritto Commerciale*, 2022, fascicolo speciale, 472, «le criptovalute [...] nel bypassare la necessità per gli utenti di avvalersi di intermediari negli scambi di valore digitale, intaccano la premessa fattuale su cui è basata la normativa antiriciclaggio – per scambiare valore *online* è necessario avvalersi di un intermediario – diminuendone fortemente la cogenza concreta».

²⁷ Si tratta di *asset* il cui valore è legato ad altre valute aventi o meno corso legale, oppure ad altri beni (come l'oro).

²⁸ Cfr., sul punto, il *report* di Elliptic, *NFTs and Financial Crime*, reperibile in <https://www.elliptic.co/resources/nfts-financial-crime>.

²⁹ Cfr., al riguardo, l'articolo di Chainalysis, *DeFi Takes on Bigger Role in Money Laundering But Small Group of Centralized Services Still Dominate*, reperibile in <https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/>.

³⁰ Per una guida in materia, v. il *report* di Europol, *Policing in the metaverse: what law enforcement needs to know*, reperibile in <https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know>.

³¹ Si pensi alla strategia sviluppata dagli Stati Uniti attraverso l'*Office of Foreign Assets Control* (OFAC) per sanzionare a livello economico le maggiori organizzazioni criminali del settore (<https://ofac.treasury.gov/>). Cfr., al riguardo, l'articolo di Chainalysis, *OFAC and Crypto Crime: Every OFAC Specially Designated National with Identified Cryptocurrency Addresses*, in <https://www.chainalysis.com/blog/ofac-sanctions/>.

3. Di fronte a un quadro tanto problematico come quello descritto nel paragrafo precedente, gli ordinamenti sovranazionali e interni non potevano rimanere a lungo inerti. Onde evitare che il settore in esame si dimostrasse attrattivo per i criminali già solo perché caratterizzato da una «latitanza della legge»³², era, infatti, inevitabile che i legislatori reagissero sul piano normativo, cercando di imbrigliarne la natura deformalizzata.

In particolare, si sono a oggi susseguite tre macrofasi di regolazione del fenomeno³³.

In un primo momento, la strategia cardine su cui si è puntato è stata quella di intercettare i principali punti di contatto in “entrata” e in “uscita” del mercato delle cripto-attività, (ri)modulando e aggiornando in questo senso l’insieme dei presidi antiriciclaggio tradizionali. A tale riguardo, deve osservarsi come un ruolo propulsivo sia stato assunto dalla *Financial Action Task Force* (FATF), le cui indicazioni hanno rappresentato, sin dal principio, il “modello” seguito dal legislatore europeo nell’approntare una regolamentazione della materia³⁴. In tale contesto, va menzionata la Quinta Direttiva antiriciclaggio (Direttiva 2018/843/UE), la quale ha avuto il pregio di obbligare i c.d. *exchanges* (cioè, quegli operatori che svolgono il ruolo di cambiavalute tra denaro FIAT e valute virtuali e/o viceversa) e i c.d. *custodian wallet provider* (ovverosia quegli operatori che custodiscono le chiavi private dei portafogli di criptovalute) a rispettare i classici vincoli imposti agli istituti di credito in materia di antiriciclaggio³⁵. In tal modo, si è evidentemente cercato di gettare le basi per ricostruire, pure in questo settore “dematerializzato”, quella rete di intermediari finanziari che costituisce l’ossatura dei presidi AML³⁶.

³² Cfr. F. Consulich, *Nella wunderkammer del legislatore penale contemporaneo: monete virtuali che causano danni reali*, in *DPP* 2022, 153.

³³ Per uno studio analitico della tematica, cfr. G. Soana, *The Anti Money Laundering*, cit., 69 ss.

³⁴ FATF, *Report “Virtual Currencies Key Definitions and Potential AML/CFT Risks”*, 2014; FATF, *Guidance for a Risk-Based Approach to Virtual Currencies*, 2015.

³⁵ Si tratta di una strategia basata sulla condivisibile intuizione per cui, data la ancora scarsa utilizzabilità nel mondo fisico di tali beni, prima o poi essi saranno portati a scambiarle per denaro avente corso legale, dovendo perciò rivolgersi a tali *service provider*.

³⁶ Queste fonti sono state prontamente recepite sul versante nazionale. Ciò è avvenuto dapprima con il d.lgs. 25.5.2017 n. 90 – che ha individuato tra i soggetti obbligati ai fini antiriciclaggio tutti i prestatori di servizi di conversione di valute virtuali in valute aventi corso forzoso – e, in seguito, con il d.lgs. 4.10.2019 n. 125, di attuazione della Quinta Direttiva antiriciclaggio. Quest’ultimo, in particolare, si è spinto – per una volta – oltre il contenuto degli atti sovranazionali: esso non si è limitato, infatti, a modificare nuovamente la definizione di

Nonostante gli sforzi profusi a livello europeo e nazionale, deve darsi conto del fatto che – come era stato preconizzato dalla stessa Direttiva 2018/843/UE³⁷ – siffatta serie di norme non è stata sufficiente a contenere i rischi criminogeni degli strumenti in esame. Sfruttando la rapida evoluzione che caratterizza il settore delle cripto-attività, i *bad actors* hanno, invero, ben presto sviluppato molteplici strategie volte ad aggirare i presidi di tutela approntati dal legislatore. Le principali minacce a questo riguardo sono rappresentate, per un verso, dall'implementazione di strumenti sempre più sofisticati volti a offuscare le transazioni e farle apparire “lecite” (si pensi all'impiego di meccanismi come *mixers*³⁸; oppure all'utilizzo di “ponti” tra una *blockchain* e l'altra³⁹, oppure, ancora, di criptovalute incentrate sulla *privacy*⁴⁰) e, per un altro verso, dall'utilizzo di cambiavalute non conformi con gli obblighi AML⁴¹.

A fronte di tali problematiche, è stata inaugurata una “seconda era” nell'ambito della disciplina sovranazionale del fenomeno delle cripto-attività, volta – in linea con le nuove indicazioni provenienti dalla FAFT⁴² – a favorire una più adeguata regolamentazione e protezione del mercato, degli investitori, nonché degli scambi che avvengono al suo interno. Si colloca precisamente in questa direzione la recente approvazione del Regolamento 2023/1114/UE relativo ai mercati delle cripto-attività

valuta virtuale, ma ha anche lodevolmente esteso gli obblighi in esame, oltretutto ai «prestatori di servizi di portafoglio digitale», pure ai «prestatori di servizio all'utilizzo di valute virtuali», intesi come tutti coloro che prestano «servizi di emissione, collocamento, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, negoziazione, intermediazione delle valute».

³⁷ Cfr., il considerando n. 9, dove si affermava che «l'inclusione dei prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute reali e dei prestatori di servizi di portafoglio digitale non [avrebbe risolto] completamente il problema dell'anonimato delle operazioni in valuta virtuale».

³⁸ Trattasi di strumenti che consentono agli utenti di oscurare la cronologia delle proprie transazioni, aggregando un certo numero di trasferimenti e quindi mischiando l'origine e la destinazione dei pagamenti effettuati: cfr. D. Carlisle, *op. cit.*, 39 ss.

³⁹ V., al riguardo, Elliptic, *The state of cross-chain crime*, reperibile in <https://www.elliptic.co/hubfs/Cross%20Chain%20Report%20exec.pdf>.

⁴⁰ Si pensi a *Dash*, *Monero* o *ZCash*, le quali si differenziano dalle criptovalute “tradizionali” (come *Bitcoin*) per non essere trasparenti, cioè liberamente osservabili sulla rete. Esse si basano, infatti, su varie tecnologie pensate proprio per offuscare le transazioni e aumentare così il livello di anonimato dei soggetti coinvolti. Sull'impiego di queste criptovalute da parte dei criminali, v. sempre D. Carlisle, *op. cit.*, 59 ss. L'asset più problematico è *Monero*, il quale, pur non essendo del tutto immune al tracciamento, lo rende estremamente difficoltoso: cfr., sul punto, le interessanti ricerche pubblicate da TRM, *The Rise of Monero: Traceability, Challenges, and Research Review*, reperibili al seguente link: <https://www.trmlabs.com/post/the-rise-of-monero-traceability-challenges-and-research-review>.

⁴¹ Possono, ad esempio, essere menzionati gli *exchanges* russi *Bizlato*, *Cryptex* e *PM2BTC* recentemente sanzionati dalle autorità statunitensi (OFAC e FINCEN) come enti «*primary money laundering concern*».

⁴² FATF, *Report to the G20 Finance Ministers and Central Bank Governors*, 2018; FAFT, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, 2019.

(c.d. regolamento MiCA), la cui finalità è proprio quella di introdurre una disciplina finalizzata, tanto a favorire lo sviluppo della finanza digitale nei settori «non ancora coperti da atti legislativi dell’Unione in materia di servizi finanziari»⁴³, in modo conforme a una concorrenza leale, quanto a proteggere i detentori di *crypto-assets* e a garantire la stabilità del mercato. Siffatti scopi sono concretamente perseguiti attraverso un duplice meccanismo: da un lato, si è imputata agli operatori del settore una dettagliata serie di obblighi, il cui mancato rispetto deve essere prontamente sanzionato dalle autorità competenti; dall’altro, si è prescritta agli Stati membri l’adozione di meccanismi punitivi adeguati a reprimere una serie di violazioni, individuate mediante un puntuale rinvio a specifiche disposizioni regolamentari. Va, al riguardo, rilevato come la normativa europea abbia espressamente autorizzato i singoli Stati a impiegare tanto sanzioni di carattere amministrativo, quanto di natura penale. Da questa prospettiva, il nostro ordinamento, con l’approvazione del d.lgs. 5.9.2024 n. 129⁴⁴, si è limitato a introdurre una singola fattispecie delittuosa di abusivismo legato a operazioni di cripto-attività, privilegiando, per il resto, almeno sulla carta, la strada dell’illecito amministrativo punitivo.

Il regolamento MiCA è stato poi affiancato da un nuovo articolato pacchetto di misure, approvate dalle istituzioni UE tra il 2023 e il 2024, le quali hanno aperto una terza stagione regolatoria del fenomeno *de quo*, volta a meglio intercettare i pericoli specifici determinati dal funzionamento tecnologico degli *asset* basati su registri-distribuiti. Il riferimento va, in prima battuta, al Regolamento (UE) 2023/1113, riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cripto-attività (c.d. Regolamento *travel-rule*), il quale è stato adottato per garantire che le indicazioni della *FAFT* in tema di estensione della c.d. “regola di viaggio” alle cripto-attività (consistente nell’obbligo, per i prestatori di servizio di corredare i trasferimenti di fondi di dati informativi relativi all’ordinante e al beneficiario) venissero applicate in modo uniforme in tutta l’Unione⁴⁵. Per quanto qui rileva, va segnalato che, accanto a questa novità di ordine generale, tale atto spicca, non solo perché ha inteso attribuire determinati obblighi ai gestori dei c.d. *Bitcoin ATM* (*Automated Teller Machine*) o BTM

⁴³ Considerando n. 5 del Regolamento.

⁴⁴ Per un’analisi del quale, si consenta il rinvio a 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 questa Rivista.

⁴⁵ In merito a tale atto, cfr. la monografia di G. Soana, *The Anti Money Laundering*, cit., 212 ss.

(*Bitcoin Teller Machine*)⁴⁶, dato il loro potenziale uso legato al riciclaggio⁴⁷, oppure perché ha esplicitamente invitato l'Autorità bancaria europea a emanare orientamenti che specifichino la possibilità di avvalersi di *software* di *blockchain analysis* a fini preventivi, nei casi in cui vi sia una transazione a rischio particolarmente alto⁴⁸. L'innovazione principale del provvedimento sta, invero, nel fatto che, modificando in modo significativo l'approccio mantenuto in precedenza, l'Unione ha ricompreso nel suo ambito operativo pure le transazioni tra *service provider* e *wallet* gestiti in modo autonomo dagli utenti (c.d. *wallet* "auto-ospitati"⁴⁹). Così facendo, si è evidentemente cercato di mitigare, almeno in quota parte, il rischio che portafogli digitali di questo tipo si trasformino in uno strumento utile per aggirare l'insieme dei presidi antiriciclaggio faticosamente (ri)costruiti a livello sovranazionale e interno⁵⁰. Di riflesso, è chiaro come, in tal modo, si sia voluto attribuire un sempre più chiaro ruolo di primi guardiani della legalità del settore ai prestatori professionali di servizio di cripto-attività.

Ed è proprio in quest'ottica che si pone anche il nuovo *AML Package*⁵¹, composto dalla VI Direttiva antiriciclaggio (Dir. 2024/1640/UE), dal Regolamento *AMLA* (Regolamento 1620/2024/UE) e dal Regolamento antiriciclaggio (il Regolamento 1624/2024/UE, c.d. *single rulebook*). È degno di nota come in particolare quest'ultimo provvedimento contenga svariate previsioni innovative per il settore in esame, tra cui spiccano: a) la scelta di obbligare i prestatori di servizi per le cripto-attività ad applicare misure di adeguata verifica della clientela anche per le operazioni occasionali, che risultano rafforzate sopra la soglia di 1.000 euro di controvalore (art. 19); b) la previsione di ulteriori misure di mitigazione dei rischi in relazione a operazioni con

⁴⁶ Art. 2 par. 1 e considerando n. 25.

⁴⁷ D. Carlisle, *op. cit.*, 83 ss.; M. Hyman, *Bitcoin atm: criminal's laundromat for cleaning money*, in *St. Thomas Law Review* 2015, 296 ss., ai quali si rinvia anche per più ampie considerazioni in merito al funzionamento tecnico di tali strumenti.

