
XIX LEGISLATURA

Doc. **XXIII**
n. **25**

**COMMISSIONE PARLAMENTARE DI INCHIESTA
SUL FENOMENO DELLE MAFIE E SULLE ALTRE
ASSOCIAZIONI CRIMINALI, ANCHE STRANIERE**

(istituita con legge 2 marzo 2023, n. 22)

(composta dai deputati: *Colosimo, Presidente, Ascari, Barbagallo, Bicchielli, Cafiero De Raho, Vicepresidente, Carrà, Castiglione, Congedo, D'Attis, Vicepresidente, Gallo, Ghio, Segretario, Gubitosa, Iaia, Kelany, La Salandra, Maiorano, Michelotti, Piccolotti, Pittalis, Pretto, Provenzano, Serracchiani, Sudano, Tenerini, Zinzi*, e dai senatori: *Bilotti, Cantalamessa, Della Porta, Floridia, Gasparri, Melchiorre, Minasi, Mirabelli, Musolino, Nave, Paita, Potenti, Rando, Rastrelli, Segretario, Russo, Sallemi, Salvitti, Scarpinato, Sigismondi, Silvestroni, Sisler, Spelgatti, Valente, Verini, Zanettin*)

**LA RETE INVISIBILE DELLA MAFIA:
DALLE CRIPTOVALUTE ALLE COMUNICAZIONI CIFRATE**

(Relatore: **on. Mauro D'Attis**)

Approvata dalla Commissione nella seduta del 15 luglio 2026

*Comunicata alle Presidenze il 15 luglio 2026
ai sensi dell'articolo 1, comma 1, lettera dd), della legge 2 marzo 2023, n. 22*

PAGINA BIANCA

*Camera dei Deputati - Senato della Repubblica*

COMMISSIONE PARLAMENTARE DI INCHIESTA
SUL FENOMENO DELLE MAFIE E SULLE ALTRE
ASSOCIAZIONI CRIMINALI, ANCHE STRANIERE

IL PRESIDENTE

Gentile Presidente,

Le trasmetto, ai sensi dell'articolo 1, comma 1, lett. dd) della legge 2 marzo 2023, n. 22, la “Relazione sulle infiltrazioni mafiose nelle istituzioni territoriali e negli enti locali. Applicazione degli istituti di cui all'articolo 143 e seguenti del T.U.E.L.” (Doc. XXIII, n. 24) e la relazione “La rete invisibile della mafia: dalle criptovalute alle comunicazioni cifrate” (Doc. XXIII, n. 25), approvate dalla Commissione nella seduta del 15 luglio 2026.

La ringrazio e Le invio i più cordiali saluti.

Chiara Colosimo

On. Lorenzo FONTANA
Presidente della
Camera dei Deputati
S E D E

CHIARA FONTANA
CAMERA DEI DEPUTATI
15.07.2026 14:25:10 UTC

PAGINA BIANCA

*Camera dei Deputati - Senato della Repubblica*

COMMISSIONE PARLAMENTARE DI INCHIESTA
SUL FENOMENO DELLE MAFIE E SULLE ALTRE
ASSOCIAZIONI CRIMINALI, ANCHE STRANIERE

IL PRESIDENTE

Gentile Presidente,

Le trasmetto, ai sensi dell'articolo 1, comma 1, lett. dd) della legge 2 marzo 2023, n. 22, la "Relazione sulle infiltrazioni mafiose nelle istituzioni territoriali e negli enti locali. Applicazione degli istituti di cui all'articolo 143 e seguenti del T.U.E.L." (Doc. XXIII, n. 24) e la relazione "La rete invisibile della mafia: dalle criptovalute alle comunicazioni cifrate" (Doc. XXIII, n. 25), approvate dalla Commissione nella seduta del 15 luglio 2026.

La ringrazio e Le invio i più cordiali saluti.

Chiara Colosimo

Sen. Ignazio LA RUSSA
Presidente del
Senato della Repubblica
R O M A

CHIARA CATANIA
CAMERA DEI DEPUTATI
15.07.2026 14:24:38 UTC

PAGINA BIANCA

Sommario

Parte I – Note di sistema	1
1. Legge istitutiva della commissione: composizione, compiti e finalità	1
2. Istituzione del X comitato e avvio dell’attività	1
3. Quadro delle audizioni svolte	4
4. Il paradigma della mafia silente e invisibile	5
4.1. I tratti somatici della “mafia 4.0”	8
4.2. Lo strascico del vuoto normativo	12
Parte II – Nuove tecnologie e limiti investigativi	13
Sezione I – Uso illecito delle criptovalute	13
1. Premesse di metodo	13
2. Dati e scenari criminosi	14
3. Stato dell’arte normativo	19
3.1. La disciplina antiriciclaggio	20
3.1.1. Il quadro sovranazionale	20
3.1.2. Il fronte interno	26
3.2. La normativa finanziaria	28
3.2.1. Il regolamento 2023/1114/UE (MiCAR)	28
3.2.2. Il decreto legislativo di attuazione del regolamento MiCAR	31
3.3. Il sistema di <i>asset-recovery</i>	33
3.3.1. Il sequestro di criptovalute nel codice di rito	33
3.3.2. Congelamento e confisca in ambito europeo	35
3.4. La normativa fiscale	36
4. La criptovaluta: definizione, caratteristiche strutturali e potenzialità criminose	37
4.1. La <i>blockchain</i> e il paradosso delle identità opache	42
4.2. I <i>miners</i> e il meccanismo di validazione	43
4.3. Il <i>wallet</i> e la crittografia asimmetrica	44
5. Metodologia investigativa	46
5.1. Tracciamento e de-anonimizzazione: tecniche e limiti	48
5.2. Il sequestro di criptovalute	51
5.2.1. Trasferimento e destinazione	53
5.2.1.1. Transazioni e commissioni: spese di giustizia?	55
5.2.2. Deposito e custodia	56
Sezione II – Uso illecito della crittografia	57
1. Metodi e scenari	57
2. Crittografia <i>end-to-end</i> e limiti investigativi	59

2.1. Il problema tecnico: dal MitM al captatore.	59
2.2. Il problema regolatorio: gli operatori “ <i>Over The Top</i> ”	63
3. Criptofonia, <i>cryptophones</i> e capacità investigative.	65
3.1. La criptofonia e il <i>business</i> mafioso “ <i>as-a-service</i> ”	65
3.2. Definizione e caratteristiche strutturali dei <i>cryptophones</i>	67
3.3. I <i>cryptophones</i> tra <i>privacy</i> ed elusione investigativa.	68
3.3.1. Reazioni e risposte: la compromissione del <i>server</i>	70
4. L’inarrestabile processo di “bunkerizzazione”: scenari e prospettive.	72
Parte III – Conclusioni e prospettive di riforma	75
1. Sintesi dei risultati.	75
2. Proposte in tema di “uso illecito di criptovalute”	76
2.1. Interventi di modifica del codice di procedura penale.	76
2.2. Potenziare la formazione.	77
2.3. Riorganizzazione interna della polizia giudiziaria.	78
2.4. Potenziamento di strumenti e risorse tecnologiche.	78
2.5. Protocolli di collaborazione.	79
2.6. Sollecitare un’implementazione del Regolamento MiCAR.	80
2.7. Obblighi di collaborazione per i <i>CASPs</i>	81
3. Proposte in tema di “uso illecito della crittografia”.	82
3.1. Obblighi per gli operatori OTT.	82
3.1.1. La parificazione regolatoria.	83
3.1.2. Introduzione di un nuovo regime d’autorizzazione.	84
3.2. Armonizzazione della normativa europea sugli OTT	86
3.3. Utilizzabilità processuale del materiale probatorio già acquisito all’estero.	87
3.4. Istituzione di un centro di competenza nazionale.	87
3.5. Estensione delle operazioni sotto copertura.	88
4. Considerazioni conclusive: le mafie sono cambiate. Lo Stato deve cambiare con loro.	89

Parte I – Note di sistema

1. Legge istitutiva della commissione: composizione, compiti e finalità.

Con l. 2 marzo 2023, n. 22, pubblicata nella Gazzetta Ufficiale n. 62 del 14 marzo 2023, è stata istituita, ai sensi dell'art. 82 Cost., e per la durata della XIX legislatura, la Commissione parlamentare di inchiesta sul fenomeno delle mafie e sulle altre associazioni criminali, anche straniere.

Le funzioni della Commissione – esercitate anche attraverso i Comitati (art. 3 l. n. 22 del 2023) – corrono, in chiave sistemica, lungo un duplice asse, conoscitivo e propositivo, secondo la scansione funzionale tracciata dall'art. 1 della legge istitutiva: da un lato, l'accertamento delle dinamiche evolutive dei sodalizi mafiosi, delle loro modalità di infiltrazione nell'economia legale e nelle istituzioni, nonché dei meccanismi di riciclaggio e reimpiego dei proventi illeciti; dall'altro, l'elaborazione di proposte normative, raccomandazioni operative e linee di intervento idonee a rafforzare il contrasto preventivo e repressivo.

In tale cornice, l'evoluzione tecnologica impone di integrare le tradizionali aree di osservazione con i nuovi spazi digitali della criminalità organizzata. In particolare, l'emersione della crittografia avanzata e delle tecnologie a registro distribuito come infrastrutture operative delle economie criminali rende necessario che le funzioni conoscitive della Commissione si estendano allo studio dei protocolli di anonimizzazione, delle piattaforme di scambio decentralizzate e delle modalità di occultamento dei flussi finanziari basati su criptovalute, al fine di comprendere come tali strumenti agevolino il traffico di stupefacenti, le frodi transnazionali, il finanziamento illecito, il riciclaggio ed ogni altra forma di illecito arricchimento possibile.

L'approfondimento su comunicazioni cifrate e uso illecito di criptovalute non rappresenta un ambito accessorio, ma una declinazione ormai necessaria del mandato della Commissione, poiché consente di adeguare l'azione di contrasto alle trasformazioni dell'ecosistema criminale contemporaneo, preservando, al contempo, l'equilibrio tra sicurezza, garanzie individuali e innovazione tecnologica.

2. Istituzione del X comitato e avvio dell'attività.

Sin dall'avvio dei lavori, la Commissione ha avuto contezza dell'attuale polifonia di un fenomeno antico. Ha subito riconosciuto un panorama di gran lunga più problematico e preoccupante rispetto a quello in cui è stata chiamata ad operare nelle precedenti legislature.

Sulla crescente insidiosità della mafia è difficile non convenire. Non è solo un fatto transitorio, è nella natura stessa del fenomeno. Eppure, una criminalità mafiosa che combina simultaneamente più “linee melodiche” – discrezione strategica, attitudine affaristico-imprenditoriale, capacità di silente infiltrazione, ampia specializzazione tecnologica –, destinate ad intrecciarsi armoniosamente contribuendo ciascuna con il proprio carattere e colore ad uno spazio sonoro multidimensionale, era difficile da immaginare nell’immediato orizzonte temporale.

Le enormi difficoltà riscontrate durante le indagini condotte dalla magistratura e dalle forze di polizia documentano come nell’incessante – e fisiologico – processo di adattamento alla mutevolezza dei contesti, vi sia stata una accelerazione singolare verso un “modello (di *business*) mafioso” non semplicemente migliorato, bensì reinventato.

Non è solo innovazione, ma un processo di “rottura” – una “*disruption*”, potremmo dire – che, introducendo comportamenti e interazioni nuove, ha trasformato le regole del gioco. Le conoscenze tecnologiche acquisite e, soprattutto, i modi di organizzarle e utilizzarle, hanno determinato un vero e proprio mutamento di paradigma, ossia l’insorgere di un diverso modo – rispetto al passato – di fare, pensare o interpretare ciò che la mafia circonda (v. *infra*, parte I, §§ 4-4.2.).

È doveroso sottolineare che l’impatto di una “innovazione di rottura” è sempre in qualche modo imprevedibile: puoi definirla tale solo dopo che ne hai visto riconoscere in modo diffuso il “valore” e portare reali cambiamenti nel contesto in cui si è inserita.

A partire da questa consapevolezza, non sfugge il forte significato di una scelta, in base alla quale la Commissione ha istituito, a norma dell’art. 13, comma 1 del Regolamento interno, un inedito Comitato, il decimo – dedicato a “*Mafie e nuove tecnologie: l’utilizzo da parte della mafia di piattaforme di comunicazione criptata e valute virtuali*” –, coordinato dall’On. Mauro D’Attis, per creare un presidio che potesse fungere da metronomo di queste mutazioni e, al tempo stesso, da fucina di idee per contrastare il pericolo – oggi quanto mai concreto ed attuale – di una deriva mafiosa inarrestabile.

L’attività istruttoria del Comitato ha condotto all’elaborazione della presente Relazione. Il lavoro di preparazione della stessa si è articolato su due livelli distinti.

Base di partenza è stata una rilettura organica dell’istruttoria svolta dal marzo 2024 al luglio 2025.

Il Comitato coordinato dall’On. D’Attis, infatti, ha attivato un proficuo confronto con soggetti di comprovata esperienza sulle materie trattate, provenienti da istituzioni¹, associazioni² e imprese³ di

¹ Bruno Frattasi, Direttore generale dell’Agenzia per la Cybersicurezza Nazionale (audizione del 12 giugno 2025).

² Gianfranco Torriero, Vicedirettore generale vicario dell’ABI (audizione del 25 febbraio 2025).

³ In ordine cronologico: Eugenio Santagata, *Chief Public Affairs & Security Office* del Gruppo TIM (audizione del 12 marzo 2024); Andrea Formenti, amministratore delegato di Area S.p.a. (audizione del 26 giugno 2024); Giovanni Nazzaro, Direttore della *Lawful Interception Academy* (audizione del 26 giugno 2024).

settore, forze di polizia⁴ e dal mondo accademico⁵, acquisendo, sui medesimi temi, sia il punto di vista teorico sia quello tecnico-pratico, pubblico e privato.

I soggetti ufficialmente convocati sono stati spesso accompagnati da collaboratori, i quali, appartenendo al medesimo ente, comando o reparto e potendo offrire un supporto tecnico, in alcuni casi sono intervenuti nel corso dell'audizione (di tanto ne è stata data menzione nel resoconto stenografico della seduta)⁶.

Anche in concomitanza con lo svolgimento delle audizioni, sono stati acquisiti numerosi documenti e relazioni.

Successivamente, le tante informazioni raccolte sono state ricomposte in una paziente ricostruzione d'insieme e poi sviluppate nei contenuti.

Si è trattato di un lavoro intenso, di natura critica, calibrato in ogni sua parte. In questa prospettiva, si è dato puntualmente conto di quanto emerso nelle audizioni, registrando in modo sistematico l'insieme delle posizioni espresse e delle informazioni fornite, senza tuttavia ridursi ad un semplice assemblaggio testuale. Ciascun contributo conoscitivo, infatti, è stato ricondotto al contesto in cui è stato formulato, messo in relazione con gli altri elementi istruttori e sottoposto a una valutazione argomentata.

Il risultato è un prodotto omogeneo e approfondito, dotato di autonomia analitica, che fornisce al Parlamento, agli interlocutori istituzionali e all'opinione pubblica una lettura aggiornata degli strumenti più utilizzati dalle mafie contemporanee e un'indicazione di possibili linee di intervento per arginare efficacemente, in concreto, il nuovo atteggiarsi del fenomeno mafioso.

⁴ In ordine cronologico: Luca Flebus, Comandante del Reparto Indagini Telematiche del ROS dei Carabinieri (audizione del 18 aprile 2024); Ivano Gabrielli, Direttore del Servizio Polizia Postale e delle Comunicazioni (audizione del 15 maggio 2024); Vincenzo Nicoli, Direttore del Servizio Centrale Operativo della Polizia di Stato (audizione del 24 luglio 2024); Gianluca Vitagliano, Comandante del Reparto Antifalsificazione Monetaria dei Carabinieri (audizione del 22 gennaio 2025); Antonio Mancazzo, Comandante del Nucleo Speciale Tutela *Privacy* e Frodi Tecnologiche della Guardia di Finanza (audizione del 25 febbraio 2025).

⁵ In ordine cronologico: Jacopo della Torre, Docente di Diritto processuale penale presso la Facoltà di Giurisprudenza dell'Università di Genova (audizione del 17 ottobre 2024); Agnese Del Giudice, Assegnista di ricerca in Diritto processuale penale presso il Dipartimento di Scienze Giuridiche dell'Università del Salento (audizione del 14 novembre 2024). Entrambi successivamente nominati Consulenti della Commissione.

⁶ Per Eugenio Santagata (audizione del 12 marzo 2024): Sabina Strazzullo, responsabile *national institutional affairs & trade associations* di TIM; Massimo Romiti, responsabile servizi autorità giudiziaria standard e fuori standard di TIM; Angelo Di Marzio, *lead cyber developer* di Telsy; Francesca Nuti, *head of national institutional affairs* di TIM. Per Luca Flebus (audizione del 18 aprile 2024): Giuseppe Specchio, Comandante della 3^a Sezione del Reparto Indagini Telematiche del ROS; Vincenzo Ferrigno, addetto alla 1^a Sezione del III Reparto analisi del ROS. Per Andrea Formenti (audizione del 26 giugno 2024): Eduart Biasizzo. Per Gianluca Vitagliano (audizione del 22 gennaio 2025): Simone Vecchiarello, Comandante Sezione Criptovalute del Reparto Antifalsificazione Monetaria dei Carabinieri. Per Antonio Mancazzo (audizione del 25 febbraio 2025): Magg. Francesco Venditti. Per Gianfranco Torriero (audizione del 25 febbraio 2025): Francesca Palisi, direttore centrale dell'ABI, Maria Carla Gallotti, responsabile ufficio rapporti istituzionali italiani dell'ABI.

Si anticipa che la complessità del tema trattato – per sua natura intersettoriale e tecnicamente connotato – ha imposto un approccio multidisciplinare. Un approccio – è agevole intenderlo – che nasce dall’esigenza di fornire risposte agli interrogativi sollevati da prassi investigative emergenti, prevenendo semplificazioni inopportune e conclusioni affrettate connesse alla mancanza di riferimenti normativi e alla necessità di efficaci strumenti di contrasto a fenomeni criminali di deflagrante pericolosità: solo comprendendo gli elementi fondamentali di un apparato tecnologico (soprattutto se complesso, come in questo caso) è possibile declinare, nel rispetto dei diritti costituzionali e sovranazionali, le migliori “soluzioni” da intraprendere.

Il lavoro conferma quella stretta interazione tra giuridicità e tecnicità che sempre più va connotando il procedimento penale; del resto, che per penetrare e smantellare le reti di questa criminalità mafiosa sempre più sofisticata sia fondamentale combinare indagini finanziarie e patrimoniali a competenze tecniche e tecnologiche all’avanguardia è un’evidenza non più trascurabile.

In questa prospettiva, allora, la Relazione proseguirà con un’analisi del mutamento di paradigma delle mafie contemporanee (parte I, § 4), con un *focus* sui tratti somatici della “mafia 4.0” (parte I, §§ 4.1-4.2.).

Saranno analizzati, a seguire, strumenti e sistemi digitali che, fondandosi sulla crittografia, assicurano l’impenetrabilità (parte II). In particolare, un’intera sezione sarà dedicata all’uso illecito delle criptovalute (parte II, sez. I, §§ 1-5.2.2.), l’altra alla crittografia e agli apparati cifrati (parte II, sez. II, §§ 1-4), concentrando l’attenzione sul funzionamento di questi nuovi strumenti, sulla relativa terminologia, non sempre d’uso comune, e sull’appetibilità criminale.

Un’altra parte, la terza, sarà dedicata esclusivamente alle proposte di riforma, finalizzate a migliorare complessivamente lo *status quo* e, soprattutto, a contenere la proliferazione incontrollata di prassi applicative disomogenee.

3. Quadro delle audizioni svolte.

Il X Comitato ha svolto le seguenti audizioni dal marzo 2024 al luglio 2025:

Data	Soggetto audito	Qualifica/Ente	Modalità	Documenti depositati
12 marzo 2024	Eugenio SANTAGATA	Chief Public Affairs & Security Office del Gruppo TIM	Libera	DOC. n. 107.1
18 aprile 2024	Luca FLEBUS	Comandante del Reparto Indagini Telematiche del ROS dei Carabinieri	Segreta	DOC. n. 139.1

15 maggio 2024	Ivano GABRIELLI	Direttore del Servizio Polizia Postale e delle Telecomunicazioni	Libera/ Segreta	DOC. n. 167.1 DOC. n. 193.001
26 giugno 2024	Giovanni NAZZARO	Direttore della <i>Lawful Interception Academy</i>	Libera	DOC. n. 192.1
26 giugno 2024	Andrea FORMENTI	Amministratore Delegato di Area S.p.A.	Segreta	DOC. n. 194.1 DOC. n. 205.1
24 luglio 2024	Vincenzo NICOLÌ	Direttore del Servizio Centrale Operativo della Polizia di Stato	Libera/ Segreta	DOC. n. 214.1
17 ottobre 2024	Jacopo DELLA TORRE	Docente di Diritto processuale penale presso la Facoltà di Giurisprudenza dell'Università di Genova	Libera	DOC. n. 247.1
14 novembre 2024	Agnese DEL GIUDICE	Assegnista di ricerca in Diritto processuale penale presso il Dipartimento di Scienze Giuridiche dell'Università del Salento	Libera	DOC. n. 265.1
22 gennaio 2025	Gianluca VITAGLIANO	Comandante del Reparto Antifalsificazione Monetaria dei Carabinieri	Libera	DOC. n. 287.1
25 febbraio 2025	Antonio MANCAZZO	Comandante del Nucleo Speciale Tutela <i>Privacy</i> e Frodi Tecnologiche della Guardia di Finanza	Libera	DOC. n. 316.1
25 febbraio 2025	Gianfranco TORRIERO	Vicedirettore generale vicario dell'Associazione Bancaria Italiana	Libera	DOC. n. 315.1
12 giugno 2025	Bruno FRATTASI	Direttore generale dell'Agenzia per la Cybersicurezza Nazionale	Libera	DOC. n. 392.1

4. Il paradigma della mafia silente e invisibile.

È bene iniziare da ciò che risulta ormai evidente: un profondo mutamento ha investito assetti considerati intangibili; la mafia ha progressivamente sostituito l'uso della violenza manifesta con strategie di silenziosa interazione e infiltrazione, approfittando della disponibilità di ingenti capitali illeciti e di una spiccata capacità di coniugare tradizione e modernità imprenditoriale.

L'abilità di adattarsi ai cambiamenti economici e sociali, pur preservando riti e codici di comportamento primevi, ha consentito alle organizzazioni criminali di sviluppare formule organizzative e modalità d'azione sempre più performanti perché sempre meno “appariscenti”.

Nella prospettiva di un approccio tradizionale – nel quale la presenza mafiosa viene percepita solo in concomitanza di episodi violenti ed eclatanti – si potrebbe pensare a un crescente declino del

fenomeno. Così non è. L'uso dell'intimidazione manifesta, proprio perché foriero di allarme sociale e di attenzione giudiziaria, è ormai confinato in circostanze “assolutamente necessarie”.

La mafia, invero, si è evoluta; ha da tempo intuito l'opportunità di rafforzare il vincolo associativo mediante la ricerca del consenso⁷, profittando del ricordo stabile oramai impiantato nella memoria della collettività circa l'esercizio della forza da parte dell'associazione.

In un “quadrato ambientale” in cui sono a tutti note la presenza e le “*regulae vitae*” della consorteria mafiosa (spietatezza dei metodi, ineluttabilità delle reazioni “sanzionatorie” e codici di comunicazione), non è più necessario che essa, nel perseguire i propri fini, si esponga al rischio di essere attenzionata dall'autorità, potendosi limitare ad utilizzare la forza che il vincolo ha acquisito nel corso del tempo come arma di pressione nei confronti dei consociati.

Il metodo mafioso, oggi, quando il sodalizio ha già raggiunto un alto grado di fama criminale⁸ (per mezzo di un pregresso e continuato utilizzo della violenza), si manifesta attraverso modalità sempre meno evidenti (“silenti”).

Le organizzazioni più radicate prediligono, ormai, la strategia del “basso profilo” a vocazione affaristico-imprenditoriale, perché ampiamente più congeniale all'infiltrazione del tessuto socio-economico e alla scalata dei gangli della cosa pubblica⁹. Il risultato è un'aggressione del territorio non più orientata, in modo esclusivo, alla preminenza “militare”, ma finalizzata all'esercizio

⁷ In molti casi, le imprese mafiose operano come vere e proprie società di servizi, offrendo beni a costi irrisori, grazie all'evasione fiscale e al mancato versamento di contributi previdenziali. In altri, approfittando dei servizi offerti dai pubblici funzionari corrotti, offrono opportunità di facili guadagni, pilotando – ad esempio – l'assegnazione di appalti in favore di talune imprese del territorio prive dei requisiti. In altri ancora, valendosi di imprenditori compiacenti, l'organizzazione mafiosa garantisce la disponibilità di posti di lavoro “da assegnare” per creare consenso sociale al sodalizio, ovvero la possibilità di assumere fittiziamente nell'azienda i propri sodali, così da creare apparenti provviste lecite che possano giustificare un altrimenti sproporzionato quadro reddituale. Se non che, l'ingresso nel “circuitto mafioso” di commercianti, imprenditori, professionisti e funzionari pubblici rappresenta un'opportunità solo apparentemente vantaggiosa, perché destinata ad innescare, progressivamente, meccanismi di asservimento sempre più pregnanti a vantaggio dell'organizzazione criminale.

⁸ Fanno eccezione, a tutta evidenza, le mafie straniere (albanesi, romene, nigeriane, sudamericane, russe, cinesi etc.) e quelle c.d. “autoctone”, ossia le organizzazioni criminali autonome e “prive di storia” che utilizzano metodi e perseguono scopi corrispondenti alle associazioni mafiose già note. Trattandosi di aggregazioni criminali di nuova emersione, che necessitano, quindi, di imporsi nel territorio di insediamento, il metodo – finalizzato sia alla conquista del mercato illecito, sia alla progressiva penetrazione del tessuto politico, economico e imprenditoriale – si manifesta normalmente attraverso atti di violenza e minaccia manifesti.

⁹ L'abilità delle mafie di intessere relazioni collusive con esponenti della politica locale e della pubblica amministrazione rappresenta un elemento di perdurante criticità. Tali rapporti hanno consentito, nel tempo, l'illecita acquisizione di appalti pubblici, finanziamenti statali e assunzioni clientelari, compromettendo l'integrità delle istituzioni e minando la libera concorrenza economica.

d'impresa, nonché alla corruttela e alla connivenza¹⁰, secondo logiche parassitarie e funzionali al conseguimento di risorse economiche e posizioni di privilegio¹¹.

L'“oggetto sociale”, infatti, non è cambiato: moltiplicare i guadagni – traghettando l'enorme ricchezza illecita nell'economia legale – e trasformarli in potere.

La capacità di stare al passo con le più avanzate strategie di investimento, anche per cogliere le occasioni offerte dai fondi pubblici nazionali e comunitari, rappresenta un dato di struttura dell'impresa mafiosa: è con il denaro, del resto, che si ottengono vantaggi competitivi, si producono nuove opportunità criminali, si costruiscono i “ponti” a doppio senso (c.d. “area grigia”), si moltiplicano i satelliti e si rafforza la provvidenziale “cintura di salvataggio” di cui l'organizzazione si circonda¹², garantendone sviluppo e sopravvivenza¹³. Nonostante le specificità territoriali, infatti, tutte le mafie, a partire da quelle storiche – cosa nostra, camorra, ‘ndrangheta e sacra corona unita –, continuano ad essere accomunate dall'inesausta ricerca di ricchezza, potere e controllo sociale.

La rivoluzione digitale, poi, ha fornito alle organizzazioni del vecchio secolo la possibilità, immediatamente colta, di sfruttare tecnologie d'avanguardia per fare affari anche nel *cyber*-spazio¹⁴. Che la società stia attraversando, a livello globale, un momento di sviluppo inedito e rapidissimo sul piano dell'elaborazione e dell'impiego di strumenti tecnologici innovativi, in tutti i campi della vita individuale e collettiva, oggi è solo una constatazione. Il grado di penetrazione di questo arsenale tecnologico nell'esistenza quotidiana delle collettività è tale da rendere ormai impensabile il farne a meno e da porlo come componente ineludibile di ogni ambito della vita sociale. L'area criminale e, in seno ad essa, quella mafiosa – che è parte integrante del tessuto sociale ed economico in cui vive e agisce –, chiaramente non fanno eccezione¹⁵.

¹⁰ Soprattutto tramite l'inquinamento delle competizioni elettorali – ove gli eletti sono diretta espressione dell'organizzazione mafiosa – o la corruzione di uomini delle istituzioni (dirigenti, funzionari o anche semplici impiegati). Il sistema della corruttela consente ai sodalizi di conseguire le utilità offerte dal comparto pubblico e di svolgere liberamente attività di impresa, anche per l'assenza dei controlli – dovuta, appunto, alla complicità dei dipendenti corrotti – cui le pubbliche amministrazioni sono, di regola, deputate.

¹¹ La pressoché assenza di episodi eclatanti o cruenti non significa, però, che le organizzazioni mafiose abbiano rinunciato del tutto all'uso della violenza: ci si trova spesso dinanzi a gruppi criminali in grado di “cambiare pelle” in relazione all'ambiente in cui agiscono. La violenza rimane, in ogni caso, un'opzione sempre attivabile a scopo intimidatorio.

¹² Cfr. il resoconto stenografico dell'audizione della Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato.

¹³ L'impulso al reinvestimento costituisce condizione di sviluppo e, al tempo stesso, di sopravvivenza delle economie criminali, tanto da poter ritenere – sulla base di attendibili regole di esperienza attinenti propriamente al fenomeno – che allorquando l'organizzazione non gode più dei suoi profitti perde, inevitabilmente, potere contrattuale e competitività, diviene “vulnerabile” nella gestione dei rapporti di controllo sociale delle istituzioni e la sua conflittualità interna può facilmente assumere caratteri autodistruttivi della stessa organizzazione. Cfr. il resoconto stenografico dell'audizione della Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato.

¹⁴ Cfr. il resoconto stenografico dell'audizione della Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato.

¹⁵ A ben vedere, il fenomeno riguarda, in generale, tutta la criminalità, non solo quella organizzata o quella organizzata di tipo mafioso. Come sottolineato dal Dott. Ivano Gabrielli nel corso della sua audizione, «stiamo parlando di una

Oggi le mafie si muovono come *holding* e utilizzano gli applicativi più sofisticati messi a disposizione dai *leader* tecnologici, mettendo in crisi l'attuale sistema investigativo che non riesce a stare al passo con l'evolversi velocissimo delle tecniche di arricchimento e di elusione d'ogni controllo possibile. Lo scenario è piuttosto chiaro. La commistione – oramai irreversibile – tra mafia e tecnologia ha amplificato e potenziato il modello preesistente: non più un'organizzazione asserragliata nel territorio di origine e incline a reclutare solo per fedeltà e sangue, ma un'associazione ibrida, smaterializzata e delocalizzata, silente e invisibile, ossia una mafia in grado di operare in modo fluido – *i.e. online* e “*offline*” – su scala globale, massimizzando risorse, competenze e reti logistiche, avvantaggiandosi della apolidia del *web* (che, per definizione, non conosce confini) e della vulnerabilità umana; una vera e propria impresa, a struttura complessa, che ovunque allaccia relazioni, stringe accordi, crea vincoli di fiducia, integra risorse umane con competenze specifiche per raggiungere obiettivi economici e di potere prima inimmaginabili o difficilmente raggiungibili. Una mutazione rapida e mirata che ha reso la mafia più veloce, più potente, più efficiente e, soprattutto, invisibile.

4.1. I tratti somatici della “mafia 4.0”.

Gli architravi di questo *upgrade* della mafia sono facilmente individuabili.

Un primo elemento cardine è certamente rappresentato dall'integrazione sinergica tra attività criminali tradizionali e nuove operazioni digitali.