⁴⁸ Considerando n. 17. Cfr. EBA, *Guidelines on templates for explanations and opinions, and the standardised test for the classification of crypto-assets, under Article 97(1) of Regulation (EU) 2023/1114*, 10.12.2024, nelle quali sono contenute varie *red flags* utili per identificare transazioni di matrice particolarmente sospetta.

⁴⁹ Ovverosia quelli in cui il cliente ha il pieno controllo delle chiavi crittografiche private. Cfr. *sub par.* 4.

⁵⁰ A ogni modo, rimangono ancora fuori dalla disciplina le transazioni dirette tra persona e persona (cd. P2P). Nondimeno, in proposito il considerando n. 58 precisa che, visti i potenziali rischi determinati da tali tipologie di transazioni, la Commissione UE sarà tenuta entro il 1° luglio 2026 a valutare la necessità di ulteriori misure specifiche in materia.

⁵¹ Pubblicato sulla G.U. dell'Unione il 19 giugno 2024, e destinato a divenire completamente operativo il 10 luglio 2029. Per una visione d'insieme, v. G. Soana, *The Anti Money Laundering*, cit., 203 ss.

indirizzi auto-ospitati (art. 40); c) la scelta di vietare ai prestatori di servizi per le cripto-attività la fornitura e la custodia di conti di cripto-attività anonimi o di conti che consentono l'anonimizzazione o un maggiore offuscamento delle operazioni (es. *wallet* con *mixer* integrati, come il celebre *Wasabi Wallet*⁵²), anche attraverso monete incentrate sull'anonimato (art. 79).

Va, da ultimo, segnalato che l'Unione europea non si è fermata però qui, ma nel 2024 ha potenziato il proprio sistema di contrasto alla criminalità nel settore in esame mediante la nuova Direttiva 2024/1260/UE, riguardante il recupero e la confisca dei beni⁵³. Sebbene, come ribadiremo in seguito, tale provvedimento non detti, in modo criticabile, una disciplina ablatoria *ad hoc* per i beni in esame⁵⁴, esso presenta perlomeno il pregio di ricomprendere esplicitamente gli stessi nelle procedure dalla stessa regolate. Il che rappresenta comunque un segnale di come il legislatore europeo si sia reso conto del fatto che i *crypto-asset* non possono essere oramai più tralasciati, laddove si vogliano contrastare i profitti illeciti delle organizzazioni criminali e riaffermare, anche in questo settore, la validità della massima per cui "il crimine non deve pagare"⁵⁵.

4. Nel paragrafo precedente, si è avuto modo di osservare che, negli ultimi anni, è stata introdotta una rete sempre più fitta di previsioni, volte a facilitare il contrasto ai traffici illeciti che si riconnettono a cripto-attività. Come testimoniato dai dati pubblicati dall'Unità di Informazione Finanziaria presso la Banca d'Italia, questi sforzi regolatori stanno effettivamente producendo risultati positivi. Le nuove regole sono,

⁵² Per un'analisi del ruolo che tale tipologia di *wallet* ha nei traffici criminali, cfr. Elliptic, *Elliptic Research Shows a Dramatic Increase in the Use of Privacy Wallets to Launder Proceeds of Crime in Cryptoassets*, reperibile in <https://www.elliptic.co/media-center/elliptic-research-privacy-wallets-crime-in-cryptoassets>. Non a caso, la FinCEN americana, onde far fronte a tale minaccia, ha proposto di adottare una regolamentazione tesa a «identifies international Convertible Virtual Currency Mixing (CVC mixing) as a class of transactions of primary money laundering concern» (cfr. *FinCEN Proposes New Regulation to Enhance Transparency in Convertible Virtual Currency Mixing and Combat Terrorist Financing*, reperibile in <https://www.fincen.gov/news/news-releases/fincen-proposes-new-regulation-enhance-transparency-convertible-virtual-currency>).

⁵³ A commento della quale, v. A. Del Giudice, *La nuova direttiva europea sul sistema di asset recovery. Novità, impatti, prospettive*, in *RIDPP* 2024, 1011 ss.; S. Finocchiaro, *La nuova direttiva dell'Unione europea in materia di sequestro e confisca*, in *www.sistemapenale.it*, 6, 2024, 105 ss.; A.M. Maugeri, *La nuova direttiva 2024/1269 per il recupero e la confisca dei beni: un complessivo sforzo di armonizzazione per la lotta al crimine organizzato e all'infiltrazione criminale nell'economia*, in *www.sistemapenale.it*, 30.12.2024.

⁵⁴ Per condivisibili critiche circa tale lacuna, v. A. Del Giudice, *op. cit.*, 1022 ss. (v. anche *sub* § 7).

⁵⁵ Sul quale cfr., per tutti, V. Manes, *L'ultimo imperativo della politica criminale: nullum crimen sine confiscatione*, in *RIDPP* 2015, 1260.

infatti, riuscite ad aumentare, in modo esponenziale, le segnalazioni per operazioni sospette (SOS) riconducibili a *virtual asset*. Basti, in proposito, pensare che si è passati da appena 732 SOS ricevute nel 2019 a 3.453 nel 2021, sino a superare le 5.000 già nel 2022⁵⁶. Il che, evidentemente, dimostra un miglioramento significativo delle capacità preventive e repressive dell'ordinamento.

Se ciò è vero, va, del pari, rilevato come, tanto il MiCAR, quanto la corposa disciplina antiriciclaggio approvati in questo settore, non possano essere considerati dei punti d'arrivo, ma solo i primi passi di un percorso che deve essere necessariamente più ampio e ambizioso. Onde contrastare in modo efficace i traffici illeciti che abbiano a oggetto cripto-attività è, invero, indispensabile focalizzare l'attenzione anche su profili ancora non sufficientemente esplorati, tra cui spicca il piano più strettamente investigativo e processuale. Al riguardo, va, infatti, osservato che, se – come accennato – per quanto concerne il diritto penale sostanziale e quello amministrativo punitivo sono già stati fatti diversi passi avanti, la situazione risulta molto più critica a livello processualpenalistico. E ciò in quanto, da questo angolo visuale, si assiste, finora, a un preoccupante immobilismo legislativo quasi totale, sia a livello sovranazionale, sia interno. Il che rischia di creare problemi di rilevanza cruciale, dal momento che non sempre le previsioni generali contenute nei codici di rito riescono ad adattarsi alle peculiarità del fenomeno *de quo*, venendosi a determinare aree grigie (se non veri e propri vuoti di tutela) pericolose, sia per il rispetto dei diritti fondamentali degli individui, sia per la “tenuta processuale” delle ipotesi accusatorie.

Al fine di dimostrare tale assunto, è necessario ripercorrere – seppur per sommi capi – lo schema di base che caratterizza gli scambi di cripto-valute. Al riguardo, deve anzitutto ribadirsi che, onde trasferire questi beni, è indispensabile avere un “portafoglio” (cosiddetto *wallet*)⁵⁷, cioè uno strumento contenente le chiavi che consentono a livello tecnico le transazioni. Esse si basano, più propriamente, su uno schema a “criptografia asimmetrica”, richiedendo l'utilizzo contestuale di due diverse tipologie di “chiavi”⁵⁸: una “chiave pubblica”, impiegata sia per generare gli indirizzi all'interno dei quali sono ricevuti gli *asset*, sia per crittografare i dati della transazione;

⁵⁶ Cfr. Newsletter 5-2022 della UIF, reperibile all'indirizzo <https://uif.bancaditalia.it/pubblicazioni/newsletter/2022/newsletter-2022-5/index.html>.

⁵⁷ Molteplici sono le tipologie di *wallet* esistenti: *Paper wallet*; *Software wallet*; *Hosted wallet*; *Self-hosted wallet*; *Hot wallet* e *Cold wallet*. Cfr. per un'ampia analisi sul punto, N. Furneaux, *Investigating Cryptocurrencies*, cit., 95 ss.

⁵⁸ Sul punto, v. la chiara analisi di G. Soana, *The Anti Money Laundering*, cit., 41 ss.

e una “chiave privata”, la quale ha la funzione di autorizzare la spesa. Per trasferire una somma è sufficiente conoscere l'indirizzo del destinatario e siglare la transazione con la chiave privata, senza per forza rivolgersi a un intermediario. A questo punto, il sistema genera una stringa di dati nella quale è indicata la somma trasmessa e gli indirizzi interessati. Dopodiché, intervengono degli utenti (per il *Bitcoin* chiamati “miners”) che hanno il compito di raccogliere le transazioni in un blocco e di “validarlo”⁵⁹, cioè di controllare che i vari passaggi di valore siano coerenti con i precedenti blocchi della catena⁶⁰. Una volta compiuta questa operazione, essi aggiungono il nuovo gruppo di transazioni alle precedenti: ed è proprio da questa prospettiva che si coglie il senso del termine *blockchain*, che rappresenta, per l'appunto, una “catena di blocchi” delle transazioni via via compiute.

Senonché è importante ricordare che le *blockchain* non sono tutte uguali, ma vengono, tradizionalmente, divise in quattro categorie: pubbliche, private, ibride o federate⁶¹. Per quanto qui rileva, va ricordato che le principali *blockchain* del settore delle cripto-attività – come quella di *Bitcoin* – rientrano nella prima categoria. Esse sono, più in particolare: a) *immutabili*, senza il consenso della rete (difatti, varie copie della *blockchain* sono contenute nei nodi della rete, il che consente al sistema di essere affidabile, evitando la doppia spesa delle somme); b) *decentralizzate*, atteso che non esiste un'autorità regolatoria centrale che prenda in carico gli scambi, ma esse sono gestite dagli utenti; c) *trasparenti*, nel senso che l'importo, la data, l'indirizzo di invio e l'indirizzo di ricezione di ogni transazione sono liberamente osservabili da chiunque; d) *tracciabili*, poiché si può risalire all'esatta provenienza di ogni trasferimento cristallizzato sul registro; e) *pseudo-anonime*⁶², in quanto le transazioni pur fornendo uno scudo di riservatezza, dal momento che sono identificate solo in forma criptata mediante una sequenza di numeri e lettere (c.d. *transaction hash*) e non mediante i nominativi del cedente e del cessionario, ben possono, tuttavia, essere de-

⁵⁹ Le modalità di validazione cambiano a seconda del diverso “algoritmo del consenso” su cui si fonda la singola *blockchain* di riferimento: al riguardo, v. N. Furneaux, *There's No Such Thing as Crypto Crime*, cit., 139 ss.

⁶⁰ Cfr., ancora, G. Soana, *The Anti Money Laundering*, cit., 36 ss.

⁶¹ V. R. Verma e N. Dhanda, *Blockchain types: A characteristic view*, in Aa.Vv., *Distributed Computing to Blockchain Architecture, Technology, and Applications*, Cambridge 2023, 69 ss.

⁶² Circa tale caratteristica, v. A. Balaskas e V.N.L. Franqueira, *Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges*, in *International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Glasgow 2018, 5; C. Rueckert, *Cryptocurrencies and fundamental rights*, in *Journal of Cybersecurity* 2019, 3; G. Soana, *The Anti Money Laundering*, cit., 45 ss.

anonimizzate, mediante l'ausilio di determinate tecniche⁶³.

Ebbene, è evidente che le notazioni appena compiute producono un duplice ordine di conseguenze sul versante investigativo.

In primo luogo, ciò consente di comprendere come nei procedimenti penali legati alle cripto-attività le tecniche d'indagine tradizionali (pur sempre essenziali) debbano essere necessariamente supportate da metodologie di ricerca della prova aventi carattere altamente tecnologico⁶⁴. L'esperienza insegna, infatti, che l'attività di contrasto alla criminalità avente a oggetto *crypto-asset*, oltre ad avere spesso una matrice transnazionale, richiede l'impiego incrociato di plurimi atti di indagine digitali. Si allude, in particolare, sia al compimento di attività *under cover* telematiche, sia alla raccolta massiva di dati da fonti aperte (c.d. *open source intelligence* – c.d. OSINT)⁶⁵ e, in particolare, da *social network* (c.d. SOCMIT)⁶⁶, sia, infine, all'utilizzo di metodi variegati di analisi della *blockchain* (c.d. *blockchain analysis*)⁶⁷. Le autorità di *law enforcement* hanno, infatti, ben presto imparato a sfruttare alcune caratteristiche intrinseche dei registri-distribuiti delle principali criptovalute, tra cui, in particolare, il loro essere di norma pubblici e liberamente accessibili⁶⁸, per ricostruire tramite tecniche di questo tipo i flussi di cripto-attività illeciti e per de-anonimizzarli. E se è vero che diverse attività possono essere compiute in modo manuale dagli operatori⁶⁹, va ricordato che, con il tempo, è nata una vera e propria industria di *software* specializzati, utili per scandagliare il *web* alla ricerca di dati di rilievo e per seguire i

⁶³ Per un'aggiornata guida operativa sul punto, cfr. N. Furneaux, *There's No Such Thing as Crypto Crime*, cit., 239 ss. Come anticipato, bisogna ribadire che tale operazione di de-anonimizzazione è, invece, molto più complessa, per alcune *privacy coin* come *Monero*.

⁶⁴ Cfr. N. Furneaux, *There's No Such Thing as Crypto Crime*, cit., 109 ss. Nella letteratura italiana, v. G. Costabile, *Le indagini digitali*, in Aa.Vv., *Cyber Forensics e indagini digitali*, Torino 2021, 128.

⁶⁵ Si veda sul punto NATO, *Open Source Intelligence Handbook*, 2001.

⁶⁶ Sulla quale, v., *amplius*, D. Omand, *Social Media Intelligence (SOCMINT)*, in R. Dover, H. Dylan, M.S. Goodman (a cura di), *The Palgrave Handbook of Security, Risk and Intelligence*, Londra 2017, 355 ss.

⁶⁷ In argomento, v., *ex multis*, H. Atlam (et. al), *Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions*, in *Electronics* 2024, 1 ss.; D. Carlisle, *op. cit.*, 63 s.; A. Balaskas e V.N.L. Franqueira, *op. cit.*, 1-8; Elliptic, *Blockchain Analytics & Analysis*, reperibile in <https://www.elliptic.co/hubfs/Blockchain%20and%20Analytics%20Guide.pdf>; N. Furneaux, *There's No Such Thing as Crypto Crime*, cit., 125 ss.; S. Salisu e V. Filipov, *Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation*, in R.L. Wilson e B. Curran (a cura di), *Proceedings of the 18th International Conference on Cyber Warfare and Security*, Reading 2023, 338 ss.; G. Soana, *The Anti Money Laundering*, cit., 224 ss.; C. Pelker Alden, C. Brown e R. Tucker, *Using Blockchain Analysis from Investigation to Trial*, in *Department of Justice Journal of Federal Law and Practice* 2021, 59 ss.

⁶⁸ Come si è accennato, fanno eccezione a queste caratteristiche una serie di criptovalute incentrate sulla *privacy*, come *Dash*, *Monero* o *ZCash*.

⁶⁹ Cfr., per numerosi esempi al riguardo, N. Furneaux, *Investigating Cryptocurrencies*, cit., 175 ss.

flussi di denaro⁷⁰. Siffatto *modus operandi*, tuttavia, induce a riflettere, come vedremo a breve, circa la compatibilità di queste nuove metodologie di indagine con il diritto alla riservatezza e alla tutela dei dati personali, specialmente qualora dette operazioni siano compiute in maniera continuativa e massiva, al fine di ricavare un quadro atomistico della “vita finanziaria” (e non solo) dei singoli bersagli⁷¹.

In secondo luogo, le peculiari caratteristiche della tecnologia della *blockchain* incidono, in modo determinante, anche sulle procedure di sequestro aventi ad oggetto le criptomonete collegate a traffici illeciti⁷². Al riguardo, fermo l'interesse degli ordinamenti giuridici a imporre vincoli reali di diverso tipo su tali beni⁷³, va registrato il fatto che l'esecuzione degli stessi determina molteplici complessità, tanto di ordine teorico, quanto pratico. Dalla prima prospettiva, occorre sottolineare come, in realtà, gli *asset* virtuali, in quanto beni immateriali, non possono essere tecnicamente oggetto di un sequestro in quanto tale (se inteso come spossessamento fisico di una *res*), potendosi solamente ottenere un effetto giuridico equivalente⁷⁴. Ma ciò che più rileva è il secondo angolo visuale: ci riferiamo, in particolare, al fatto che il fortissimo rischio di dissipazione che caratterizza i beni in esame, i quali possono essere trasferiti altrove in un attimo con un *click*, eludendo alla radice le misure ablatorie dell'autorità, rende indispensabile adottare plurimi accorgimenti, onde assicurarsi che le stesse possano andare a buon fine.

Preso atto di ciò, nei prossimi paragrafi ci si concentrerà separatamente sui problemi che i temi appena menzionati pongono per l'ordinamento italiano, a causa della già

⁷⁰ Sulla nascita di questa industria, cfr. D. Carlisle, *op. cit.*, 63 ss.

⁷¹ Cfr. *sub* par. 5.

⁷² Per una panoramica operativa delle tecniche da seguire per sequestrare efficacemente le cripto-attività, cfr. N. Furneaux, *There's No Such Thing as Crypto Crime*, cit., 445 ss., nonché A. Owen, M. Nizzero e A. Larkin, *Seizing Crypto: When Asset Recovery Goes Digital*, reperibile in <https://www.rusi.org/explore-our-research/publications/commentary/seizing-crypto-when-asset-recovery-goes-digital>. Nella letteratura italiana, v. M. Antinucci e D. Scampoli, *Il sequestro e la confisca di bitcoin*, in *DPP* 2024, 1083; F. Cajani, *Sequestri di files e Bitcoin: i riflessi della dematerializzazione di beni e valute sulla disciplina penal-processualistica italiana*, ivi 2021, 742; P. Dal Checco, *Sequestro e confisca: tecnica e procedura*, in S. Carpaccioli (a cura di), *Criptoattività, criptovalute e Bitcoin*, Milano 2021, 329; R. Lupo, *Quale sequestro per le criptovalute?*, in *ilCentuario* 2020, 50.

⁷³ Idealmente, è possibile disporre un vincolo reale sulle monete virtuali attraverso un sequestro probatorio (e, eventualmente, una successiva confisca), in quanto *corpus delicti*, cioè, prodotto, profitto o prezzo del reato (art. 253, co.2, Cpp). Parimenti, esse possono rappresentare l'oggetto di un sequestro conservativo (art. 316 Cpp) o preventivo (art. 321 Cpp): cfr. Cass. 26.10.2022 n. 44378, in *OneLegale*.

⁷⁴ Al pari di quanto avviene nel caso di un sequestro di una pagina *Internet*, infatti, pure l'ablazione dei *bitcoin* non può essere realizzata mediante lo spossessamento fisico della *res*, trattandosi, per l'appunto di beni immateriali.

ricordata inerzia legislativa che caratterizza il settore delle indagini penali in cui vengano in rilievo cripto-attività.

5. Come si è accennato, gli strumenti automatici di tracciamento rappresentano degli ausili fondamentali per contrastare, in modo efficace, i reati connessi alle cripto-attività. Non a caso, anche in Italia, vari *software* di analisi della *blockchain* sono oramai in dotazione delle autorità di *law enforcement*, le quali li utilizzano quotidianamente in un'ottica di *follow the crypto*. Essi vengono, più in particolare, impiegati per ordinare, a monte, e seguire poi, a valle, la marea di flussi di scambi di *asset* presenti sui diversi registri-distribuiti.

Il più delle volte gli investigatori impiegano i *tools* con un obiettivo preciso: quello di riuscire a individuare mediante gli stessi un prestatore di servizi di cripto-attività, come un *exchange*, a cui rivolgere, poi, un ordine di fornire informazioni circa le generalità dei soggetti coinvolti nelle transazioni, riuscendosi così a de-anonimizzare la catena delle stesse⁷⁵. Nel caso si abbia a che fare, invece, con un *provider* che gestisca direttamente le chiavi private dei *wallet* per i propri clienti, il vantaggio sarà ancora maggiore, dal momento che si potranno a questo punto finanche bloccare i fondi di interesse, notificando al medesimo un provvedimento di sequestro.

Se ciò è vero, va osservato che, a differenza di quanto accade in altri ordinamenti⁷⁶, il nostro codice di rito non detta alcuna previsione specifica, né con riguardo all'OSINT, né in merito agli *investigative tools* atti a tracciare, in maniera più o meno massiva e continuativa, le cripto-attività.

In ossequio a una prima lettura, si potrebbe, tuttavia, essere portati a giustificare la mancanza di una regolamentazione specifica sul punto in forza della circostanza per cui i dati analizzati dagli applicativi in questione risultano perlopiù *open access*. Come si è detto, infatti, la maggior parte delle *blockchain* sono pubbliche, così come i dati connessi alle transazioni sul *web* o nei *social network* ricercati tramite applicativi di OSINT. Posto, dunque, che nessuna aspettativa di *privacy* potrebbe essere invocata a

⁷⁵ Si tratta, evidentemente, di dati che i *provider* sono tenuti a raccogliere proprio in forza delle sopra esaminate regole antiriciclaggio, approvate negli ultimi anni a livello sovranazionale e interno. Dal che se ne desume come i *tools* di analisi della *blockchain* costituiscano l'apparato tecnico chiave per consentire di sfruttare al meglio la capacità preventiva e repressiva degli obblighi di adeguata verifica della clientela, posti dalla disciplina AML.

⁷⁶ Cfr. B.J. Koops, *Police Investigations in Internet Open Sources: Procedural-Law Issues*, in *Computer Law & Security Review* 2013, 654 ss.

fronte di notizie liberamente e consapevolmente esposte “in bella vista”⁷⁷ al pubblico, si potrebbe ritenere insussistente un obbligo del legislatore di regolare in modo dettagliato i casi e i modi di un loro utilizzo, onde rendere proporzionata l'intrusione nella sfera giuridica del singolo. Ove stessero così le cose, la polizia giudiziaria ben potrebbe avvalersi in autonomia di tali applicativi, utilizzando i propri poteri investigativi generali riconosciuti dal sistema processuale, non essendo, invece, tenuta a richiedere alcun provvedimento autorizzativo emesso da un giudice o dal pubblico ministero.

È opportuno rilevare come un'interpretazione analoga a questa sia stata effettivamente avallata da una delle prime sentenze che, nel panorama mondiale, si è confrontata con simili problematiche. Il riferimento va al caso *Stati Uniti c. Gratkowski*⁷⁸, nel quale un imputato aveva chiesto di escludere degli elementi di prova raccolti dagli investigatori grazie all'impiego di uno strumento di analisi della *blockchain*, in forza del rilievo per cui tale attività sarebbe stata compiuta in violazione del suo diritto alla riservatezza, protetto dal IV Emendamento della Costituzione USA. Ebbene, è degno di nota come la *Court of Appeal* per il Quinto Circuito statunitense abbia rigettato tale censura, valorizzando proprio la natura pubblica e liberamente accessibile dei dati contenuti in tale registro-distribuito. Più in particolare, secondo tale pronuncia, poiché la “catena di blocchi” risulta «*transparent by design*», sarebbe categoricamente da escludersi ogni possibile rilevanza del diritto alla riservatezza con riguardo agli stessi, con la conseguente piena utilizzabilità del materiale ivi raccolto.

Nonostante la presenza di questo precedente, siffatta lettura non convince, per più ordini di ragioni.

In prima battuta, perché essa pare affetta da un vizio logico. Ci si riferisce al fatto che tale esegesi ricava dalla natura *open access* di molte *blockchain* una sorta di rinuncia implicita dell'individuo alla riservatezza delle transazioni che lo riguardino. Ma le cose non stanno così: se è, infatti, vero che vari registri-distribuiti sono pubblici,

⁷⁷ Cfr. B.J. Koops, *op. cit.*, 654 ss. Come sottolinea, benché in una più ampia prospettiva, S. Signorato, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Torino 2018, 166, non «sembrano profilarsi questioni di compatibilità con l'art. 8 Cedu [...] nel momento in cui un soggetto immette dati in un luogo della rete pubblico o aperto al pubblico». Egli, infatti, «accetta il rischio che quei dati possano essere visualizzati ed appresi ovunque, da chiunque, e per qualunque fine. Quindi anche per finalità investigative».

⁷⁸ Il riferimento va a *United States c. Gratkowski*, 964 F.3d 307, 312–13 (5th Cir. 2020). A commento della pronuncia, v. D. Penn, *The Fifth Circuit, The Fourth Amendment, and the Third-Party Doctrine: Two Takeaways from the Court's First Ruling on Bitcoin Privacy*, in *Science and Technology Law Review* 2021, 125 ss.

è altrettanto indiscutibile che, come abbiamo ricordato, gli scambi ivi cristallizzati appaiono in forma criptata, sotto forma di sequenza alfanumerica non riconoscibile, proprio per salvaguardare la *privacy* dei singoli utenti. Che poi gli investigatori, incrociando tali dati con varie tipologie di informazioni, rinvenibili o meno *online*, possano riuscire a de-anonimizzare i passaggi di *asset* virtuali è un elemento che, a nostro avviso, non elimina l'aspettativa di riservatezza di base che, comunque, il singolo ragionevolmente continua a mantenere circa il *contenuto* dei flussi di dati che lo riguardano. Un'aspettativa che si fonda sul fatto che, per la collettività, ogni passaggio di valore presente sulle *blockchain* appare in forma tale da non essere decodificabile, se non con la collaborazione dell'utente o a patto di impiegare mezzi particolarmente intrusivi. Non è, del resto, un caso che, esattamente sulla base di queste ragioni, una parte della giurisprudenza italiana abbia individuato nell'impiego delle cripto-attività una via per occultare all'autorità dei valori, visto il grado di anonimato dalle stesse garantito⁷⁹. Insomma, è proprio perché non bisogna fare confusione tra *forma* della transazione (che può anche essere pubblica) e *oggetto* della stessa (riservata, perché sotto forma di codice *hash*) che ci sembra possa sostenersi che la persona conservi una ragionevole aspettativa di *privacy* con riguardo al *contenuto* dei dati reperibili sulle *blockchain*⁸⁰.

In secondo luogo, va osservato che, come sostenuto da attenta dottrina, l'attività di monitoraggio massivo e di stoccaggio tramite *software* dei flussi di *crypto* di un individuo, a differenza di un'acquisizione "manuale" *una tantum*, determina, comunque, un'ingerenza di non trascurabile gravità nella sfera riservata dell'individuo⁸¹. E ciò perché, attraverso il complesso di queste operazioni, l'autorità è messa nelle condizioni di ricostruire una porzione tale della "vita economica" del bersaglio, da poter trarre poi conclusioni precise, o addirittura molto precise, su vari aspetti della sua vita privata, come le abitudini quotidiane, le attività esercitate, le relazioni intrattenute, e così via.

⁷⁹ Cfr., ad esempio, Cass. 7.7.2022 n. 27023, in *OneLegale*, in materia di autoriciclaggio.

⁸⁰ Da questa prospettiva non sembra, infatti, che si possa slegare il momento della raccolta dei dati presenti sulle *blockchain* dal complesso delle operazioni compiute dagli investigatori, le quali sono nel loro insieme finalizzate a de-anonimizzare le transazioni e, quindi, a squarciare il velo di riservatezza assicurato dalle stesse.