Diversamente da quanto si potrebbe pensare, la mafia non ha abbandonato le attività storiche per concentrarsi esclusivamente sul mondo *cyber*; piuttosto, ha sviluppato un modello ibrido in cui il l'agire “analogico” e quello digitale coesistono e si alimentano reciprocamente.

L'esperienza dei mercati illegali nel *dark web* e nel *deep web* è emblematica in tal senso: attraverso il ricorso al “lato oscuro” di *internet*, la criminalità ha trovato una nuova dimensione in cui condurre le tradizionali attività del traffico di droghe e di armi. Si pensi, banalmente, anche alla possibilità di drenare proventi illeciti *on-line* – ad esempio, attraverso il *phishing* – da reinvestire nei traffici “analogici” tipici dell'organizzazione. Numerose sono, altresì, le manifestazioni del reato di riciclaggio: il *cyberlaundering* puro, con cui la mafia “ripulisce” i proventi in criptovaluta su piattaforme digitali, si affianca alle ipotesi in cui la tecnologia viene sfruttata per immettere il denaro “tradizionale” (cioè non dematerializzato) – provento, quindi, di delitti commessi in maniera del tutto

criminalità che l'ultimo *report* della convenzione di Nuova Delhi tenuta l'anno scorso a livello di *Interpol* definisce da tutte le agende internazionali e di polizia come il problema più significativo e più importante che avremo da qui in avanti. È stato stimato che 10.5 trilioni di dollari sarà il prodotto di questa economia criminale che attinge al *cyber crime*. Non da meno tutto ciò che oggi è il *know how* del *cyber crime* viene di volta in volta trasferito a criminalità organizzata già nota, comune che già conosciamo, con forme di trasferimento di tecnologia o addirittura di capitali che poi vengono reimpiegati» (cfr. resoconto stenografico, seduta del 15 maggio 2024, X Comitato, p. 9).

“analogica” – nel sistema finanziario o bancario, per celarne l’origine delittuosa e reinserirlo nell’economia legale.

La natura ibrida consente alle mafie di sfruttare le vulnerabilità di entrambi gli ambienti e di modulare la propria presenza in base alle opportunità e ai rischi contingenti. L’armamentario tecnologico funge, in sostanza, da moltiplicatore della capacità criminale.

Da questo punto di vista si deve anche considerare l’uso sempre più consapevole dell’*AI*, che ha potenziato a dismisura l’efficacia di un già rinnovato agire criminoso, consentendo alle organizzazioni mafiose di moltiplicare le occasioni di profitto e di ridurre, ulteriormente, costi e livelli di rischio. Preso atto di quanto i sistemi di intelligenza artificiale abbiamo già profondamente influenzato il nostro modo di vivere e di lavorare, nonché lo svolgersi delle relazioni personali ed economiche, sarebbe assurdo credere che invece il fenomeno mafioso ne sia rimasto immune.

Ed infatti, sono numerosi i casi di impiego di algoritmi per *hackerare* dati e gestire flussi di informazioni al riparo dalle autorità giudiziarie o per produrre *deep fake* finalizzati a manipolare gli utenti (truffe c.d. “sentimentali” o “*romance scams*”¹⁶; frodi *fintech*, etc.) e a gestire il mercato illegale nel *dark web* (attraverso “identità sintetiche” create *ad hoc*), ovvero per confondere i flussi finanziari illeciti ed eludere i controlli antiriciclaggio (si pensi, ad esempio, al c.d. “*smurfing* automatizzato”)¹⁷, oppure per generare in tempo reale codici malevoli di infezione e ricatto (*ransomware* “potenziato”)¹⁸.

L’ibridazione connota, chiaramente, anche la struttura organizzativa.

¹⁶ Come riportato dal Comandante del Nucleo Speciale Tutela *Privacy* e Frodi Tecnologiche della Guardia di Finanza – Gen.B. Antonio Mancazzo – nel corpo della relazione depositata a corredo della sua audizione (tenutasi il 25 febbraio 2025), «il fenomeno delle truffe sentimentali trova nell’intelligenza artificiale strumenti sempre più sofisticati per risultare credibili agli occhi delle vittime. Vengono utilizzate tecniche *deepfake* per creare sui social i profili falsi con cui ingannare la persona scelta, avviando relazioni sentimentali “virtuali” aventi lo scopo finale di estorcere denaro. L’IA è in grado di generare immagini realistiche di uomini e donne di qualsiasi età, creare profili *social* che sembrano autentici, generare testi adattando il linguaggio e lo stile a seconda dell’interlocutore. Può risultare perfino più naturale e coinvolgente di una persona reale e conquistare così la fiducia della vittima. Non solo, l’IA inoltre è in grado di operare in diverse lingue, consentendo ai truffatori un respiro internazionale, raggiungendo un pubblico estremamente ampio. Le vittime sono molto spesso persone avanti con gli anni che vivono momenti di solitudine o di vulnerabilità affettiva e di cui i truffatori si approfittano senza alcuna remora. L’intelligenza artificiale è sfruttata dai malintenzionati per generare risposte automatiche alle richieste delle vittime contattate» (cfr. DOC. n. 316.1, p. 10-11).

¹⁷ Si tratta di una tecnica di riciclaggio in cui i proventi illeciti vengono suddivisi in piccole somme, spesso distribuite su più conti e/o più soggetti, per restare sotto le soglie e ridurre la probabilità di controlli e/o segnalazioni. Quando si parla di “*smurfing* automatizzato” la frammentazione e l’instradamento delle micro-transazioni vengono orchestrati da *script* generati dall’AI, così da aumentare volume e velocità delle operazioni ripetute, distribuire l’attività su più conti/canali e, infine, rendere più difficile ricostruire il *pattern*.

¹⁸ I *ransomware* sono virus informatici che rendono inaccessibili i file dei computer infettati e chiedono il pagamento di un riscatto per ripristinarli. Nella sua nuova espansione, il *ransomware*, anziché basarsi su uno *script* fisso, utilizza l’AI per generare in tempo reale codice malevolo, rendendo ogni esecuzione potenzialmente diversa dalla precedente. Grazie alla generazione dinamica di *script*, ogni infezione può assumere tratti unici, rendendo inefficaci le tradizionali tecniche di rilevamento basate su firme statiche o comportamenti ricorrenti.

Le associazioni mafiose hanno progressivamente incorporato risorse adeguate al mondo *cyber*, mantenendo, al contempo, i propri fondamenti identitari e gerarchici.

Subordinati al nucleo dirigenziale dei “veterani” – che conserva e perpetua riti, codici comportamentali e meccanismi decisionali della tradizione – operano, infatti, giovani membri con elevata *digital literacy*, spesso discendenti di famiglie già affiliate, in grado di comprendere il linguaggio contemporaneo e sfruttare le nuove metodologie operative messe a disposizione dall’evoluzione tecnologica. Il risultato è un ponte generazionale che consente di trasferire valori e codici mafiosi ancestrali e di acquisire competenze tecniche, giuridiche ed economiche moderne. Non solo.

È ormai evidente l’inclusione di soggetti altamente specializzati, anche non formalmente affiliati all’organizzazione. Piuttosto che sviluppare internamente tutte le competenze necessarie, processo che richiederebbe tempo e risorse significative, le mafie hanno optato per un modello di *outsourcing* selettivo, reclutando nel *dark web* (e non solo), sulla base di expertise specifiche necessarie per particolari operazioni, veri e propri “*contractors*” digitali: *hacker* offensivi per la creazione e fornitura di *malware* “chiavi in mano”, esperti di sicurezza informatica, *broker* nel mercato delle criptovalute, specialisti in *social engineering* e manipolazione psicologica, etc. È abbastanza intuitivo come questa strategia consenta alle mafie di accedere rapidamente a competenze tecniche avanzate già consolidate, senza tuttavia alterare la gestione interna, e garantisca, al contempo, una resilienza strutturale – fondata, appunto, sulla interscambiabilità – che permette al sodalizio di resistere agevolmente agli interventi repressivi.

Altri due elementi essenziali di questo *upgrade* della mafia sono la dimensione intrinsecamente transnazionale dell’*internet*, da un lato, e il significativo innalzamento del livello di anonimato garantito dai prodotti tecnologici, dall’altro; elementi, avvinti da un rapporto di stretta interdipendenza, attraverso i quali le consorterie mafiose hanno sviluppato una versatilità tattica straordinaria.

La rete, infatti, trascende i confini territoriali consentendo operazioni simultanee su scala globale, senza necessità di spostamenti fisici o complesse operazioni logistiche e con costi operativi del tutto insignificanti rispetto ai profitti.

È evidente che una tale propagazione geografica non solo ostacola enormemente le attività investigative, frammentandole attraverso molteplici giurisdizioni, ma determina, altresì, una drastica riduzione dell’esposizione fisica dei membri dell’organizzazione.

La possibilità, poi, di operare attraverso reti anonimizzate, sistemi di comunicazione criptati, piattaforme di *minig*, *software* di cifratura e *server off-shore* riduce esponenzialmente il rischio di

identificazione, permettendo anche ai vertici dell'associazione di mantenere un controllo diretto sulle operazioni illecite senza esporsi ai rischi propri della sorveglianza fisica.

Agire attraverso tecnologie – *lato sensu* intese – in grado di assicurare l'impenetrabilità¹⁹ (investigativa) rappresenta il vero cuore pulsante delle mafie contemporanee.

Di qui la scelta di concentrare i valori della Commissione sulla crittografia, a cui la mafia attinge a piene mani.

Anzitutto per ciò che concerne l'infrastruttura comunicativa²⁰: le consorterie si avvantaggiano di nuovi e "blindati" canali di comunicazione – con cui, ad esempio, messaggi cifrati "all'origine" raggiungono il *server* dedicato e da questo vengono restituiti in chiaro al solo destinatario (v. *infra*, parte II, sez. II) –, i quali facilitano, peraltro, preoccupanti alleanze transnazionali²¹.

Ma anche per generare ricchezza. Le mafie hanno rapidamente compreso l'enorme potenziale delle criptovalute e della *blockchain* per occultare e riciclare i proventi delle attività illecite, sfruttando, da un lato, i vantaggi connessi alla dematerializzazione della ricchezza e approfittando, dall'altro lato, dei tanti "paradisi normativi" sparsi per il globo²²: in pochi e rapidi passaggi la rete veicola transazioni in criptovaluta da un nodo ad un altro, da una società ad un'altra, da un continente all'altro, senza alcuna intermediazione o passaggio per la dimensione reale dell'economia e in modo fortemente riservato²³ (v. *infra*, parte II, sez. I). Questa interconnessione ha generato un'economia sommersa globale di smisurata entità che condiziona mercati, distorce (o annulla) la concorrenza e mina la sicurezza nazionale.

Ebbene, la possibilità di comunicare, arricchirsi ed espandersi "riservatamente" è ormai senza limiti²⁴.

¹⁹ Cfr. Report Europol, *Do criminals dream of electric sheep? How technology shapes the future of crime and law enforcement*, 2019, in www.europol.europa.eu, p. 13.

²⁰ Lo suggerisce anche il Dott. Ivano Gabrielli nel corpo della relazione depositata in occasione della sua audizione del 15 maggio 2024, X Comitato: «[l]e indagini sinora svolte hanno rilevato oltre 200 mila apparati in Europa (circa il 10% in Italia) e consentito di acquisire milioni di conversazioni (*chat*, *file* e immagini) la maggior parte delle quali attinenti a reati di criminalità organizzata o corruzione» (cfr. DOC. n. 193.1, p. 1).

²¹ Si tratta di collaborazioni che consentono di unire risorse, competenze e reti logistiche, amplificando la portata e l'efficacia delle operazioni criminali su scala globale. Contrariamente al recente passato, si assiste ad un'interazione sempre più frequente tra mafie nazionali e sodalizi stranieri, i quali agiscono in posizione pressoché paritaria rispetto alle prime, soprattutto nel *business* degli stupefacenti, dove sono sempre più frequenti le reti criminali "cross-border" improntate a criteri di convenienza reciproca tra le diverse compagini delinquenziali. Cfr., da ultimo, l'audizione di Lincoln Gakiya, procuratore del Ministero Pubblico di San Paolo, tenutasi il 13 gennaio 2026 in seduta Plenaria.

²² Si pensi agli *exchange offshore*, ossia alle piattaforme di *crypto trading* situate in una giurisdizione a bassa regolamentazione: tra le più popolari, *KuCoin* e *MEXC* (Seychelles), *Bitfinex* (Isole Vergini Britanniche), *Bitget* (Singapore). Si tratta di piattaforme di scambio che prevedono un livello più basso di restrizioni KYC (*Know Your Customer*), acronimo che identifica quell'insieme di procedure obbligatorie che le aziende devono seguire per identificare, verificare e monitorare l'identità dei propri clienti al fine di prevenire il riciclaggio di denaro, il finanziamento del terrorismo e altre attività illecite, rispettando normative AML (*Anti-Money Laundering*). Esse richiedono la raccolta di documenti d'identità, prove di residenza e verifica dei dati.

²³ Cfr. il resoconto stenografico dell'audizione della Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato.

²⁴ L'operatore ne è pienamente consapevole: cfr., ad esempio, la Relazione DIA, II semestre 2021, in <https://direzioneeinvestigativaantimafia.interno.gov.it/relazioni-semestrali/>, p. 327, ove si sottolinea come «la criminalità

Da un punto di vista economico, infatti, il rapporto tra rischio e rendimento è particolarmente favorevole: l'approvvigionamento di stupefacenti può raggiungere volumi e capillarità impensabili se pianificato e coordinato utilizzando sistemi criptati di comunicazione; il riciclaggio attraverso il *trading* di criptovalute offre possibilità di arricchimento e occultamento dei capitali prima inaccessibili; un solo attacco *DDoS* (*Distributed Denial of Service*) o *ransomware* con richiesta di riscatto in criptovaluta può generare profitti equivalenti a mesi di estorsioni fisiche, con un livello di esposizione personale quasi nullo.

4.2. Lo strascico del vuoto normativo.

Lo scenario è ulteriormente complicato dalla perdurante assenza di una normativa adeguata a contrastare il fenomeno.

Volgendo lo sguardo al nostro ordinamento, se, per quanto concerne il piano sostanziale, alcuni passi avanti sono stati fatti, sul piano processuale si deve constatare l'arretratezza del codice di rito in merito ai mezzi investigativi e/o probatori ad alto contenuto tecnologico²⁵, oggi essenziali per il contrasto alla nuova criminalità, soprattutto di tipo mafioso. È nelle fessure, infatti, nelle faglie di un sistema sconnesso che germina e si radica con più facilità il potere criminoso, specie di tipo mafioso. Su questo punto il discorso assume un andamento circolare preoccupante: l'assenza di una disciplina performante consente alle organizzazioni mafiose di operare indisturbate e, conseguentemente, di rafforzarsi in uno *step up* incessante che, al tempo stesso, rende più difficile al legislatore aggiornare il proprio ecosistema normativo ed operativo per cercare di affrontarle. Viepiù considerando che, quando si tratta di tecnologie, uno studio allo stato esaustivo è destinato ad essere superato nel volgere di pochi mesi.

Un esempio su tutti: l'ultimo approdo del processo di "bunkerizzazione" delle comunicazioni, ossia lo *smart contract*. Si tratta di un applicativo pensato per automatizzare l'esecuzione di obbligazioni contrattuali²⁶ attraverso la *blockchain*, ma che, sfruttato in tutta la sua potenzialità, consente alla

organizzata cerchi di acquisire potere e influenza all'interno dei mercati legali guardando alle nuove frontiere di *internet*, dove poter sviluppare attività di riciclaggio su vasta scala e poter comunicare indisturbatamente».

²⁵ Sul punto, cfr. il resoconto stenografico dell'audizione della Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato, pp. 6-7; altresì, quello del Prof. Jacopo Della Torre, seduta del 17 ottobre 2024, X Comitato, p. 5.

²⁶ Gli *smart contract* consentono di eseguire accordi tra parti senza intermediari. Essi operano secondo la logica del "*if this then that*": secondo questo meccanismo, nel momento in cui si realizza una determinata condizione, che può essere automaticamente verificata mediante un codice oppure per il tramite di un "oracolo", lo *smart contract* esegue l'obbligazione.

criminalità di comunicare al riparo da qualunque attività intercettiva, più di quanto non facciano i *cryptophones*²⁷.

In quella che appare essere “*una corsa contro il tempo*” è dunque necessario elaborare al più presto una disciplina “elastica”, in grado di adattarsi ad un sistema che si evolve continuamente.

Certamente, di fronte ad un fenomeno così complesso, proteiforme che, come detto, non (ri)conosce confini, tutti gli ordinamenti giuridici contemporanei – a partire da quello europeo – dovrebbero assumere un atteggiamento proattivo.

Questa certezza, tuttavia, non neutralizza la necessità di una disciplina domestica *ad hoc* sulle investigazioni digitali, nonché, come diremo, in punto di *crypto funds recovery*. Le previsioni generali oggi contenute nel nostro codice di procedura penale, infatti, mal si adattano alle peculiarità degli applicativi cifrati, con tutto ciò che ne consegue sul piano della “tenuta processuale” delle ipotesi accusatorie e di tutela dei diritti fondamentali.

Avere un approccio realistico significa comprendere la “torsione tecnologica” del fenomeno mafioso e fare i conti con essa in maniera organica, implementando un rinnovato approccio interdisciplinare che tenga conto del “terreno di coltura”, ponderando adeguatamente esigenze investigative – funzionali a garantire un’efficace prevenzione e repressione dei reati – e tutela di alcune prerogative fondamentali. L’indifferenza al metodo, infatti, postula una (inammissibile) indifferenza al risultato. Di questo infatti, tra tante incertezze, si deve essere profondamente convinti.

Parte II – Nuove tecnologie e limiti investigativi

Sezione I – Uso illecito delle criptovalute

1. Premesse di metodo.

Per il mondo giuridico e, in particolare, per la giustizia penale, il tema delle criptovalute si pone come particolarmente complesso, perché si tratta di elaborare una disciplina normativa per controllare e prevenire le derive criminose di un fenomeno che nasce proprio con la volontà di sottrarsi al controllo e alla regolamentazione degli attuali sistemi giuridico-finanziari.

Invero, come verrà meglio evidenziato nel prosieguo di questa Relazione, gli stessi tratti che sono alla base del successo delle criptovalute in ambito economico-finanziario – velocità, facilità di

²⁷ Sul punto, il Magg. Francesco Venditti riferisce, testualmente, che «[s]i tratta di comunicazioni attualmente non intercettabili ancor più dei criptofonini, sono molto più sicure perché gestite direttamente da parte a parte»: cfr. resoconto stenografico dell’audizione del Gen.B. Mancazzo, seduta del 25 febbraio 2025, X Comitato, p. 7.

scambio, bassi costi di transazione, anonimato – rappresentano, al contempo, i fattori che hanno determinato le mafie – costantemente impegnate nella ricerca di metodi innovativi per reinvestire i proventi illeciti²⁸ – a farvi ordinariamente ricorso nell’esercizio della propria “attività”.

A ben vedere, tali strumenti hanno esaudito il grande sogno della mafia: effettuare transazioni pressoché istantanee e “anonime” in tutto il mondo, senza passare per gli ordinari intermediari finanziari.

È intuibile che, in questa materia, il profilo tecnico e quello giuridico procedono con la stessa falcata. Ciò è emerso sin dalle prime audizioni: la criminalità organizzata sfrutta la complessità tecnica del mondo *crypto* per eludere il rilevamento ed espandere la sua rete²⁹.

L’unico serio antidoto ad un fenomeno di tal fatta resta, allora, la comprensione; e la vera comprensione del diritto – quale che sia il suo oggetto – implica sempre la conoscenza, prima ancora che della norma, del fenomeno che la norma vuole regolamentare.

In questa prospettiva, dopo aver dato conto del panorama criminoso (parte II, sez. I, § 2) e dello *status quo* della normativa – domestica e sovranazionale – oggi vigente (parte II, sez. I, §§ 3-3.4.), la Relazione fornirà indicazioni sulle caratteristiche generali della criptovaluta e della *blockchain*, evidenziando le ragioni per le quali il sistema *crypto* rappresenta un’industria fiorente (anche) per la criminalità mafiosa (parte II, sez. I, § 4), per poi analizzare come si svolge il *trading* (parte II, sez. I, §§ 4.1.-4.3.) in quanto aspetto assolutamente necessario per esaminare, a seguire, quelle che sono le attività investigative richieste agli inquirenti per disvelare il sistema criminoso (parte II, sez. I, §§ 5-5.1.), sequestrare le criptovalute (parte II, sez. I, §§ 5.2.-5.2.1.), depositarle e custodirle in attesa che il procedimento penale si concluda (parte II, sez. I, § 5.2.2.).

2. Dati e scenari criminosi.

Come accennato, il mercato delle criptovalute, un tempo di nicchia, si è trasformato in un *asset class mainstream*, parte integrante della finanza moderna, che coinvolge milioni di persone.

Gli aspetti positivi legati all’uso (lecito) delle criptovalute sono, invero, numerosi. Basti pensare alla grande diminuzione dei costi di transazione: dinanzi all’assenza di intermediari per la buona riuscita della transazione – funzione sostituita dalla tecnologia *peer-to-peer* e dall’algoritmo di funzionamento del registro pubblico distribuito – i costi di transazione si azzerano quasi del tutto. Di certo non trascurabile è la rapidità delle transazioni (in media pochi minuti): se si confronta questo

²⁸ Europol Spotlight, Cryptocurrencies: tracing the evolution of criminal finances, in www.europol.europa.eu, 26 gennaio 2022.

²⁹ Sulla questione, *amplius*, cfr. il resoconto stenografico dell’audizione della Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato, p. 3 ss.

dato con i tempi del sistema bancario classico, soprattutto per quanto concerne i trasferimenti internazionali di fondi (che impiegano di norma più giorni lavorativi), si comprende quale possa essere la reale differenza tra questo sistema di pagamento e il circuito bancario tradizionale. Non ultima, l'irreversibilità dei pagamenti effettuati: una volta che viene disposto il trasferimento di una certa quantità di criptovaluta da un *wallet* ad un altro, la transazione è immodificabile, anche nel caso in cui sia stata effettuata per errore.

I dati messi a disposizione della Commissione, pur limitati ad un breve arco temporale, sono esemplificativi di questo successo.

Uno studio condotto dall'Osservatorio *Blockchain e Web 3* del Politecnico di Milano rivela che i progetti globali basati su questa tecnologia sono aumentati del 725% tra il 2016 e il 2023. In Italia, l'interesse per le criptovalute e i *token* coinvolge circa 3,6 milioni di utenti che dichiarano di possederli o conoscerli; parallelamente, l'adozione della tecnologia *blockchain* da parte di aziende italiane ha generato un fatturato di 38 milioni di euro, con un incremento del 58% rispetto al 2022.

Il mercato globale delle criptovalute ha registrato una crescita straordinaria nel 2024, con un incremento del 110% rispetto al 2023. Il valore complessivo ha raggiunto circa 3.500 miliardi di dollari, suddivisi in: 52% Bitcoin, 18% Ethereum e 30% Altcoin. A partire da gennaio 2024, questo slancio è stato ulteriormente favorito, dall'approvazione, da parte della *Securities and Exchange Commission* (SEC) statunitense, degli *ETF Spot (Exchange-Traded Funds)*³⁰ legati al Bitcoin, che ha permesso agli investitori di acquistare e detenere questa criptovaluta attraverso prodotti finanziari tradizionali negoziati in borsa³¹.

In ordine al rapporto tra *crypto* e criminalità, invece, è difficile avere dati precisi sul fenomeno, perché tutte le stime delle varie società di consulenza del settore prendono in esame soltanto le transazioni già associate ad attori criminali. Esse, dunque, non fotografando il reale "sommerso", vanno necessariamente lette al ribasso.

Tra le stime più utilizzate vi sono quelle della società americana *Chainalysis*. Nel corso dell'istruttoria sono stati prodotti i dati relativi agli anni dal 2021 al 2023. Si è appreso, in particolare, come dal 2021

³⁰ Gli *ETF Spot* sono «fondi negoziati in borsa che replicano direttamente il prezzo di un asset sottostante, come oro, azioni o criptovalute, detenendolo fisicamente. Offrono un'esposizione trasparente e fedele al prezzo *spot*, senza dipendere da derivati o *futures*. Sono semplici e liquidi, ma includono costi di custodia per gli *asset* fisici»: così, Gen.B. Gianluca Vitagliano nella relazione depositata in occasione della sua audizione del 22 gennaio 2025, X Comitato, DOC. n. 287.1, p.1, nt. 1.

³¹ I dati indicati nel secondo e terzo capoverso sono richiamati nella relazione del Gen.B. Gianluca Vitagliano (DOC. n. 287.1, p. 1) depositata in occasione della sua audizione del 22 gennaio 2025, X Comitato.

in poi la quantità di criptovalute frutto di traffici illeciti avrebbe sempre superato i 20 miliardi di dollari: nel 2021 la somma sarebbe stata di 23,2 miliardi, nel 2022 di 39,6 e nel 2023 di 24,2³².

Oggi, volendo fornire una lettura aggiornata dei dati offerti nel corso delle audizioni, è possibile affermare che le stime relative al biennio 2024-2025 virano su livelli ben più significativi.

Nel 2024 gli indirizzi associati ad attività illecite hanno ricevuto almeno 40,9 miliardi di dollari in criptovalute³³, dato poi aggiornato a 57,2 miliardi³⁴, mentre nel 2025 – con un aumento di circa +162% rispetto alla stima aggiornata dell’anno precedente – di circa 154 miliardi di dollari. Il flusso di denaro illecito si muove, in particolare, verso alcune giurisdizioni, tra cui spiccano Russia, Cina, Corea del Nord e Iran³⁵.

Con particolare riferimento al riciclaggio *on-chain*, *Chainalysis* descrive un ecosistema che nel 2025 supera gli 82 miliardi di dollari, in forte crescita rispetto ai circa 10 miliardi stimati nel 2020. Dentro questa dinamica, l’ultimo *report* mette in evidenza le *Chinese-language money laundering networks* (CMLNs - reti di riciclaggio di denaro di lingua cinese): nel 2025 avrebbero processato circa 16,1 miliardi di dollari, con un’operatività media indicativa di circa 44 milioni di dollari al giorno e oltre 1.799 *wallet* attivi, arrivando a rappresentare circa un quinto ($\approx 20\%$) dell’attività di riciclaggio illecito “nota” nel *dataset* di *Chainalysis*³⁶.

In ordine alla fenomenologia criminosa, invece, non sorgono difficoltà di sorta, pur nella consapevolezza del suo rapido evolvere. Diversi dati di matrice eurounitaria³⁷ documentano come l’utilizzo criminale delle *criptocurrencies* non sia affatto confinato ai reati informatici, ma si ricollegli a ogni tipologia di reato che abbia a che fare con la trasmissione di pagamenti.

Il paniere appare piuttosto ricco: si va dal traffico di droga, al traffico di esseri umani e di armi alla prostituzione, sino al commercio di materiale pedopornografico, all’usura e alle truffe *pig-*

³² Si tratta dei dati riportati nel *Crypto Crime Report 2024* di *Chainalysis*: cfr. relazione del Prof. Jacopo Della Torre (DOC. n. 247.1, p. 3) e del Gen.B. Gianluca Vitagliano (DOC. n. 287.1, p. 3 ss.) depositate in occasione delle rispettive audizioni del 17 ottobre 2024 e del 22 gennaio 2025, X Comitato.

³³ Cfr. The Chainalysis 2025 Crypto Crime Report, in <https://go.chainalysis.com/2025-Crypto-Crime-Report.html>.

³⁴ Tutti i dati di *Chainalysis* sono il frutto di una stima minima (“*lower bound*”), destinata tipicamente ad aumentare man mano che vengono scoperti e clusterizzati nuovi indirizzi collegati ad attività illegali.

³⁵ Cfr. The Chainalysis 2026 Crypto Crime Report, in <https://www.chainalysis.com/reports/crypto-crime-2026/>.

³⁶ I dati sono consultabili su <https://www.chainalysis.com/blog/2026-crypto-money-laundering/>.

³⁷ Cfr. 6th Annual SIRIUS EU Electronic Evidence Situation Report 2024, consultabile al seguente *link*: www.europol.europa.eu/cms/sites/default/files/documents/SIRIUS_E_Evidence_Situation_Report_2024.pdf, EU Innovation Hub (2024), First Report on Encryption by the EU Innovation Hub for Internal Security (Europol), reperibile su www.europol.europa.eu/publications-events/publications/first-report-encryption; Interpol Global Financial Fraud Assessment (2024), consultabile su www.interpol.int/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology; altresì, Report Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024, in <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024>; Europol Spotlight, Cryptocurrencies: tracing the evolution of criminal finances, in www.europol.europa.eu, 26 gennaio 2022.

*butchering*³⁸, *rug-pull*³⁹ o *pump and dump*⁴⁰, anche potenziate dall'uso dell'*AI*⁴¹; dal riscatto per condotte *cyber-estorsive* (*ransomware payments*) al *cryptojacking*⁴².

In generale, le criptovalute vengono ampiamente utilizzate come mezzo di pagamento nel *dark web*⁴³. Tale conclusione risulta suggerita già dal celebre caso *Silk Road*, cioè il primo *darknet market*, lanciato nel 2011, che, sino alla sua chiusura da parte del *FBI* nel 2013, gestiva i pagamenti (quantificabili in svariati miliardi di dollari) in Bitcoin. Guardando all'Europa, può altresì essere segnalato il sequestro di *Hydra* nel 2022 da parte delle autorità tedesche, un sito del *dark web* in lingua russa che gestiva il traffico di droga e offriva servizi di *mixing* – progettati per riciclare le criptovalute e renderle più difficili da rintracciare – e servizi di conversione (*cash-out*), che permettevano ai clienti di scambiare i proventi in criptovalute ottenute illegalmente con rubli russi. Si pensi, altresì, all'operazione *Darknet.drug*, eseguita dal Nucleo Speciale Tutela *Privacy* e Frodi Tecnologiche della Guardia di Finanza, che ha consentito il sequestro del *black market* considerato dagli acquirenti come il più importante a livello internazionale per quantità di oggetti in vendita, per

³⁸ Questo tipo di frode prende il nome dall'analogia con l'ingrasso dei maiali prima della macellazione, dove le vittime vengono "ingrassate" con false promesse di guadagni facili prima di essere derubate. Cfr. Interpol Global Financial Fraud Assessment (2024), consultabile su <https://www.interpol.int/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology>, p. 16.

³⁹ Nel *rug pull* gli sviluppatori di criptovalute emergenti attirano i primi investitori e poi abbandonano il progetto o portando via quanto raccolto o rivendendolo improvvisamente. Sul punto, cfr. la relazione del Gen.B. Mancazzo, depositata in occasione dell'audizione del 25 febbraio 2025, X Comitato, DOC. n. 316.1, p. 12: «[s]i tratta di una truffa perpetrata dagli ideatori di una criptovaluta, i quali, mantenendo la maggior parte della liquidità di tale *asset*, sono in grado di manipolare il mercato e di far crollare "a comando" il valore di quella moneta virtuale, impossessandosi in maniera fraudolenta dei fondi degli ignari acquirenti».

⁴⁰ Si tratta di una pratica fraudolenta in cui «i truffatori promuovono l'acquisto di azioni spesso a basso costo (note come *penny stock*), [...] prospettando guadagni rapidi e ingenti. [...] [G]li utenti - convinti della possibilità di ottenere lauti guadagni in tempi ridotti - iniziano ad acquistare le azioni, [...] con il risultato di far salire artificiosamente il prezzo del titolo (*pump*). Quando il valore raggiunge un livello elevato, i promotori di tale iniziativa vendono in massa le loro azioni, realizzando con ciò un lauto profitto; al tempo stesso, però, provocano un crollo improvviso del prezzo (*dump*), che lascia gli altri investitori con forti perdite»: cfr. Comunicazione Consob, Attenzione agli schemi di tipo "*pump&dump*" tramite social e app di messaggistica, 28 ottobre 2025, in <https://www.consob.it/web/area-pubblica/avvisi-ai-risparmiatori/ultime>.