⁸¹ Cfr., a questo riguardo, le condivisibili affermazioni di C. Rueckert, *op. cit.*, 6, secondo il quale «*the mere browsing of and searching for data in the blockchain (e.g. with tools like blockchain.info) is not deemed an interference in the right to protection of personal data. However, an intervention in the right to protection of personal data is conceivable, when law enforcement agencies, prosecutors and/or regulators systematically collect, store and/or process data from the blockchain*».

Per quanto concerne il diritto dell'Unione europea, non va poi trascurato il fatto che, tanto l'art. 3 della Direttiva 2016/680/UE, quanto l'art. 4 del Regolamento GDPR, fanno rientrare nel novero dei *personal data* tutti quelli che sono in grado di rendere identificabile un utente. E non è difficile rendersi conto che i dati presenti nelle *blockchain* pubbliche rientrano in tale categoria proprio perché permettono di risalire, indirettamente, alle generalità degli interessati⁸². Stando così le cose, l'impiego dei *software* in esame, dando vita a un trattamento automatizzato di dati personali, finalizzato ad analizzare la situazione economica e il comportamento di uno o più soggetti, pare rientrare, più in particolare, nel novero delle c.d. "profilazioni", dovendo, pertanto, sottostare al relativo *acquis* eurounitario in materia⁸³.

Da ultimo, la tesi sopra esaminata non convince alla luce di vari orientamenti pretori – strettamente legati – sviluppati in seno alla giurisprudenza della Corte europea dei diritti dell'uomo.

Per un verso, i giudici di Strasburgo hanno, a loro volta, riconosciuto, in tema di indagini penali realizzate sui conti correnti bancari, che la memorizzazione o la raccolta di dati relativi alla situazione finanziaria di un individuo costituisce un'ingerenza nella riservatezza, a prescindere dalla tipologia e dalla natura delle informazioni raccolte⁸⁴.

Per altro verso, è degno di nota il fatto che la Corte europea abbia affermato che il concetto di "vita privata", cui si riferisce l'art. 8 CEDU, va inteso in senso ampio, ricomprendendovi anche quelle attività che si svolgono in contesti pubblici⁸⁵, come le

⁸² V., ancora, C. Rueckert, *op. cit.*, 7.

⁸³ Cfr., al riguardo, A. Lyle, *Legal considerations for using open source intelligence in the context of cybercrime and cyberterrorism*, in B. Akhgar, P.S. Bayerl, F. Sampson (a cura di), *Open Source Intelligence Investigation: From Strategy to Implementation*, Londra 2016, 277 ss.; A. Shere, *Reading the Investigators their Rights: A review of literature on the General Data Protection Regulation and open-source intelligence gathering and analysis*, in *The New Collection*, 3, 2020, 1 ss.; G. Soana, *The Anti Money Laundering*, cit., 241 ss. Al riguardo, deve, tuttavia, evidenziarsi una certa contraddittorietà tra la normativa europea in tema di *data protection* – che mira a rafforzare la tutela della riservatezza in ogni suo aspetto – e le norme in materia AML, le quali, all'opposto, sono volte ad agevolare intrusioni nella sfera privata per finalità di contrasto alla criminalità economica.

⁸⁴ Cfr. C. eur., 1.12.2015, *Brito Ferrinho Bexiga Villa-Nova c. Portogallo*, § 42 ss.; C. eur., 7.7.2015, *N. et autres c. San Marino*, § 51. Cfr., sul punto, G. Lasagni, *Banking Supervision and Criminal Investigation. Comparing the EU and US experiences*, Cham 2019, 334.

⁸⁵ Cfr., benché con riguardo al tema del riconoscimento facciale realizzato in luoghi pubblici, C. eur., 4.7.2023, *Glukhin c. Russia*, § 64: «the Court reiterates that the concept of "private life" is a broad term not susceptible to exhaustive definition. It can embrace multiple aspects of the person's physical and social identity. It is not limited to an "inner circle" in which the individual may live his or her own personal life without outside interference, but also encompasses the right to lead a "private social life", that is, the possibility of establishing and developing relationships with others and the outside world. It does not exclude activities taking place in a public context. There

attività professionali e finanziarie, tra le quali, come si intuisce, ben possono annoverarsi le transazioni monetarie realizzate attraverso la *blockchain*.

Infine, va ricordato che i giudici europei hanno precisato che la mera attività di stoccaggio da parte delle pubbliche autorità «*of data relating to the private life of an individual amounts to an interference within the meaning of Article 8*»⁸⁶, non essendo neppure necessario che le informazioni raccolte vengano poi utilizzate.

Dall'insieme di queste considerazioni, ne consegue una conclusione univoca: l'utilizzo di *software* di *blockchain analysis* per de-anonimizzare le transazioni nell'ambito di un'indagine penale, provoca un'ingerenza, che può raggiungere anche un rilievo significativo⁸⁷, nel diritto alla vita privata e alla protezione dei dati personali, protetti dall'art. 8 CEDU, nonché dagli artt. 7 e 8 della Carta di Nizza⁸⁸. Non sembra, del resto, un caso che la stessa FAFT, pur riconoscendo l'importanza di questi *tools* ai fini AML, abbia ricordato che «*it is important to consider any potential implications for privacy and data protection in the use of such tools, if they allow transparency that is not otherwise available (e.g. on public blockchains)*»⁸⁹.

Ne consegue, a cascata, che i legislatori nazionali sono tenuti a rispettare il corrispondente *standard* minimo di garanzie derivante dall'insieme di tali previsioni, il quale è riassumibile nella necessaria presenza di: a) una fonte legale; b) del perseguimento di legittimi scopi di contrasto alla criminalità; e, soprattutto, c) nel rispetto del principio di proporzionalità⁹⁰. E proprio quest'ultimo requisito – inteso

is thus a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life".

⁸⁶ V., per tutte, C. eur., 4.12.2008, *S. and Marper c. Regno Unito*, § 67.

⁸⁷ Ciò vale, ad esempio, per quei *software* (tra cui anche alcuni tra quelli più utilizzati nel mercato italiano) che cercano di de-anonimizzare le transazioni mischiando, contemporaneamente, le transazioni con altre informazioni *off-chain* sul soggetto, ottenute da fonti come documenti giudiziari, *social media* e più in generale tramite OSINT. In tal modo, viene creata una vera e propria rete a strascico di dati, atta a ricostruire la vita privata dell'individuo.

⁸⁸ Nello stesso senso, v. anche G. Soana, *The Anti Money Laundering*, cit., 244 e C. Rueckert, *op. cit.*, 6 s.

⁸⁹ FAFT, *Virtual assets and virtual asset service providers*, ottobre 2021, 71.

⁹⁰ Pertanto, è, a questo proposito, necessario rispettare gli insegnamenti in materia di rapporto tra mezzi di ricerca della prova tecnologici e principio di proporzionalità sviluppati, negli ultimi anni, dalla Corte di giustizia. Cfr., tra le molte pronunce sul punto, C.G.U.E., 4.10.2024, *Bezirkshauptmannschaft Landeck*, C-548/21; C.G.U.E., 30.4.2024, *La Quadrature du Net*, C-470/21; C.G.U.E., 7.9.2023, *Lietuvos Respublikos generalinė prokuratūra*, C-162/22; C.G.U.E., 17.11.2022, *Spetsializirana prokuratura*, C-432/22; C.G.U.E., 20.9.2022, *VD e SR*, C-339/20 e C-397/20; C.G.U.E., 20.9.2022, *Space Net*, C-793 e 794/19; C.G.U.E., 5.4.2022, *Commissioner of An Garda Síochána e. a.*, C-140/20; C.G.U.E., 2.3.2021, *H.K. c. Prokuratuur*, C-746/18; C.G.U.E., 6.10.2020, *Privacy International*, C-623/17; C.G.U.E., 6.10.2020, *La Quadrature du Net*, C-511/18, C-512/18 e C-520/18; C.G.U.E., 2.4.2018, *Ministerio Fiscal*, C-207/16; C.G.U.E., 21.12.2016, *Tele 2 e Watson*, C-203/15 e C-698/15; C.G.U.E., 8.4.2014, *Digital Rights Ireland*, C-293/12 e C-594/12. Come noto, il punto focale di questa giurisprudenza consiste nel rilievo per cui le ingerenze gravi

nella sua duplice componente di legalità in astratto e legalità in concreto – rende inadeguate a soddisfare il livello di garanzie imposto dalla fonte sovraordinata previsioni generali come: a) l'art. 189 Cpp, in tema di prove atipiche; b) gli artt. 55, 348, o 359 Cpp, riguardanti le attività investigative delle autorità di *law enforcement*; o, ancora, c) l'art. 234-bis Cpp, concernente l'acquisizione di documenti e dati informatici⁹¹.

I problemi sollevati dai *tools* in esame non finiscono però qui.

Va, invero, segnalata una questione di “trasparenza algoritmica” che caratterizza alcuni tra gli applicativi più utilizzati nel settore. Ci si riferisce, in particolare, al fatto che, essendo molti di essi sviluppati da aziende private, le limitazioni derivanti dai diritti di proprietà intellettuale che li caratterizzano non rendono possibile conoscere nel dettaglio le “euristiche” che ne regolano in funzionamento⁹². Il che, come intuibile, incide direttamente, tanto sulla possibilità di valutarne, *cognita causa*, l'affidabilità, quanto di esercitare in modo effettivo il diritto di difesa e al contraddittorio.

Da questa prospettiva, è interessante ricordare la recente decisione adottata dalla

negli artt. 7 e 8 della Carta di Nizza, per essere proporzionate ai sensi dell'art. 52 della medesima Carta, devono essere autorizzate da un giudice o da un'autorità amministrativa indipendente, che deve essere in grado di garantire un giusto equilibrio tra i legittimi interessi in gioco. A questo riguardo, la Corte di Lussemburgo ha, del pari, chiarito che la gravità dell'ingerenza nei diritti fondamentali dipende da quanto precise siano le conclusioni rispetto alla vita privata della persona interessata che l'accesso ai dati può determinare. Da ciò ne consegue che, perlomeno nei casi in cui l'impiego dei software di *blockchain analysis* finisca, tenuto conto della mole di transazioni analizzate/stoccate e della durata cronologica di controllo su un bersaglio, per produrre l'effetto di consentire di tracciare un quadro analitico della vita finanziaria e dei rapporti sociali di una persona, dovrebbe essere assicurato il medesimo *standard* minimo di garanzie. Per altro verso, un ulteriore punto di riferimento obbligato è costituito dall'art. 20 co.2 d.lgs. 21.6.2017 n. 108, di attuazione della Direttiva 2014/41/UE, relativa all'ordine europeo di indagine penale, il quale prevede che all'acquisizione in tempo reale di flussi informatici o telematici, provenienti o diretti a banche e istituti finanziari, il procuratore della Repubblica provvede, se necessario, mediante richiesta al g.i.p. secondo quanto previsto dagli artt. 266 e ss. Cpp in materia di intercettazioni. Si potrebbe, infatti, ritenere che, data la natura finanziaria dei flussi di transazione di cripto-attività, l'impiego *live* di algoritmi di analisi della *blockchain* per tracciare le stesse nell'ambito di un'indagine penale richieda, per coerenza del sistema, la strutturazione di una disciplina equivalente.

⁹¹ Al riguardo, è utile ricordare che nella recente sentenza C.G.U.E., 4.10.2024, *Bezirkshauptmannschaft Landeck*, C-548/21, § 99 in materia di sequestro di *device*, la Corte ha stabilito che di fronte a un mezzo di ricerca della prova potenzialmente lesivo degli artt. 7 e 8 della Carta di Nizza, al fine di rispettare l'art. 52 della stessa, il legislatore nazionale è tenuto a «definire in modo sufficientemente preciso gli elementi, in particolare la natura o le categorie dei reati di cui trattasi, da prendere in considerazione». Si tratta, evidentemente, di un requisito non rispettato da nessuna delle disposizioni del codice di rito menzionate nel testo.

⁹² Il termine “euristica” è impiegato per descrivere le tecniche di raggruppamento (*clustering*) delle criptovalute. Un esempio è l'euristica del *co-spending*: essa assume che più indirizzi su *blockchain* che finanziano una singola transazione siano controllati da un unico soggetto, perché la condivisione di chiavi private tra soggetti diversi è improbabile.

United States District Court per il distretto della Columbia nel caso *Sterlingov c. USA*⁹³. In tale circostanza, l'imputato era accusato di associazione a delinquere finalizzata al riciclaggio di denaro, attraverso la gestione di un noto *mixer* di *Bitcoin*. Per lo svolgimento delle indagini l'autorità inquirente aveva impiegato uno tra i più importanti *software* privati utilizzati anche in Italia (*Chainalysis Reactor*), che aveva consentito di raggruppare e attribuire al *mixer* tutta una serie di indirizzi, transazioni e prelievi illeciti. Nonostante le censure addotte dalla difesa, volte a mettere in luce l'inaffidabilità dello strumento, definito «*unscientific and unreliable*» e a escludere, di riflesso, le evidenze così raccolte, la Corte lo ha comunque ritenuto conforme ai criteri *Daubert* e alla *Federal Rule of Evidence 702*⁹⁴.