⁴¹ Con riferimento alle "criptotruffe" potenziate dall'*AI*, cfr. la relazione del Gen.B. Mancazzo, depositata in occasione dell'audizione del 25 febbraio 2025, X Comitato, DOC. n. 316.1, p. 11: «la popolarità delle criptovalute è in costante aumento negli ultimi anni ma è parallelamente aumentato il numero delle truffe legate agli investimenti in valute virtuali, sempre sfruttando l'intelligenza artificiale per ingannare le vittime ignare, aspetto particolarmente insidioso un quanto estremamente difficile da riconoscere. I truffatori utilizzano l'*IA* per creare siti *web*, *account social*, video che sembrano autentici, risultando molto convincenti. [...] La consapevolezza dei rischi associati alle criptotruffe è fondamentale: si può affermare che "se qualcosa sembra troppo bello per essere vero, probabilmente è una truffa"».

⁴² È un tipo di crimine informatico in cui un criminale utilizza segretamente la potenza di calcolo della vittima (*computer* e dispositivi mobili) per generare criptovaluta. Ciò avviene per mezzo di *malware di cryptojacking* che funzionano da processi in *background* sottraendo risorse *hardware* a danno dell'utente.

⁴³ Come riportato nella relazione del Gen.B. Gianluca Vitagliano (cfr. DOC. n. 287.1, p. 2) «le criptovalute come Bitcoin, Monero, Litecoin, USDT rappresentano anche lo strumento privilegiato di pagamento per la compravendita di prodotti illegali presenti all'interno di "vetrine online" dei *marketplace* o *darkmarket*, in cui l'offerta è amplissima e riferibile alla vendita di stupefacenti, armi, farmaci, di banconote e documenti contraffatti, profili falsi e servizi illegali di ogni tipo». Cfr., altresì, Report Europol, Do criminals dream of electric sheep? How technology shapes the future of crime and law enforcement, 2019, in www.europol.europa.eu, p. 13.

la qualità dello stupefacente spedito (in particolare per la cocaina), per la puntualità delle spedizioni e per l'accuratezza del confezionamento⁴⁴.

Un ruolo prioritario è svolto, altresì, dai canali *Telegram*, utilizzati come vetrine *on-line* per attività illecite finanziate e ripagate in criptovalute. Mentre, infatti, l'accesso al *Dark Web* richiede l'utilizzo di *software* e motori di ricerca specifici, l'accesso alle piattaforme social – quali *Telegram* – è più diretto e più semplice⁴⁵.

Chiaramente, l'ambito illecito privilegiato resta pur sempre il *cyberlaundering*. L'*European Cybercrime Centre* (EC3) identifica le piattaforme decentralizzate quale mezzo privilegiato dalla criminalità per il riciclaggio⁴⁶.

La ragione è piuttosto intuibile e dipende – come già accennato – dalle caratteristiche intrinseche della *blockchain* (tracciabilità pseudo-anonima delle transazioni e assenza di intermediari finanziari tradizionali); viepiù considerando la possibilità di utilizzare servizi e tecnologie progettati specificamente per aumentare il grado di anonimato delle operazioni (si pensi al *money mule*, ai servizi *mixer/tumbler*, ai protocolli “*chain-cross bridge*”, etc. – sul punto, v. *infra*, parte II, sez. I, § 5.1.). Transazioni più rapide e immediate vuol dire, infatti, anche flussi finanziari più dispersi(vi) e immersi(vi), quando l'obiettivo è occultarne l'origine illecita.

Vale segnalare come le fasi di riciclaggio tramite criptovalute seguano un processo analogo a quello che caratterizza il denaro contante, che comprende «piazzamento, stratificazione e integrazione». Nella prima, i proventi illeciti vengono introdotti nel sistema *blockchain* tramite piattaforme di scambio (*exchange*) o strumenti specifici come gli ATM per cripto-attività. Successivamente, vengono utilizzate tecniche di offuscamento per rendere ancora più difficile risalire all'origine dei fondi (come detto, *mixer*, schemi “*chain-hopping*”, etc.). Infine, nella fase di integrazione, le criptovalute vengono convertite in moneta tradizionale o utilizzate per acquistare beni di valore, reinserendo così i fondi nel circuito economico legale⁴⁷.

⁴⁴ Cfr. relazione del Gen.B. Mancazzo, depositata in occasione dell'audizione del 25 febbraio 2025, X Comitato, DOC. n. 316.1, p. 8.

⁴⁵ Il Gen.B. Gianluca Vitagliano segnala nella sua relazione che «una recente attività che ha permesso di arrestare un soggetto cinese, gravemente indiziato dei delitti di esercizio abusivo di attività finanziaria e riciclaggio, attraverso l'acquisto di criptovalute. Nel corso dell'indagine è emerso che il soggetto proponeva lo scambio di grandi somme di contante in cambio di criptovalute definendosi un “Bancomobile Decentralizzato disponibile 24 ore su 24”, capace di eseguire scambi anche per oltre 100.000 euro per singola transazione. In circa tre anni l'indagato ha movimentato la somma di 8.800.000,00 euro, con un numero di operazioni e scambi superiore a 3000, percependo una commissione per ogni transazione compresa tra il 5% e il 10%. Nel corso dell'esecuzione della misura, sono state sequestrate criptovalute per un importo pari a circa 600.000,00 euro» (cfr. DOC. n. 287.1, p. 7).

⁴⁶ Cfr. Report Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024, in <https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024>.

⁴⁷ Cfr. relazione del Dott. Gianfranco Torriero, depositata in occasione della sua audizione del 25 febbraio 2025, X Comitato, DOC. n. 315.1, p. 8.

3. Stato dell'arte normativo.

Nel corso delle audizioni è stato dedicato ampio spazio alla ricostruzione dell'assetto normativo – domestico e sovranazionale – oggi vigente.

Si tratta di una regolamentazione “a macchia di leopardo”, in cui si intrecciano disposizioni, linee guida e raccomandazioni in tema di antiriciclaggio, di regolamentazione finanziaria e – con le precisazioni che seguiranno – in punto di *asset-recovery*.

Ci si potrebbe limitare a riportare, per ogni settore, il quadrante normativo di riferimento. Preme tuttavia evidenziare sin da subito quelli che sono i nodi problematici.

Guardando al fronte eurounitario, se «molte norme sono ormai entrate in vigore per arginare l'uso illecito delle cripto-attività [...]», rimangono ad oggi due ostacoli: la natura transfrontaliera delle tecnologie utilizzate, cui si associa una regolamentazione attualmente asimmetrica (più severa a livello unionale rispetto ad altre giurisdizioni); la circostanza che le normative che regolano il settore siano entrate in vigore solo di recente [...]»⁴⁸. Riguardo al primo ostacolo segnalato, è stato evidenziato uno degli attuali problemi operativi che di fatto compromette il buon esito di un'indagine penale: la mancata collaborazione degli *exchanges* con le forze di polizia. Peraltro – è stato osservato –, i *server* di tali piattaforme sono per la maggior parte collocati al di fuori degli Stati membri dell'Unione Europea: si stima che esistano oltre 300 *exchange* attivi a livello globale, con i più grandi operanti principalmente negli Stati Uniti, in Asia e in altri Paesi. Questo significa che la collaborazione con quelli *extra* UE, in caso di indagini, risulta estremamente difficoltosa⁴⁹, anche a causa dei tempi delle rogatorie internazionali⁵⁰.

Volgendo, invece, lo sguardo all'ordinamento interno si deve constatare uno *status quo* più preoccupante: spicca certamente una normativa antiriciclaggio (quindi, di tipo sostanziale), contiamo presidi in ambito finanziario e anche una regolamentazione fiscale, ma manca del tutto una disciplina processualpenalistica adeguata a contrastare i crimini connessi alle cripto-attività⁵¹.

Come è stato sottolineato, infatti, «la disciplina del nostro codice di rito che riguarda l'attività investigativa ad alto contenuto tecnologico è figlia, sostanzialmente, delle scelte legislative del 2008»⁵², eccezion fatta per la normativa sulle intercettazioni che è stata più volte rivista e interpolata

⁴⁸ In questi termini si esprime il Dott. Gianfranco Torriero nel corpo della sua relazione: cfr. DOC. n. 315.1, p. 7.

⁴⁹ Cfr. relazione del Gen.B. Gianluca Vitagliano, DOC. n. 287.1, p. 18.

⁵⁰ Cfr. relazione del Dott. Gianfranco Torriero, DOC. n. 315.1, p. 15.

⁵¹ Cfr. Prof. Jacopo Della Torre (audizione del 17 ottobre 2024, X Comitato), e Dott.ssa Agnese Del Giudice (audizione del 14 novembre 2024, X Comitato).

⁵² Cfr. il resoconto stenografico dell'audizione della Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato, p. 6, la quale prosegue sottolineando che «In quell'occasione, peraltro, il legislatore si è limitato ad adeguare gli strumenti esistenti, prevedendo che il pubblico ministero e la polizia giudiziaria assicurassero soltanto quelle modalità tecniche idonee a garantire genuinità e integrità del dato informatico raccolto».

nel corso degli anni; quest'ultima, tuttavia, appare tuttora deficitaria, sol si pensi che la «disciplina del captatore [...] è [ancora] limitata ad una sola delle sue funzionalità [pur essendo un fenomeno conosciuto] all'ordinamento da più di un trentennio»⁵³.

Non solo. Non disponiamo di una disciplina adatta per sequestrare e confiscare le criptovalute (v. *infra*, parte II, sez. I, § 3.3.1.).

Al riguardo, merita essere evidenziato come la stessa Direttiva 2024/1260/UE, introdotta per potenziare, a livello unionale, la disciplina di *asset recovery* – ossia di tracciamento, identificazione, congelamento, confisca e destinazione dei beni – di tutti i Paesi membri, in punto di cripto-attività «si è limitata a una manifestazione di intenti [...] le istituzioni europee ci dicono che nella definizione di bene noi dobbiamo includere le cripto-attività e, quindi, anche le criptovalute, ma gli strumenti che abbiamo a disposizione perdono la loro consueta efficacia dinanzi a questo fenomeno»⁵⁴ che combina in sé le potenzialità della finanza decentralizzata (la quale coinvolge una miriade di soggetti, di infrastrutture e di servizi in tutto il globo) e dematerializzata, della crittografia asimmetrica e dei servizi offuscamento. Il pacchetto europeo di nuovo conio non adegua l'odierno assetto normativo alla crescente digitalizzazione della ricchezza illecita (v. *infra*, parte II, sez. I, § 3.3.2.).

Pertanto, pur apprezzando lo sforzo profuso dalle istituzioni europee, appare piuttosto chiaro che solo l'elaborazione di una disciplina comune e adeguata al fenomeno potrà arginare la diffusione di “paradisi normativi” e privare la criminalità del vantaggio derivante dall'apolidia della criptovaluta. Se così stanno le cose, è abbastanza intuitivo che il paniere della regolamentazione ben può ancora essere arricchito. È con questa consapevolezza che deve leggersi quanto di seguito elencato sulla disciplina già in vigore, per non cedere alla rassicurante – ma illusoria – idea che vi sia già una copertura giuridica performante.

3.1. La disciplina antiriciclaggio.

3.1.1. Il quadro sovranazionale.

La lotta contro il riciclaggio di denaro attraverso le cripto-attività ha mosso i primi passi concreti a livello internazionale grazie al lavoro del *Financial Action Task Force* (GAFI-FATF).

⁵³ Cfr. resoconto stenografico della seduta del 14 novembre 2024, X Comitato, audizione della Dott.ssa Agnese Del Giudice, p. 6.

⁵⁴ Così, la Dott.ssa Agnese Del Giudice nel corso della sua audizione del 14 novembre 2024, X Comitato (cfr. resoconto stenografico della seduta, p. 7).

Quest'organismo⁵⁵ ha rivestito un ruolo fondamentale nell'elaborare le prime linee guida per introdurre presidi sul settore delle cripto-attività. Tali raccomandazioni, aggiornate nel corso degli anni, pur trattandosi di atti aventi natura non vincolante (*soft law*), hanno rappresentato, sin dal principio, il “modello” seguito dal legislatore europeo nell'approntare una regolamentazione della materia.

Il GAFI ha elaborato un primo *report* sulle *virtual currencies* già nel 2014, seguito da una *guidance* nel 2015⁵⁶. Con essi è stata inaugurata una prima fase di reazione sovranazionale nei confronti dell'uso illecito delle criptovalute incentrata sull'obiettivo di intercettare i punti di contatto in “entrata” e in “uscita” del mercato in esame.

Un passaggio cruciale si è avuto, però, nell'ottobre 2018, quando il GAFI ha aggiornato la Raccomandazione 15 al fine di consolidare e rendere espressamente applicabile, nel contesto delle nuove tecnologie, l'approccio regolatorio fondato sul rischio (*risk-based approach*)⁵⁷. Le attività in criptovalute vengono trattate come un'area “a rischio” da gestire con regole AML/CFT (antiriciclaggio e contrasto al finanziamento del terrorismo), non come un settore “fuori perimetro”. L'intento dichiarato era quello di chiarire l'applicazione della normativa antiriciclaggio nell'ambiente dei *virtual assets*, delle attività finanziarie concernenti tali *assets* e dei *Virtual Assets Service Providers* (VASP). In ragione di tanto, gli Stati sono stati chiamati a valutare i rischi legati a *crypto-asset* e servizi collegati e a introdurre norme e controlli coerenti. Gli operatori del settore, ossia i *virtual asset service providers* (VASPs) – *exchange*, piattaforme di scambio, *custodian wallet* e altri fornitori di servizi su *crypto* – diventano, così, “entità obbligate”: i Paesi devono assicurare che essi siano assoggettati a disciplina AML/CFT (che richiede l'identificazione/verifica del cliente - KYC, il monitoraggio delle operazioni, la segnalazione di attività sospette e altre misure proporzionate al rischio), registrati e sottoposti a monitoraggio/supervisione efficace per la conformità agli *standard* FATF.

Il GAFI, intercettando la profonda evoluzione che ha interessato il mercato delle cripto-attività a seguito della nascita delle migliaia di criptovalute alternative al *Bitcoin* (*altcoins*), ha inaugurato una

⁵⁵ Il Gruppo di Azione Finanziaria Internazionale (GAFI) costituisce la principale organizzazione intergovernativa che si occupa di sviluppare *standard* globali in materia di integrità finanziaria, contrasto al riciclaggio, al finanziamento al terrorismo e alla proliferazione di armi di distruzione di massa.

⁵⁶ Cfr. FATF (2014), Report Virtual Currencies Key Definitions and Potential AML/CFT Risks, Paris, consultabile al seguente link: <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, FATF (2015), Guidance for a Risk-Based Approach to Virtual Currencies, Paris, consultabile su <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-RBA-Virtual-Currencies.pdf.coredownload.inline.pdf>.

⁵⁷ Cfr. FATF (2018), Report to the G20 Finance Ministers and Central Bank Governors, Paris, in <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/FATF-Report-G20-FM-CBG-July-2018.pdf>, FATF (2019), Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, Paris, consultabile su <https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Italian-Guidance-RBA-VA-VASP.pdf.coredownload.inline.pdf>.

regolazione non più limitata ai punti di entrata e di uscita, ma estesa anche agli scambi che avvengono all'interno del mercato *crypto*.

Tuttavia, come emerge dai dati, riferiti al 2024, riportati nella relazione ABI, il livello di conformità internazionale alle raccomandazioni del GAFI⁵⁸ risulta ancora largamente insufficiente. Ben il 75% delle giurisdizioni monitorate – vale a dire 97 su 130 – risulta parzialmente o totalmente non conforme alla Raccomandazione 15. Il 29% delle giurisdizioni non ha ancora effettuato alcuna valutazione dei rischi legati alle crypto-attività, mentre il 27% non ha neppure deciso se e come regolamentare il settore. Particolarmente significativo è il dato relativo all'enforcement: solo il 26% delle giurisdizioni che hanno adottato normativa sulla travel rule ha effettivamente intrapreso azioni di applicazione coattiva delle disposizioni⁵⁹.

Il primo intervento organico del legislatore comunitario è avvenuto con la V Direttiva Antiriciclaggio (Direttiva 2018/843/UE, recepita in Italia dal d.lgs. 4 ottobre 2019, n. 125), la quale ha segnato una svolta decisiva includendo, per la prima volta, tra i soggetti obbligati agli adempimenti antiriciclaggio, gli operatori che offrono servizi connessi alle crypto-attività⁶⁰.

Il provvedimento europeo, dopo aver riportato la definizione di *virtual currencies* – «rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente» (art. 3, § 18) – ha esteso l'ambito soggettivo della normativa ai prestatori di servizi relativi a valute virtuali (VASP), ossia agli *exchanges* – piattaforme di scambio tra valute *fiat* e criptovalute o tra diverse criptovalute – e ai fornitori di servizi di custodia di *wallet* digitali (art. 3, § 5), sottoponendoli, quindi, all'obbligo di effettuare una corretta verifica della clientela (KYC - *Know Your Customer*), calibrata in base al livello di rischio di riciclaggio di denaro o di finanziamento del terrorismo (artt. 17-19). I VASP hanno l'obbligo di conservare i dati per 10 anni (art. 31) e segnalare, attraverso la UIF (Unità di Informazione Finanziarie), tutti i soggetti sui quali ci siano motivi ragionevoli per sospettare che siano in corso o che siano state compiute operazioni di riciclaggio o di finanziamento del terrorismo o connessi ad attività criminosa (art. 35)⁶¹.

Come osservato, questa prima fase normativa si è concentrata sulla necessità di individuare nuovi intermediari nel sistema delle crypto-attività. Venuta meno la centralità delle banche tradizionali nel

⁵⁸ Cfr., da ultimo, FATF (2025), *Asset Recovery Guidance and Best Practices*, FATF, Paris, in https://www.dt.mef.gov.it/export/sites/sitodt/modules/documenti_it/prevenzione_reati_finanziari/prevenzione_reati_finanziari/Asset-Recovery-Guidance-Best-Practices.EN.pdf.

⁵⁹ Cfr. relazione del Dott. Gianfranco Torriero, depositata in occasione della sua audizione del 25 febbraio 2025, X Comitato, DOC. n. 315.1, pp. 11 ss. e p. 14.

⁶⁰ Cfr. relazione del Dott. Gianfranco Torriero, DOC. n. 315.1, p. 11.

⁶¹ Cfr. relazione del Gen.B. Gianluca Vitagliano, DOC. n. 287.1, p. 8.

processo di intermediazione finanziaria – aspetto che costituiva il nucleo dell’attrattività delle criptovalute per scopi illeciti – il legislatore ha cercato di ricostruire i presidi antiriciclaggio identificando negli scambiatori di valute i nuovi soggetti obbligati, pur nella consapevolezza (Considerando n. 9) di non risolvere completamente il problema dell’anonimato delle operazioni in valuta virtuale, posto che gli utenti possono effettuare operazioni anche senza ricorrere a tali prestatori.

L’evoluzione della normativa europea, e conseguentemente quella nazionale, ha conosciuto, da questo momento, uno sviluppo costante e progressivo.

La prima tappa coincide con l’approvazione del Regolamento (UE) 2023/1113, noto come *Transfer of Funds Regulation* (TFR) o “Regolamento sulla *Travel Rule*”, che ha trovato applicazione a partire dal 30 dicembre 2024 (recepito in Italia dal d.lgs. 27 dicembre 2024, n. 204).

Esso introduce requisiti specifici per i trasferimenti di cripto-attività, differenziati in base all’importo della transazione e alla natura del *wallet* utilizzato. L’obiettivo dichiarato è quello di combattere il riciclaggio di denaro assicurando l’applicazione uniforme nel territorio unionale delle raccomandazioni del *Financial Action Task Force* (FATF), in particolare l’obbligo per i prestatori di servizi di includere informazioni sull’ordinante e sul beneficiario nei trasferimenti (c.d. “*Travel Rule*”)⁶².

Per i CASP (*Crypto-Asset Service Providers*) si introduce l’obbligo di raccogliere e rendere disponibili alle autorità competenti i dati relativi a cedenti e cessionari dei trasferimenti di cripto-attività di cui sono parte. Queste informazioni potranno essere utilizzate da forze dell’ordine, Unità di Informazione Finanziaria (UIF) e istituzioni finanziarie per individuare e segnalare transazioni sospette (AML). In particolare, le regole prevedono che i CASP identifichino i propri utenti e segnalino transazioni di valore superiore a 1.000 euro, anche per operazioni occasionali.

Sebbene le disposizioni non si applichino ai trasferimenti diretti tra persone (P2P)⁶³, particolare articolare attenzione è dedicata ai trasferimenti che coinvolgono fornitori CASP e i *wallet* gestiti autonomamente dall’utente (c.d. “*unhosted wallet*” o “*wallet non-custodial*”, definito anche, nel contesto normativo europeo, indirizzo auto-ospitati o *self-hosted addresses*), quindi non collegati a CASP o soggetti equivalenti. Ogni volta che un CASP è coinvolto in un trasferimento di importo superiore a 1.000 euro verso un indirizzo auto-ospitato, il fornitore dei servizi deve adottare misure

⁶² Cfr. relazione del Dott. Gianfranco Torriero, DOC. n. 315.1, p. 12.

⁶³ Nondimeno, 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.

adeguate a valutare se quell'indirizzo è posseduto o controllato dal proprio cliente. Per i trasferimenti di importi inferiori, i CASP non sono tenuti a richiedere tali informazioni⁶⁴.

Così facendo, si è evidentemente cercato di mitigare, almeno in parte, il rischio che portafogli digitali di questo tipo si trasformino in uno strumento utile per aggirare l'insieme dei presidi antiriciclaggio. Il provvedimento europeo si distingue, altresì, per avere esplicitamente invitato l'Autorità Bancaria Europea (EBA) a emanare *Guidelines* sulle politiche, le procedure e i controlli interni per garantire l'attuazione delle misure restrittive dell'Unione e nazionali quando si eseguono trasferimenti di fondi e crypto-attività ai sensi del regolamento medesimo (art. 19, § 4)⁶⁵.

Attualmente, le *Travel Rule Guidelines* (EBA/GL/2024/11) sono state affiancate dalle *ML/TF Risk Factors Guidelines* (EBA/GL/2024/01) sulle valutazioni dei fattori di rischio di riciclaggio e finanziamento del terrorismo (ML/TF) per includere indicazioni specifiche sui *crypto-asset* e sui fornitori dei relativi servizi (CASP)⁶⁶. In particolare, l'EBA individua quali fattori di rischio legati ai *crypto-asset*: a) i trasferimenti da *wallet* auto-ospitati; b) l'impiego di tecnologie che aumentano l'anonimato (*mixer, tumblers, privacy features*); c) i canali di scambio decentralizzati; d) il fatto che il beneficiario dell'operazione si collochi in una giurisdizione ad altro rischio; e) l'impiego di crypto-ATM; f) l'impiego dei cosiddetti ponti tra diverse *blockchain*; f) l'impiego di criptovalute incentrate sulla *privacy*.

Il passaggio più significativo del processo di perfezionamento della disciplina si è avuto con l'adozione del pacchetto legislativo sull'antiriciclaggio (*AML Package*), approvato il 24 aprile 2024 e pubblicato nella Gazzetta Ufficiale dell'Unione Europea il 19 giugno 2024.

Questo intervento, destinato ad entrare in vigore progressivamente tra il 2025 e il 2027, introduce importanti innovazioni specificamente rivolte al settore delle crypto-attività e si articola in tre provvedimenti fondamentali:

1) la VI Direttiva Antiriciclaggio (Direttiva 2024/1640/UE, nota anche come Direttiva AML), la quale introduce regole aggiornate sulla valutazione dei rischi nazionali e sovranazionali AML/CFT, rafforza la cooperazione all'interno dei collegi di supervisione e con gli omologhi di paesi terzi e

⁶⁴ Cfr. relazione del Gen.B. Gianluca Vitagliano, DOC. n. 287.1, pp. 12-13.

⁶⁵ Cfr. EBA/GL/2024/11, *Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113* (note come "*Travel Rule Guidelines*"), 4 luglio 2024, in <https://www.eba.europa.eu/sites/default/files/2024-07/6de6e9b9-0ed9-49cd-985d-c0834b5b4356/Travel%20Rule%20Guidelines.pdf>.

⁶⁶ EBA/GL/2024/01, *Final Amending Guidelines on ML/TF Risk Factors* che modifica le linee guida esistenti EBA/GL/2021/02. L'adozione delle EBA/GL/2024/01 è una conseguenza indiretta del mandato attribuito all'EBA dall'art. 19, § 4, del Regolamento (UE) 2023/1113 e si inserisce nel più ampio aggiornamento del quadro AML/CFT volto a includere i fornitori di servizi su *crypto-asset*, mediante modifica delle precedenti EBA/GL/2021/02. Le linee guida sono consultabili al seguente link: <https://www.eba.europa.eu/sites/default/files/2024-01/a3e89f4f-fbf3-4bd6-9e07-35f3243555b3/Final%20Amending%20%20Guidelines%20on%20MLTF%20Risk%20Factors.pdf>.

interviene sulla trasparenza della «titolarità effettiva». Le disposizioni dovranno essere recepite dagli Stati membri entro il 2027, con scadenze anticipate per alcune misure, come il registro dei titolari effettivi previsto per il 2026⁶⁷;

2) il Regolamento “*single rulebook*” (UE 2024/1624), che stabilisce norme uniformi a livello europeo sull’identificazione dei clienti, sulla trasparenza relativa ai titolari effettivi e sulle limitazioni agli strumenti anonimi, inclusi i *cripto-asset*⁶⁸.

Già dai considerando iniziali il provvedimento europeo auspica una “gestione” globale del rischio AML/CFT (*Anti-Money Laundering e Countering the Financing of Terrorism*) associato alle cripto-attività. Il Considerando n. 7 rileva, infatti, come «la tecnologia continua a evolversi, offrendo al settore privato l’opportunità di sviluppare nuovi prodotti e sistemi per scambiare fondi o valore. Tale fenomeno, seppur positivo, può generare nuovi rischi di riciclaggio e finanziamento del terrorismo, in quanto i criminali riescono continuamente a trovare modi per sfruttare le vulnerabilità al fine di occultare e trasferire fondi illeciti in ogni parte del mondo. I fornitori di servizi per le criptoattività e le piattaforme di *crowdfunding* sono esposti all’uso improprio di nuovi canali per la circolazione di denaro illecito e si trovano nella posizione ideale per individuare tali movimenti e mitigare i rischi. L’ambito di applicazione della legislazione dell’Unione dovrebbe pertanto essere esteso a tali soggetti, in linea con le norme del FATF/GAFI in materia di cripto-attività [...]».

Di particolare rilievo è il divieto espresso sull’uso dei conti anonimi e delle cripto-attività incentrate sull’anonimato (art. 79, § 1): «i conti di cripto-attività anonimi e altri strumenti anonimizzanti non consentono la tracciabilità dei trasferimenti di cripto-attività, e rendono difficile l’individuazione di operazioni collegate che potrebbero destare sospetti o l’applicazione di un livello appropriato di adeguata verifica della clientela. Al fine di garantire l’efficace applicazione degli obblighi in materia di AML/CFT alle cripto-attività, è necessario 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, anche attraverso monete incentrate sull’anonimato» (Considerando n. 160)⁶⁹. Come pure è stato evidenziato⁷⁰, il divieto sull’uso della *privacy coin* come Monero o Zcash – non era mai stato formulato in termini così perentori, né dal MiCAR-*Markets in Crypto-Assets Regulation*, né dal TFR-*Transfer of Funds Regulation* (v. *infra*).

Tra le svariate previsioni innovative per il settore in esame, spiccano, quindi: a) la scelta di obbligare i prestatori di servizi per le cripto-attività ad applicare misure di adeguata verifica della clientela

⁶⁷ Cfr. relazione del Gen.B. Gianluca Vitagliano, DOC. n. 287.1, p. 14.

⁶⁸ Cfr. relazione del Gen.B. Gianluca Vitagliano, DOC. n. 287.1, p. 15.

⁶⁹ Cfr. relazione del Dott. Gianfranco Torriero, DOC. n. 315.1, pp. 13-14.

⁷⁰ Cfr. resoconto stenografico della seduta del 22 gennaio 2025, X Comitato, audizione del Gen.B. Gianluca Vitagliano, p. 13.

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 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 (ad esempio, *wallet* con *mixer* integrati, come il celebre “*Wasabi Wallet*”), anche attraverso monete incentrate sull'anonimato (art. 79)⁷¹;

3) il terzo pilastro del pacchetto AML è costituito dal Regolamento UE 2024/1620, che istituisce l'AMLA (*Anti-Money Laundering Authority*), la nuova Autorità europea antiriciclaggio con sede a Francoforte, destinata a divenire operativa dal 2025. L'AMLA avrà il compito di supervisionare direttamente gli enti finanziari ad alto rischio e indirettamente quelli sottoposti ai supervisori nazionali, garantendo l'armonizzazione delle prassi AML/CFT; potrà, inoltre, imporre sanzioni in caso di violazioni gravi e supporterà anche il settore non finanziario.

All'AMLA è affidato un ruolo centrale nell'emanazione delle metodologie di intercettazione dei rischi AML e nella conduzione delle analisi dei rischi dell'Unione europea. In particolare, l'Autorità dovrà emanare orientamenti per specificare i criteri e gli elementi di cui i prestatori di servizi per le cripto-attività devono tenere conto per condurre la valutazione sulle misure da adottare in caso di rapporti di corrispondenza transfrontalieri con soggetti non stabiliti nell'Unione⁷².

3.1.2. Il fronte interno

L'ordinamento domestico ha recepito la V Direttiva Antiriciclaggio con il d.lgs. 4 ottobre 2019, n. 125, che ha introdotto, nel corpo del d.lgs. 21 novembre 2007, n. 231, apposite misure per prevenire il riciclaggio connesso all'impiego di valute virtuali.

Il nostro legislatore, invero, aveva già apportato modifiche in questa direzione con il d.lgs. 25 maggio 2017, n. 90 (di attuazione della IV Direttiva Antiriciclaggio UE 2015/849), introducendo la definizione di valuta virtuale ed inserendo, tra i soggetti destinatari degli obblighi di prevenzione, anche i prestatori di servizi “di conversione di valute virtuali da ovvero in valute aventi corso forzoso” (gli *exchanges* - art. 3, comma 5, lett. i, d.lgs. n. 231/2007).

Il d.lgs. n. 125/2019 non si è limitato ad intervenire sul concetto di “valuta virtuale” – definita dall'art.1, comma 2, lett. qq, d.lgs. n. 231/2007, in seguito alle modifiche apportate, come «la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'Autorità

⁷¹ Cfr. relazione del Prof. Jacopo Della Torre, DOC. n. 247.1, p. 9.

⁷² Cfr. relazione del Dott. Gianfranco Torriero, DOC. n. 315.1, p. 16.

pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente» –, ma ha anche lodevolmente esteso gli obblighi in esame ai «prestatori di servizi di portafoglio digitale» (i *wallet provider* - art. 1, comma 2, lett. ff-*bis*, d.lgs. n. 231/2007) e 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» (art. 1, comma 2, lett. ff, d.lgs. n. 231/2007)⁷³.

Con queste modifiche il legislatore nazionale ha colmato le lacune di tutela presenti nella precedente disciplina, che di fatto consentiva una verifica ai fini antiriciclaggio solo in fase di conversione delle valute virtuali in moneta fisica, lasciando esenti dalla collaborazione i soggetti che ne consentivano la detenzione e la movimentazione come tali. Inizialmente, invero, le strategie di contrasto si basavano sull'idea che, prima o poi, data la scarsa utilizzabilità delle cripto-attività nel vivere quotidiano, i criminali le avrebbero scambiate per denaro avente corso legale.