Se ciò è vero, va osservato come neppure tale decisione sembri costituire un valido “precedente” per gli ordinamenti europei, in generale, e per quello italiano, in particolare. Si afferma un tanto, in ragione della forte valorizzazione che il principio di “trasparenza algoritmica” ha avuto, sia nell'ambito delle Carte sovranazionali volte a dettare i primi principi di fondo dell'applicazione di forme di intelligenza artificiale nell'ambito della giustizia penale⁹⁵, sia da una parte della giurisprudenza interna. È, ad esempio, utile ricordare come uno *standard* molto elevato sul punto sia stato fissato dal Consiglio di Stato, il quale ha esplicitamente sostenuto che le esigenze di trasparenza delle forme algoritmiche devono considerarsi prevalenti su quelle di riservatezza delle imprese produttrici dei meccanismi informatici utilizzati⁹⁶. E se tali principi valgono sul piano amministrativo, lo stesso non può che accadere – e a maggior ragione – anche in ambito penale, vista la maggiore posta in gioco che caratterizza questo ramo dell'ordinamento.

⁹³ Il riferimento va a *United States District Court, District of Columbia, Sterlingov c. Unites States* (2024), 9.2.2024.

⁹⁴ *Sterlingov c. Unites States*, cit.

⁹⁵ Il riferimento va, *in primis*, alla Carta etica europea sull'utilizzo dell'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi, 2018, per un commento alla quale, v. S. Quattrocolo, *Intelligenza artificiale e giustizia: nella cornice della Carta etica europea, gli spunti per un'urgente discussione tra scienze penali e informatiche*, in www.la legislazione penale.eu, 18 dicembre 2018. V. anche l'art. 8 della *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*, CM(2024)52-final. Sul piano eurounitario, v. il considerando n. 27 del Regolamento 2024/1689/UE sull'IA, ove si sottolinea l'importanza nel garantire la «trasparenza» dei sistemi algoritmici, ovvero sia il fatto che gli stessi siano «sviluppati e utilizzati in modo da consentire un'adeguata tracciabilità e spiegabilità, rendendo gli esseri umani consapevoli del fatto di comunicare o interagire con un sistema di IA e informando debitamente i *deployer* delle capacità e dei limiti di tale sistema di IA e le persone interessate dei loro diritti».

⁹⁶ Cfr. Cons. Stato, 4.2.2020, n. 881, in *OneLegale*. Sia consentito il rinvio sul punto a J. Della Torre, *Le decisioni algoritmiche all'esame del Consiglio di Stato*, in *RDP* 2021, 713 ss.

Ancora, bisogna evidenziare come i *software* in questione, in quanto impiegati per supportare le autorità di contrasto nel valutare «l'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati», sembrano rientrare nei meccanismi ad “alto rischio” di cui al combinato disposto tra l'art. 6 e l'allegato III, n. 6, lett. c) del Regolamento 2024/1689/UE⁹⁷ (c.d. Regolamento IA). Collocandosi in questa prospettiva, dunque, i *tools* di tracciamento dovrebbero essere sviluppati, sin dalla fase di progettazione, in modo che possano essere effettivamente controllati dagli operatori umani nel corso del loro impiego (art. 14 par. 1 del Regolamento AI). L'elaborazione *by design* rappresenta, a ben vedere, una scelta costituzionalmente ed eurounitariamente imposta, giacché solo in tal modo è possibile assicurare l'utilizzo di siffatte strumentazioni in maniera conforme ai diritti fondamentali della persona⁹⁸. Purtroppo, va osservato come, anche da questa prospettiva, i *software* più impiegati in commercio si dimostrino deficitari, a causa del velo di opacità che li caratterizza. Spesso, infatti, non si hanno informazioni sufficienti circa: 1) i tassi di errore che caratterizzano gli algoritmi⁹⁹; 2) il percorso di “allenamento” a cui gli *engine* vengono sottoposti; 3) i presidi volti a evitare possibili effetti discriminatori causati dalla macchina, nonché abusi dei dati personali raccolti; 4) le garanzie specifiche tese a ridurre il rischio che l'IA si comporti come una *black box*, ovvero «sistemi in cui *input* e *output* sono osservabili, mentre il funzionamento interno [del sistema] rimane oscuro persino ai suoi stessi programmatori»¹⁰⁰.

Infine, va rilevato che questi strumenti dovrebbero poter essere utilizzati anche

⁹⁷ I sistemi ad alto rischio sono definiti dal Regolamento come quelli che possono avere «un impatto nocivo significativo sulla salute, la sicurezza e i diritti fondamentali delle persone nell'Unione» (considerando n. 46). Per poter qualificare uno strumento come “ad alto rischio”, occorre che siano soddisfatte le condizioni di cui all'art. 6: «a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I; b) il prodotto, il cui componente di sicurezza a norma della lettera a è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I» – e di quelli indicati nell'Allegato III. Per una sintesi dei profili processual-penalistici del Regolamento, cfr. S. Quattrocchio, *Intelligenza artificiale e processo penale: le novità dell'AI Act*, in www.dirittodidifesa.eu, 16.1.2025; M. Torre, *Il Regolamento europeo sull'intelligenza artificiale: i profili processuali*, in *PPG* 2024, 1534 ss.

⁹⁸ Cfr., per più ampie considerazioni sul punto, B.J. Koops, J.H. Hoepman, R. Leenes, *Open-source intelligence and privacy by design*, in *Computer Law & Security Review* 2013, 676 ss.

⁹⁹ Proprio un problema di questo tipo era stato denunciato dalla difesa nel già citato caso *Sterlingov c. Unites States*, cit. nei confronti del *software Chainalysis Reactor*.

¹⁰⁰ La citazione è tratta da G. Contissa, G. Lasagni, G. Sartor, *Quando a decidere in materia penale sono (anche) algoritmi e IA: alla ricerca di un rimedio effettivo*, in *Dir. di internet* 2019, 620.

dalla difesa per realizzare un controllo *ex post* sui dati raccolti dall'accusa, oppure per sostenere una propria ipotesi alternativa. Da questa prospettiva, il principio di parità delle parti e il diritto al contraddittorio sembrano, infatti, ostare a un utilizzo degli strumenti in questione in un'ottica unicamente "a carico", spingendo, per converso, per un loro possibile impiego anche in favore del prevenuto. Il che, visti i costi notevoli che hanno i più avanzati tra questi *software*, richiederebbe che la difesa possa quantomeno ottenere che un proprio consulente sia messo nelle condizioni di utilizzare gli strumenti a disposizione dell'autorità. Nulla di tutto ciò, è, peraltro, previsto, né a livello sovranazionale, né nel codice di rito.

L'insieme di queste considerazioni ci porta a ritenere che, in assenza di una normativa che ne disciplini nel dettaglio i casi e i modi di utilizzo, l'impiego di *software* automatizzati di *blockchain analysis* dovrebbe, a rigore, considerarsi inibito nel nostro ordinamento processuale penale, data la compressione – non adeguatamente bilanciata da un vaglio di proporzionalità in astratto e in concreto – che gli stessi determinano su plurimi diritti fondamentali della persona. Con la conseguenza che dovrebbe essere vietata l'acquisizione dei loro risultati e/o utilizzazione nel procedimento. E ciò, in primo luogo, sulla base del "combinato disposto" tra artt. 189 e 191 Cpp: al riguardo, pare, invero, da condividere la tesi di chi ritiene che dall'art. 189 si ricavi un divieto probatorio implicito nei confronti di elementi probatori non disciplinati dalla legge acquisiti in spregio alle garanzie primarie dell'uomo, la cui violazione è causa di inutilizzabilità patologica¹⁰¹.

Un'interpretazione di questo tipo pare imposta, a maggior ragione, in virtù dei problemi di trasparenza sopra segnalati, i quali impediscono alla difesa di avere un contraddittorio effettivo sull'affidabilità e sul funzionamento di tali strumenti. Come affermato da attenta dottrina, in un'evenienza di questo tipo, infatti, onde salvaguardare i pilastri del *fair trial*, nelle sue articolazioni del contraddittorio e della parità delle armi, è necessario agire a monte direttamente sul piano dell'ammissibilità probatoria, rispetto a quello della valutazione, prevedendo che «*the court should exclude the "black box evidence" from the adjudication on the defendant's guilt*»¹⁰².

¹⁰¹ In tal senso, v. C. Conti, *Accertamento del fatto e inutilizzabilità nel processo penale*, Padova 2007, 173; P. Tonini, C. Conti, *Il diritto delle prove penali*, Milano 2014, 105. *Contra*, invece, M. Daniele, *Indagini informatiche lesive della riservatezza. Verso un'inutilizzabilità convenzionale?*, in *CP* 2013, 370.

¹⁰² Testualmente, S. Quattrocolo, *Artificial Intelligence, Computational Modelling and Criminal Proceedings. A Framework for A European Legal Discussion*, Cham 2020, 96, nonché M. Gialuz e S. Quattrocolo, *Predictive justice in Italy*, in *Revue Internationale de Droit Pénal* 2023, 205. V. anche L. Lupária Donati e G. Fiorelli, *Diritto*

Al proposito, non va, infine, tralasciato come, nonostante la nota ritrosia delle istituzioni sovranazionali a imporre regole circa l'ammissibilità e la valutazione delle prove¹⁰³, questa conclusione trovi supporto anche nella giurisprudenza della Corte di giustizia. E ciò in quanto i giudici del Lussemburgo hanno negli ultimi anni messo in rilievo, in un numero via via più ampio di sentenze, la necessità di escludere informazioni ed elementi di prova¹⁰⁴, ottenuti in violazione degli artt. 7, 8, 47 e 48 della Carta di Nizza, laddove vi sia il rischio che l'ammissibilità degli stessi impedisca alla difesa «di svolgere efficacemente le proprie osservazioni in merito a un mezzo di prova rientrante in una materia estranea alla conoscenza dei giudici e idoneo ad influire in modo preponderante sulla valutazione dei fatti»¹⁰⁵. Ebbene, dati i gravi problemi di opacità che affliggono molti *software* di *blockchain analysis*, è difficile negare che si ricorra proprio in una situazione di questo tipo, la quale impone l'esclusione del mezzo di prova al fine di evitare una violazione siffatta.

Se questa soluzione è imposta dal doveroso rispetto delle garanzie della persona, va, tuttavia, ammesso come la stessa non sia affatto a costo zero per l'ordinamento. E ciò, in quanto, come abbiamo avuto modo di osservare, i *tools* in questione sono assolutamente indispensabili per un efficiente contrasto alla criminalità. Alla luce di un tanto, non stupisce che, nella prassi, gli investigatori, pur di non privarsi di tali mezzi, siano soliti utilizzare un *escamotage*: essi continuano a impiegarli, ma solo come “spunti investigativi”, che vengono poi riscontrati tramite atti di indagine tradizionali, validamente utilizzabili in fase procedimentale e processuale. Non sfuggirà che l'operazione da ultimo descritta, pur riducendo l'impatto negativo della tecnologia in esame sui diritti fondamentali, fa comunque pagare ai singoli prevenuti la criticabile inerzia del legislatore in questa materia¹⁰⁶.

probatorio e giudizi criminali ai tempi dell'Intelligenza Artificiale, in *DPenCont – Riv. Trim.* 2022, 2, 43.

¹⁰³ Cfr., *amplius*, A. Cabiale, *I limiti alla prova nella procedura penale europea*, Milano 2019.

¹⁰⁴ Cfr., al riguardo, tra le tante, C.G.U.E., 5.9.2024, *M.S.*, C-603/22, § 172; C.G.U.E., 14.5.2024, *Stachev*, C-15/24; C.G.U.E., 30.4.2024, *M.N.*, C-670/22, § 131; C.G.U.E., 2.3.2021, *H.K.*, C-746/18, par. 44; C.G.U.E., 6.10.2020, *La Quadrature du Net e a.*, C-511/18, C-512/18 e C-520/18, cit., § 226.

¹⁰⁵ La citazione è tratta da C.G.U.E., 6.10.2020, *La Quadrature du Net e a.*, C-511/18, C-512/18 e C-520/18, cit., § 226.

¹⁰⁶ Difatti, spesso l'intera catena probatoria e indiziaria trova origine proprio nell'impiego – non regolato – di tali applicativi. Purtroppo, non essendo stata accolta dalla giurisprudenza italiana la teoria dei “frutti degli alberi avvelenati”, ma quella del *male captum bene retentum*, questo vizio originario è, attualmente, privo di un rimedio effettivo. Per una recente analisi critica del tema, cfr. F.R. Dinacci, *L'inutilizzabilità e il male captum bene retentum: vecchie superstizioni e nuove consapevolezze*, in *Arch. pen. (web)*, 2023, 2.

6. Come si è avuto modo di anticipare, la struttura decentralizzata della rete *blockchain* assume particolare importanza pure con riguardo alla procedura di ablazione avente ad oggetto le cripto-attività. Infatti, se, con riguardo alla “moneta analogica”, gli investigatori possono ricercare e sequestrare documenti e conti bancari con relativa agilità rivolgendosi agli istituti di credito, per quanto concerne gli *asset* digitali in esame, la possibile mancanza di un *service provider* che funga da intermediario e la loro estrema volatilità, rende infruttuose siffatte modalità operative classiche¹⁰⁷.

A fronte di ciò, si comprende la ragione per cui varie organizzazioni internazionali – come il GAFILAT, l’INTERPOL, l’OSCE e il Consiglio d’Europa¹⁰⁸ – abbiano emanato *guidelines* specifiche in materia, al fine di supportare le autorità di *law enforcement* nello sviluppo di un’efficace attività tesa all’ablazione reale delle criptomonete legate a operazioni illecite. Proprio in quest’ottica si spiega il perché, nell’ambito del Fondo Monetario Internazionale, si sia finanche affermato che il fenomeno in esame «*require adjusting some legal requirements and practices (e.g., freezing/seizing orders to be issued by a court)*», onde consentire di realizzare un’attività di prevenzione e di repressione efficiente¹⁰⁹.

Come abbiamo avuto modo di anticipare, anche l’Unione europea ha cominciato a interessarsi della materia, attraverso l’approvazione della Direttiva 2024/1260/UE. Tale provvedimento, infatti, menziona esplicitamente le cripto-attività tra i beni che possono essere sottoposti a sequestro e confisca nell’ambito di un procedimento penale¹¹⁰. Per di più, va segnalato che, proprio perché il legislatore eurounitario, rendendosi conto del grande rischio di dissipazione che concerne tali *asset*, li ha ricompresi tra quelli che dovrebbero poter essere “appresi” tramite “azioni immediate” degli Uffici per il recupero dei beni, istituiti per agevolare la cooperazione

¹⁰⁷ C. Rueckert, *op. cit.*, 4.

¹⁰⁸ Cfr., ad es., Council of Europe and European Union, *Guidelines for the management of seized assets*, 2023; Interpol, *Guidelines for the Seizure and Sale of Virtual Assets*; Cybercrime Programme Office of the Council of Europe, *Guide on seizing cryptocurrencies*, 2021; Financial Action Task Force of Latin America, *Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Assets*, 2021; iPROCEEDS-2, *Guide on seizing cryptocurrencies*, 2021.

¹⁰⁹ Così si esprime, testualmente, il report del Fondo Monetario Internazionale, redatto da N. Schwarz (e altri), *Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations*, in *FinTech Notes* No 2021/002.

¹¹⁰ Considerando n. 12 e art. 3, co.1, par. 1, n. 2.

transfrontaliera in relazione alle indagini per il reperimento dei beni¹¹¹. Se un tanto è vero, va, tuttavia, messo in rilievo che la Direttiva in questione presenta ancora il vistoso limite di non contemplare una procedura ablatoria *ad hoc* per le cripto-attività, andando, dunque, estese alle stesse le fattispecie generali ivi regolate¹¹². Dal che ne consegue come gli Stati membri godano ancora di grande discrezionalità nel valutare come adattare le proprie forme di sequestro e confisca al contesto in esame.

Ciò nondimeno, va osservato che diversi ordinamenti non sono comunque rimasti inerti, ma hanno già adottato linee guida specifiche, se non veri e propri *corpus* normativi organici sul punto.

Dalla prima prospettiva, possono menzionarsi, a mero titolo esemplificativo, le *guidelines* elaborate dal *Ministerio Público Fiscal de la Nación* in Spagna¹¹³ e dalla Procura generale slovena¹¹⁴, nelle quali sono stati cristallizzati una serie di principi e di buone prassi da seguire nel corso delle procedure ablative aventi ad oggetto valute virtuali¹¹⁵. Pur trattandosi di atti non aventi carattere vincolante (*soft law*), essi presentano indubbiamente il pregio di individuare *standard* uniformi applicabili su tutto il territorio nazionale.

Sul secondo versante, merita menzionare, in particolare, la ricca regolamentazione implementata in materia dal Regno Unito. Ci si riferisce alla Sezione 180-Allegato 9 dell'*Economic Crime and Corporate Transparency Act 2023*¹¹⁶, la quale ha introdotto disposizioni *ad hoc* all'interno del *Proceeds of Crime Act 2002* (POCA), con l'intento di disciplinare analiticamente «*searches, seizure and detention of cryptoassets*»¹¹⁷. Si tratta di un provvedimento al quale occorre guardare con vivo interesse, atteso che rappresenta uno dei primi tentativi su scala globale di fornire un quadro normativo

¹¹¹ In Italia, tali uffici già sono istituiti presso il Servizio per la Cooperazione Internazionale di Polizia, strutturalmente incardinato presso il Ministero dell'Interno.

¹¹² In questo senso, v. anche A. Del Giudice, *op. cit.*, 1022.

¹¹³ Cfr. Ministerio Público Fiscal de la Nación, *Guía práctica para la identificación, trazabilidad e incautación de criptoactivos. Consideraciones teórico-prácticas sobre activos virtuales basados en la tecnología de cadena de bloques y su investigación penal*, 2023.

¹¹⁴ V. State Prosecutor General of the Republic of Slovenia, *Ktrzb-9/11/2019/AF-nf*.

¹¹⁵ Cfr., ad esempio, Indiana State Police, *Seizure of Cryptocurrency and Virtual Currencies*, 2018; CyberSecurity Malaysia, *Policy and procedure for seizing cryptocurrencies*; Regional Organized Crime Information Center, *Bitcoin and Cryptocurrencies: Law Enforcement Investigative Guide*.

¹¹⁶ Il testo del provvedimento è reperibile al seguente link: <https://bills.parliament.uk/bills/3339>.

¹¹⁷ L'espressione *cryptoasset* è definita come «*a cryptographically secured digital representation of value or contractual rights that uses a form of distributed ledger technology and can be transferred, stored or traded electronically*».

organico di tale complessa materia.

Il primo dato da prendere in considerazione è che la riforma in esame è intervenuta, tanto sulle misure ablatorie di matrice strettamente penalistica, regolate dalle parti 2, 3 e 4 del *POCA*, quanto sulle azioni ablatorie di matrice civilistica (o azioni *in rem*), regolate nella parte 5 del *POCA*, che non richiedono una condanna del prevenuto, attraverso cui in tale ordinamento è possibile ordinare l'immediato spossessamento di beni che si ritiene siano stati ottenuti attraverso una condotta illecita (o destinati a un tale scopo).

Sul piano penalistico, le modifiche principali apportate sono sostanzialmente tre.

In primo luogo, è stato rimosso il requisito che una persona sia stata arrestata prima di poter utilizzare i poteri di sequestro. Questa modifica si applica a tutti i beni, ma è stata ritenuta particolarmente utile nel contesto dei *crypto-asset*.

In secondo luogo, in conformità alle più avanzate *guidelines* sviluppatesi a livello sovranazionale, sono state introdotte disposizioni atte a modificare i poteri di perquisizione, sequestro e custodia, in modo tale da rendere esplicitamente chiaro il potere della autorità di *law enforcement* di “ricreare” portafogli di criptovalute e trasferire i beni in un portafoglio controllato dalle forze dell'ordine (c.d. *Government-controlled wallet*).

In terzo luogo, si è attribuito alle *Magistrates' Court* (come autorità responsabili per l'esecuzione degli ordini di confisca) il potere di autorizzare la vendita di qualsiasi *crypto-asset*, nello stesso modo in cui esse potevano già farlo con i contanti, oppure i fondi detenuti in conti bancari.

Con riguardo alle *civil forfeiture*, è stato introdotto un intero sottoinsieme di poteri ablatori specifici, finalizzati a consentire all'autorità di recuperare le cripto-attività di sospetta origine illecita il più rapidamente possibile. Per quanto qui rileva, l'*Economic Crime and Corporate Transparency Act 2023*, si compone di quattro capitoli, idealmente rappresentativi dei diversi momenti che caratterizzano il complesso *iter* ablativo.

Il primo (3C) è dedicato alla fase del «*seizure and detention of cryptoassets*». Si stabilisce, al riguardo, che un *enforcement officer* può ricercare un qualunque oggetto collegato alle criptovalute – denominato «*cryptoasset-related item*»¹¹⁸ – a condizione

¹¹⁸ A tali fini, la locuzione «*cryptoasset-related item*» è intesa in senso ampio, ossia come qualsiasi bene che contiene o può dare accesso a informazioni potenzialmente utili per un eventuale sequestro. Si pensi, ad esempio, a pezzi di carta in cui sono state scritte le *password* per accedere al *wallet*, a varie tipologie di *hardware*

che vi siano «*reasonable grounds*» per sospettare che in un determinato luogo si trovino uno o più beni connessi ad attività illecite. Una volta rinvenute eventuali cripto-attività, l'autorità è legittimata a sequestrarle, laddove vi siano ragionevoli motivi per ritenere che tali *asset* siano di provenienza delittuosa o siano a ciò destinati. Più in particolare, il provvedimento stabilisce, anche in questo caso, che venga operato un trasferimento delle criptomonete «*into a crypto wallet controlled by the enforcement officer*», al fine di garantire l'effettivo spossessamento della *res*.

Il Capitolo 3D della legge attribuisce poi poteri ulteriori agli ufficiali di polizia, legittimandoli a richiedere un ordine di congelamento («*crypto wallet freezing order*») delle criptovalute detenute in portafogli crittografici gestiti da un «*UK-connected cryptoasset service provider*»¹¹⁹, laddove vi siano ragionevoli motivi per sospettare che ivi siano presenti beni destinati all'uso in condotte illecite¹²⁰.

Una volta concluso l'*iter* di spossessamento, il Capitolo 3E, intitolato «*forfeiture of cryptoassets following detention or freezing order*», consente all'autorità giudiziaria di ordinare la confisca civilistica di alcuni o di tutti i *crypto-asset* detenuti in conformità a un ordine di sequestro (Capitolo 3C) o di congelamento (Capitolo 3D).

L'ultimo passaggio della procedura è disciplinato dal Capitolo 3F, il quale regola la delicata questione relativa alla conversione dei *crypto-assets*. Attesa l'estrema volatilità di tali beni, si stabilisce che l'*enforcement officer* o la persona a cui sono stati sequestrati i cripto-valori possano richiedere al giudice competente di emettere un'ordinanza che imponga la loro conversione in valuta FIAT. A fronte della richiesta, è prevista l'instaurazione di una fase in contraddittorio, che coinvolge tutti i soggetti interessati, all'esito della quale il magistrato adotterà la propria decisione basandosi sulla probabilità che i beni (nel loro complesso) possano subire una significativa perdita di valore durante il periodo che precede il rilascio o la confisca¹²¹.

memory sticks utilizzate per memorizzare una chiave privata o, ancora, a *smartphone* contenenti applicazioni che forniscono all'utente il controllo su un portafoglio di criptovalute.

¹¹⁹ La disposizione prevede che all'interno di tale categoria debbano essere incluse tutte quelle entità che: a) hanno una sede legale nel Regno Unito e le loro attività quotidiane sono svolte da tale ufficio o da un'altra sede nel Regno Unito; b) hanno termini e condizioni con le persone a cui forniscono servizi che prevedono che una controversia legale possa essere dibattuta nei tribunali del Regno Unito; c) conservano nel Regno Unito i dati relativi alle persone a cui forniscono servizi.

¹²⁰ Merita di essere sottolineato che la legge non individua una soglia minima per gli ordini di congelamento del portafoglio crittografico.

¹²¹ Occorre ricordare come la disciplina in questione sia ispirata dal principio generale per cui la conversione delle valute deve avvenire «*in the manner best calculated to maximise the amount of money obtained for the cryptoassets*».

7. Purtroppo, va rilevato che il panorama italiano risulta molto diverso rispetto a quello appena descritto. Anche a questo proposito il legislatore interno ha, infatti, manifestato un atteggiamento di completa apatia. Né all'interno del codice di rito, né in alcuna legge speciale, è dato rinvenire una disciplina specifica in punto di misure ablatorie che interessino le cripto-attività. Si tratta di una situazione che merita di essere stigmatizzata, specie in ragione del fatto che la procedura volta al sequestro di questa categoria di beni è caratterizzata, come già anticipato, da molteplici rischi, attesa la loro natura immateriale e volatile.

Dal punto di vista teorico, vi è, anzitutto, la necessità di distinguere a seconda della tipologia di *wallet* che si voglia apprendere¹²².

Si consideri, in primo luogo, il caso di un *custodian wallet*, con riguardo al quale è necessario effettuare una richiesta di sequestro a un *service provider* per chiedere e ottenere il congelamento di somme di cripto-attività già individuate. Da questa prospettiva, invero, i tempi, spesso tutt'altro che brevi, necessari per ottenere una risposta a un ordine rivolto a un prestatore di servizio di cripto-attività, specie se collocato all'estero, rischiano di risultare incompatibili con l'estrema rapidità necessaria per sequestrare i beni in esame.

Nell'ipotesi di un portafoglio gestito in autonomia dall'utente (c.d. *self-hosted*) invece, le operazioni sono più complesse. Laddove, la chiave privata sia rappresentata su un bene fisico (si pensi, ad esempio, a un foglio di carta o a un diario), è necessario anzitutto riconoscerla e, in secondo luogo, sequestrarla. Per contro, nel caso in cui essa sia conservata all'interno di un *device* digitale, la sua apprensione presuppone la conoscenza del *pin* di sblocco del dispositivo. Ciò, tuttavia, il più delle volte impone di ottenere la collaborazione dell'indagato (o di un terzo possessore del *device*), atteso che l'eventuale forzatura del dispositivo da parte delle forze dell'ordine – nel tentativo di indovinare la *password* – potrebbe cagionare la perdita definitiva di tutti i dati ivi contenuti¹²³. Si pone, da questa prospettiva, il tema, più ampio, della rilevanza assunta dal diritto al silenzio e dal diritto contro l'autoincriminazione, a fronte di una richiesta di consegna della *password* da parte dell'autorità inquirente. A differenza della scelta compiuta in altri ordinamenti, tra cui proprio il Regno Unito, che si sono spinti così in

¹²² Per approfondimenti, v. P. Dal Checco, *op. cit.*, 336-340.

¹²³ Si parla della cd. funzionalità *wipe*. Nel caso di *Ledger*, ad esempio, il sistema si resetta dopo tre tentativi falliti di inserimento del *pin*.

là da concepire finanche degli obblighi penalmente sanzionati per coloro che non forniscano all'autorità informazioni utili a sbloccare il dispositivo¹²⁴, il legislatore italiano si è finora del tutto disinteressato della questione, omettendo di fornire qualsivoglia indicazione, anche solo di matrice processuale, al riguardo¹²⁵. Il che, peraltro, non stupisce data la criticabile lacuna che ancora oggi affligge il sistema processuale penale nostrano con riguardo alla più generale tematica del sequestro dei *device* digitali¹²⁶; lacuna che, come è facile intuire, è foriera di significativi problemi pratici nel contesto in esame, proprio per l'importanza che gli applicativi informatici rivestono nel settore *de quo*.