Il decreto del Ministero dell'Economia e delle Finanze del 13 gennaio 2022 (G.U. n. 40 del 17 febbraio 2022), in attuazione del d.lgs. n. 125/2019, ha stabilito, da un lato, che i *wallet providers* e gli *exchanges* debbano iscriversi in una sezione speciale del registro dei cambiavalute presso l'Organismo Agenti e Mediatori (OAM) per poter operare sul territorio nazionale. È previsto che siano tenuti a fornire: a) informazioni anagrafiche; b) dettagli sui servizi offerti, compresi sportelli automatici ATM e indirizzi *web*; c) le modalità di erogazione dei servizi, inclusi gli indirizzi fisici e digitali; d) trimestralmente, i dati relativi alle loro transazioni. La sanzione per gli operatori inadempienti prevede la sospensione o la cancellazione dal registro, mentre l'esercizio abusivo dell'attività è soggetto a sanzioni pecuniarie comprese tra 2.065 e 10.329 euro.

Secondo l'analisi dell'OAM, nel primo trimestre del 2024 in Italia, ben 1,3 milioni di persone detenevano cripto-attività presso VASP, per un controvalore complessivo di 2,7 miliardi di euro, con una crescita dell'85% rispetto al quarto trimestre del 2023.

Tuttavia, è stata evidenziata una criticità significativa: i VASP inviano all'OAM i dati delle transazioni in forma aggregata, creando forti limitazioni e rallentamenti alle analisi investigative⁷⁴.

Con il d.lgs. 27 dicembre 2024, n. 204, il legislatore ha recepito le disposizioni del Regolamento UE 2023/1113 (TFR), modificando la normativa italiana antiriciclaggio contenuta nel d.lgs. n. 231/2007. Uno dei punti principali del decreto è dato dall'obbligo per i CASP di identificare sia il cedente che il cessionario delle cripto-attività, compresi i rispettivi titolari effettivi, anche nel caso in cui il

⁷³ Cfr. relazione del Prof. Jacopo Della Torre, DOC. n. 247.1, p. 7.

⁷⁴ Cfr. relazione del Gen.B. Gianluca Vitagliano, DOC. n. 287.1, pp. 8-9.

trasferimento avvenga tramite indirizzi auto-ospitati. Il provvedimento attuativo introduce nel tessuto normativo d.lgs. n. 231/2007 il nuovo art. 16-*bis*, che impone ai prestatori di servizi per le cripto-attività l'obbligo di individuare e valutare i rischi di riciclaggio e finanziamento del terrorismo associati ai trasferimenti diretti a o provenienti da indirizzi auto-ospitati.

Altra importante novità è rappresentata dall'innesto, sempre nella trama del d.lgs. n. 231/2007, del nuovo art. 25-*bis*, che disciplina gli obblighi di adeguata verifica rafforzata della clientela nei rapporti di corrispondenza transfrontalieri che prevedono servizi per le cripto-attività. I prestatori di servizi devono verificare che l'intermediario corrispondente sia autorizzato a operare nel settore, sia soggetto alla vigilanza delle autorità competenti e adotti controlli antiriciclaggio adeguati. Prima di aprire nuovi conti o instaurare rapporti economici, è necessario ottenere le opportune autorizzazioni interne e formalizzare un accordo scritto che disciplini i reciproci obblighi⁷⁵.

3.2. La normativa finanziaria.

3.2.1. Il regolamento 2023/1114/UE (MiCAR).

Il legislatore europeo ha cercato di creare un quadro normativo specifico e armonizzato per i mercati delle cripto-attività adottando il 31 maggio 2023 il Regolamento (UE) 2023/1114, noto come *Markets in Crypto-Assets Regulation* (MiCAR), entrato integralmente in vigore il 30 dicembre 2024.

Questo regolamento rappresenta il primo tentativo organico a livello mondiale di disciplinare in modo completo il settore delle cripto-attività e dei relativi servizi.

Invero, la stessa sensibilità dimostrata dal legislatore europeo – e domestico – in ordine al *money laundering* e al finanziamento del terrorismo (documentata anche dalla recente approvazione del nuovo *AML Package*), non era stata finora manifestata riguardo alle modalità di emissione, offerta al pubblico, negoziazione e prestazione di servizi per le cripto-attività. Il vuoto normativo risultava intollerabile, dato l'enorme flusso di *asset* virtuali scambiati ogni giorno e l'inarrestabile capacità dei *bad actors* di aggirare i presidi di tutela antiriciclaggio. Lungo questa china si collocano anche i fallimenti di *exchanges* come FTX o di *stablecoins* come “Terra Luna”, i quali hanno causato perdite su scala globale per miliardi di dollari, minacciando, così, a cascata, la stabilità dell'intero mercato finanziario⁷⁶.

Le finalità perseguite dal MiCAR sono chiare: introdurre una disciplina uniforme per favorire lo sviluppo della finanza digitale, in modo conforme a una concorrenza leale e, al contempo, proteggere i detentori di *crypto-assets*.

⁷⁵ Cfr. relazione del Gen.B. Gianluca Vitagliano, DOC. n. 287.1, pp. 13-14.

⁷⁶ Cfr. relazione del Prof. Jacopo Della Torre, DOC. n. 247.1, p. 8.

Il MiCAR definisce, anzitutto, le cripto-attività come «una rappresentazione digitale di valore o diritti trasferibili o archiviabili elettronicamente tramite tecnologie basate su registri distribuiti (DLT) o tecnologie simili» (art. 3).

Disciplina, poi, l'emissione, l'offerta e la negoziazione di tre categorie specifiche di cripto-attività. Si tratta dei *token* collegati ad attività (ART – *Asset-Referenced Tokens*; art. 3 § 1, n. 6), i *token* di moneta elettronica (EMT – *E-Money Tokens*; art. 3, § 1, n. 7) e *token* diversi – c.d. “*other than*” – da ART e EMT (art. 3, § 1, n. 9), quali, ad esempio, gli *utility token*, ossia strumenti destinati unicamente a fornire l'accesso a un bene o a un servizio prestato dal suo emittente⁷⁷.

Sono esclusi dal perimetro del MiCAR i servizi offerti in modo completamente decentralizzato. L'affermazione è suggerita da vari argomenti.

In effetti, pur rientrando nell'ampia definizione di cripto-attività e potendo astrattamente assolvere a funzioni di pagamento o di investimento (*payment tokens*), le criptovalute non paiono incasellabili in nessuna delle categorie richiamate dal Regolamento (EMT, ART e *other than*). Esse, invero, da un lato, non sono ancorate ad alcun bene o moneta ufficiale di riferimento (*unbacked crypto-asset*), sicché non possono essere ricondotte nella categoria delle *stablecoins*, e, dall'altro, non possono essere assimilate neppure agli *utility tokens*, non assolvendo a una funzione di utilità o di godimento. Peraltro, come è stato evidenziato⁷⁸, all'applicabilità del Regolamento osterebbe lo stesso dato letterale.

In sostanza, l'impianto del MiCAR, quanto al segmento dell'emissione e dell'offerta al pubblico, è strutturalmente costruito attorno alla figura dell'emittente e agli obblighi di trasparenza (*in primis* il *white paper*) imputabili a un soggetto determinato. Le criptovalute *permissionless* (Bitcoin, Ethereum, Monero, Z-Cash, etc.), in quanto decentralizzate, sono prive di un emittente identificabile e di un centro di imputazione giuridica delle dichiarazioni e delle condotte tipiche dell'offerta; ciò rende inapplicabili, in via ordinaria, le disposizioni che presuppongono un *issuer/offeror*, non già perché l'*asset* sia ontologicamente estraneo al perimetro normativo, ma perché difetta il presupposto soggettivo di imputazione che consente al Regolamento di operare sul versante “primario” dell'emissione. Ciò non significa, tuttavia, che il fenomeno resti privo di presidio normativo. Al contrario, l'intervento regolatorio si sposta dal piano dell'oggetto (Bitcoin, Ethereum, Monero, etc.) a quello dei soggetti che ne rendono possibile la circolazione economica (i CASP), privilegiando,

⁷⁷ Cfr. relazione del Gen.B. Gianluca Vitagliano, DOC. n. 287.1, p. 10.

⁷⁸ Cfr. resoconto stenografico della seduta del 14 novembre 2024, X Comitato, audizione della Dott.ssa Agnese Del Giudice, p. 7. Ci si riferisce all'art. 4, § 3, lett. b del Regolamento – che fa riferimento all'attività di *mining* – e al Considerando n. 22. Nello stesso senso, v. relazione del Gen.B. Gianluca Vitagliano, DOC. n. 287.1, p. 12.

dunque, la supervisione dei *gatekeeper* rispetto alla pretesa, di fatto impraticabile, di regolamentare direttamente un'infrastruttura tecnologica decentralizzata.

Il MiCAR ha previsto, infatti, che i *Crypto-Assets Service Providers* (CASP), ossia i fornitori di servizi relativi alle cripto-attività (art. 3, § 1, n. 15), siano sottoposti a un rigoroso regime autorizzativo e di controllo che impone il rispetto di plurimi requisiti organizzativi, professionali e di onorabilità (primo fra tutti la mancata condanna per reati nell'ambito del riciclaggio o del finanziamento del terrorismo)⁷⁹.

I CASP rappresentano un'evoluzione rispetto ai precedenti VASP, volta a migliorare la sorveglianza e la trasparenza del settore in risposta alle criticità evidenziate nel Rapporto dell'Autorità Bancaria Europea (EBA) sulle criptovalute del 9 gennaio 2019.

I servizi afferenti alle cripto-attività seguiranno un modello simile a quelli di investimento su strumenti finanziari, come già stabilito dalla Direttiva MiFID II⁸⁰, e saranno pertanto soggetti a regolamentazioni e requisiti di autorizzazione analoghi a quelli applicati agli strumenti finanziari tradizionali.

Per la legittima prestazione di servizi nell'Unione Europea, i CASP devono soddisfare requisiti prudenziali minimi, disporre di una *governance* organizzativa con sede legale in uno Stato membro, ottenere un regime autorizzativo sui singoli servizi offerti ed essere iscritti in un registro centrale dell'ESMA, sottoposti a vigilanza da parte delle Autorità nazionali competenti⁸¹.

Il Regolamento stabilisce inoltre regole di *marketing* per fornire informazioni chiare ai clienti, come la gestione dei “*white paper*” delle cripto-attività oggetto del servizio. I CASP devono disporre di fondi propri patrimoniali, di una polizza assicurativa e di procedure interne di gestione del rischio e devono garantire affidabilità e sicurezza nei propri servizi informatici in conformità con il Regolamento DORA (2022/2554/UE)⁸².

Il MiCAR impone ai CASP obblighi precisi per la tutela dei fondi dei clienti, con particolare attenzione alla segregazione delle cripto-attività. Per gli importi in euro, il Regolamento prevede il deposito su conti dedicati presso banche dell'Unione Europea, garantiti dal Fondo Interbancario di Tutela dei Depositi con una copertura fino a 100.000 euro.

La segregazione è fondamentale per garantire che, in caso di problemi finanziari del CASP, i clienti possano recuperare i propri fondi in modo sicuro. Per questo motivo, è stato sottolineato⁸³, le regole

⁷⁹ Cfr. relazione del Dott. Gianfranco Torriero, DOC. n. 315.1, pp. 11-12.

⁸⁰ La Directive 2014/65/UE, nota come MiFID II (*Markets in Financial Instruments*) è una normativa europea, in vigore dal 3 gennaio 2018, che disciplina i mercati finanziari e i servizi di investimento nell'UE.

⁸¹ Cfr. relazione del Gen.B. Gianluca Vitagliano, DOC. n. 287.1, p. 10.

⁸² Cfr. relazione del Gen.B. Gianluca Vitagliano, DOC. n. 287.1, p. 12.

⁸³ Cfr. relazione del Gen.B. Gianluca Vitagliano, DOC. n. 287.1, p. 19.

di segregazione devono essere chiare, rigorose e verificabili, senza lasciare margini di interpretazione normativa.

Il Regolamento richiede, inoltre, ai CASP di stipulare una polizza assicurativa, sebbene questa potrebbe risultare insufficiente in caso di frodi o atti dolosi, poiché i massimali previsti coprono solo i requisiti minimi di vigilanza prudenziale.

Il MiCAR, all'art. 97, § 1, impone, poi, alle tre Autorità europee di vigilanza – *European Banking Authority* (EBA), *European Securities and Markets Authority* (ESMA) ed *European Insurance and Occupational Pensions Authority* (EIOPA) – di elaborare linee guida congiunte per portare maggiore chiarezza e coerenza nell'applicazione del quadro normativo europeo sui *crypto-asset* sotto il Regolamento MiCAR.

In ragione di tanto, ha visto la luce un pacchetto di *guidelines* (*ESAs Guidelines*)⁸⁴ su: a) i *template standard* per le spiegazioni che accompagnano i *crypto-asset white paper*⁸⁵; b) i modelli di opinione legale (soprattutto per gli *asset-referenced token*⁸⁶); c) un *test* standardizzato di classificazione dei *crypto-asset* ai fini normativi, per facilitare una classificazione omogenea da parte degli operatori di mercato e delle autorità nazionali competenti, riducendo discrepanze interpretative tra Stati membri. Infine, va ricordato che il provvedimento europeo riveste una rilevanza indiretta anche ai fini antiriciclaggio. Difatti, coerentemente con la scelta di intervenire tramite Regolamento, l'UE ha rinviato alla definizione ivi contenuta di cripto-attività (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) pure nei nuovi provvedimenti caratterizzati da più diretta rilevanza penalistica⁸⁷.

3.2.2. Il decreto legislativo di attuazione del regolamento MiCAR.

In Italia, il Regolamento MiCAR è stato recepito con il d.lgs. 5 settembre 2024, n. 129, con l'effetto di abrogare gradualmente la precedente disciplina nazionale, frammentaria e basata sulla registrazione dei Virtual Asset Service Providers (VASPs) ai fini antiriciclaggio. Il decreto attuativo segna, infatti, il definitivo superamento dell'impostazione nazionale previgente, incentrata su presidi

⁸⁴ 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 dicembre 2024, in <https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/asset-referenced-and-e-money-tokens-micar/esas-guidelines-templates-explanations-and-opinions-and-standardised-test-classification-crypto>.

⁸⁵ Quando un emittente pubblica un *white paper* per un *crypto-asset* che non è un *electronic money token* (EMT) o un *asset-referenced token* (ART), deve spiegare perché quel *crypto-asset* non rientra in categorie escluse dal campo di applicazione di MiCAR o non è un EMT/ART.

⁸⁶ Per gli *asset-referenced tokens* (ARTs) è richiesta una opinione legale che illustri la qualificazione normativa – ad esempio dimostrando che non è un EMT né un *crypto-asset* escluso da MiCAR.

⁸⁷ Cfr. relazione del Prof. Jacopo Della Torre, DOC. n. 247.1, p. 8.

essenzialmente antiriciclaggio e su un sistema di mera registrazione dei prestatori di servizi in valute virtuali.

L'intervento del legislatore si colloca, dunque, in una prospettiva di armonizzazione sostanziale, volta a integrare in modo organico la disciplina europea nel diritto positivo italiano mediante un riassetto complessivo delle fonti, delle competenze di vigilanza e degli strumenti sanzionatori.

Sotto il profilo sistematico, il decreto recepisce le categorie tipologiche elaborate dal MiCAR (*token* collegati ad attività, *token* di moneta elettronica e cripto-attività "residuali") e ne assume le relative discipline di emissione, offerta al pubblico e ammissione alla negoziazione, conferendo loro diretta operatività nell'ordinamento interno. Parallelamente, viene introdotto un regime autorizzatorio pienamente strutturato per i prestatori di servizi per le cripto-attività (CASP), che sostituisce il precedente modello VASP.

Di particolare rilievo è il riparto di competenze tra le autorità nazionali. Il decreto individua espressamente la Banca d'Italia quale autorità nazionale competente per la vigilanza prudenziale sugli emittenti di EMT e ART, sui prestatori di servizi per cripto-attività (CASP) e sugli aspetti di antiriciclaggio/contrasto al finanziamento del terrorismo connessi a tali soggetti, mentre attribuisce alla Consob le funzioni in materia di trasparenza, correttezza della condotta, integrità del mercato e tutela degli investitori, nonché vigilanza sulle cripto-attività diverse da EMT e ART.

Il decreto, inoltre, introduce un articolato regime transitorio destinato agli operatori già attivi, volto a garantire continuità operativa e certezza giuridica nella fase di passaggio dal sistema nazionale previgente al nuovo quadro europeo. In particolare, i soggetti già iscritti nella sezione speciale del registro OAM alla data del 27 dicembre 2024 possono proseguire temporaneamente l'attività, a condizione di presentare istanza di autorizzazione MiCAR entro termini prestabiliti, beneficiando di una proroga funzionale a prevenire vuoti regolatori e interruzioni di mercato. Questo meccanismo è volto a evitare vuoti autorizzativi e a consentire una transizione ordinata dal precedente regime nazionale (VASP) al nuovo regime europeo (CASP).

Sul piano della tutela degli investitori, il decreto recepisce uno dei capisaldi del MiCAR, ossia il principio di segregazione patrimoniale delle cripto-attività e dei fondi detenuti per conto della clientela, che devono rimanere distinti dal patrimonio del prestatore e non risultano aggredibili dai suoi creditori in caso di insolvenza. A ciò si affiancano stringenti obblighi di organizzazione interna, gestione dei conflitti di interesse, continuità operativa e controllo dei rischi, nonché il divieto per i CASP di utilizzare le risorse dei clienti per finalità proprie, delineando un presidio avanzato di protezione degli utenti.

Rilevante è anche il rafforzamento degli obblighi informativi e di trasparenza, imperniato sulla disciplina del *white paper*: gli emittenti sono tenuti a fornire un'informativa completa, chiara e non

fuorviante sulle caratteristiche delle cripto-attività, sui rischi connessi e sulle condizioni dell'offerta, secondo standard uniformi a livello europeo. In tal modo, il legislatore mira a colmare l'asimmetria informativa strutturale che ha storicamente caratterizzato il mercato *crypto*, avvicinando il grado di protezione dell'investitore a quello previsto nei mercati finanziari regolamentati.

Sul versante repressivo, il d.lgs. n. 129/2024 predispone un sistema punitivo misto, nel quale a un'unica fattispecie penale – relativa all'esercizio abusivo di attività riservate – si affianca un complesso apparato di sanzioni amministrative, affidate alla Banca d'Italia e alla CONSOB, modulabili in funzione della gravità della violazione e della dimensione dell'operatore. L'impianto sanzionatorio, in linea con il MiCAR, privilegia una logica dissuasiva e proporzionata, valorizzando l'effettività della vigilanza più che il ricorso alla penalizzazione generalizzata.

Nel complesso, il decreto attuativo rappresenta un momento di svolta per l'ordinamento italiano in materia di cripto-attività: esso non si limita a un recepimento formale del regolamento europeo, ma realizza un vero e proprio riassetto sistematico della materia, integrando disciplina di mercato, presidi prudenziali, regole di condotta e meccanismi sanzionatori in un quadro coerente e unitario. Ne emerge un modello regolatorio orientato alla stabilità, alla trasparenza e alla tutela degli investitori, che colloca il settore *crypto* all'interno dell'architettura finanziaria europea, segnando il passaggio da una fase sperimentale a una piena normalizzazione giuridica del fenomeno.

3.3. Il sistema di *asset-recovery*.

3.3.1. Il sequestro di criptovalute nel codice di rito.

Il Codice di procedura penale, come già accennato, non contempla una disciplina specifica sul sequestro di criptovalute o, più in generale, di *crypto-asset*, né prevede un modulo procedurale *ad hoc* per la loro apprensione e gestione. Ne consegue che l'ablazione temporanea della *criptocurrencies*, nella prassi applicativa, si fonda sull'impiego degli strumenti cautelari e probatori ordinari, reinterpretati alla luce della natura immateriale e tecnologicamente mediata del bene digitale in questione.

Vengono, dunque, in rilievo, a seconda della finalità perseguita, il sequestro probatorio (art. 253 c.p.p.), diretto all'acquisizione del corpo del reato o delle cose pertinenti al reato, nonché il sequestro preventivo (art. 321 c.p.p.), predisposto per impedire la prosecuzione o l'aggravamento delle conseguenze del reato o la commissione di ulteriori illeciti (comma 1 - c.d. "impeditivo") ovvero finalizzato alla confisca (comma 2), quale strumento funzionale ad assicurare l'effettività della futura ablazione, sia essa diretta o per equivalente, secondo gli schemi della legislazione penale sostanziale applicabile al caso concreto.

Si tratta – intuibilmente – di previsioni concepite con riferimento ad un “mondo analogico”, ove il vincolo reale si perfeziona con la materiale *adprehensio* del bene, mentre la criptovaluta si presenta come bene immateriale, privo di consistenza fisica, il cui controllo dipende dalla disponibilità esclusiva delle credenziali (*private key* – v. *infra*) o, nel caso di custodia presso intermediari centralizzati, dal potere di accesso e disposizione sull'*account*.

Come verrà di seguito precisato, infatti, l'oggetto immediato del sequestro non è il “*token*” come *res corporales*, che non esiste nel mondo fisico, bensì la disponibilità giuridico-fattuale della risorsa digitale, resa possibile dal controllo della chiave privata⁸⁸ o, nei contesti *custodial*, dalla disponibilità dell'*account*, sicché la misura si traduce, sul piano funzionale, in una sottrazione del potere di disposizione analoga a quella che, nel mondo finanziario tradizionale, si realizza mediante il congelamento di un conto o di un deposito.

Dal punto di vista operativo, l'assenza di una procedura codificata ha generato prassi disomogenee che, pur muovendosi entro l'alveo delle misure reali, sono prive di regole dettagliate su custodia, sicurezza, responsabilità per perdita delle chiavi o malfunzionamenti, e, soprattutto, sui criteri di gestione dell'elevata volatilità della criptovaluta sequestrata, che può incidere sensibilmente sulla proporzionalità del vincolo e sulla concreta tutela delle posizioni soggettive coinvolte, sia dell'indagato, sia di eventuali terzi in buona fede.

Sul piano dei principi, la costruzione giurisprudenziale del sequestro di criptovalute solleva interrogativi non marginali rispetto alle esigenze di tipicità e prevedibilità della coercizione reale: se è vero che le norme generali consentono, in via interpretativa, di ricomprendere beni immateriali nel concetto di “cosa” o di “pertinenza”, è altrettanto vero che l'innovazione tecnologica tende a spingere l'interprete verso letture estensive e funzionali che possono mettere in tensione, se non governate da criteri rigorosi, il canone di legalità in materia cautelare, che esige quantomeno una sufficiente determinazione del contenuto della misura e delle sue modalità esecutive.

In aggiunta, la dimensione transnazionale delle infrastrutture di scambio e custodia, nonché la struttura decentralizzata di talune tecnologie, possono trasformare la misura in un vincolo di difficile attuazione o, all'opposto, in un intervento di fatto eccedente, se eseguito mediante strumenti tecnici non adeguatamente regolati.

Infine, l'esatta qualificazione della criptovaluta incide non solo sulla scelta tra vincolo probatorio o preventivo, ma anche sul rapporto tra sequestro e confisca: a seconda che la criptovaluta sia considerata profitto immediato o semplice utilità economicamente fungibile, viene meno l'opportunità di valersi del mezzo di ricerca della prova, ovvero mutano i presupposti e i limiti della

⁸⁸ Cfr. documento depositato dalla Dott.ssa Agnese Del Giudice in occasione della sua audizione del 14 novembre 2024, X Comitato, DOC. n. 265.1, p. 26.

confisca (diretta o per equivalente) e, per riflesso, la legittimità e l'estensione del sequestro ad essa finalizzato; in questa materia, la necessità di un accertamento puntuale del nesso di pertinenzialità o della riconducibilità della ricchezza al fatto illecito diviene ancora più pressante, anche per evitare automatismi ablatori incompatibili con il principio di proporzionalità.

3.3.2. Congelamento e confisca in ambito europeo.

È chiaramente nota l'esistenza di un quadro europeo volto a rendere più efficace l'individuazione, il congelamento e la confisca dei proventi illeciti in tutto il territorio unionale.

L'architave è, senz'altro, il Regolamento (UE) 2018/1805 sul mutuo riconoscimento dei provvedimenti di congelamento e confisca, che mira a far circolare, con meccanismi di riconoscimento reciproco, gli ordini emessi da ciascuno Stato membro, rafforzando la capacità di colpire beni e disponibilità al di fuori della giurisdizione nazionale.

Il perno più recente è rappresentato dalla Direttiva (UE) 2024/1260, che innalza il livello di armonizzazione minima in materia di *asset recovery*, rafforzando l'idea che l'asset tracing debba divenire un "riflesso automatico" nelle indagini sui fenomeni criminali più gravi, riducendo, altresì, gli spazi di arbitraggio territoriale tipici delle ricchezze digitali.

Se riguardo al primo obiettivo prefissato – rafforzare la capacità delle competenti autorità nazionali di reperire, identificare, congelare, confiscare, gestire e destinare i beni derivanti da attività criminali e di implementare i sistemi di coordinamento e comunicazione – la direttiva sembrerebbe cogliere nel segno, rispetto al secondo dei due obiettivi prefissati – estendere l'ambito applicativo della disciplina sul recupero e la confisca ai *virtual-assets* – il provvedimento europeo, come già segnalato, appare inadeguato.

Esso amplia la portata definitoria della direttiva 2014/42/UE, estendendo il concetto di "bene" (suscettibile di congelamento e confisca) anche alle cripto-attività, tra cui le criptovalute.

Che le *cryptocurrencies* abbiano attirato l'attenzione della criminalità organizzata l'Europa ne è da tempo consapevole: già in fase di proposta la Commissione UE aveva sottolineato come «[...] gli strumenti di confisca esistenti non copr[issero] tutti i mercati che assicurano ai criminali ingenti proventi e non ineris[sero] a tutte le complesse strutture e metodi a cui fanno ricorso le organizzazioni criminali»⁸⁹; in quest'ordine di idee, Parlamento e Consiglio hanno, poi, opportunamente richiamato l'attenzione dei Paesi membri sulla necessità di consentire azioni immediate di recupero e di

⁸⁹ Proposal for a directive of the European Parliament and of the Council on asset recovery and confiscation, COM(2022)245 *final*, in www.europol.europa.eu, 25 maggio 2022, p. 2.

identificazione dei «beni che potrebbero sparire molto rapidamente (come le cripto-attività)» (Considerando n. 23).

È evidente, però, che l'idea, indubbiamente meritoria, di estendere il sistema di *asset recovery* anche al mercato delle criptovalute necessita di un radicale cambiamento delle metodologie operative, da compendiare in una disciplina dedicata, costruita tenendo conto dei profili tecnici e operativi del *trading*, del quasi totale anonimato dei contrenti garantito dal sistema e dalla vocazione transnazionale del mercato *crypto*. Vale ribadirlo⁹⁰: le tradizionali tecniche di tracciamento, identificazione e recupero dei beni sono del tutto inadeguate a contrastare efficacemente le più recenti e le inedite modalità di occultamento dei proventi illeciti dematerializzati.

Allo stato attuale, quindi, qualche beneficio può trarsi solo in via mediata dalla convergenza funzionale dei provvedimenti europei già in vigore.

Come già evidenziato, l'oggettiva transnazionalità del sistema *crypto* pone in ordine al congelamento di cripto-attività un problema, prima ancora che di qualificazione dogmatica, di eseguibilità.

A riguardo, il Regolamento sul mutuo riconoscimento (2018/1805/UE) consente di “portare” più rapidamente l'ordine di *freezing* nello Stato dove, ad esempio, il prestatore di servizi *crypto* (CASP) è stabilito o dove è possibile incidere operativamente sulle disponibilità, riducendo il rischio di dissipazione tipico di *asset* ad alta mobilità.

Il MiCAR, a sua volta, potrebbe aumentare la probabilità che un ordine di congelamento sia tecnicamente eseguibile quando l'*asset* è detenuto presso un intermediario regolato (CASP), rendendo più agevole l'identificazione del soggetto destinatario dell'ordine e più controllabile la catena di custodia successiva.

Tuttavia, non possiamo ignorare un problema di fondo. Chi delinque in ambito *crypto* raramente si avvale dell'opera di *exchanges* o *wallet provider* (CASPs): le criptovalute sono normalmente detenute in modalità *non-custodial* (v. *infra*, parte II, sez. I, § 5.1.).

Permane, dunque, l'esigenza di una più compiuta tipizzazione delle modalità di apprensione e gestione, onde evitare che l'innovazione tecnica imponga, di fatto, soluzioni prassistiche non pienamente governate dal criterio di proporzionalità.

3.4. La normativa fiscale.

La legge di bilancio del 2023 (l. 29 dicembre 2022, n. 197) era già intervenuta sulla regolamentazione fiscale delle cripto-attività, definendo le modalità di dichiarazione fiscale, le tassazioni applicabili

⁹⁰ Cfr. resoconto stenografico della seduta del 14 novembre 2024, X Comitato, audizione della Dott.ssa Agnese Del Giudice, p. 7.

alle plusvalenze e alle minusvalenze, oltre a introdurre la possibilità di regolarizzare situazioni pregresse. Successivamente, il 20 dicembre 2024, il Senato ha approvato la legge di bilancio 2025 (l. 30 dicembre 2024, n. 207), apportando ulteriori modifiche alla fiscalità dei *cripto-asset*⁹¹. In particolare, consolida il regime delle cripto-attività quale sottocategoria dei redditi diversi *ex art.* 67, comma 1, lett. c-*sexies*, TUIR, applicando per il periodo d'imposta 2025 l'imposta sostitutiva del 26% sulle plusvalenze e sugli altri proventi, ed eliminando contestualmente la franchigia di euro 2.000, con conseguente generalizzazione dell'imponibilità. La medesima manovra introduce una facoltà transitoria di rideterminazione del valore fiscale delle cripto-attività detenute al 1° gennaio 2025, mediante imposta sostitutiva del 18%, e predispone normativamente l'innalzamento dell'aliquota al 33% con decorrenza dal 1° gennaio 2026.

La legge di bilancio 2026 (l. 30 dicembre 2025, n. 199) dà attuazione a tale incremento, rendendo operativa l'aliquota del 33% quale misura ordinaria del prelievo sui redditi da cripto-attività. In parallelo, introduce un regime derogatorio per i *token* di moneta elettronica denominati in euro (EMT/MiCAR), per i quali resta ferma l'aliquota del 26% e viene sancita la neutralità fiscale della conversione in euro e del rimborso al valore nominale.

In termini sistematici, il passaggio dal 2025 al 2026 segna il completamento di una manovra bifasica: prima la normalizzazione della base imponibile (abolizione della franchigia e rivalutazione opzionale), poi l'inasprimento strutturale dell'aliquota, temperato da una disciplina speciale per gli *euro-token*, in un quadro di progressivo allineamento agli *standard* europei promosso anche dal Ministero dell'Economia e delle Finanze.

4. La criptovaluta: definizione, caratteristiche strutturali e potenzialità criminose.

Per comprendere il sistema *crypto* è necessario partire dai suoi elementi base: la criptovaluta, la *blockchain*, i *miner* e i *wallet*.

La definizione di criptovaluta si innesta in una bipartizione conosciuta, ossia quella tra moneta fisica e moneta elettronica.

La prima comprende le monete metalliche e le banconote: è anonima, accessibile a chiunque e facilmente percepibile nella sua materialità. Diversamente, la seconda non è immediatamente percepibile perché immateriale: *consente di effettuare pagamenti a distanza, ma rappresenta pur sempre una trasposizione digitale di moneta a valore corrente, depositata su un conto corrente*

⁹¹ Cfr. relazione del Gen.B. Gianluca Vitagliano, DOC. n. 287.1, p. 14.

apposito presso un istituto bancario (in altre parole, si tratta di una rappresentazione digitale di moneta reale)⁹².

La criptovaluta rappresenta, quindi, un valore digitale che, da un lato, consente di effettuare pagamenti a distanza (in questo ricalcando le caratteristiche della moneta elettronica⁹³) e, dall'altro lato, garantisce una certa forma di pseudonimato (similmente a quanto avviene per il contante).