Un'ulteriore tematica sulla quale occorre interrogarsi riguarda la possibilità di impiegare il captatore informatico quale mezzo di ricerca della prova occulto, al fine apprendere il *pin* di un dispositivo contenente la chiave privata di accesso al *wallet*, o finanche indirettamente quest'ultima. Mediante l'impiego della funzionalità cd. *keylogger*, il *malware* – controllato in remoto dalle forze dell'ordine – consente, invero, teoricamente di acquisire in tempo reale tutto ciò che viene digitato sulla tastiera di un *device*¹²⁷ e, dunque pure una *password*. Tuttavia, come noto, il legislatore italiano ha disciplinato l'utilizzo del *trojan horse* solamente come peculiare modalità di intercettazione¹²⁸. Non è stato regolamentato, invece, un impiego diverso, come il caso della modalità *online surveillance*, *online search* o, per l'appunto, della *keylogger function*. A fronte di ciò, occorre chiedersi se il semplice gesto di digitare una parola sul proprio *smartphone* o *computer* integri un vero e proprio comportamento

¹²⁴ Nella circolare 004/2024: *Economic Crime and Corporate Transparency Act – cryptoasset confiscation order provisions*, 26.4.2024, attuativa della riforma del 2023, si precisa, infatti, che «*appropriate officers have the power to require a person to provide information which is stored in electronic form*», e che «*if a person fails to comply with a requirement, then they may have committed an obstruction offence*». Va, a ogni modo, precisato che, in virtù della nozione ampia del diritto al silenzio e di non collaborare sviluppata dalla Consulta (cfr., da ultimo, C. cost., 5.6.2023, n. 111), nel nostro ordinamento disposizioni di questo tenore si esporrebbero a inevitabili censure di legittimità costituzionale, per violazione del diritto di difesa.

¹²⁵ Cfr., sul punto, A. Mangiaracina, *Nuove fisionomie del diritto al silenzio. Un'occasione per riflettere sui vuoti domestici... e non solo*, in *PPG* 2021, 729 ss.

¹²⁶ Si veda, al riguardo, il recente d.d.l. S 19.7.2023 n. 806 recante «Modifiche al codice di procedura penale in materia di sequestro di dispositivi, sistemi informatici o telematici o memorie digitali», volto a introdurre nel codice di rito un nuovo art. 254-ter.

¹²⁷ Cfr. M. Griffo, *Il captatore informatico e la filosofia del doppio binario*, Napoli 2019, 200 ss.; W. Nocerino, *Il captatore informatico nelle indagini interne e transfrontaliere*, Milano 2021, 182.

¹²⁸ Si vedano, in proposito, M. Miraglia, *Il "Trojan (non) di Stato": una disciplina da completare*, in *PPG* 2023, 1227 ss. e W. Nocerino, *op. cit.*, 141 ss., a cui si rinvia anche per i cospicui riferimenti dottrinali e giurisprudenziali citati.

comunicativo. In caso di risposta positiva, si potrebbe sostenere che il *pin* del dispositivo o finanche la chiave privata di un *wallet* ben potrebbero essere oggetto di intercettazione mediante *trojan* ai sensi dell'art. 266-bis Cpp. Diversamente, l'utilizzo del *virus*, provocando un'ingerenza nel domicilio informatico tutelato all'art. 14 Cost.¹²⁹, dovrebbe ritenersi precluso, in base al principio per cui nel corso delle indagini penali tutto ciò che non è espressamente consentito dalla legge deve ritenersi vietato, perlomeno qualora il mezzo di ricerca della prova incida sui diritti fondamentali della persona¹³⁰.

Il tema è complesso, poiché la nozione di comunicazione, specialmente nell'era digitale, è assai controversa. Al riguardo, la giurisprudenza di legittimità, pur non avendo ancora assunto una posizione esplicita su questo specifico profilo, sembra offrire argomentazioni a favore della prima prospettazione or ora richiamata. In una recente pronuncia, infatti, la Corte di cassazione ha affermato che il comportamento consistente nella redazione di un *file Excel* sul proprio *computer*, «pur non costituendo una “comunicazione” in senso stretto, costituisce certamente, invece, un comportamento cd. comunicativo, del quale è ammessa la captazione [mediante *trojan*]»¹³¹. La conclusione è stata giustificata in ragione del fatto che la semplice composizione di una parola sulla tastiera di un *electronic device* dovrebbe qualificarsi come un flusso unidirezionale di dati che transitano all'interno di un unico dispositivo. In altre parole, i giudici di legittimità sembrano identificare una condotta comunicativa nel “dialogo” che verrebbe a instaurarsi tra l'utente (*rectius*, la tastiera del *computer*) e il sistema informatico centralizzato (il *software*). Se si seguisse questa interpretazione – con riguardo alla quale, però, la dottrina ha giustamente manifestato numerose perplessità¹³² – dovrebbe ritenersi ammissibile l'apprensione attraverso l'impiego del *malware* della chiave di accesso digitata sulla tastiera del *device* in uso al titolare del *wallet*.

Ma non è tutto. Ulteriori problemi si manifestano pure quando l'autorità inquirente

¹²⁹ Sull'esigenza di estendere la copertura dell'art. 14 Cost. anche al “domicilio informatico”, v., da ultimo, le condivisibili considerazioni di M. Miraglia, *op. cit.*, 1227 ss.

¹³⁰ In questi termini, v. O. Mazza, *I diritti fondamentali dell'individuo come limite della prova nella fase di ricerca e in sede di assunzione*, in *DPenCont. – Riv. Trim.* 2013, 4 ss.

¹³¹ Cfr. Cass. 1.2.2021 n. 3591, in *OneLegale*.

¹³² Si vedano, al riguardo, le osservazioni critiche mosse da L. Algeri, *Lo screenshot eseguito (senza garanzie?) dal Trojan di Stato*, in *GI* 2022, 2780 ss.; A. Malacarne, *Il trojan horse “a cavallo” tra perquisizione ed intercettazione: il problema del cd. screenshot di file multimediali*, in *Dir. di internet* 2022, 592 ss.; A. Procaccino, *Piccoli equivoci senza importanza: tra intercettazioni di flussi informatici, perquisizioni e prove atipiche*, in *CP* 2022, 3112 ss.

sia riuscita a ottenere la chiave privata. L'indagato – o un suo complice – potrebbe aver copiato e archiviato (in formato digitale o cartaceo) la *password*, ovvero comunque averne la disponibilità da remoto, potendo così accedere al *wallet* e trasferire le criptovalute ivi presente altrove¹³³. Inoltre, l'utilizzo del cd. *backup recovery seed*¹³⁴, consentendo di recuperare in ogni momento il controllo delle somme legate a un *wallet*, a sua volta potrebbe permettere di eludere il vincolo reale imposto sul bene¹³⁵. Quel che si vuole dire, è, in altre parole, che neppure l'ottenimento da parte degli investigatori della chiave di accesso garantisce l'ablazione definitiva della *res* e, dunque, non è sufficiente per eseguire un sequestro "a regola d'arte"¹³⁶.

La migliore soluzione al problema appena esposto è quella di trasferire i fondi su un altro *wallet*, controllato direttamente dallo Stato. Si tratta, in effetti, della procedura prospettata nelle principali linee guida adottate in numerosi ordinamenti e dai più autorevoli organismi a livello internazionale¹³⁷, nonché, come si è accennato in precedenza, adottata dal legislatore britannico nell'*Economic Crime and Corporate Transparency Act 2023*. Epperò, anche in questo caso in Italia non è rintracciabile alcuna fonte di rango primario (e neppure secondario) che disciplini in maniera dettagliata l'*iter* procedimentale da seguire in dette circostanze. Di conseguenza, la scelta circa le modalità operative del sequestro è rimessa alla prassi, che si sta effettivamente sviluppando in modi affatto uniformi a seconda della singola autorità di contrasto chiamata ad operare, con buona pace del principio di legalità processuale (art. 111, comma 1, Cost.)¹³⁸.

Ma anche laddove l'autorità inquirente riuscisse a eseguire lo spossessamento della *res*, l'estrema fluttuazione del valore delle criptomonete rende elevato il rischio di un loro improvviso deprezzamento. Il che risulta un problema di non poco conto, laddove vada eseguito un sequestro di tipo preventivo e conservativo¹³⁹. Senza contare che si

¹³³ Cfr. F. Cajani, *op. cit.*, 742, nt. 45; G. Costabile, *op. cit.*, 127.

¹³⁴ Si tratta di una sequenza di parole di *backup*, che serve all'utente per ripristinare l'accesso a un portafoglio.

¹³⁵ Cfr. D. King, P. Warrack, *Real considerations for law enforcement in seizing virtual currency*, 26.6.2016, all'indirizzo <https://www.acamstoday.org/real-considerations-for-law-enforcement-in-seizing-virtual-currency/>.

¹³⁶ V., al riguardo, P. Dal Checco, *op. cit.*, 329.

¹³⁷ Cfr. *supra* nt. 108.

¹³⁸ Un problema delicato è, ad esempio, come garantire la sicurezza delle cripto-attività apprese anche da eventuali attacchi di agenti infedeli (problema che si è posto negli USA già nel caso *Silk Road*). Onde risolvere tale questione, alcune forze di polizia hanno sviluppato la buona prassi non solo di videoregistrare le operazioni, ma anche di utilizzare *wallet* a firma multipla per poter spostare le cripto-attività, così da richiedere l'intervento di più soggetti contemporaneamente.

¹³⁹ ...atteso che, in detti casi, ciò che interessa è il "valore" equivalente del bene (*rectius*, la moneta virtuale)

potrebbero porre spinose questioni in proposito in tutti i casi in cui la legge impone la restituzione del bene oggetto di sequestro¹⁴⁰.

Per far fronte alla volatilità delle criptomonete, le buone prassi di molti Stati europei consigliano, dopo aver trasferito, come detto, le monete virtuali in un *wallet* intestato alla procura o al tribunale, di convertirle in moneta FIAT, attraverso la vendita delle stesse nel mercato¹⁴¹. Questa procedura presenta un triplice vantaggio: i) risolve alla radice il problema di un deprezzamento del suo valore nel caso in cui debba poi essere restituita; ii) evita il rischio che i *wallet* impiegati per custodire le criptomonete nel corso del procedimento siano oggetto di attacchi *cyber*, con conseguente perdita del denaro virtuale¹⁴²; iii) consente, una volta operata la conversione, di intestare la moneta FIAT al Fondo Unico Giustizia¹⁴³.

Tuttavia, in assenza di una normativa *ad hoc*, è necessario chiedersi, *de iure condendo*, quale procedura debba essere seguita per la vendita e la conversione delle criptomonete.

Duplici sono, allo stato dell'arte, le opzioni astrattamente percorribili.

Si potrebbe, per un verso, ritenere applicabile l'art. 104-*bis* disp. att. Cpp, il quale, come noto, stabilisce che nel caso in cui il sequestro preventivo¹⁴⁴ o la confisca abbiano a oggetto «beni» esclusi da quelli destinati a confluire nel Fondo Unico Giustizia, di cui è necessario assicurare l'amministrazione, l'autorità giudiziaria debba nominare un custode giudiziario o un amministratore, a cui affidare il compito della conversione, specie in caso di repentine fluttuazioni del mercato. Muovendosi in queste coordinate, sarebbe possibile ipotizzare di affidare a un terzo il potere di convertire, su richiesta, la moneta virtuale in valuta avente corso legale, nel caso in cui venisse ravvisato il pericolo di un imminente e brusco deprezzamento del bene.

oggetto di apprensione. Nell'ipotesi del sequestro ex artt. 253 ss. Cpp, invece, non sembrano profilarsi problemi di sorta, fino all'eventuale fase della confisca, atteso che tale mezzo di ricerca della prova è finalizzato a vincolare non il "valore" della cosa, ma la cosa in sé: cfr. R. Lupo, *op. cit.*, 52.

¹⁴⁰ Al riguardo, infatti, occorre stabilire, ad esempio, quale sia il valore oggetto di restituzione, ossia quello originario ovvero quello corrente, nonché individuare il soggetto chiamato eventualmente a rispondere per il deprezzamento subito dal bene.

¹⁴¹ P. Dal Checco, *op. cit.*, 344; F. Cajani, *op. cit.*, 743.

¹⁴² Cfr. E. Valente, M. Torre, *La regolamentazione delle "criptovalute": condotte illecite e strategie di contrasto*, in *Riv. di diritto privato* 2019, 571; G. Costabile, *op. cit.*, 128.

¹⁴³ Si tratta di un profilo operativo di importanza chiave, dal momento che, a oggi, le cripto-attività non possono, in quanto tali, essere intestate al FUG.

¹⁴⁴ La norma si riferisce esplicitamente solo al sequestro preventivo, ma è pacifico che il suo raggio di applicazione possa estendersi anche al sequestro probatorio: in questi termini, v. pure F. Cajani, *op. cit.*, 743, nt. 50.

Un'altra soluzione prospettabile è quella di applicare, in via analogica, la regolamentazione prevista all'art. 260, comma 3, Cpp relativa ai beni deperibili¹⁴⁵. La disposizione prevede che, qualora le cose oggetto di sequestro¹⁴⁶ possano alterarsi – cioè, siano soggette a modificazione sostanziale o strutturale –, l'autorità giudiziaria debba disporre l'alienazione o la distruzione¹⁴⁷. A tal proposito, non v'è dubbio che le cripto-attività, pur non rappresentando, secondo alcuni, delle vere e proprie monete¹⁴⁸, debbano essere classificate come "beni", potendo dunque essere ricomprese nella sfera applicativa della disposizione. Così come non sembra potersi discutere la loro natura altamente volatile. Per di più, giova osservare come la giurisprudenza di legittimità abbia affermato che il concetto di deterioramento cui si riferisce la disposizione debba essere interpretato in senso ampio ed estensivo, potendo ricomprendere sia il caso di un deterioramento fisico del bene, sia un deprezzamento¹⁴⁹.

Entrambe le esegesi qui proposte, tuttavia, rappresentano una soluzione di compromesso, lasciando aperte diverse questioni di ordine pratico¹⁵⁰.

A fronte di un fenomeno così dirompente, le vigenti disposizioni codicistiche, quali quelle in tema di sequestro, si rivelano, in definitiva, del tutto inadeguate, richiedendo plurimi adattamenti su profili di rilievo cruciale. Il che, peraltro, non può stupire dal momento che esse sono state concepite per un contesto del tutto diverso rispetto all'ambiente iper-dinamico, nel quale vengono oggi scambiati gli *asset* virtuali.

8. A fronte di quanto osservato nel corso del presente lavoro, ci si sarà resi ben conto di come il tema del rapporto tra criminalità, giustizia penale e criptovalute debba, necessariamente, rappresentare una tematica prioritaria per il legislatore italiano. Si

¹⁴⁵ Cfr. R. Lupo, *op. cit.*, 53.

¹⁴⁶ Benché la disposizione richiami solamente il sequestro probatorio, la giurisprudenza ne ha esteso l'ambito di operatività pure al sequestro preventivo: Cass. 12.9.2018 n. 53341, in *OneLegale*.

¹⁴⁷ Al riguardo, la Cassazione ha stabilito che «la decisione dell'autorità giudiziaria di distruggere la cosa non ha natura di accertamento tecnico non ripetibile, suscettibile di applicazione delle modalità previste dall'art. 360». Si tratterebbe – secondo questa impostazione –, di «un "semplice adempimento esecutivo", da realizzare senza particolari formalità. Ne discende, pertanto, che l'omissione dell'avviso al difensore non è in alcun modo sanzionabile, posto che l'art. 83 disp. att. lo prevede soltanto con riferimento ai prelievi di campioni»: Cass. 19.11.2019 n. 2202, in *OneLegale*.

¹⁴⁸ V., al riguardo, P. Carrière, *Le "criptovalute" sotto la luce delle nostrane categorie giuridiche di "strumenti finanziari", "valori mobiliari" e "prodotti finanziari"; tra tradizione e innovazione*, in *Riv. di diritto bancario* 2019, 117 ss.; M. Semeraro, *Moneta legale, moneta virtuale e rilevanza dei conflitti*, *ivi* 2019, 237 ss.

¹⁴⁹ Cass. 9.12.2016 n. 1916, in *OneLegale*.

¹⁵⁰ La legge, ad esempio, non individua il momento in cui andrebbe operata la conversione, né a quali *exchanges* dovrebbe rivolgersi l'autorità giudiziaria, né, ancora, quali e quante commissioni andrebbero pagate.

tratta, infatti, di tecnologie che sono quotidianamente sfruttate dalle organizzazioni criminali per i loro traffici, causando problemi finanche di sicurezza nazionale.

Sul versante processual-penalistico, si è cercato di mettere in luce come le indagini che vedono coinvolte cripto-attività assumano spesso una natura molto articolata. Non solo esse hanno perlopiù matrice transnazionale, ma richiedono pure l'impiego incrociato di plurimi strumenti di investigazione, tradizionali e altamente tecnologici. Con ciò si vuole dire che, per contrastare in modo efficace tutte le forme di criminalità che sfruttano il potenziale della *blockchain*, è indispensabile avere a disposizione un ecosistema normativo capace di affrontare le grandi sfide poste dalla criminalità contemporanea. Esso deve, infatti, permettere alle autorità di *law enforcement* di seguire in tempo reale e in tutto il globo i flussi di denaro criptati e, se del caso, di sequestrarli, in brevissimo tempo.

Sennonché, va preso atto che il nostro codice di procedura penale non risulta – a oggi – assolutamente all'altezza di questo presupposto di fondo. Da un lato, gli strumenti di indagine più tradizionali (quali, *in primis*, il sequestro probatorio) si rivelano inadeguati, non essendo calibrati sulla nuova realtà virtuale nella quale operano i “criminali 2.0”. Dall'altro, il nostro codice, nonostante le critiche costantemente sollevate dalla dottrina¹⁵¹, continua a non regolare affatto numerosi mezzi investigativi di stampo tecnologico (basti pensare, oltre ai già menzionati *software* di *blockchain forensic*, all'OSINT e al sequestro di *device*, al pedinamento GPS e alle videoriprese investigative), con tutto ciò che ne consegue in termini di perdita di efficacia del sistema repressivo, così come di problemi di tutela dei diritti fondamentali. Al riguardo, i modelli cui ispirarsi – si pensi, ad esempio, alla grande riforma compiuta in Spagna nel 2015¹⁵² o, con specifico riguardo alle “*crypto*-indagini”,

¹⁵¹ In generale, sulla necessità di un intervento legislativo volto a regolamentare queste nuove strumentazioni investigative, v., pur con differenti prospettive di riforma, M. Gialuz, *Premessa*, in *Le nuove intercettazioni. Legge 28 febbraio 2020 n. 7*, in *Dir. di internet* 2020, Supplemento al n. 3, 7; S. Marcolini, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *CP* 2015, 789 ss.; F. Nicolichia, *I controlli occulti e continuativi come categoria probatoria. Una sistematizzazione dei nuovi mezzi di ricerca della prova tra fonti europee e ordinamenti nazionali*, Milano 2020; e, volendo, J. Della Torre, A. Malacarne, *L'utilizzo dei file di log per scopi di contrasto alla criminalità: nodi problematici e possibili soluzioni*, in www.archiviopenale.it, 22.12.2023.

¹⁵² Il sistema processuale spagnolo è senz'altro all'avanguardia sul versante della regolamentazione dei moderni strumenti intrusivi impiegati nella fase delle indagini preliminari. Il riferimento corre alla *Ley Organica* 5 ottobre 2015, n. 13, con la quale il legislatore ha modificato la *Ley de Enjuiciamiento Criminal* con il dichiarato obiettivo di disciplinare «*las medidas de investigación tecnológica*» e, contestualmente, rafforzare «*las garantías procesales*» dei soggetti coinvolti nell'accertamento. Per una panoramica sui contenuti della legge, v. F. Bueno De Mata, *Las diligencia de investigacion penal en la cuarta revolucion industrial. Principios teoricos y problemas*

al sistema recentemente implementato nel Regno Unito – sono ormai numerosi. Ciò che occorre, allora, è solo la buona volontà di seguirli.

Tuttavia, dobbiamo essere consapevoli del fatto che pure una riforma normativa sul fronte interno non potrebbe, di per sé, bastare.

Ulteriori sono i versanti sui quali è necessario intervenire.

Per un verso, è indispensabile sviluppare in questo settore un articolato piano di formazione continua e omogenea delle varie forze dell'ordine, così come della magistratura e dell'avvocatura¹⁵³. E ciò dal momento che, come si è avuto modo di dimostrare, le indagini in esame richiedono una notevole dose di specializzazione da parte di tutti gli attori coinvolti e, in particolare, di coloro che sono chiamati a intervenire nelle prime battute dell'indagine.

A livello di autorità di *law enforcement*, un valido modello da seguire è, ad esempio, quello sperimentato negli ultimi anni dall'Arma dei Carabinieri. A partire dal 2021, tale forza dell'ordine ha, infatti, per un verso, formato gruppi di agenti e ufficiali di polizia giudiziaria, dislocati nelle diverse parti del territorio nazionale, e, per un altro, creato una sezione specializzata nel settore, con sede a Roma, chiamata a occuparsi solo di queste fattispecie di reato, risolvendo i casi più complessi¹⁵⁴. Questo modello “binario” pare vincente, perché capace di coniugare la diffusione di una conoscenza minima delle problematiche del settore agli operatori dislocati a livello locale, con la creazione di un corpo d'*élite*, in grado di fornire risposte proporzionate rispetto alle singole minacce in gioco.

Per altro verso, è essenziale potenziare anche i meccanismi di cooperazione internazionale¹⁵⁵. L'esperienza maturata sul campo, infatti, insegna che le attività di

practicos, Cizur Menor 2019.

¹⁵³ Insistono giustamente sul punto, sin dall'inizio del loro *report*, N. També, A. Owen e M. Nizzero, *Crypto-Asset Recovery Challenges, Observed Practices and Strategies*, Londra 2024, 1. V. anche le articolate raccomandazioni di Europol e del Basel Institute on Governance, *A race against time: Europol – Basel Institute on Governance recommendations on preventing and combating the criminal use of cryptocurrencies*, reperibili in <https://baselgovernance.org/publications/race-against-time-europol-basel-institute-governance-recommendations-preventing-and>.

¹⁵⁴ Trattasi della “Sezione Criptovalute del Comando Carabinieri Antifalsificazione Monetaria” che, come è dato leggere nel sito dell'Arma, è stata istituita il 4 ottobre 2021 «con il compito di contrastare le emergenti dinamiche criminali legate all'utilizzo illecito delle criptovalute e l'uso di piattaforme informatiche illegali per la vendita di valuta ed altri prodotti contraffatti di specifica competenza del Comando» (<https://www.carabinieri.it/chi-siamo/oggi/organizzazione/mobile-e-speciale/comando-carabinieri-antifalsificazione-monetaria#:~:text=Il%204%20ottobre%202021%20%20C3%A8,d%20o%20valuta%20ed%20altri%20prodotti>).

¹⁵⁵ È questo, del resto, l'auspicio manifestato dagli stessi appartenenti alle forze dell'ordine che quotidianamente sono impegnati nell'attività di contrasto a questo tipo di criminalità: v. V. Giordano, *L'attività della Guardia di*

contrasto rivelatesi maggiormente efficaci sono state quelle caratterizzate dall'operare congiunto di numerose forze appartenenti a diversi Stati membri¹⁵⁶.

Al riguardo, un *focus* specifico dovrebbe essere dedicato agli attuali sistemi di scambio informativo di polizia a livello europeo (quali, ad esempio, SIRENE¹⁵⁷), i quali dovrebbero essere aggiornati in modo tale da consentire un'interazione più celere ed efficace nell'ambito delle operazioni investigative digitali comuni.

Inoltre, è auspicabile, da un lato, incrementare gli sforzi per lo sviluppo di *software* di *blockchain analysis* "europei", creati *by design* in modo conforme all'*acquis* dell'Unione in materia di *privacy*, *data protection* e di intelligenza artificiale¹⁵⁸, nonché, dall'altro lato, dettare regole sovranazionali più avanzate in tema di sequestro e confische di *crypto-asset*, che coprano sia i profili procedurali dell'ablazione di tali beni, sia quelli di gestione e di vendita dei medesimi¹⁵⁹.

Come rilevato da Europol e dal Basel Institute on Governance ci troviamo, insomma, di fronte a una vera e propria "lotta contro il tempo"¹⁶⁰. È, infatti, essenziale aprire al più presto un ambizioso cantiere di riforma, sia a livello italiano, sia europeo, dedicato al rapporto tra giustizia penale e tecnologie criptate. Solo così si potrà sperare di stare al passo delle organizzazioni criminali, evitando che si realizzi lo scenario preconizzato, sul finire del secolo scorso, dai manifesti *cypherpunk*, ovvero sia che uno spettro continui a infestare «*the modern world, the specter of crypto anarchy*»¹⁶¹.

Finanza nell'ambito del sistema antiriciclaggio ed il contrasto all'utilizzo dei cryptoassets per finalità illecite, in *Rivista della Guardia di Finanza* 2022, 512.

¹⁵⁶ Si veda, ad es., l'operazione realizzata da Europol, in collaborazione con l'*European Financial and Economic Crime Centre* (EFECC), che ha portato al sequestro e alla confisca di ingenti somme in criptovalute di provenienza illecita (<https://www.europol.europa.eu/media-press/newsroom/news/europol-holds-largest-ever-operation-to-increase-seizures-of-criminal-assets-worldwide>).

¹⁵⁷ Ciascun Paese che utilizza il Sistema di Informazione Schengen-SIS ha istituito un ufficio SIRENE nazionale, operativo 24 ore al giorno, 7 giorni alla settimana, responsabile dello scambio di informazioni e del coordinamento delle attività connesse alle segnalazioni SIS.

¹⁵⁸ Da questa prospettiva, sicuramente un primo passo è costituito dalla recente pubblicazione della *call* HORIZON-CL3-2024-FCT-01-08, *Tracing of cryptocurrencies transactions related to criminal purposes*, la quale si propone di finanziare lo sviluppo di *software* di tracciamento delle cripto-attività specifici per le esigenze dell'Unione europea.

¹⁵⁹ Da questa prospettiva, sarebbe auspicabile creare una rete europea di agenzie statali, dotate di una serie di compiti in tema di gestione e di vendita di cripto-attività, in modo tale da ridurre i rischi (finanche di fallimento) degli operatori privati coinvolti in tali attività e di limitare gli esborsi economici (dovuti, ad esempio, alle commissioni da pagare ai *provider*).

¹⁶⁰ Cfr. le raccomandazioni di Europol e del Basel Institute on Governance, *A race against time*, cit.

¹⁶¹ *The Crypto Anarchist Manifesto*, cit.