A livello tecnico le criptovalute non possono considerarsi valute o monete, perché non assicurano le tre funzioni tipiche di una moneta.

Se la moneta a corso legale, infatti, consente di conservare (e accumulare) nel tempo la quota di reddito che non viene utilizzata nell'immediato per consumare beni e/o servizi (riserva di valore), la criptovaluta difetta dei presupposti a tal fine necessari, mancando un'autorità monetaria o uno Stato che ne imponga l'accettazione e ne sostenga la stabilità mediante politica monetaria e strumenti di intervento e il suo prezzo è determinato esclusivamente dall'incontro tra domanda e offerta, sicché quanto più saranno utilizzate per il pagamento di beni e servizi, tanto più aumenteranno di valore.

La moneta a corso legale, poi, può essere scambiata istantaneamente con beni e servizi consentendo l'estinzione delle obbligazioni pecuniarie (mezzo di pagamento); le criptovalute, invece, non hanno corso legale in nessun angolo del pianeta⁹⁴ e, dunque, l'accettazione come mezzo di pagamento è su base volontaria.

Infine, la moneta a corso legale si usa per confrontare in maniera omogenea il valore di prodotti e servizi molto diversi tra loro, agevolando, così, le decisioni economiche e gli accordi contrattuali (unità di conto); le criptovalute, invece, si distinguono per l'elevata volatilità (i prezzi delle principali criptovalute sono soggetti a fluttuazioni molto ampie, anche all'interno delle stesse giornate, quindi non è possibile prezzare beni e servizi in unità di criptovalute)⁹⁵.

Obiettivo degli ideatori del sistema *crypto* è stato quello di costituire un nuovo sistema economico basato su una nuova ricchezza sottratta all'egemonia dei circuiti bancari, ossia all'esistenza di un'autorità centrale che la emetta o ne tracci/validi le transazioni.

Possiamo, quindi, definire le criptovalute la rappresentazione di un valore digitale "protetto" non da un'autorità finanziaria centrale, ma da crittografia.

⁹² Cfr. resoconto stenografico della seduta del 14 novembre 2024, X Comitato, audizione della Dott.ssa Agnese Del Giudice, p. 3.

⁹³ Tuttavia, la criptovaluta, potendo essere frazionata fino al centomillesimo (Bitcoin) ed oltre (l'unità più piccola di Ethereum è il *wei* che, in centesimi di euro, è un valore prossimo allo zero assoluto), unitamente ai bassi costi di transazione, può essere utilizzata come metodo di pagamento anche per piccoli scambi a differenza di quanto avviene con i pagamenti in moneta elettronica, i quali per importi ridotti risultano svenienti.

⁹⁴ Sia la Repubblica Centrafricana (CAR) che El Salvador hanno sperimentato il Bitcoin come moneta legale; entrambi i Paesi, tuttavia, hanno successivamente optato per l'accettazione volontaria.

⁹⁵ Cfr. documento depositato dalla Dott.ssa Agnese Del Giudice in occasione della sua audizione del 14 novembre 2024, X Comitato, DOC. n. 265.1, p. 3.

Esse, infatti, possono essere depositate e scambiate solo su piattaforme DLT (*Distributed Ledger Technology*), rispettando le regole del protocollo *blockchain*.

A questo punto è facile intuire perché il sistema abbia rappresentato un'industria fiorente per la criminalità organizzata.

Il mercato *crypto* si fonda essenzialmente su quattro pilastri: decentramento, integrità, sicurezza, *privacy*⁹⁶.

Il decentramento. La criptovaluta può essere scambiata in modalità *peer-to-peer* (P2P), ovvero tra due dispositivi collegati alla rete *internet* (c.d. “nodi”), senza necessità di intermediari istituzionalizzati (come, ad esempio, la banca) per la buona riuscita delle operazioni.

Nel sistema bancario tradizionale tutte le parti coinvolte in una transazione hanno fiducia nel fatto che l'istituto di credito muova regolarmente il denaro, verificando e certificando che le operazioni economiche vengano compiute in valuta corrente. La finanza decentralizzata (DeFi)⁹⁷, invece, non prevede un'autorità di governo centrale; utilizza, piuttosto, i meccanismi di consenso “distribuito”, cioè sono gli utenti che partecipano alla rete (nodi) che garantiscono la regolarità delle transazioni (*Proof of Work* e *Proof of Stake*)⁹⁸. Il *Proof of Work* (PoW), in particolare, è il sistema maggiormente utilizzato nel mondo delle criptovalute per verificare la validità e l'integrità delle transazioni che vengono aggiunte a una *blockchain* come nuovi blocchi (sul punto, v. *infra*, parte II, sez. I, § 4.2).

Il decentramento implica, quindi, l'assenza di un'autorità centrale che controlli e regoli le transazioni, nonché l'assenza di vincoli geografici.

È evidente che un sistema distribuito rende molto difficile un'azione di controllo da parte dell'Autorità giudiziaria e delle Forze di polizia.

Un esempio su tutti: se il Pubblico ministero intende conoscere i conti correnti di un soggetto interroga l'anagrafe bancaria e individua l'istituto bancario al quale chiedere di fornire informazioni sui titolari dei conti. Nel mondo della criptovaluta, come detto, non esiste un organo terzo che operi in funzione di garanzia delle transazioni a cui chiedere qualsivoglia informazione. Peraltro, anche quando l'operazione avviene tramite i prestatori di servizi (*exchanges* e *wallet provider*) – eventualità certa per chi delinque in ambito *crypto* (v. *infra*, parte II, sez. I, § 5.1.) – una richiesta dell'inquirente in tal senso si risolverebbe in un nulla di fatto: perché il più delle volte trattasi di operatori allocati

⁹⁶ Cfr. documento depositato dalla Dott.ssa Agnese Del Giudice in occasione della sua audizione del 14 novembre 2024, X Comitato, DOC. n. 265.1, pp. 5-6.

⁹⁷ Con il termine di “finanza decentralizzata” (*Decentralised Finance* – DeFi) si fa riferimento a tutti quei servizi in cui l'utente interagisce, anziché con un soggetto, direttamente con *software* eseguibili dai nodi della rete che automatizzano azioni predeterminate e irreversibili al ricorrere delle condizioni previste: così, relazione del Dott. Gianfranco Torriero, DOC. n. 315.1, p. 5, nt. 9.

⁹⁸ Cfr. resoconto stenografico della seduta del 14 novembre 2024, X Comitato, audizione della Dott.ssa Agnese Del Giudice, p. 3.

all'estero (sui quali non grava alcun obbligo di fornire informazioni) e perchè l'ipotesi della fattiva collaborazione appare, in concreto, poco plausibile. Sul punto, infatti, è doveroso notare come i prestatori di servizi di crypto-attività si esporrebbero al rischio di perdere una parte consistente della propria clientela: il *trader* di criptovalute ha particolarmente a cuore la propria *privacy*, per cui difficilmente sceglierebbe di affidarsi ad un *wallet provider* o ad un *exchange* che collabori – o collabori facilmente – con la pubblica autorità⁹⁹.

Integrità e immutabilità. Il controllo del sistema è distribuito equamente tra tutti i computer collegati alla rete per impedire a chiunque di frodare il sistema (mediante attacchi *denial of service* o *distributed denial of service*¹⁰⁰; hackeraggio; *wash trading*¹⁰¹ etc.).

Nella teoria informatica una rete “*peer to peer*” è un'architettura di sistema nella quale tutti i *computer* connessi (nodi) svolgono la funzione sia di *client* (inviare richieste di risorse) che di *server* (fornire servizi e dati ad altri nodi); questo significa che nessuno dei nodi della rete (cioè nessun utente collegato) ha un peso specifico maggiore degli altri.

L'architettura decentralizzata elimina i *single points of failure* (tipici dei sistemi centralizzati); un attacco, per essere efficace, deve compromettere simultaneamente una porzione ampia della rete. Di conseguenza, mentre la manipolazione dei dati o l'interruzione del servizio richiedono risorse computazionali molto elevate (per superare i meccanismi di consenso e le firme crittografiche) e costi economici crescenti (hardware, energia, coordinamento), la ridondanza dei nodi consente al sistema di continuare a operare anche in presenza di guasti o attacchi localizzati, aumentando così la resilienza sistemica complessiva.

Secondo la teoria dei giochi, il protocollo implementa una struttura “*trustless*” in cui la massimizzazione del profitto individuale è allineata con la sicurezza collettiva: seguire le regole massimizza il rendimento atteso (la validazione corretta dei blocchi dà accesso ai *block reward* e alle

⁹⁹ Così la Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato (cfr. resoconto stenografico, p. 4).

¹⁰⁰ Il *Denial of Service* (DoS) è un attacco finalizzato ad ingolfare le risorse di un sistema informatico che fornisce un determinato servizio ai computer connessi, inondandolo di false richieste di accesso. Nel gergo informatico si dice che ne viene saturata la banda di comunicazione e i siti web o i naviganti che cercano di raggiungere quella determinata risorsa online incontrano difficoltà o non riescono ad accedervi. I *Distributed Denial of Service* (DDoS) sono attacchi che perseguono la stessa finalità, ma si manifestano su ampia scala. Nel caso dei Dos, infatti, bisogna difendersi da una sola sorgente di traffico informatico (ad esempio, un numero elevato di e-mail in arrivo contemporaneamente); durante gli attacchi DDoS, invece, le domande fasulle arrivano nello stesso momento da più fonti.

¹⁰¹ Il *wash trading* è una pratica illegale finalizzata a manipolare il mercato. Può essere eseguita in diversi modi: un broker e un trader possono cospirare per acquistare e vendere lo stesso asset a un prezzo convenuto, creando l'illusione di una domanda o di un'offerta significativa per influenzare il prezzo del bene al rialzo o al ribasso; oppure, un singolo operatore può commerciare con se stesso, cioè acquista e vende lo stesso asset simultaneamente o in rapida successione per produrre false informazioni di mercato, cioè per creare l'illusione di una domanda o di un'offerta significativa (la creazione di un'immagine di interesse e di domanda può spingere gli investitori a partecipare al mercato, aumentando potenzialmente il prezzo del bene e consentendo ai partecipanti al *wash trading* di trarre profitto). Le criptovalute – come già accennato (v. *supra*, parte II, sez. I, § 2) – sono particolarmente soggette a schemi di *pump-and-dump*, in cui un volume di scambi artificialmente gonfiato, una pubblicità significativa o raccomandazioni da parte di addetti ai lavori vengono utilizzati per aumentare il valore di un *token* e, conseguentemente, i profitti.

commissioni di transazione), mentre “barare” aumenta il rischio senza offrire un vantaggio sostenibile (qualsiasi deviazione viene automaticamente penalizzata dal consenso distribuito, che rifiuta blocchi invalidi e rende, quindi, nullo l’investimento computazionale sostenuto).

Chiaramente, la criminalità beneficia sia della natura distribuita che del modello cooperativo nella misura in cui essi rendono particolarmente sicuro e stabile il processo di validazione della transazione, cioè garantiscono certezza sul buon fine dell’operazione illecita¹⁰².

La *privacy*. Il pilastro del sistema *crypto* (con gestione decentrata) che più favorisce la deriva criminosa è l’eccellente grado di *privacy* garantito sia con riferimento alla persona dell’utente, che in rapporto all’oggetto delle compravendite.

Il mercato si fonda sulla c.d. “crittografia asimmetrica” a chiave pubblica-privata: la prima è destinata ad essere diffusa per avviare la transazione, la seconda è idonea ad essere conosciuta solo dal proprietario (a riguardo, v. *infra*, parte II, sez. I, § 4.3.).

Sebbene tutte le transazioni siano registrate nella *blockchain*, e quindi siano visibili a tutti gli utenti della rete, esse non recano il nome delle parti, bensì pseudonimi.

Ne consegue che nessuno può dire con certezza che un determinato soggetto sia “titolare” di un indirizzo *crypto* (chiave pubblica) alla stregua di quanto accade con i tradizionali metodi di pagamento che non si basano sui contanti (moneta elettronica, carte di pagamento, bonifici bancari, etc.).

Tuttavia, è doveroso precisare come tale *standard* nativo di *privacy* ben può essere rafforzato – sino a lambire il puro anonimato – utilizzando criptovalute che garantiscono sistemi di *privacy* integrata nel loro codice base (come Monero), ovvero programmi e reti di navigazione che mischiano le transazioni impedendo di risalire al mittente e al destinatario¹⁰³.

Quindi, il sistema consente il trasferimento di criptovalute in “modalità protetta”, perché, da un lato, non esiste alcun tipo di intermediario che abbia l’obbligo di censire l’utente e di segnalare alle autorità eventuali transazioni “a rischio”¹⁰⁴ e, dall’altro, è possibile farlo avvalendosi di pseudonimi connessi ai *wallet* (che non identificano direttamente il possessore dello stesso).

Attraverso l’uso delle criptovalute è, dunque, tecnicamente possibile riciclare denaro o realizzare traffici illegali senza essere attenzionati dall’Autorità giudiziaria¹⁰⁵.

¹⁰² Così, testualmente, la Dott.ssa Agnese Del Giudice: cfr. resoconto stenografico della seduta del 14 novembre 2024, X Comitato, p. 4.

¹⁰³ Cfr. documento depositato dalla Dott.ssa Agnese Del Giudice in occasione della sua audizione del 14 novembre 2024, X Comitato, DOC. n. 265.1, p. 23.

¹⁰⁴ Proprio l’assenza di intermediari non consente di innestare punti di controllo funzionali ad associare indirizzi e identità: cfr. relazione del Dott. Gianfranco Torriero, DOC. n. 315.1, p. 6.

¹⁰⁵ Come si legge nella relazione depositata dal Dott. Gianfranco Torriero in occasione della sua audizione, «[s]otto un profilo operativo, la tracciabilità pseudo-anonima delle transazioni, propria della *blockchain*, unita alla possibilità di operare senza intermediari finanziari tradizionali ha reso le crypto-attività particolarmente attraenti per attività quali il

Bisogna ammettere che questo è il vero punto dolente delle criptovalute – e dei relativi protocolli *blockchain* – che hanno una gestione decentrata (*permissionless*), contrariamente alle *permissioned blockchain* che possono essere soggette a forme di controllo e verifica dall’alto: l’utente, infatti, deve necessariamente essere approvato per essere abilitato a convalidare le transazioni.

Eppure, le caratteristiche del “paradiso virtuale” delle mafie punta anche su altri fattori rilevanti, che verranno messi in evidenza nel prosieguo della Relazione.

4.1. La *blockchain* e il paradosso delle identità opache.

Alla base di ogni criptovaluta troviamo una *blockchain*, cioè il registro pubblico – accessibile *on-line* – sul quale vengono “annotate” tutte le operazioni di acquisto/vendita di *cryptocurrencies*.

Si tratta di un database distribuito e condiviso tra tutti i nodi di una rete (DLT – *distributed ledger technology*), suddiviso in blocchi, digitalmente concatenati (da qui il nome “*block-chain*”, “catena di blocchi”), memorizzati in ordine cronologico e validati dai *miners* attraverso un peculiare meccanismo che ne garantisce l’immodificabilità¹⁰⁶ (v. *infra*, parte II, sez. I, § 4.2.).

Ogni blocco è un contenitore di transazioni: raggiunta la sua capienza massima¹⁰⁷ il blocco può essere validato e le transazioni successive confluiscono nel blocco successivo.

Malgrado la complessità, il funzionamento della *blockchain* nelle sue linee essenziali può essere sintetizzato in pochi passaggi: ipotizziamo che A voglia inviare una criptovaluta a B; la transazione viene inserita in un blocco dal *miner* (che ne ha controllato la correttezza: firma valida, soldi davvero disponibili, niente doppia spesa) e viene messa in stato di validazione; il blocco viene visualizzato da tutti gli altri nodi collegati alla rete che, a questo punto, iniziano a gareggiare tra loro (*Proof of Work* – si parla di gara perché il *miner* che per primo valida il blocco ottiene una ricompensa in criptovalute); una volta validato, il blocco si aggancia alla catena di blocchi precedenti e B riceve le sue criptovalute¹⁰⁸. La catena di blocchi è una sorta di DNA delle transazioni.

All’interno di ciascuna *blockchain* sono, dunque, memorizzate tutte le transazioni effettuate dalla genesi di una determinata criptovaluta sino al presente. In questo si rinviene il paradosso del registro

commercio illegale sul *dark web*, la realizzazione di schemi di frode e l’estorsione attraverso ransomware. In questi contesti, i fondi acquisiti attraverso attività illecite possono essere convertiti in valute a corso legale tramite piattaforme di scambio (*exchange*), complicando ulteriormente l’identificazione delle origini dei proventi» (cfr. DOC. n. 315.1, pp. 4-5).

¹⁰⁶ Cfr. documento depositato dalla Dott.ssa Agnese Del Giudice in occasione della sua audizione del 14 novembre 2024, X Comitato, DOC. n. 265.1, p. 8.

¹⁰⁷ L’algoritmo alla base di ciascuna *blockchain* definisce la dimensione del blocco, in termini di numero di transazioni o di dati che lo stesso può contenere. Ad esempio, per la *blockchain* applicata alla criptovaluta Bitcoin la capienza del blocco è pari ad 1 MB.

¹⁰⁸ Il funzionamento è così riportato nel documento depositato dalla Dott.ssa Agnese Del Giudice in occasione della sua audizione del 14 novembre 2024, X Comitato, DOC. n. 265.1, p. 10.

pubblico distribuito: la coesistenza, all'interno del medesimo sistema, di una trasparenza radicale dei dati e di un'endemica opacità soggettiva.

Vero è che l'architettura della *blockchain* consente a chiunque di verificare integralmente tutte le transazioni effettuate da sempre, assicurando tracciabilità cronologica e pubblicità delle movimentazioni, ma, allo stesso tempo, tale possibilità è riferita esclusivamente a indirizzi crittografici (pseudonimi), con la conseguenza che il collegamento tra operazioni economiche e persone fisiche o giuridiche resta, in via ordinaria, precluso, salvo interventi esterni di de-anonimizzazione.

In questa tensione strutturale tra esigenze di *accountability* e tutela della riservatezza che si è accomodata la nuova criminalità.

4.2. I *miners* e il meccanismo di validazione.

Nel contesto delle criptovalute, i *miners* sono gli utenti della rete (nodi) che svolgono la funzione di validare le transazioni all'interno di una *blockchain*.

La denominazione richiama l'estrazione mineraria tradizionale: così come i minatori fisici investono lavoro ed energia per estrarre risorse dal sottosuolo, i *miners* digitali impiegano potenza di calcolo ed energia elettrica per “estrarre” le criptovalute e, simultaneamente, garantire sicurezza, integrità e decentralizzazione del sistema.

Come utilmente spiegato¹⁰⁹, il *Proof of Work* richiede ai *miners* di risolvere un problema matematico complesso – il calcolo dell'*hash* crittografico – e di dare prova del risultato ottenuto alla *community* (per dimostrare che il lavoro svolto sia corretto: *proof-of-work*, appunto!), la quale, a sua volta, è chiamata a confermarne l'esattezza.

I calcoli per trovare l'*hash* sono svolti dai *computer* che devono generare una serie di tentativi di calcolo finché non raggiungono l'obiettivo: tanto più il *computer* utilizzato è performante tanto meno tempo verrà impiegato nel risolvere l'enigma matematico.

L'*hash* altro non è che una “impronta digitale” del contenuto originale (del blocco): questo processo è deterministico (lo stesso *input* produce sempre lo stesso *output*), non invertibile (dal *digest* non è computazionalmente fattibile ricostruire l'*input*), altamente sensibile alle variazioni (anche una modifica minima dell'*input* genera un *hash* completamente diverso) e resistente alle collisioni (è estremamente improbabile ottenere lo stesso *hash* da contenuti differenti). Tecnicamente, la funzione

¹⁰⁹ Cfr. documento depositato dalla Dott.ssa Agnese Del Giudice in occasione della sua audizione del 14 novembre 2024, X Comitato, DOC. n. 265.1, pp. 13-15.

crittografica di *hash* consente di trasformare un insieme di dati (cioè il blocco) in una stringa di lunghezza predefinita (codice *hash*).

Il *miner* che per primo risolve il problema matematico – riuscendo a trovare un “*hash* valido”, cioè che rispetta la *difficulty* richiesta dal protocollo – e che ottiene la conferma dagli altri nodi della rete, si aggiudica la possibilità di agganciare il blocco alla catena dei blocchi precedenti e riceve una ricompensa in criptovalute. Quando il blocco viene aggiunto alla *blockchain* le transazioni contenute al suo interno giungono a destinazione.

Questo appena descritto è il meccanismo che determina l’immutabilità del registro pubblico: una volta validato dalla *community* il blocco non può più essere modificato, perché è stato “sigillato” con un codice *hash* creato a partire – in sostanza – dalle informazioni contenute nell’*hash* del blocco che lo precede¹¹⁰.

Ogni blocco validato (successivo al primo), infatti, contiene la “targa” alfanumerica identificativa del blocco precedente a cui è agganciato (*previous hash*), il numero sequenziale che indica la sua posizione all’interno della catena (*index*), l’ora esatta in cui è stato minato (*timestamp*), i dati delle transazioni (cioè oggetto e chiave pubblica associata ai conti coinvolti) e il proprio codice *hash* d’identificazione, calcolato dal *miner* in base a tutte le informazioni appena elencate, compreso – si badi – il *previous hash*. Pertanto, per modificare i dati contenuti in un blocco è necessario ricalcolare tutti quelli precedenti ad esso, dal momento che l’*hash* dell’uno è stato generato a partire dall’*hash* del blocco precedente.

4.3. Il *wallet* e la crittografia asimmetrica.

Come evidenziato¹¹¹, a monte e a valle d’ogni transazione contenuta in un blocco opera un *wallet*, che custodisce due diverse chiavi, una pubblica, che durante il *trading* viene inviata al mittente affinché inoltri il pagamento in criptovaluta, e una privata, che permette l’accesso alle criptovalute, entrambe necessarie per effettuare l’operazione.

La prima – che funge da indirizzo (crittografico) – assolve alla medesima funzione dell’IBAN: può essere liberamente condiviso con chiunque, ma non fornisce accesso al denaro presente sul conto. La seconda è l’equivalente del codice PIN di un bancomat e consente al titolare del *wallet* di autenticarsi crittograficamente, firmare digitalmente le transazioni e dimostrare la titolarità e il controllo degli *asset* associati alla sua chiave pubblica.

¹¹⁰ Cfr. resoconto stenografico della seduta del 14 novembre 2024, X Comitato, audizione della Dott.ssa Agnese Del Giudice, p. 5.

¹¹¹ Cfr. resoconto stenografico della seduta del 14 novembre 2024, X Comitato, audizione della Dott.ssa Agnese Del Giudice, p. 6.

Le criptovalute ricevute, infatti, non confluiscono in un “conto” detenuto presso un intermediario, bensì risultano attribuite, in termini di disponibilità giuridico-fattuale, all’indirizzo indicato dal destinatario: in concreto, l’avvenuta ricezione si traduce nell’iscrizione sulla *blockchain* di una o più unità trasferibili (a seconda dell’architettura del protocollo; ad esempio, UTXO di Bitcoin¹¹²), che restano nella disponibilità del titolare fino a successivo atto di disposizione validamente firmato con la chiave privata.

Il *crypto wallet*, quindi, non contiene criptovalute, bensì le credenziali d’accesso che consentono di autorizzare le transazioni e di esercitare il controllo sugli *asset* digitali registrati sulla *blockchain*, dimostrando la titolarità dell’indirizzo associato¹¹³.

Quanto precede consente di evidenziare uno degli aspetti più rilevanti, ossia che nel sistema *crypto* la possibilità di spendere la criptovaluta non è legata all’identità di una persona, bensì ad una capacità, quella di essere gli unici in grado di eseguire un comportamento: creare e usare correttamente il set di chiavi pubblica-privata. Ne consegue, che se più soggetti conoscono la chiave privata, ciascuno di essi può “spostare” le criptovalute ad essa associate su un *wallet* generato altrove¹¹⁴.

Da un punto di vista operativo assume rilevanza il tipo di *wallet* utilizzato dall’utente. Le tecniche investigative, come si avrà modo di precisare (v. *infra*, parte II, sez. I, § 5), sono chiaramente influenzate dalle caratteristiche strutturali e di funzionamento *del crypto wallet* di volta in volta considerato.

I *cold wallet* – in quanto dispositivi di *storage offline* – si distinguono dagli *hot wallet*, che invece sono sempre connessi a *internet*¹¹⁵.

Tra i primi figurano il *paper wallet* (supporto cartaceo dove sono riportate le chiavi di accesso), l’*hardware wallet* (dispositivo fisico di archiviazione non connesso alla rete come, ad esempio una chiavetta USB) e il *brain-wallet* (con memorizzazione della *passphrase*)¹¹⁶.

Nei secondi, invece, si inquadrano i *wallet software* – che si distinguono, a loro volta, per modalità di utilizzo e di accesso alle chiavi private in *wallet mobile* (programma scaricato sullo smartphone) e *desktop wallet* (che conserva e gestisce le chiavi sul *computer* o altro sistema Android o iOS su cui è

¹¹² La criptovaluta è il valore in sé, mentre gli UTXO sono contenitori monouso di quel valore.

¹¹³ Per un esempio di tutte le tappe del *trading*, cfr. documento depositato dalla Dott.ssa Agnese Del Giudice in occasione della sua audizione del 14 novembre 2024, X Comitato, DOC. n. 265.1, p. 19.

¹¹⁴ Testualmente si legge a p. 21 del documento depositato dalla Dott.ssa Agnese Del Giudice in occasione della sua audizione del 14 novembre 2024, X Comitato, DOC. n. 265.1.

¹¹⁵ Questo tipo di *wallet* è evidentemente esposto ad attacchi informatici, che potrebbero causare il c.d. “*data breach*” (distruzione, perdita, modifica, divulgazione non autorizzata o accesso alle informazioni detenute nel *wallet*, ossia il set di chiavi).

¹¹⁶ In questi casi la chiave privata corrisponde a “x(*passphrase*)”; significa che partendo dalla *passphrase* si calcola direttamente la chiave privata applicando una funzione crittografica deterministica. In pratica il *computer* prende la *passphrase* come *input*, la trasforma matematicamente (*hash/Key Derivation Function*) e produce un numero che viene usato come chiave privata. Chiunque conosca (o indovini) la *passphrase* può ricostruire identicamente la *private key*.

stato scaricato il *software*) – e i *web wallet* (o *wallet online*), i quali operano nel *cloud* e sono accessibili attraverso un *browser* da qualsiasi dispositivo in qualunque momento.

Guardando alla gestione delle chiavi private, tutti i *wallet* si dividono in due macro-categorie: *custodial* e *non-custodial*.

I primi, infatti, offerti dagli *exchanges* di criptovalute o dai *wallet providers*, obbligano gli utenti ad affidare le loro chiavi private al servizio scelto, avendo il solo compito di conservare e custodire i dati di accesso alla piattaforma del servizio (nome utente, *password* e, auspicabilmente, un *token* per l'autenticazione a due fattori).

Diversamente, i secondi consentono agli utenti di esercitare il pieno controllo sui propri dati, eliminando la necessità di ricorrere ad altri gestori per la protezione delle *private keys*¹¹⁷.

Questa è chiaramente la distinzione più significativa nell'ottica dell'uso illecito delle criptovalute: nei modelli *custodial*, il potere di disporre del proprio set di chiavi (soprattutto di quella privata) è mediato dall'intermediario che le detiene – il quale, almeno teoricamente – potrebbe fornire informazioni e eseguire un eventuale ordine di “congelamento”, mentre nei modelli *non-custodial* esso permane in capo all'utente, unico soggetto in grado di disporre in modo irreversibile degli *asset* associati al suo indirizzo¹¹⁸.

Peraltro, sempre nell'ottica dell'elusione di ogni controllo possibile, è doveroso segnalare come ciascun utente possa anche generare una chiave pubblica diversa per ogni transazione (quella privata resta unica), possibilità che ostacola enormemente l'individuazione del soggetto *target*.

5. Metodologia investigativa.

Il modello è nitido: la natura intrinsecamente decentralizzata delle criptovalute, la frammentazione soggettiva resa possibile dalla vocazione globale di *internet* e dalla moltiplicazione delle chiavi pubbliche riconducibili a uno o più utenti contemporaneamente e il ricorso a strumenti di offuscamento delle tracce concorrono a produrre un ambiente operativo caratterizzato da elevata opacità, ridotta tracciabilità e accentuata transnazionalità.

In tale contesto, l'autorità inquirente si trova a dover fronteggiare una duplice criticità: da un lato, la difficoltà di ricostruire la titolarità effettiva delle posizioni giuridico-patrimoniali che si esprimono attraverso indirizzi crittografici formalmente neutri; dall'altro, la dispersione delle evidenze

¹¹⁷ Cfr. documento depositato dalla Dott.ssa Agnese Del Giudice in occasione della sua audizione del 14 novembre 2024, X Comitato, DOC. n. 265.1, p. 27.

¹¹⁸ Sul punto, cfr. documento depositato dalla Dott.ssa Agnese Del Giudice in occasione della sua audizione del 14 novembre 2024, X Comitato, DOC. n. 265.1, p. 22.

probatorie lungo registri distribuiti che, pur essendo teoricamente pubblici e immutabili, risultano di fatto impermeabili a un'immediata riconduzione personalistica.

Ne discende che l'attività investigativa deve strutturarsi secondo una sequenza logico-operativa rigorosa, che muove dall'accertamento preliminare dell'esistenza di *wallet* sospetti e della generazione di flussi transattivi, prosegue con l'individuazione delle operazioni illecite o comunque sospette e dei relativi indirizzi e culmina nella fase decisiva dell'attribuzione soggettiva, vale a dire nell'associare i poli della transazione a persone fisiche determinate¹¹⁹.

Se, normalmente, a partire da un codice IBAN è possibile conoscere il nome del correntista, con una chiave pubblica non è consentito replicare lo stesso passaggio, perché manca – giova ribadirlo – un *server* centrale che contenga le informazioni che circolano sulla rete e un gestore che le renda disponibili a richiesta della pubblica autorità o degli altri utenti. Inoltre, come già accennato, un utente *crypto* può autonomamente generare un indirizzo diverso per ogni transazione, per un numero potenzialmente infinito.

L'attività di "abbinamento", che rappresenta il punto di frizione tra l'astrattezza algoritmica del sistema e l'esigenza processuale di personalizzazione della responsabilità, impone il ricorso a complesse tecniche di *blockchain analysis* – la cui efficacia dipende da diversi fattori (v. *infra*, parte II, sez. I, § 5.1.) –, integrate con strumenti tradizionali di indagine, quali intercettazioni, perquisizioni, acquisizioni documentali, anche attraverso i meccanismi di cooperazione giudiziaria.

Solo all'esito di questa ricostruzione è possibile procedere efficacemente al congelamento dei "fondi", che, nel settore delle cripto-attività, assume connotati peculiari: il sequestro non può limitarsi a una mera apprensione materiale, ma implica la necessità di trasferire le disponibilità digitali in un ambiente centralizzato, sottoposto a gestione e controllo pubblici, idoneo a garantire integrità, conservazione del valore e non dispersione del bene (v. *infra*, parte II, sez. I, §§ 5.2.-5.2.2.).

Come già più volte affermato, il nostro Codice di rito non prevede una disciplina dei mezzi di ricerca della prova adeguata al fenomeno, né una normativa *ad hoc* di tipo patrimoniale.

Nell'ipoacusia generale si sono sviluppate prassi diverse tra le forze dell'ordine: urge, pertanto, che sia il legislatore a decidere se e quale prediligere, risolvendo alla fonte il problema. In quest'ordine di idee, la presente Relazione mira ad illustrare il metodo possibilmente più virtuoso rappresentato nel corso delle audizioni, proponendo correlativamente – nella terza parte di questo lavoro – delle proposte di intervento che non siano un mero adattamento tecnico delle categorie tradizionali, quanto, piuttosto, una ricostruzione funzionale degli istituti investigativi e reali alla luce del fenomeno tecnico-giuridico da fronteggiare, al fine di evitare che l'anonimato tecnologico e la

¹¹⁹ Cfr. resoconto stenografico della seduta del 14 novembre 2024, X Comitato, audizione della Dott.ssa Agnese Del Giudice, p. 7.

decentralizzazione infrastrutturale si traducano in una strutturale zona franca, senza, però, scardinare l'architettura garantista tipica del nostro procedimento penale.

5.1. Tracciamento e de-anonimizzazione: tecniche e limiti.

Da un punto di vista tecnico, l'attività di tracciamento e di de-anonimizzazione si fondano su tre attività complementari di *blockchain forensics*: il *labeling*, il *clustering* e la *mixnet recognition*.

Nel complesso, si tratta di attività che consentono di individuare le transazioni illecite, di aggregare gli indirizzi e di associarli – eventualmente tramite analisi euristiche – a un soggetto o a un *exchange* dove l'utente potrebbe avere un'identità digitale¹²⁰.

Il *labeling* consiste, in particolare, nell'associare identità o categorie funzionali a indirizzi e transazioni sulla base di evidenze *on-chain* e *off-chain* (*pattern* di spesa, interazioni note con *exchanges*, dati OSINT), trasformando dati grezzi in informazioni semantiche utilizzabili per l'analisi. Semplicemente, è come mettere “etichette” a conti altrimenti anonimi, ad esempio riconoscendo che un certo indirizzo appartiene probabilmente a un servizio di pagamento perché riceve molti piccoli importi e li consolida periodicamente.

Il *clustering* mira, invece, a raggruppare indirizzi che con alta probabilità sono controllati dalla stessa entità, sfruttando euristiche come il *co-spending* (più *input* nella stessa transazione), la gestione del *change address* e la temporalità dei flussi: in sostanza, se più “portafogli” si muovono sempre insieme o seguono schemi coerenti, vengono trattati come un unico attore.

La *mixnet recognition*, infine, è finalizzata a riconoscere automaticamente l'uso servizi o schemi di offuscamento mediante l'osservazione di “firme comportamentali specifiche”, cioè schemi statistici e temporali ricorrenti nel flusso dei dati. L'obiettivo non è de-anonimizzare direttamente gli utenti, ma identificare la presenza e il tipo di infrastruttura di anonimizzazione o di tecniche di mascheramento del traffico che viene, quindi, distinto dal traffico “normale” mediante modelli analitici o algoritmi di *machine learning* addestrati su tali *pattern*.

Nel corso dell'istruttoria è stato osservato come il buon esito dell'attività di tracciamento e di de-anonimizzazione dipenda da diversi fattori¹²¹.

Innanzitutto dal tipo di *blockchain*. In quelle “trasparenti” – ad esempio, Bitcoin, Ethereum, Litecoin, XRP, etc. – l'attività di tracciamento è agevolata: i dati essenziali della transazione – tra cui importo e indirizzi coinvolti – sono visibili pubblicamente. In questo caso, chiaramente, le Forze di polizia

¹²⁰ In questi termini la Dott.ssa Agnese Del Giudice, resoconto stenografico della seduta del 14 novembre 2024, X Comitato, p. 7.

¹²¹ Cfr. documento depositato dalla Dott.ssa Agnese Del Giudice in occasione della sua audizione del 14 novembre 2024, X Comitato, DOC. n. 265.1, p. 23.

possono analizzare tutte le movimentazioni a ritroso, fino alla prima mai avvenuta, senza dover attivare alcun tipo di collaborazione. Possono farlo attraverso un’ispezione esplorativa della *blockchain* – che può essere scaricata *off-line* o analizzata *on-line* attraverso gli “esploratori” (*blockchain explorer*)¹²² – oppure grazie a *software* di taratura *enterprise* (del tipo *Chainalysis* e *Crystal Blockchain*) in grado di offrire monitoraggio in tempo reale, analisi dei rischi delle transazioni e tracciamento dei fondi.

L’unico problema, in questa ipotesi, resta la de-anonimizzazione. Gli inquirenti ben potrebbero valersi di una previa verifica effettuata da *exchanges* e *wallet providers*, i quali, di regola, conservano indirizzi IP, informazioni e documenti d’identità richiesti ai propri utenti al momento dell’iscrizione, nonché informazioni complete e accurate sui beneficiari dei trasferimenti di fondi e cripto-attività. Tuttavia, l’ipotesi della fattiva collaborazione appare, in concreto, poco plausibile, dal momento che i prestatori di servizi si esporrebbero al rischio di perdere una parte consistente della propria clientela: il *trader* di criptovalute ha particolarmente a cuore la propria *privacy*, per cui difficilmente sceglierebbe di affidarsi ad un *wallet provider* o ad un *exchange* che collabori (facilmente) con la pubblica autorità. Peraltro, l’esperienza insegna che, nella gran parte dei casi, chi delinque in ambito *crypto* non utilizza affatto i prestatori di servizi, oppure si rivolge a quelli meno “disponibili” a interagire con l’autorità giudiziaria, ma più frequentemente si serve di *wallet non-custodial* che garantiscono una maggiore protezione in termini di riservatezza¹²³.

Diversamente, ove manchi la trasparenza “*by design*” la *blockchain* omette di indicare l’importo della transazione e/o gli indirizzi dei *wallet* coinvolti. A fronte di un registro pubblico non completamente trasparente, le Forze di polizia incontrano difficoltà significative – se non dei veri e propri sbarramenti – nell’attività sia di tracciamento che di de-anonimizzazione.

Il mercato delle criptovalute si è notevolmente diversificato negli ultimi anni. Il Bitcoin – prima criptovaluta conosciuta – condivide il mercato con molte altre monete, note come “*altcoin*”, molte delle quali offrono non solo più elevati livelli di velocità della transazione, ma soprattutto un livello superiore di *privacy*.

¹²² Si tratta di siti *web* (come *Etherscan.com*, *Blockchain.info* o *Blockchair.com*), liberamente accessibili, che consentono di navigare, ispezionare e analizzare in tempo reale i dati di una specifica *blockchain*.

¹²³ Così, testualmente, il documento depositato dalla Dott.ssa Agnese Del Giudice in occasione della sua audizione del 14 novembre 2024, X Comitato, DOC. n. 265.1, p. 22. Cfr. anche il resoconto stenografico dell’audizione del Gen.B. Antonio Mancazzo, seduta del 25 febbraio 2025, X Comitato, p. 6, ove afferma «[l]a nostra difficoltà è di cercare di dare un nome e cognome al titolare di un *wallet*. [...] [C]on la *blockchain analysis* [...] riusciamo a individuare dei portafogli [...] però quel portafoglio innanzitutto dobbiamo trovarlo nel possesso del soggetto del signor Alfa. Per arrivare a capire chi è il signor Alfa dobbiamo sfruttare qualche punto debole di tutta la catena e cioè cercare di avere i dati attraverso un *Exchange compliant*. È chiaro che i criminali si rivolgono *Exchange non compliant* che sono spesso dall’altra parte del mondo. [...] Per noi *compliant* vuol dire affidabile».

Secondo quanto riportato da un'indagine dell'Europol condotta nel 2022¹²⁴, nei primi anni successivi alla diffusione delle cripto-attività, la criminalità riteneva che l'uso di Bitcoin garantisse un elevato livello di anonimato. Tuttavia, il progresso degli strumenti di analisi della *blockchain* ha rapidamente dimostrato che il Bitcoin non era né completamente anonimo, né irrintracciabile, come dimostrato dal successo di numerose operazioni investigative. Questo ha spinto le organizzazioni criminali ad adottare nuove strategie per aumentare il grado di riservatezza, ricorrendo a criptovalute che non consentono alcuna tracciabilità.

Due esempi su tutti. Monero permette di effettuare transazioni anonime nascondendo gli indirizzi di invio e di ricezione e gli importi delle transazioni utilizzando diverse tecniche e tecnologie. Monero vanta, in realtà, un triplice livello di *privacy by default*: una tecnologia per nascondere il destinatario (*stealth addresses*, cioè indirizzi “usa-e-getta” per ogni transazione), una per nascondere l'importo inviato (RingCT, con cui la quantità trasferita viene divisa in più importi gestiti come fossero transazioni separate) e una per nascondere il mittente (il sistema seleziona casualmente chiavi pubbliche passate dalla *blockchain* per formare un anello di firme “esca”)¹²⁵.

Zcash, invece, supporta sia indirizzi trasparenti, che schermati. In quest'ultima ipotesi si avvale di una forma di crittografia a conoscenza zero (*ZK-Snark – Zero-Knowledge Succinct Non-Interactive Argument of Knowledge*), cioè una tecnologia crittografica che permette a una parte (il «*prover*») di dimostrare a un'altra parte (il «*verifier*») di conoscere un'informazione (un «*witness*») senza rivelare l'informazione stessa: le transazioni schermate sono completamente crittografate sulla *blockchain*, ma comunque verificate come valide secondo le regole di consenso della rete utilizzando le «*prove ZK-Snark*».

L'esito dell'attività investigativa funzionale al tracciamento e alla de-anonimizzazione è ampiamente influenzato anche dall'utilizzo di servizi e sistemi di offuscamento.

Con l'uso dei VPN (*virtual private network*) o della rete TOR (*the Onion Router*), ad esempio, il proprio *computer* risulterà collocato in un'altra città, in un altro Paese o, addirittura, in un altro continente. Utilizzando servizi di *mixers/tumblers* si interrompe il legame diretto tra indirizzo di origine e indirizzo di destinazione: eseguono, ad esempio, un'attività di filtraggio e riassegnazione casuale di una serie di transazioni in entrata, oscurando la connessione tra l'operazione in entrata a quella in uscita¹²⁶, oppure aggregano i fondi di più utenti in un *pool* comune e successivamente

¹²⁴ Europol Spotlight, Cryptocurrencies: tracing the evolution of criminal finances, in www.europol.europa.eu, 26 gennaio 2022.

¹²⁵ L'*output* è come un assegno: quando qualcuno paga 10 Monero, il destinatario riceve un *output* di 10 XMR presi dal portafoglio del mittente.

¹²⁶ Una delle tecniche più efficaci utilizzate dai *mixer* è il “CoinJoin”. Questo processo mescola gli *input* e *output*, rendendo difficile determinare chi ha inviato cosa e chi, aumentando così l'anonimato delle transazioni: cfr. relazione del Gen.B. Gianluca Vitagliano, DOC. n. 287.1, p. 3, nt. 4.

ridistribuiscono importi equivalenti – al netto di commissioni – verso nuovi indirizzi¹²⁷. Impiegando la *chain hopping*, invece, fondi di provenienza criminale vengono trasferiti rapidamente attraverso più *blockchain* diverse, spezzando la continuità analitica delle transazioni, attraverso *swap* (diretto e immediato) tra criptovalute – eseguibile su *exchange* centralizzati (CEX) o decentralizzati (DEX) –, oppure facendo leva sui *cross-chain bridges*¹²⁸, ovvero piattaforme cc.dd. “*multi-chain*” che consentono e promuovono l’interoperabilità tra più *blockchain*¹²⁹. Ancora. La criminalità si avvale, altresì, dei cc.dd. “*money mule* di criptovaluta”, ossia di individui reclutati, spesso inconsapevolmente, per trasferire i fondi ottenuti illegalmente: questi ricevono criptovalute da una fonte per spostarle a un’altra, fungendo da intermediari per nascondere l’origine illecita dei fondi¹³⁰. È di immediata evidenza l’ostacolo, quasi insormontabile, che si frappone tra l’autorità di *law enforcement* e la criminalità. Chi “ricicla” ricchezza ha un’unica esigenza che corrisponde alla necessità di nascondere l’effettiva titolarità del bene e di celare l’origine criminale dei fondi impiegati per acquistare criptovaluta o l’origine criminale della stessa laddove la ricchezza illecita si produca direttamente in *virtual-asset*.

5.2. Il sequestro di criptovalute.

È stato evidenziato con estrema chiarezza: l’errore più frequente è quello di pensare che per apporre il vincolo di indisponibilità sulle criptovalute sia sufficiente sequestrare il *wallet* ad esse associato per eseguire una copia del *set* di chiavi¹³¹.

Questa conclusione è suggerita dalla fisionomia tecnica di un fenomeno che, come già rimarcato, non è legato all’identità di una persona, ma alla capacità di creare e usare correttamente il set di chiavi pubblica-privata.

Prendiamo ad esempio l’*hardware wallet* (sulla classificazione v. *supra*, parte II, sez. I, § 4.3.) e, in particolare, una chiavetta USB. Si potrebbe eseguire il classico sequestro del dispositivo, per poi analizzarlo ed estrarre le chiavi, ma sarebbe un’attività del tutto infruttuosa dal punto di vista investigativo: perché il soggetto a cui è stato sottratto il “contenitore” ben potrebbe aver fatto un

¹²⁷ Cfr. documento depositato dalla Dott.ssa Agnese Del Giudice in occasione della sua audizione del 14 novembre 2024, X Comitato, DOC. n. 265.1, p. 23.

¹²⁸ Nello specifico, le soluzioni di interoperabilità tra *blockchain* possono essere di due tipi: *bridge burn-and-mint*, che bloccano l’*asset* sulla *blockchain* di partenza, prima di crearlo su quella di destinazione; e *bridge lock-and-mint*, che invece eliminano l’*asset* prima di riprodurlo sulla DLT di destinazione. In entrambi i casi, l’effetto finale è lo stesso: il medesimo valore monetario si trasforma in un nuovo *digital asset*, corrente su un diverso registro informatico.

¹²⁹ Cfr. Banca d’Italia, *Riciclaggio e blockchain: si può seguire una traccia nel mondo crypto?*, Occasional Paper n. 893, 2024, in <https://www.bancaditalia.it/pubblicazioni/qef/2024-0893/index.html>.

¹³⁰ Cfr. relazione del Gen.B. Gianluca Vitagliano, DOC. n. 287.1, p. 3, nt. 3.

¹³¹ Così, testualmente, la Dott.ssa Agnese Del Giudice, resoconto stenografico della seduta del 14 novembre 2024, X Comitato, p. 9.

backup del “contenuto” (il set di chiavi) e, quindi, potrebbe accedere al suo *wallet* da un altro dispositivo e spostare le criptovalute (anche escludendo l’agire fraudolento, il soggetto potrebbe eseguire uno spostamento anche a seguito di dissequestro disposto in sede di riesame della misura cautelare reale); perché, pur avendo certezza che nessuno abbia effettuato il *backup* delle chiavi o conosca la chiave privata, il detentore potrebbe avere a disposizione la c.d. “*master key*”, la quale gli consentirebbe di recuperare la chiave privata e ripristinare il suo *wallet* altrove¹³². In questa dinamica, l’unico caso in cui il sequestro “fisico” del dispositivo sarebbe idoneo a sottrarre i “fondi” al soggetto che ne abbia la disponibilità è quello in cui quest’ultimo non abbia memorizzato le parole che compongono la *mnemonic* (*seedphrase*) della *master key* da nessuna parte. Caso piuttosto inusuale e poco probabile, perché il rischio di danneggiamento o perdita del *device* è debitamente tenuto in considerazione da chi ne fa uso, il quale salverà in uno o più luoghi diversi le parole di *mnemonic*. Guardando al *web wallet* il risultato non cambia. Si tratta di un portafoglio ospitato su un sito *web*, accessibile da qualsiasi dispositivo dotato di connessione a *internet*, le cui chiavi private sono conservate sul *server* del fornitore.

L’accesso ai *wallet on-line* avviene, di regola, con il *login* sul proprio *account*. Gli inquirenti ben potrebbero cambiare le *password* di accesso; tuttavia, il soggetto potrebbe, dal suo canto, eseguire un *reset* delle credenziali (tutte le piattaforme *online* lo consentono) e ottenere nuovamente accesso all’*account web*. Ne consegue che l’autorità giudiziaria dovrebbe potersi rivolgere al prestatore di servizio affinché “conghi” il *wallet target* o l’*account*, così da spostare l’ammontare in un fondo controllato¹³³. A riguardo – come più volte sottolineato – il braccio di mare che sempre divide l’essere dal dover essere si è ampliato a dismisura: numerose sono le criticità legate alla possibile collocazione estera del prestatore di servizi e alla necessità di strumenti di cooperazione giudiziaria per l’effettiva esecuzione.

Se questa è la situazione, la conclusione, allora, è piuttosto ovvia: per guadagnare il controllo sul *wallet* non è certamente sufficiente limitarsi a eseguire una copia della chiave privata, così come non sempre è utile procedere al sequestro del PC, della periferica USB, dello *smartphone* etc. con successiva copia forense dei sistemi.

¹³² Per queste riflessioni cfr. il resoconto stenografico dell’audizione della Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato, p. 9, la quale prosegue: «[I]a *master key* sostanzialmente è il nostro codice PUK della SIM: quando sbagliamo a inserire nella SIM il nostro codice PIN, mettiamo il codice PUK che ci rigenera l’accesso. La *master key* funziona esattamente allo stesso modo. È composta dalla *mnemonic*, ossia da dodici, diciotto o ventiquattro parole generate a caso dal sistema che la crea, che il soggetto può memorizzare o scriversi da qualche parte, che una volta inserita nel sistema è in grado di rigenerare il *wallet* compromesso».

¹³³ Cfr. resoconto stenografico dell’audizione della Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato, p. 10.

L'attività di sequestro deve essere sempre calibrata sul tipo di *wallet target*, avendo ben chiaro che, per apporre il vincolo di indisponibilità sulle criptovalute, è necessario guadagnare il “controllo” sul *wallet*.

È stato già anticipato che l'oggetto immediato del sequestro non è il “*token*” in senso materiale, bensì la disponibilità giuridico-fattuale della risorsa digitale, resa possibile dal controllo della chiave privata¹³⁴.

L'*iter* prospettato in sede di audizione, e di seguito riportato, non risponde ad uno schema codificato, ma è frutto di un'analisi ragionata delle caratteristiche strutturali e del funzionamento dei *crypto-wallet*: «per guadagnare il controllo sul *wallet* l'inquirente deve ottenere la disponibilità esclusiva della chiave privata del soggetto; ottenuta la disponibilità esclusiva l'inquirente deve immediatamente trasferire le criptovalute in un conto controllato dalla pubblica autorità per garantire la stabilità del valore di quanto sequestrato ed evitare che chiunque possa sottrarre i “fondi” vanificando l'attività investigativa»¹³⁵.

È oltremodo necessario che l'esigenza investigativa funzionale alla prevenzione e repressione dei reati non si traduca in un sacrificio indebito delle facoltà difensive. In quest'ordine di idee, appare necessario garantire il controllo difensivo, quantomeno nelle forme compatibili con le esigenze di segretezza e di urgenza dell'atto, assicurando la tracciabilità delle operazioni, la conoscibilità (*ex post*) delle modalità esecutive – da rendere standardizzate e verificabili – e la possibilità di contestarne la legittimità, anche sotto il profilo della proporzionalità. Per consentire alla difesa di verificare l'integrità della catena di custodia digitale è doverosa una documentazione analitica delle operazioni (incluse le evidenze informatiche relative a indirizzi, *hash* e transazioni) (sulle proposte a riguardo, v. *infra*, parte III, § 2.1.).

5.2.1. Trasferimento e destinazione.

Guadagnare la disponibilità esclusiva della *private key* – come anticipato – non esaurisce l'attività di sequestro, la quale si perfeziona con il trasferimento della risorsa digitale in un “fondo” a controllo pubblico.

Sul punto vengono in rilievo due problemi. Il primo: stabilire verso quale destinazione spostare le criptovalute “oggetto” di sequestro. Il secondo: gestire materialmente l'attività di trasferimento.

¹³⁴ Cfr. il resoconto stenografico dell'audizione del Gen.B. Antonio Mancazzo, seduta del 25 febbraio 2025, X Comitato, p. 4: «l'ablazione non è simile a quella che avviene in un sequestro normale quando procediamo su fondi su un conto corrente. Non togliamo la criptovaluta dalla *blockchain* ma togliamo soltanto il possesso e la disponibilità in capo al titolare, ammesso che siamo in grado di individuarlo».

¹³⁵ Cfr. documento depositato dalla Dott.ssa Agnese Del Giudice in occasione della sua audizione del 14 novembre 2024, X Comitato, DOC. n. 265.1, p. 26.

La destinazione. Allo stato attuale, dove la rete dei doveri in capo ai *providers* di crypto-attività a volte è addirittura inesistente (in ragione della collocazione geografica *extra* UE), l'apertura di un conto intestato al Tribunale presso un *exchange* sul quale trasferire le “somme” sequestrate non rappresenta la mossa più saggia.

La comodità di accedere ad un conto basandosi sulla titolarità, con minori rischi di perdita credenziali e chiavi di accesso, va, infatti, controbilanciata con i rischi che si corrono nel lasciare a un'azienda, sostanzialmente privata, la disponibilità delle criptovalute sequestrate e la responsabilità della loro conservazione. Sono frequenti le notizie di *exchanges* che subiscono attacchi, furti, ammanchi o più semplicemente scompaiono nel nulla¹³⁶.

Si ritiene conveniente e – comunque – preferibile creare un *wallet ad hoc*: la prassi investigativa si è già incanalata nel senso di creare un *wallet* in sede di sequestro, rimettendo la scelta sul tipo di portafoglio da generare agli operatori di polizia giudiziaria¹³⁷, nel rispetto di alcuni accorgimenti.

Nel corso dell'istruttoria è stata messa in evidenza la prassi più virtuosa (tra quelle conosciute)¹³⁸ per ridurre al minimo il rischio di responsabilità degli operatori: creare un *wallet multisig*, cioè applicare il c.d. “Schema di Shamir”, che consiste nel proteggere il *wallet* con codici generati da più operatori e tutti necessari per accedere. In tal caso, nessun operatore conosce integralmente la chiave privata, eliminando un punto critico di vulnerabilità e aumentando significativamente la protezione contro gli attacchi informatici.

Lo si anticipa sin d'ora: anche per sollevare la polizia giudiziaria dell'onere di creare un *wallet* per ogni singola attività – incombenza non semplice da gestire soprattutto *in live* – sarebbe preferibile creare un “*wallet* centrale”, in funzione di sezione del FUG, così che ogni trasferimento di criptovalute su scala nazionale possa dirsi centralizzato e controllato per conto del Ministero della Giustizia¹³⁹.

¹³⁶ Per queste riflessioni, cfr. resoconto stenografico dell'audizione della Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato, p. 10. Al contrario, ritiene sufficiente individuare un *exchange compliant* il Gen.B. Antonio Mancazzo: cfr. resoconto stenografico, seduta del 25 febbraio 2025, X Comitato, p. 4.

¹³⁷ Ad esempio, come rappresentato dal Gen.B. Antonio Mancazzo nella sua relazione, è possibile creare un *paper wallet*; «onde evitare la possibilità di recuperare le credenziali di accesso al *paper wallet*, tutte le operazioni di creazione avvengono in modalità “*live*”, che consente la distruzione irreversibile dei dati al termine delle operazioni (coincidenti con la chiusura del programma “*live*”, detto “macchina virtuale”). la stampa delle credenziali di accesso ai fondi sequestrati che possono essere una “chiave privata” o una “*seed phrase*”, avviene mediante stampante offline, sempre al fine di non consentire un recupero dei dati di stampa. Nel tempo, è stato progettato dai militari in forza al reparto, un software in grado di gestire il processo di generazione delle credenziali di accesso al *paper wallet*» (cfr. DOC. n. 316.1, p. 14).

¹³⁸ Cfr. resoconto stenografico dell'audizione della Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato, p. 10.

¹³⁹ Tanto propone la Dott.ssa Agnese Del Giudice nella sua audizione, seduta del 14 novembre 2024, X Comitato, p. 10 del resoconto stenografico.

Il trasferimento. Esso si perfeziona, naturalmente, con la movimentazione delle criptovalute dal portafoglio in uso all'indagato verso il *wallet* controllato dalla polizia giudiziaria. Tale attività è assai delicata e complessa, anche perché, una volta terminata, risulta imm modificabile sia nell'*an* che nel *quantum*. Ne consegue la necessità, per gli operatori, di prestare un elevato livello di attenzione a tutte le attività da porre in essere, per le quali non esistono margini di errore accettabili¹⁴⁰.

Trasferite le somme il sequestro può dirsi perfezionato.

Da un punto di vista strettamente processuale, i profili di maggior delicatezza riguardano l'eventuale partecipazione dell'indagato all'attività di creazione del *wallet* e di trasferimento delle criptovalute.

Le caratteristiche funzionali delle criptovalute – quali l'“anonimato”, l'immaterialità, il trasferimento immediato e senza confini, l'assenza di un organo di controllo centrale – rendono difficile optare per una soluzione diversa da quella dell'attività tecnica svolta unilateralmente dagli inquirenti. L'art. 360 c.p.p., imponendo gli avvisi alle parti, introduce inevitabilmente una finestra temporale nella quale sussiste il rischio che le criptovalute vengano movimentate.

Del resto, si discute pur sempre di un atto palese, il cui “effetto sorpresa” – garante, soprattutto in questo contesto investigativo, di risultati diversamente non ottenibili – potrebbe dirsi adeguatamente temperato da un controllo *ex post*, attraverso la motivazione del provvedimento, senza necessità di eseguire l'attività tecnica nella forma partecipata¹⁴¹.

Resta, dunque, degna di considerazione l'esigenza di reperire con prontezza beni che, con straordinaria facilità, potrebbero essere oggetto di dispersioni o spostamenti, accidentali o intenzionali.

Nondimeno è necessario prevedere *standard* operativi rigorosi e codificare il percorso di corretta acquisizione (sulle proposte a riguardo, v. *infra*, parte III, § 2.1.).

5.2.1.1. Transazioni e commissioni: spese di giustizia?

Viene in rilievo, anzitutto, il problema delle commissioni di transazione endogene al protocollo (*transaction fee*). Si tratta di un costo strutturale del mezzo di trasferimento, variabile in funzione della congestione della rete e dei meccanismi di mercato che determinano la *fee*. Il trasferimento verso il *wallet* controllato ha, dunque, un costo per lo Stato.

È doveroso considerare, come pure è stato evidenziato, che le commissioni di transazione determinano priorità di inclusione, producendo effetti allocativi e distributivi. Questo significa che i

¹⁴⁰ In questi termini, il Gen.B. Antonio Mancazzo nella sua relazione: cfr. DOC. n. 316.1, p. 14.

¹⁴¹ Cfr. resoconto stenografico dell'audizione della Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato, p. 11.

miners tendono ad includere per prime le transazioni che offrono commissioni più elevate, perché massimizzano il proprio rendimento¹⁴².

È, dunque, consigliabile non essere troppo parchi per non correre il rischio di dover attendere ore (se non giorni, nei periodi “peggiori”) per poter vedere le transazioni andate a buon fine e, quindi, per poter confermare che il sequestro è stato eseguito correttamente.

Le commissioni di transazione vanno tenute in considerazione anche ai fini di un eventuale dissequestro (quale onere tecnico inevitabile per la restituzione del bene nella sua forma nativa) o in fase di vendita a seguito di ablazione definitiva. In sostanza, sequestrare 10 Bitcoin e dissequestrarli avrà un costo che dipenderà dal periodo, dalla concorrenza, dai minatori (il valore di mercato di una criptovaluta dipende, cioè dalla legge della domanda e dell’offerta: più è richiesta e più il suo valore aumenta e viceversa). Tali costi dovrebbero, dunque, essere qualificati come “spese di giustizia”¹⁴³.

5.2.2. Deposito e custodia.

Depositare le criptovalute in un “luogo sicuro” sottoposto a gestione e controllo pubblico impone una riflessione sulla possibilità di convertire le criptovalute in moneta fiat per poi depositarle presso il Fondo Unico Giustizia (FUG).

Nonostante alcune iniziali incertezze, la prassi investigativa pare essersi consolidata nel senso della utilità di una conversione, ponendo l’ulteriore e correlato problema del momento esatto in cui eseguirla, se già in sede di sequestro o, piuttosto, di confisca definitiva.

La scelta non è agevole, principalmente per due ordini di ragioni che spingono in senso opposto. Il valore della criptovaluta è fortemente volatile, con oscillazioni di prezzo ampie e repentine; sicché sarebbe utile “congelarlo” immediatamente per evitare la dispersione. D’altro canto, la conversione ha dei costi rilevanti¹⁴⁴ (commissioni di *trading/spread*, costi di prelievo, consulenze), che non potrebbero essere recuperate in caso epilogo favorevole all’indagato.

Al riguardo è stato osservato come alcune Procure includano nel decreto di perquisizione e sequestro l’avviso per l’indagato di un termine (spesso non superiore ai 30 giorni) per decidere se aderire alla conversione¹⁴⁵. Il fine è chiaramente quello di preservare il valore “attuale” del *quantum* sequestrato.

¹⁴² Cfr. resoconto stenografico dell’audizione della Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato, pp. 10-11.

¹⁴³ Cfr. resoconto stenografico dell’audizione della Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato, pp. 10-11.

¹⁴⁴ Cfr. resoconto stenografico dell’audizione del Gen.B. Antonio Mancazzo, seduta del 25 febbraio 2025, X Comitato, p. 4.

¹⁴⁵ Cfr. resoconto stenografico dell’audizione del Gen.B. Antonio Mancazzo, seduta del 25 febbraio 2025, X Comitato, p. 4.

Tuttavia, è doveroso sottolineare che, ad oggi, la conversione in moneta legale, pur utile a fissare il valore delle criptovalute sequestrate, rappresenterebbe – a rigore – un intervento che esorbita dal compito di mera custodia assegnato agli inquirenti (art. 259 c.p.p.) e potrebbe, dunque, divenire, in caso di esito negativo dell’*iter* processuale, motivo di doglianza da parte dell’indagato qualora il valore della criptovaluta avesse, nel frattempo, subito un rialzo e si fosse registrato, per effetto del sopravvenuto sequestro, un mancato guadagno¹⁴⁶.

Queste osservazioni rendono ormai indifferibile un preciso intervento di modifica (sulle proposte a riguardo, v. *infra*, parte III, § 2.1.).

Sezione II – Uso illecito della crittografia

1. Metodi e scenari.

L’indagine conoscitiva ha preso le mosse dalla constatazione che le organizzazioni criminali (anche) di stampo mafioso hanno progressivamente adottato strumenti tecnologici avanzati per le proprie comunicazioni, sfruttando, in particolare, le piattaforme di messaggistica con crittografia *end-to-end* e dispositivi appositamente modificati – i cc.dd. “criptofonini” – per garantire l’anonimato e resistere ai tentativi di intercettazione.

Quest’ultimi, in particolare, formalmente definiti come *Hardened Secure Communication Platforms* (HSCPs) o *Dedicated Encrypted Communication Devices* (DECDs), rappresentano da più di un decennio il principale mezzo di comunicazione in uso alle organizzazioni criminali nazionali e transfrontaliere, in quanto funzionali all’elusione di qualunque attività di sorveglianza da parte delle autorità. Essendo “non intercettabili” – neppure, s’intende, con lo strumento creato per aggirare la crittografia *end-to-end* implementata dalle moderne *app* di comunicazione – ed avendo costi di licenza contenuti, essi vengono impiegati anche da sodalizi di più “basso rango criminale”¹⁴⁷, rendendo vano l’uso dei tradizionali mezzi di ricerca della prova su tutti i livelli.

Questo secondo passaggio evolutivo (dalla crittografia *end-to-end* alla criptofonia) ha determinato una significativa erosione delle capacità investigative tradizionali, creando un divario sempre più ampio tra gli strumenti di captazione a disposizione delle forze dell’ordine e quelli utilizzati dalla criminalità mafiosa e, in generale, organizzata.

¹⁴⁶ In questi termini la Dott.ssa Agnese Del Giudice nel corso della sua audizione, seduta del 14 novembre 2024, X Comitato (cfr. resoconto stenografico, p. 11).

¹⁴⁷ Cfr. documento depositato dal Ten. Col. Luca Flebus a corredo della sua audizione del 18 aprile 2024, X Comitato, DOC. n. 139.1, p. 8.

L'istruttoria del X Comitato ha evidenziato con chiarezza come il problema non sia tanto di natura tecnologica, quanto di tipo regolatorio: gli OTT, ossia operatori che offrono servizi e contenuti attraverso la rete *internet* (*Over-The-Top*)¹⁴⁸ operano in un sostanziale vuoto normativo, senza essere soggetti agli obblighi che gravano sugli operatori di telecomunicazioni tradizionali; si aggiunga l'assenza di qualsivoglia disciplina su accesso, acquisizione e conservazione dei dati allocati presso i *server* (in Italia o all'estero) che gestiscono servizi di criptofonia, nonché, a monte, la mancanza di una qualificazione giuridica delle attività intrusive (*hacking* governativo, acquisizione preventiva dei *server*, captazione generalizzata) (v. *infra*, parte II, sez. II, §§ 2.2. e 3.3.1.).

Le audizioni svolte dal X Comitato in quest'ambito tematico hanno coinvolto rappresentanti del settore delle telecomunicazioni (Gruppo TIM), delle Forze di polizia (Polizia Postale e SCO), del settore privato delle intercettazioni legali (Area S.p.A.) e degli organismi di standardizzazione e formazione (*Lawful Interception Academy*), con l'obiettivo di: comprendere la natura tecnica del problema posto dalla crittografia (E2E – criptofonia); analizzare il quadro regolatorio vigente e le sue lacune, anche esaminando le esperienze investigative europee e internazionali; formulare proposte concrete per recuperare efficacia investigativa nel rispetto delle garanzie costituzionali.

Nel redigere la presente Relazione si è ritenuto altresì opportuno dar conto delle ultime prospettive evolutive delle comunicazioni “blindate”, assumendo i tre spunti emersi in sede di audizione a riguardo come base di partenza di un'analisi autonoma.

Resta ferma, tuttavia, l'assenza di qualsiasi pretesa di completezza. L'analisi proposta non intende esaurire la complessità del fenomeno, né offrire, in questa sede, una trattazione sistematica e compiuta delle sue implicazioni teoriche e applicative. L'intento è solo quello di misurare l'orizzonte di adattamento dell'ordinamento anche rispetto a scenari nei quali l'indisponibilità tecnica del contenuto comunicativo deriva, a volte, dalla combinazione di automatizzazione *trustless* (senza fiducia), pseudonimia crittografica e resilienza infrastrutturale (come nel caso degli *smart contract*)¹⁴⁹, altre volte dall'uso di infrastrutture diverse da quelle terrestri (ad esempio, la fonia satellitare)¹⁵⁰, ed altre ancora dall'uso di strategie di *hardening* socio-tecnico (nel caso delle piattaforme di *gaming*)¹⁵¹ (v. *infra*, parte II, sez. II, § 4).

¹⁴⁸ L'espressione “*Over-The-Top*” indica che il servizio “passa sopra” le infrastrutture degli operatori di rete tradizionali, utilizzando solo la connessione internet dell'utente.

¹⁴⁹ Il Magg. Francesco Venditti ne sottolinea l'impenetrabilità: cfr. resoconto stenografico dell'audizione del Gen.B. Mancazzo, seduta del 25 febbraio 2025, X Comitato, p. 7.

¹⁵⁰ La considera una problematica futuribile il Dott. Eugenio Santagata: cfr. resoconto stenografico dell'audizione, seduta del 12 marzo 2024, X Comitato, p. 12.

¹⁵¹ Richiama l'attenzione sull'uso dell'ecosistema videoludico come mezzo di comunicazione criminale il Dott. Eugenio Santagata: cfr. resoconto stenografico dell'audizione, seduta del 12 marzo 2024, X Comitato, p. 10.

2. Crittografia *end-to-end* e limiti investigativi.

2.1. Il problema tecnico: dal MitM al captatore.

L'intercettazione costituisce, nel sistema processuale penale, un mezzo di ricerca della prova la cui disciplina positiva si articola in un insieme di presupposti, limiti e garanzie, ma che, significativamente, non è accompagnato da una definizione codicistica. In tale lacuna definitoria si inserisce la nozione elaborata più di vent'anni fa dalla giurisprudenza di legittimità – in particolare dalle Sezioni Unite “Torcasio” – e mai messa in discussione, secondo cui l'intercettazione consiste «nell'apprensione occulta e contestuale del contenuto di una conversazione o comunicazione tra due o più persone da parte di un soggetto estraneo al colloquio»¹⁵².

Il *pivot* di questa ricostruzione è piuttosto evidente: l'intercettazione presuppone non soltanto la raccolta di segnali, ma la possibilità di apprendere un “contenuto” comunicativo; se tale contenuto è strutturalmente inaccessibile, il mezzo di ricerca della prova viene privato del suo *ubi consistam*, trasformando la captazione in un'operazione che, pur tecnicamente riuscita, risulta epistemologicamente sterile.

Che la criminalità organizzata (e non solo) abbia costantemente cercato di garantirsi tale inaccessibilità è un fatto noto: evitare canali monitorabili, usare dispositivi “puliti”, turnare le utenze, segmentare le reti relazionali, adoperare un linguaggio criptico sono solo alcune delle contromisure orientate a neutralizzare l'attività intercettiva in sé o la sua capacità rivelatrice.

Dunque, il rapporto tra intercettazioni e tecniche di elusione è sempre stato dialettico e adattivo. L'evoluzione delle modalità comunicative e la crescente disponibilità di tecniche e strumenti di “protezione” del contenuto produce da sempre un continuo spostamento del punto di equilibrio tra capacità di captazione e capacità di elusione: l'una perimetra un potere di intrusione finalizzato alla ricerca della prova, l'altra ne mette alla prova l'effettività, costringendo a ripensare continuamente – sul piano tecnico e su quello garantistico – la linea di confine tra captazione lecita e opacizzazione della sfera comunicativa.

La dimensione tecnologica ha accentuato significativamente tale dinamica, producendo una dissociazione crescente tra accesso al flusso e accesso al significato.

Invero, la classica modalità di captazione del tipo “*man in the middle*” (MitM) – così definita in ragione della posizione che l'organo investigativo assume rispetto al flusso delle comunicazioni, ovvero al centro dei due poli della conversazione – ha mostrato ben presto la sua debolezza dinanzi alle nuove forme di *virtual communication*.

¹⁵² Cass., sez. un., 24 settembre 2003, n. 36747, in *CED Cass.* n. 225467.

L'evoluzione delle strategie di gestione delle telecomunicazioni, unita alla necessità di contenimento dei costi e alla crescita esponenziale della richiesta di accesso alla rete ha determinato la deviazione della stragrande maggioranza del traffico voce su canali di trasmissione basati su protocolli *VoIP* (*Voice over IP*)¹⁵³, gestiti da licenziatari di *app* (*Whatsapp*, *Telegram*, *Facebook Messenger*, *Skype*, *Wiber*, etc.) che, allocando i propri *server* al di fuori del territorio italiano – e, quindi, non agendo quali concessionari di pubblico servizio – sfuggono alle prestazioni obbligatorie previste dalla normativa domestica, *ivi* compresa la cessione dei cc.dd. “protocolli di decodifica”, grazie ai quali l'autorità giudiziaria è in grado di leggere in chiaro il segnale digitale intercettato (sempre e solo in sequenza numerica)¹⁵⁴ (sul problema regolatorio, v. *infra*, parte II, sez. II, § 2.2.).

Si tratta, infatti, di piattaforme che integrano la c.d. “crittografia *end-to-end*” per garantire che solo mittente e destinatario (gli *endpoint*) leggano il contenuto (voce, testo, dati): il flusso comunicativo, da quando lascia il dispositivo del primo, sino alla ricezione da parte del secondo, è protetto da una chiave di cifratura che varia continuamente in lunghezza e contenuto.

Non esiste nessun algoritmo di qualunque operatore in grado di decrittare mentre l'informazione viaggia¹⁵⁵; e nemmeno il fornitore del servizio (*Whatsapp*, *Signal*, *Telegram*, *Messenger*, *RCS* di *Google*, etc.) può leggere il *plaintext*, cioè il contenuto in chiaro della comunicazione, perché le chiavi risiedono esclusivamente sui dispositivi degli utenti¹⁵⁶. È come se i messaggi o il pacchetto vocale fossero protetti con un lucchetto e solo mittente e destinatario avessero la “chiave” per sbloccarli e leggerli o ascoltarli¹⁵⁷.

Nel caso di *Whatsapp*, ad esempio, le chiavi di sessione vengono aggiornate ad ogni messaggio o pacchetto vocale (secondo il protocollo *double-ratchet*), determinando una «dinamicità elevatissima»¹⁵⁸ che rende impossibile qualsiasi tentativo di decrittazione sul flusso di trasporto.

È stato utilmente specificato come la crittografia *end-to-end* sia solitamente implementata di *default* sulle *chat* ma non sul *backup* dei dati. Questo significa che se un utente non seleziona manualmente

¹⁵³ La tecnologia *VoIP* rende possibile effettuare una conversazione telefonica, o più un generale una comunicazione audio-video in tempo reale, sfruttando una connessione alla rete internet (o una qualsiasi altra rete dedicata a commutazione di pacchetto, cioè che utilizza il protocollo *IP* senza connessione per il trasporto dati), anziché passare attraverso la rete telefonica tradizionale. I programmi *Voice over IP* trasmettono la comunicazione senza passare dal *server* del fornitore del servizio di accesso alla rete che opera sul territorio italiano, ma connettendosi in *cloud* (in condivisione *client – client*) ai *server* privati esteri che gestiscono il relativo servizio, i quali, proprio perché allocati fuori dal territorio nazionale, non hanno l'obbligo di cessione del protocollo di decodifica.

¹⁵⁴ Per questa completa sintesi, cfr. il resoconto stenografico dell'audizione della Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato.

¹⁵⁵ Cfr. resoconto stenografico dell'audizione del Dott. Eugenio Santagata, seduta del 12 marzo 2024, X Comitato, p. 9.

¹⁵⁶ Cfr. relazione del Dott. Eugenio Santagata depositata a corredo della sua audizione del 12 marzo 2024, X Comitato, DOC. n. 107.1, p. 4.

¹⁵⁷ In questi termini il Dott. Eugenio Santagata nella sua relazione: cfr. DOC. n. 107.1, p. 4.

¹⁵⁸ Cfr. resoconto stenografico dell'audizione del Dott. Giovanni Nazzaro, seduta del 26 giugno 2024, X Comitato, p. 4.

l'opzione di crittografia nel momento in cui si esegue il *backup*, i dati vengono automaticamente decrittati e archiviati in chiaro (di *default* una volta a settimana) e le autorità italiane possono, attraverso rogatoria internazionale, acquisirli. Nondimeno, negli ultimi anni sono state sviluppate anche delle applicazioni “*serverless*” che non prevedono alcun *backup*, rendendo, quindi, impossibile aggredire i dati anche nella fase *post* trasmissione¹⁵⁹.

L'impatto della crittografia *end-to-end* sull'efficacia delle investigazioni è stato deflagrante: pur potendo acquisire il segnale, il contenuto restava inaccessibile per ragioni strutturali¹⁶⁰, determinando un vero e proprio “svuotamento” della funzione probatoria dell'intercettazione.

Una greve constatazione ben presto superata dall'avanzamento della tecnica, che ha fornito agli inquirenti un'adeguata “contromisura”. Il risultato è stato quello di dislocare il baricentro delle attività tecniche dal centro della comunicazione (*Man in the Middle*) a monte o a valle della stessa, ovvero nel cuore del dispositivo utilizzato, così da privare di utilità pratica i protocolli di decodifica: il captatore informatico interviene a livello di *device* “catturando” il flusso comunicativo prima che esca dal dispositivo e sia cifrato oppure, nel caso di comunicazione in ingresso, subito dopo esser stato decriptato (subito dopo la ricezione)¹⁶¹.

Il captatore – richiamato nel corso delle audizioni anche come “*spyware*” – rappresenta, quindi, una più attuale modalità captativa di conversazioni altrimenti non intercettabili.

Si tratta, in particolare, di un *software* che, una volta inoculato nel dispositivo *target*, consente il controllo da remoto di tutte le attività svolte. Detto diversamente, diventa l'amministratore del sistema e acquisisce poteri di gestione: accesso a *screenshot* dello schermo, registrazioni della tastiera (*keylogger*), copia dei dati contenuti nella memoria, esfiltrazione di *chat*, foto, *file*, *e-mail*, accensione del microfono e della videocamera etc.

Il materiale raccolto viene poi trasferito in un archivio digitale (*server*) con procedure che ne assicurano l'integrità, attraverso connessione *internet* (attività che può erodere il *bundle* dati dell'abbonamento *target*, richiedendo interventi dell'operatore per evitare che l'utente rilevi anomalie)¹⁶².

¹⁵⁹ Così specifica il Dott. Eugenio Santagata, aggiungendo che «[q]ueste APP possono liberamente operare in Italia, fornendo il servizio dall'estero senza incorrere in alcuna sanzione, al contrario dei fornitori operanti dall'Italia che invece possono essere colpiti da interdittiva anche se il mancato adempimento è dettato da impossibilità tecnologica» (cfr. DOC. n. 107.1, pp. 4-5).

¹⁶⁰ Cfr. relazione del Dott. Eugenio Santagata a corredo della sua audizione del 12 marzo 2024, X Comitato, DOC. n. 107.1, p. 4.

¹⁶¹ Cfr. il resoconto stenografico dell'audizione della Dott.ssa Agnese Del Giudice, seduta del 14 novembre 2024, X Comitato.

¹⁶² Cfr. relazione del Dott. Eugenio Santagata depositata a corredo della sua audizione del 12 marzo 2024, X Comitato, DOC. n. 107.1, pp. 2-3.

Sono possibili due tecniche di inoculazione: in via diretta e da remoto. La prima presuppone la fisica disponibilità del dispositivo (anche spento), al quale collegare un altro *device* per installare il *software*. La seconda può essere effettuata, a sua volta, in due modi: avvalendosi di *exploit zero-click* – ossia di un attacco informatico che non richiede alcuna interazione del soggetto *target* per infettare il dispositivo (si tratta di un’infezione invisibile che avviene in *background*, ad esempio tramite un messaggio ricevuto, una chiamata persa o un pacchetto dati manipolato che il dispositivo elabora automaticamente)¹⁶³ –, oppure di tecniche *one-click*¹⁶⁴.

Ad ogni modo, l’efficacia delle tecniche di inoculazione dipende dal sistema operativo installato sul device da infettare¹⁶⁵.

Nel corso delle audizioni è stato anche rappresentato come gli OTT tendano a non gradire una simile interferenza. Esemplificativa in tal senso è la battaglia legale tra *Whatsapp* (Meta) e *NSO Group*, società produttrice dello *spyware* “*Pegasus*”, da poco conclusa con una vittoria significativa per l’*app* di messaggistica che rivendicava la violazione dei termini d’uso e delle leggi *anti-hacking* per avere *NSO Group* sfruttato una falla del sistema di chiamate vocali al fine di inviare pacchetti di dati malevoli mascherati da normale segnalazione di chiamata su *Whatsapp*; bastava che la chiamata arrivasse perché il codice venisse eseguito sul telefono, installando l’*agent* in modalità “*zero-click*”, così da aggirare crittografia e i permessi dell’*app*.

La circostanza che gli OTT possano intentare azioni legali contro le società produttrici degli *spywares* utilizzati per l’attività captativa dell’autorità giudiziaria si ritiene rappresentino un «grosso freno anche all’innovazione» giacché è «difficile, a un certo punto, che un imprenditore si prenda il rischio vero di spendere milioni per uno *spyware* veramente performante»¹⁶⁶.

¹⁶³ Sebbene gli attacchi *zero-click* possano sembrare invisibili e senza costi diretti per gli utenti, richiedono comunque un notevole investimento da parte degli attaccanti: per poter fare una inoculazione di questo tipo bisogna avere conoscenza di alcune vulnerabilità del dispositivo *target*, peraltro non note nemmeno a chi l’ha costruito. Deve aggiungersi che «nel 99 % dei casi di *zero-click* noti al mondo si tratta di *iPhone* [...] Di *zero-click* su *Android* noi non abbiamo contezza o comunque in un caso molto limitato. Quanto costa inoculare un *iPhone* con *zero-click*? Può costare milioni. Ecco perché dico che quel tipo di inoculazione non è un’attività portata in essere nella routinaria conduzione di queste operazioni da parte di forze di polizia perché è estremamente costoso. Si associa tipicamente lo *zero-click*, quindi andare a colpo sicuro, con un *target* di elevatissimo valore»: cfr. resoconto stenografico dell’audizione del Dott. Eugenio Santagata, seduta del 12 marzo 2024, X Comitato, p. 8.

¹⁶⁴ Cfr. resoconto stenografico dell’audizione del Dott. Eugenio Santagata, seduta del 12 marzo 2024, X Comitato, p. 8.

¹⁶⁵ Cfr. resoconto stenografico dell’audizione del Dott. Eugenio Santagata, seduta del 12 marzo 2024, X Comitato, p. 6.

¹⁶⁶ Cfr. resoconto stenografico dell’audizione del Dott. Eugenio Santagata, seduta del 12 marzo 2024, X Comitato, p. 12.

2.2. Il problema regolatorio: gli operatori “*Over The Top*”

Tutte le audizioni convergono nel segnalare l'esistenza di un problema regolatorio. Mentre gli operatori di telecomunicazioni sono tenuti ad assicurare, su richiesta della magistratura, le prestazioni obbligatorie previste dalla legge (art. 57, comma 1, d.lgs. 1° agosto 2003, n. 259, c.d. “Codice delle Comunicazioni Elettroniche”) — ossia, identificazione anagrafica dei titolari di servizi/abbonamenti/contratti, intercettazioni telefoniche o telematiche su rete fissa o mobile, fornitura dei dati di traffico (tabulati telefonici e telematici), geolocalizzazione in tempo reale e storica (con frequenza di 15 minuti), inibizione della navigazione attraverso l'oscuramento di siti *web* e indirizzi IP¹⁶⁷ —, gli operatori OTT (*Over The Top*), che pure forniscono servizi di comunicazione, non sono soggetti ai medesimi obblighi di collaborazione.

Il risultato è di intuitiva evidenza: il traffico dati corre lungo l'“autostrada” messa a disposizione dell'operatore di rete (che fornisce la connettività *internet*), ma il contenuto, essendo gestito interamente dall'OTT, è crittografato *end-to-end* e risulta quindi illeggibile¹⁶⁸.

Invero, la diffusione della *virtual communication* ha determinato il passaggio da un modello “verticale” e infrastrutturale delle comunicazioni elettroniche a un modello “orizzontale” e distribuito, fondato sulle reti *IP* e sulle piattaforme digitali, con conseguenze rilevanti sul piano tecnico, regolatorio e giuridico.

In origine, quando fu concepito il Codice delle Comunicazioni Elettroniche e il sistema delle prestazioni obbligatorie, il legislatore italiano ragionava secondo la logica tipica delle telecomunicazioni classiche, secondo cui l'operatore di rete (storicamente Telecom Italia) controllava l'intera filiera della comunicazione. Dunque, l'infrastruttura fisica (l'“autostrada”: cavi in rame o fibra, centrali, ponti radio) coincideva sostanzialmente con il servizio di comunicazione: lo stesso soggetto progettava (*i.e.* “ingegnerizzava”) la rete, trasportava il segnale e forniva la telefonia¹⁶⁹.

Era un sistema a commutazione di circuito, pensato specificamente per la voce, nel quale ogni chiamata occupava risorse riservate lungo tutto il percorso.

¹⁶⁷ Cfr. relazione del Dott. Eugenio Santagata depositata a corredo della sua audizione del 12 marzo 2024, X Comitato, DOC. n. 107.1, p. 1, nella quale si evidenzia, altresì, come «[o]ltre alle suddette prestazioni obbligatorie, cosiddette di “repertorio”, gli operatori si impegnano nel supportare le Forze dell'Ordine nell'analisi e nella comprensione dei dati forniti attraverso, per esempio, incontri di formazione oltre che nell'introdurre nuove modalità di ricerca o aggregazione di dati per soddisfare le esigenze investigative delle Forze dell'Ordine, in continua mutazione».

¹⁶⁸ «I *provider*, tra l'altro, non possono conservare traffico — sarebbe tecnicamente non sostenibile — ma oggi consideriamo di fatto un provider di comunicazione chi oggi offre un'autostrada. È come se dicessimo ad Autostrade di dirci qual è il contenuto del trasporto che avviene su un autotreno, è la stessa cosa. Autostrade potrebbe dire che non lo sa, sa che c'è un autotreno, che ci sono delle indicazioni esterne che possono dire che eventualmente sta trasportando un materiale o altro, ma non si può dire quale sia l'effettivo contenuto. Occorre chiederlo a chi sta svolgendo direttamente quel trasporto»: cfr. resoconto stenografico dell'audizione del Dott. Ivano Gabrielli, seduta del 15 maggio 2024, X Comitato, p. 13.

¹⁶⁹ In sostanza, la voce dell'utente veniva trasformata in un segnale elettrico o radio, instradata attraverso circuiti dedicati e ricostruita all'arrivo.

Oggi questo paradigma è radicalmente mutato. La comunicazione vocale non è più, nella maggior parte dei casi, un flusso analogico, ma un insieme di “pacchetti di dati” che viaggiano su reti *IP* condivise (*VoIP*). Tecnicamente, la voce viene digitalizzata, suddivisa in pacchetti, inserita (cioè “incapsulata”) nel traffico *internet* e inviata attraverso la rete come qualsiasi altro dato. Sicché, quando si effettua una chiamata tramite un’app, la voce non segue un canale telefonico separato, ma percorre la stessa rete usata per inviare *e-mail* o guardare *video*, mescolandosi al resto del traffico.

In questo contesto, l’operatore tradizionale continua a svolgere un ruolo essenziale nella gestione dell’infrastruttura e nel trasporto dei dati, ma non è più l’unico soggetto che “ingegnerizza” la comunicazione¹⁷⁰. La funzione comunicativa è ormai distribuita: oltre ai *provider* di accesso alla rete, intervengono, appunto, piattaforme e servizi OTT che realizzano livelli applicativi autonomi. In altre parole, la rete fornisce il trasporto, mentre la comunicazione vera e propria (codifica della voce, gestione delle sessioni, messaggistica) è progettata e controllata da soggetti diversi dall’operatore di rete, ossia – come detto – dalle piattaforme che implementano la cifratura *end-to-end*, per cui il *provider*/gestore dell’“autostrada” può trasportarla (la comunicazione) ma non leggerla¹⁷¹.

Gli OTT, ad oggi, non sono formalmente inquadrati nel sistema dei *provider*¹⁷², per cui non sono tenuti ad acquisire l’autorizzazione generale (art. 11, comma 2, d.lgs. n. 259/2003)¹⁷³ e, conseguentemente, non sono formalmente tenuti a fornire le prestazioni obbligatorie all’autorità giudiziaria (art. 57 d.lgs. n. 259/2003), tra cui i protocolli di decodifica della cifratura *end-to-end*.

I dati relativi all’elenco pubblico delle imprese autorizzate sono significativi: oltre 2.308 imprese italiane hanno l’autorizzazione generale per i servizi di accesso a *internet* (di cui 36 con sede all’estero); 164 imprese per i servizi di telefonia (20 con sede all’estero); oltre 1.411 imprese per servizio *wi-fi* pubblico; *Whatsapp*, *Telegram*, *Signal*, *iMessage* e *Trima* etc. non figurano nell’elenco delle imprese autorizzate¹⁷⁴.

¹⁷⁰ Cfr. resoconto stenografico dell’audizione del Dott. Ivano Gabrielli, seduta del 15 maggio 2024, X Comitato, pp. 13-14.

¹⁷¹ Gli operatori telefonici sono, sostanzialmente, «osservatori di questo traffico»: così il Dott. Massimo Romiti, intervenuto in qualità di collaboratore del Dott. Eugenio Santagata nella seduta del 12 marzo 2024, X Comitato, p. 11.

¹⁷² Come sottolineato dal Dott. Ivano Gabrielli, «sono *provider* di comunicazione a tutti gli effetti, ma si sottraggono o comunque non sono oggi inquadrabili nel sistema più complesso dei *provider*»: cfr. resoconto stenografico dell’audizione, seduta del 15 maggio 2024, X Comitato, p. 11.

¹⁷³ L’art. 11, comma 2, d.lgs. n. 259/2003 prevede che la fornitura di reti o servizi di comunicazione elettronica, compresi i servizi di comunicazione interpersonale indipendenti dal numero, sia assoggettata ad autorizzazione generale. L’espressione “indipendenti dal numero” ha spinto il Dott. Giovanni Nazzaro a ritenere la norma *in parte qua* obsoleta «perché oggi abbiamo applicazioni come Trima [...] una App nata lo scorso anno [...], i cui server hanno sede in Svizzera, [che] non usa numerazioni mobili, non usa identificativi, è assolutamente anonima e assegna un identificativo alfanumerico a ogni utente»: cfr. resoconto stenografico, seduta del 26 giugno 2024, X Comitato, p. 4.

¹⁷⁴ Cfr. documento depositato dal Dott. Giovanni Nazzaro in occasione della sua audizione del 26 giugno 2024, X Comitato, DOC. n. 192.1, pp. 9-10.

Com'è stato pure sottolineato, il comma 6 dell'art. 57 d.lgs. n. 259/2003 estende gli obblighi alle imprese che forniscono servizi di comunicazione «attraverso reti di accesso o trasporto non proprie», definizione che includerebbe anche gli OTT¹⁷⁵. Tuttavia, le sanzioni previste in caso di inadempimento¹⁷⁶ non vengono applicate perché tali piattaforme non hanno richiesto, a monte, l'autorizzazione generale e operano dall'estero¹⁷⁷.

Ne deriverebbe anche una disparità competitiva significativa: gli operatori di telecomunicazioni italiani sono soggetti a obblighi stringenti e costi elevati per le prestazioni obbligatorie, mentre gli OTT operano senza vincoli, creando una disparità sfruttata dalla criminalità organizzata.

Tutte le voci *audite* in seno al X Comitato sottolineano, pertanto, la necessità di una disciplina integrata che possa perlomeno facilitare una cooperazione con gli OTT.

Sul punto è stata richiamata l'attenzione¹⁷⁸ sul “*Cloud Act*” statunitense, che prevede l'obbligo per tutti i *provider* soggetti alla giurisdizione USA di eseguire ordini giudiziari validamente emessi dalle autorità americane – e dalle autorità di altri Paesi che abbiano firmato gli “*executive agreements*” – per la produzione di contenuti di comunicazioni elettroniche, metadati e informazioni di *account* in loro “possesso, custodia o controllo”, indipendentemente dalla localizzazione fisica dei *server*, purché rilevanti per un'indagine penale relativa a crimini gravi come criminalità organizzata transnazionale, terrorismo, *cybercrime* o sfruttamento o abuso di minori etc.

3. Criptofonia, *cryptophones* e capacità investigative.

3.1. La criptofonia e il *business* mafioso “*as-a-service*”.

I criptofonini sono l'ultimo frutto conosciuto di un processo di specializzazione tecnologica applicato all'economia criminale, nel quale competenze avanzate di sicurezza informatica vengono sistematicamente tradotte in prodotti commerciali destinati a una “clientela selezionata”.

¹⁷⁵ Cfr. resoconto stenografico dell'audizione del Dott. Giovanni Nazzaro, seduta del 26 giugno 2024, X Comitato, p. 4.

¹⁷⁶ Le sanzioni sono significative: da 170.000 a 2.500.000 euro; sospensione dell'attività fino a due mesi in caso di violazioni gravi o reiterate; revoca dell'autorizzazione generale in caso di inosservanza integrale.

¹⁷⁷ Al riguardo, il Dott. Giovanni Nazzaro richiama un caso meno noto di *Whatsapp*: «Google nel 2019 ha lanciato a livello mondiale questo protocollo, sostituendo esattamente gli SMS. Quindi, è una *App* nativa all'interno degli smartphone che consente di gestire le comunicazioni esattamente come *Whatsapp*. Google ha lanciato questo servizio nel 2020 in Italia e siamo, credo, sull'ordine del milione di utenti che utilizzano questo tipo di servizio. La problematica, come per *Whatsapp*, interessa *Google*, la società che fornisce questo servizio, che non ha sede in Italia, non è riconosciuta in Italia come operatore, ma ha la sede in California, in particolare tramite l'operatore *Jibe*»: cfr. resoconto stenografico dell'audizione, seduta del 26 giugno 2024, p. 4.

¹⁷⁸ Cfr. relazione depositata dal Dott. Andrea Formenti in occasione della sua audizione del 26 giugno 2024, X Comitato, DOC. n. 205.1., p. 8.

Tali dispositivi non si limitano a integrare funzioni di cifratura *end-to-end*; rappresentano, piuttosto, ecosistemi chiusi, caratterizzati da *firmware* modificato, sistemi operativi “*hardening*”, rimozione dei servizi *standard* di tracciamento e geolocalizzazione, nonché dall’adozione di infrastrutture di comunicazione proprietarie.

Invero, mentre la *virtual communication* tipica delle *app* moderne appartiene al paradigma *packet-switched* (*VoIP* + crittografia), il concetto di criptofonia è legato a un paradigma “voce-centrico” e *circuit-switched*, cioè nasce per proteggere soprattutto la riservatezza della conversazione vocale in tempo reale e utilizza sistemi di comunicazione a commutazione di circuito tipici della telefonia classica. L’idea di base è quella di cifrare una chiamata tradizionale, intesa quale comunicazione sincrona, senza trasformarla in traffico *IP* indistinto, cifrandola a livello applicativo o di trasporto. In questo paradigma, quindi, la cifratura è integrata direttamente nell’apparato telefonico o in dispositivi *hardware* dedicati e opera sul segnale vocale (analogico o digitalizzato) lungo quel circuito riservato. I criptofonini sono dispositivi *hardware/software* che implementano tale crittografia avanzata, così divenendo il “vello d’oro” della criminalità organizzata di tutto il mondo.

È importante sottolineare come la loro progettazione abbia determinato un trasferimento diretto di *know-how* tecnico verso il mercato illecito, trasformando capacità tipicamente associate alla *cybersecurity* in *asset* opachi monetizzabili. La distribuzione attraverso reti dedicate di rivenditori funge, poi, da moltiplicatore di scala, consentendo la segmentazione dell’offerta (in base a livelli di sicurezza, assistenza tecnica e aggiornamenti) e l’abbattimento delle barriere di ingresso per utenti – *i.e.* organizzazioni criminali – privi di competenze informatiche avanzate (sulla “collaborazione” di soggetti altamente specializzati v., in termini generali, *supra*, parte I, § 4.1.).

In questo scenario, il vantaggio criminale non deriva soltanto nell’*hardware* in sé, ma risiede soprattutto nei servizi accessori – manutenzione, supporto, rinnovo delle chiavi crittografiche, *hosting* dei *server* – che configurano una relazione continuativa tra fornitore e cliente. Il risultato è un modello economico pienamente assimilabile al paradigma del “*crime-as-a-service*”¹⁷⁹, in cui l’attività illegale viene modularizzata e industrializzata: gli sviluppatori forniscono l’infrastruttura tecnica¹⁸⁰, i *reseller* curano la distribuzione e l’assistenza¹⁸¹, mentre gli utilizzatori finali acquistano “pacchetti” di anonimato pronti all’uso.

¹⁷⁹ Cfr. documento depositato dal Dott. Ivano Gabrielli a corredo della sua audizione del 15 maggio 2024, X Comitato, DOC. n. 193.1, p. 1; altresì, v. documento depositato dal Ten. Col. Luca Flebus a corredo della sua audizione del 18 aprile 2024, X Comitato, DOC. n. 139.1, p. 8.

¹⁸⁰ Al riguardo, il Ten. Col. Luca Flebus rappresenta che «[a]ttività investigative hanno permesso di dimostrare che alcuni servizi di criptofonia sono stati sviluppati da ex dipendenti di società altamente specializzate nel campo dello spionaggio e della *mobile forensics*»: cfr. DOC. n. 139.1, p. 6.

¹⁸¹ Cfr. documento depositato dal Ten. Col. Luca Flebus a corredo della sua audizione del 18 aprile 2024, X Comitato, DOC. n. 139.1, p. 3. V., anche, documento depositato dal Dott. Ivano Gabrielli a corredo della sua audizione del 15 maggio 2024, X Comitato, DOC. n. 193.1, p. 1.

Questo assetto reindirizza le logiche delle piattaforme digitali legittime verso finalità criminogene, evidenziando come l'innovazione tecnologica, quando inserita in filiere opache e orientate al profitto illecito, possa favorire la professionalizzazione del crimine e la sua integrazione in “catene del valore” sempre più strutturate.

In quest'ordine di idee è stato utilmente evidenziato come una «[b]uona strategia [sarebbe] quella di cercare di dimostrare che la vendita di telefoni crittografati è, di fatto, un'attività di *Crime-as-a-service* (CaaS) ovvero di supporto tecnico-logistico, consapevole e partecipato, anche dall'esterno, rispetto ad una ben precisa organizzazione criminale, al fine di: facilitare la commissione di reati informatici abilitanti/collegati; evitare la legittima sorveglianza digitale da parte delle autorità competenti; distruggere preziose evidenze digitali mediante servizi di bonifica remota automatici ovvero *on demand*»¹⁸².

3.2. Definizione e caratteristiche strutturali dei *cryptophones*.

Il criptofonino è un telefono – solitamente *Android* o *Blackberry* – totalmente customizzato, cioè un dispositivo con un sistema operativo modificato. Si tratta, in sostanza, di telefonini a cui mancano molte delle funzionalità presenti negli altri dispositivi in commercio, ma capaci di garantire l'assoluta impenetrabilità delle comunicazioni¹⁸³.

Il sistema operativo, infatti, è modificato a livello di *kernel* per ridurre la superficie di attacco, eliminando funzionalità non necessarie, rafforzando i controlli di accesso e introducendo meccanismi di mitigazione delle vulnerabilità. In sostanza, l'*hardening* –ossia l'insieme sistematico di interventi tecnici applicati al *kernel* del sistema operativo – sposta l'*enforcement* dalle scelte dell'utente e dalle *app* a un livello privilegiato che governa l'intero comportamento della piattaforma.

In questa prospettiva, il sistema operativo installato disabilita la localizzazione GPS, i servizi *Google*, il *bluetooth*, la fotocamera, la porta USB (che rimane in funzione solo per la carica della batteria)¹⁸⁴, oscura le notifiche *push* e blocca ogni altro servizio che possa generare un rischio di intercettazione o localizzazione. Anche l'uso di schede SD esterne viene interdetto.

Rimangono attive le chiamate, ma solo in modalità VoIP, quindi senza l'uso della rete *GSM*, e la messaggistica, ma con applicazioni proprietarie e crittografate tra utenti di “gruppi chiusi”¹⁸⁵. Ne

¹⁸² In questi termini il Ten. Col. Luca Flebus: cfr. DOC. n. 139.1, p. 14.

¹⁸³ Così il Dott. Ivano Gabrielli: cfr. DOC. n. 193.1, p. 1.

¹⁸⁴ Questo implica, chiaramente, l'impossibilità di installare fisicamente qualcosa, ad esempio un captatore informatico, pur avendo la materiale disponibilità del dispositivo.

¹⁸⁵ Cfr. documento depositato dal Ten. Col. Luca Flebus a corredo della sua audizione del 18 aprile 2024, X Comitato, DOC. n. 139.1, pp. 4-5.

consegue la possibilità di comunicare soltanto con chi possiede lo stesso telefono o la stessa app¹⁸⁶ e solo se inseriti nel circuito (cioè nella stessa rete) da qualcun altro che già vi appartenga.

Il sistema operativo integra, poi, un *IMSI catcher detector* con l'obiettivo di fornire *early warning* contro sorveglianza attiva. Ma anche funzioni di *wiping* (cancellazione integrale e indelebile di tutti i dati) che possono essere attivate direttamente sul telefono, con una combinazione di tasti, oppure da remoto ("*remote wipe*") dopo un tempo programmato, oppure in caso di disconnessione dalla rete.

Si tratta di apparati che implementano, chiaramente, oltre alla oramai consueta crittografia E2E, anche un'ulteriore cifratura dei dati a riposo e in transito, anche *multi layer*. In alcuni casi, integrano anche funzioni di dissimulazione del tono vocale (in sede sia di chiamate *VoIP*, che di note vocali)¹⁸⁷.

Il telefono potrebbe funzionare anche senza SIM, utilizzando esclusivamente una rete *wi-fi* qualunque, che non lascia tracce e non crea un *file* di *log* delle chiamate. In altri casi vengono fornite SIM dedicate (straniere, quindi di fatto anonime), diverse da quelle dei *carrier* tradizionali.

Anche l'interfaccia grafica, a volte, è modificata: l'applicazione della calcolatrice potrebbe, ad esempio, nascondere l'app della messaggistica, alla quale accedere, ovviamente, digitando una *password*.

La caratteristica essenziale di questi telefoni è, chiaramente, la presenza – necessaria – di un'infrastruttura di *server* messa a disposizione del fornitore del servizio: la sicurezza dei criptofonini dipende dal modello di *trust* e di *governance* del *provider*. Il *server* gestisce l'identificativo, chi può comunicare, come vengono scambiate le chiavi, quali *app* vengono installate e quando arrivano gli aggiornamenti. Pertanto, la "promessa di sicurezza" del *cryptophone* vale solo finché l'infrastruttura centrale è robusta e degna di fiducia. Questa dipendenza strutturale crea un punto unico di controllo e, conseguentemente, il punto unico di vulnerabilità sistemica (v. *infra*, parte II, sez. II, § 3.3.1.).

3.3. I *cryptophones* tra *privacy* ed elusione investigativa.

Pur nella consapevolezza della sostanziale liceità dei sistemi di crittografia – funzionali a garantire la *privacy* dell'utente – sarebbe da miopi non notare l'esistenza di una "nesso" tra le moderne tecniche di intrusione a disposizione degli inquirenti (*spyware*) e le fattezze dei nuovi apparati crittografati (*cryptophones*), in un contesto in cui le prime hanno consentito all'Autorità giudiziaria – e, quindi, allo Stato – di superare gli ostacoli frapposti dall'uso strumentale, da parte della criminalità mafiosa (e non solo), di piattaforme di comunicazioni cifrate *end-to-end*.

¹⁸⁶ La casistica criminale conosce anche l'uso di *app* capaci di rendere simile al criptofonino un telefono qualsiasi.

¹⁸⁷ Cfr. documento depositato dal Ten. Col. Luca Flebus a corredo della sua audizione del 18 aprile 2024, X Comitato, DOC. n. 139.1, p. 6.

Nei sistemi *end-to-end*, infatti, il contenuto della comunicazione è cifrato in modo tale che solo gli *endpoints* (i dispositivi degli utenti) possano decifrarlo. L'infrastruttura intermedia – ove normalmente si posiziona l'inquirente per la captazione – vede traffico cifrato. Questo modello, tipico delle *app* moderne, ha dunque spostato l'asse della "sicurezza comunicativa" sull'integrità degli *endpoint* e sulla gestione delle chiavi. Come già evidenziato (v. *supra*, parte II, sez. II, §§ 2.1.-2.2.), il captatore informatico, nella sua configurazione tipica, è lo strumento di intrusione che ha consentito di superare i limiti dell'intercettazione "in transit" spostando il punto di raccolta a monte o a valle della cifratura: anziché cercare di decifrare il traffico, acquisisce contenuti e metadati sul terminale (ossia sugli *endpoints*), prima della cifratura o dopo la decifratura. Un criptofonino, dal suo canto, non è semplicemente un telefono con un'*app* di messaggistica cifrata; è, piuttosto, un ecosistema progettato per ridurre drasticamente le opportunità di compromissione *endpoint* e per degradare la qualità, l'ampiezza e la persistenza temporale dell'evidenza digitale anche qualora l'"intrusore" riesca ad ottenere un accesso parziale.

Se, come già specificato, l'obiettivo dell'intercettazione tradizionale è il traffico e quello del captatore è l'*endpoint*, è di intuitiva evidenza che i criptofonini puntano al secondo fronte, cercando di rendere l'*endpoint* un bersaglio fragile per l'attaccante e, soprattutto, poco "ricco" di tracce anche quando attaccabile.

Non a caso, si tratta di strumenti che non si limitano a offrire riservatezza del contenuto (come la crittografia *end-to-end*), ma implementano funzionalità che hanno un senso solo in un confronto con "antagonisti" dotati di capacità intrusiva avanzata sul terminale (*endpoint*) finalizzata all'acquisizione forense.

La riduzione della telemetria, l'eliminazione delle componenti di sincronizzazione *cloud*, la disabilitazione o il controllo spinto delle notifiche e dei *backup*, la compartimentazione delle *app*, l'uso di profili separati e la cifratura completa del dispositivo con politiche severe di autenticazione non sono ottimizzazioni "consumer" orientate alla comodità, bensì contromisure dirette ad ostacolare persistenza e raccolta silente. Analogamente, l'enfasi su messaggi a scadenza, *chat* non esportabili, assenza di *screenshot* e su funzioni di "deniability" (negabilità) e di *wipe* rapido (cancellazione dei dati) in condizioni di rischio risponde meno alla protezione del canale – già assicurabile con la cifratura *end-to-end* – e più alla riduzione dell'evidenza residua e dell'impatto di una compromissione del terminale.

In questa dialettica, allora, il criptofonino – o, se si preferisce – l'uso che ne viene fatto, rappresenta una risposta sistemica al concetto stesso di "acquisizione a monte o a valle della cifratura", sterilizzando l'utilità dell'*endpoint* come punto d'attacco dell'Autorità giudiziaria.

3.3.1. Reazioni e risposte: la compromissione del *server*.

I criptofonini sono stati progettati secondo una precisa razionalità strumentale che ne garantisce l'opacità anche rispetto a strumenti performanti come il captatore informatico: trasferire l'intero carico della sicurezza sull'architettura del sistema. Tuttavia, questa scelta progettuale, pur incrementando la resilienza del singolo dispositivo, ha introdotto inevitabilmente una fragilità sistemica. La centralizzazione delle funzioni critiche (autenticazione, instradamento dei messaggi, gestione delle chiavi o sincronizzazione dei contenuti) presso un *server* configura, infatti, un vettore privilegiato di compromissione (*point of failure*): è proprio l'interdipendenza tra dispositivo e *server* a costituire il varco attraverso cui le *law enforcement* sono riuscite a “trasformare” una piattaforma concepita per l'anonimato in uno strumento di sorveglianza retrospettiva su scala collettiva.

Nel corso delle audizioni sono state snocciolate le più importanti questioni di tipo tecnico-operativo relative alle piattaforme di comunicazione criptata utilizzate dalla criminalità organizzata e alle operazioni investigative che hanno portato alla loro neutralizzazione: *EncroChat*, *SkyECC* e *ANØM*. Le prime due, condotte attraverso *Joint Investigation Teams (JIT)*, hanno portato a risultati straordinari: oltre un miliardo e mezzo di comunicazioni cifrate deciptate, con risultati operativi incredibili dal punto di vista dei sequestri di stupefacenti, arresti e risoluzioni di omicidi irrisolti.

Si tratta, tuttavia, di operazioni nate in un contesto ordinamentale – quello francese – che prevede un regime di licenza governativa, penalmente presidiato, per chi offre servizi di comunicazione crittografata. Questo ha consentito di qualificare come “occulte” e, quindi, illegali le due piattaforme, i cui *server* erano peraltro fisicamente presenti sul territorio francese¹⁸⁸.

In particolare, nel caso *EncroChat*, la *Gendarmerie Nationale*, con il supporto di *Europol* e di una *JIT* europea, ha compromesso l'infrastruttura centrale della piattaforma, utilizzandola come un “veicolo di attacchi” verso i *client* mediante l'installazione di un *implant* sull'infrastruttura/*server* che abilitava la distribuzione automatica di uno *spyware* sui criptofonini al momento della connessione; l'*agent* acquisiva i messaggi in chiaro sul dispositivo (prima della cifratura e dopo la decifrazione), oltre a metadati e dati di rubrica/contatti, ed esfiltrava il tutto verso i sistemi di raccolta.

Nel caso *Sky ECC*, invece, un *team* congiunto di polizie francesi, inglesi e olandesi ha violato la piattaforma attraverso una complessa operazione di *hacking* nella quale è stato implementato un dispositivo tecnico riconducibile a una tecnica di tipo *man-in-the-middle*: l'intercettazione non si è limitata alla mera captazione del traffico cifrato, ma ha permesso la cattura di “elementi di decifrazione” (materiale/chiavi crittografiche) necessari a trasformare le comunicazioni in chiaro,

¹⁸⁸ Cfr. resoconto stenografico dell'audizione del Dott. Ivano Gabrielli, seduta del 15 maggio 2024, X Comitato, p. 5. V., altresì, relazione depositata dal Dott. Andrea Formenti in occasione della sua audizione del 26 giugno 2024, X Comitato, DOC. n. 205.1., p. 3.

tramite un meccanismo che interagiva con i criptofonini *Sky ECC* (mediante messaggi *push* non visibili) per indurre il rilascio di tali elementi; in questo modo gli investigatori hanno potuto decifrare sia flussi in tempo reale, che le comunicazioni precedentemente intercettate e archiviate in forma cifrata¹⁸⁹.

Contrariamente alle operazioni contro *EncroChat* e *Sky ECC* – fondati, come detto, sulla compromissione dell’infrastruttura o dei terminali tramite impianto di *malware* e successiva acquisizione massiva dei flussi comunicativi – *ANØM* (nota anche come “*Operation Trojan Shield*”) si è basata su una strategia proattiva di *platform seeding*, in cui un sistema di messaggistica cifrata è stato progettato, distribuito e controllato *ab origine* dalle autorità, in particolare dall’*FBI*, in cooperazione con *Europol* e *partner* internazionali¹⁹⁰.

L’istruttoria ha permesso di evidenziare come, ad oggi, non esista nel nostro ordinamento una previsione normativa idonea a consentire l’accesso, l’acquisizione e la conservazione dei dati allocati presso i *server* (in Italia o all’estero) che gestiscono servizi di criptofonia e che tali attività, fondamentali per l’azione delle forze di polizia – soprattutto nei procedimenti relativi alla criminalità mafiosa e ai traffici transnazionali, nei quali le piattaforme di comunicazione cifrata rappresentano un’infrastruttura ordinaria – potrebbero rischiare, peraltro, di costituire forme di sorveglianza di massa, del tutto incompatibili con le previsioni della nostra Carta Costituzionale e della CEDU.

Ne deriva uno scenario in cui l’azione investigativa è costretta a muoversi in un’area grigia, oscillando tra l’insufficienza degli strumenti legali disponibili e la tentazione di soluzioni non codificate tecnologicamente invasive, con il pericolo di una progressiva normalizzazione di pratiche emergenziali. Per non considerare le criticità che ne derivano in ordine alla catena di custodia digitale, alla verificabilità dell’integrità del dato e alla sua riproducibilità, profili che incidono direttamente sull’attendibilità della prova e sul diritto di difesa.

Ancora più marcate sono le difficoltà sul piano della cooperazione internazionale, soprattutto con Paesi *extra* UE.

I *server* che gestiscono servizi di criptofonia sono frequentemente collocati in giurisdizioni terze e l’assenza di strumenti sovranazionali equivalenti all’Ordine Europeo di Indagine, la diversa

¹⁸⁹ L’operazione comprendeva, in base alle informazioni disponibili, «intercettazione passiva del traffico telematico in entrata/uscita dai *servers*, intercettazione attiva tramite attacchi di tipo *Man in the Middle* tra i *servers* e ricorso a *spyware* nei *server* francesi di *Sky ECC* per forzare i criptofonini, attraverso una manipolazione del meccanismo delle notifiche *push*, a fornire le chiavi di decifratura»: cfr. relazione depositata dal Dott. Andrea Formenti in occasione della sua audizione del 26 giugno 2024, X Comitato, DOC. n. 205.1., p. 4.

¹⁹⁰ Alla coalizione internazionale dedicata ad *ANØM* hanno partecipato in tutto 16 paesi (molti dei quali per il tramite di *Europol*): Australia, Austria, Canada, Danimarca, Estonia, Finlandia, Germania, Ungheria, Lituania, Nuova Zelanda, Olanda, Norvegia, Svezia, Regno Unito, inclusa la Scozia, e USA: così cfr. relazione depositata dal Dott. Andrea Formenti in occasione della sua audizione del 26 giugno 2024, X Comitato, DOC. n. 205.1., p. 4.

sensibilità in materia di *privacy* e protezione dei dati, nonché l'eventuale mancanza di incriminazioni simmetriche, rendono incerta la cooperazione e favoriscono *forum shopping* tecnologico da parte delle organizzazioni criminali; viepiù ove si consideri che la qualificazione del dato cifrato come “contenuto” o “metadato” assume rilievo decisivo, poiché da essa dipende il livello di tutela applicabile e la disponibilità delle autorità straniere a collaborare.

Anche all'interno dello spazio giuridico europeo, nonostante il supporto operativo di *Europol* e il coordinamento di *Eurojust*, le indagini su piattaforme come *EncroChat* o *Sky ECC* hanno evidenziato asimmetrie normative tra Stati membri quanto alla qualificazione giuridica delle attività intrusive (*hacking* governativo, acquisizione preventiva dei *server*, captazione generalizzata), con conseguenti contestazioni sulla utilizzabilità transnazionale delle prove e sulla compatibilità con gli *standard* di tutela convenzionali.

Dunque, non è più rinviabile un intervento organico del legislatore che, da un lato, definisca obblighi specifici per gli OTT, presidiandone l'adempimento con sanzioni amministrative e penali, e, dall'altro lato, tipizzi le forme di captazione e apprensione del dato cifrato – al netto del fatto che l'uso del captatore è consentito solo per l'intercettazione tra presenti su dispositivo mobile –, disciplini puntualmente la conservazione forense e favorisca strumenti di cooperazione rapida internazionale, così da ricomporre l'equilibrio tra efficacia repressiva e garanzie fondamentali in un contesto tecnologico ormai strutturalmente deterritorializzato (sulle proposte a riguardo, v. *infra*, parte III, 3-3.5.).

4. L'inarrestabile processo di “bunkerizzazione”: scenari e prospettive.

Il quadro finora delineato, a ben vedere, è ulteriormente complicato dalla crescita inarrestabile delle strategie di “bunkerizzazione” comunicativa, da intendersi – genericamente – come un insieme di strategie socio-tecniche finalizzate a ridurre drasticamente la “superficie osservabile” dell'interazione (metadati, contenuti, identità, infrastrutture) e, quindi, ad incrementare la resilienza dell'ecosistema comunicativo criminale rispetto a intercettazioni e sequestri informatici.

Come già anticipato, questa Relazione è stata concepita non come una mera ricomposizione testuale dei contributi emersi nel corso delle audizioni, bensì come un'elaborazione critica delle informazioni acquisite. Tale impostazione muove dalla consapevolezza che, nell'ambito delle tecniche di elusione investigativa, qualsiasi ricostruzione che ambisca a un grado di esaustività risulta inevitabilmente esposta a una rapida obsolescenza, potendo essere superata nell'arco di pochi mesi dall'evoluzione delle pratiche e degli strumenti impiegati. Per questa ragione, gli spunti emersi in sede di audizione in merito ad alcune nuove strategie di “bunkerizzazione” delle comunicazioni criminali sono stati

assunti non come esiti, ma come punti di avvio per un’analisi autonoma, orientata a problematizzare il dato raccolto e a collocarlo entro una cornice interpretativa più ampia.

Invero, emerge con chiarezza come non si tratti più della sola adozione di cifratura *end-to-end* in applicazioni *mainstream* o dell’uso di apparati “blindati” dedicati come i criptofonini, ma di una migrazione verso architetture e protocolli che minimizzano fiducia e vulnerabilità informatica, sfruttando l’ibridazione fra reti decentralizzate, crittografia avanzata e automazione *trustless* tipica dei registri distribuiti¹⁹¹.

Lungo questa china si collocano certamente gli *smart contract*: l’evidenza digitale non coincide più con messaggi recuperabili, ma con tracce transazionali (annotate sulla *blockchain*) la cui interpretazione richiede inferenza probabilistica su grafi e comportamenti, spesso “disturbata” intenzionalmente da pratiche di offuscamento.

Ma il processo di “bunkerizzazione” conosce altre manifestazioni. Ad esempio, la migrazione verso *overlay network* progettate per la resistenza alla sorveglianza. In tal caso, la criminalità beneficia della frammentazione dell’infrastruttura (assenza di un *provider* univoco, distribuzione geografica dei nodi *server* e, quindi, giurisdizioni plurime), della cifratura “a strati” e dei meccanismi di instradamento e *caching* che rendono più complessa la correlazione tra sorgente e destinazione. Le *overlay network*, quindi, non implicano una invisibilità assoluta, quanto piuttosto un indebolimento dei nessi causali tra evento osservato e soggetto agente, funzionale a garantire alla criminalità l’anelata opacizzazione. L’impiego, da parte della criminalità¹⁹², di piattaforme di *gaming* per veicolare comunicazioni riservate costituisce un altro caso paradigmatico di “bunkerizzazione” delle comunicazioni, intesa come migrazione deliberata verso ambienti digitali ad alta complessità investigativa e bassa trasparenza informativa.

L’ecosistema videoludico, invero, consente forme di comunicazione “a bassa firma” (*low signature*), sfruttando identità pseudonime, *account* “usa-e-getta” e pratiche di steganografia sociale (codici condivisi, riferimenti contestuali, istruzioni incorporate in frasi apparentemente innocue o in comportamenti di gioco). La “bunkerizzazione”, in questa prospettiva, non coincide con l’adozione di crittografia forte, ma con una strategia di *hardening* socio-tecnico: selezione di contesti comunicativi ordinari, ad alta base di utenti e alto volume di traffico, in cui l’osservazione mirata risulta onerosa, l’analisi automatizzata produce falsi positivi e la cooperazione giudiziaria può essere rallentata da giurisdizioni multiple.

¹⁹¹ Per un accenno alla problematica, cfr. resoconto stenografico dell’audizione del Gen.B. Mancazzo, seduta del 25 febbraio 2025, X Comitato, p. 7.

¹⁹² Richiama l’attenzione sull’uso dell’ecosistema videoludico come mezzo di comunicazione criminale il Dott. Eugenio Santagata: cfr. resoconto stenografico dell’audizione, seduta del 12 marzo 2024, X Comitato, p. 10.

Ebbene, le nuove frontiere della “bunkerizzazione” non determinano soltanto “maggiore cifratura”, ma una trasformazione strutturale: i contenuti diventano distribuiti e temporanei; i metadati vengono deliberatamente degradati o resi ambigui; la fiducia si sposta da intermediari a protocolli; la coordinazione si incarna in stati computazionali e in prove crittografiche più che in dialoghi recuperabili. Sorgono sfide rilevanti sul piano probatorio e operativo, perché l’accesso a un singolo punto – un *server*, un *account*, un *device* – tende a essere meno risolutivo, mentre cresce l’importanza di analisi multi-sorgente non più orientate a colpire il solo canale comunicativo.

In questa prospettiva, la “bunkerizzazione” va vista per quel che è: non un insieme di “trucchi” isolati e contingenti, ma un paradigma di riduzione dell’esposizione informativa che, grazie al rapido incedere dell’evoluzione tecnologica incide enormemente sul rapporto dialettico tra capacità di occultamento e capacità di rilevazione.

In questo contesto, le comunicazioni satellitari costituiscono una frontiera emergente¹⁹³ e, per alcuni versi, qualitativamente distinta della “bunkerizzazione” strettamente intesa, perché agiscono a livello di connettività e disponibilità del mezzo trasmissivo, introducendo ridondanza rispetto alle infrastrutture terrestri (reti mobili, dorsali *IP*, cavi, *data center*).

L’attrattività criminale del satellite non risiede tanto in un presunto “anonimato intrinseco” (che non è di per sé garantito), quanto nella capacità di sottrarsi a vincoli territoriali e a *choke point* regolatori tipici degli operatori terrestri.

La fonia satellitare, garantendo un percorso multilivello e normalmente transnazionale (interamente nello spazio, oppure mediato da “stazioni di terra”), complica i tempi e le modalità di acquisizione legale. Se, infatti, l’*end-to-end* “blinda” il contenuto lasciando spesso tracce relative alla relazione (chi parla con chi, quando, per quanto) e i criptofonini cercano, invece, di “proteggere” sia il contenuto che i dati esterni alla comunicazione degli *endpoint*, questo strumento, quando impiegato in modo distorto, riduce drasticamente l’efficacia delle forme di controllo e monitoraggio che dipendono dalla cooperazione di operatori terrestri (*provider*) generalmente distribuiti su scala globale.

In definitiva, la costante tensione tra potere investigativo e capacità adattiva della criminalità mafiosa rende evidente che un’intercettazione è efficace solo nella misura in cui consente l’accesso al contenuto e non soltanto alla forma del contatto comunicativo.

Quando l’organizzazione riesce a rendere il contenuto strutturalmente inaccessibile – per cifratura, per codificazione semantica, per rarefazione informativa, per ibridazione dei canali, per dispersione geografica etc. – il mezzo di ricerca della prova subisce una torsione funzionale: da strumento di

¹⁹³ La considera una problematica futuribile il Dott. Eugenio Santagata: cfr. resoconto stenografico dell’audizione, seduta del 12 marzo 2024, X Comitato, p. 12.

conoscenza diretta a dispositivo di mera rilevazione di elementi utili (ad esempio, contatti, tempi e frequenze) ma non autosufficienti sul piano del significato del contenuto comunicativo.

È in questa metamorfosi che può cogliersi il punto critico: la captazione senza comprensione non realizza pienamente la *ratio* dell'intercettazione e impone, sul piano metodologico e probatorio, un ripensamento delle tecniche investigative in chiave integrata, per superare coscienziosamente i limiti epistemici che l'inaccessibilità del contenuto imprime alla pretesa di "tradurre" il flusso comunicativo in prova. Solo così sarà possibile garantire un'effettiva prevenzione e repressione di fenomeni criminosi ad alta "intelligenza elusiva".

Parte III – Conclusioni e prospettive di riforma

1. Sintesi dei risultati.

Nel corso delle audizioni sono stati raccolti numerosi e articolati *input* di riforma, a dimostrazione della complessità del quadro che si è cercato di rappresentare nei paragrafi che precedono, nel quale si intrecciano e si sovrappongono questioni tecniche e questioni giuridiche, quest'ultime, peraltro, di diversa natura (penali, processuali, amministrative, finanziarie, di cooperazione sovranazionale, etc.). Tutte le voci audite convergono verso la necessità di un intervento organico e sistematico. Invero, sono state ampiamente messe in luce criticità operative e applicative riconducibili all'assenza di normativa e alla inadeguatezza degli strumenti oggi disponibili rispetto ai nuovi fenomeni criminosi. Pertanto, la Relazione propone indicazioni sistemiche e di orientamento, finalizzate a migliorare complessivamente lo *status quo* e, soprattutto, a contenere la proliferazione incontrollata di prassi applicative disomogenee. L'uso illecito delle criptovalute e dei nuovi strumenti cifrati di comunicazione da parte delle organizzazioni mafiose, infatti, ha determinato una profonda trasformazione delle modalità operative dei fenomeni criminali, incidendo in modo significativo tanto sulle tecniche investigative, quanto sui tradizionali assetti di tutela delle libertà fondamentali: l'assenza di un quadro interpretativo e operativo sufficientemente coerente rischia di favorire soluzioni frammentarie, talora emergenziali, che possono compromettere l'efficacia dell'azione di contrasto, ovvero, all'opposto, determinare indebite compressioni delle garanzie individuali.

Le indicazioni che seguono mirano, pertanto, a delineare criteri tecnici idonei a rafforzare la capacità di prevenzione e repressione dei reati, di cui l'attività investigativa rappresenta il presupposto imprescindibile, senza perdere di vista la necessità di un equilibrio ragionevole e costituzionalmente orientato con la tutela dei diritti fondamentali, che deve continuare a fungere da limite sostanziale e procedurale all'esercizio del potere pubblico anche nell'era delle tecnologie cifrate e dei sistemi finanziari decentralizzati.

2. Proposte in tema di “uso illecito di criptovalute”.

2.1. Interventi di modifica del codice di procedura penale.

Come più volte sottolineato nelle pagine che precedono, le previsioni generali oggi contenute nel codice di rito mal si adattano alle peculiarità del fenomeno delle criptovalute.

Ne discende l'esigenza, non più differibile, di introdurre una disciplina *ad hoc*, specificamente calibrata sul fenomeno tecnico, che:

- a) tipizzi presupposti, oggetto e forme del sequestro (preventivo e probatorio, ove rilevante), tenendo conto della necessità di assumere il “controllo esclusivo” della chiave privata;
- b) definisca procedure tecniche standardizzate per il tracciamento e il sequestro di criptovalute, idonee a garantire tracciabilità e verificabilità;
- c) istituisca un *wallet* centralizzato – quale sezione dedicata del FUG – sottoposto a gestione pubblica e soggetto ai medesimi principi di separazione patrimoniale, trasparenza e destinazione vincolata, dove far confluire le criptovalute oggetto di sequestro, al duplice fine di garantire uniformità a livello nazionale e superare le criticità connesse alla custodia presso *wallet* privati o *exchange*, ossia rischio di dispersione, volatilità gestionale o perdita delle chiavi di accesso; il *wallet* controllato dalla pubblica autorità – intendendo tale sia quello centralizzato sia, in alternativa, quello creato di volta in volta dalla polizia giudiziaria operante – dovrebbe essere presidiato da configurazioni *multi-signature* o sistemi di *cold storage* con procedure formalizzate di accesso, in modo che ogni eventuale futura movimentazione sia tecnicamente tracciabile e giuridicamente imputabile;
- d) codifichi la c.d. “catena di custodia” relativa all'attività di acquisizione e trasferimento delle criptovalute al *wallet* centralizzato o creato dalla p.g. (attività che perfeziona il vincolo reale): sarebbe opportuno prevedere un obbligo di verbalizzazione dettagliato (*public keys*, *hash* delle transazioni, altezza del blocco di inclusione, commissioni di transazione e ogni ulteriore dato tecnico rilevante), corredato da un obbligo di videoregistrazione del *desktop* e dall'acquisizione del traffico di rete del sistema, così da avere una sorta di “*report* investigativo” su cui apporre “informaticamente” data certa, così da consentire *ex post* la verifica delle operazioni sulla *blockchain* di riferimento;
- e) regoli la custodia e l'amministrazione degli *asset* sequestrati; in particolare, è necessario disciplinare espressamente le modalità di conversione, se in moneta *fiat* o, alternativamente, in

stablecoin, in modo da contemperare l'esigenza di conservazione del valore economico con quella di certezza e stabilità della gestione pubblica;

- f) e coordini tali profili con la futura confisca, al fine di assicurare certezza applicativa, uniformità delle prassi e tenuta processuale dei provvedimenti patrimoniali.

In assenza di un simile intervento, l'inevitabile torsione interpretativa degli strumenti tradizionali rischia di tradursi in soluzioni disomogenee, talora eccessivamente espansive e talaltra paralizzanti, con effetti complessivamente pregiudizievoli sia per l'effettività della pretesa punitiva sia per la piena salvaguardia del giusto processo.

2.2. Potenziare la formazione.

È necessaria una formazione ampia e strategica di tutti gli operatori del settore giustizia e, in particolare, della magistratura e della polizia giudiziaria. Oggi essere in grado di osservare, riconoscere e monitorare *pattern* di offuscamento della proprietà effettiva (*beneficial ownership*) e dell'origine illecita di capitali digital(izzati) è un'abilità imprescindibile per ogni attore investigativo. Una strategia di formazione graduale, dai livelli base a quelli avanzati, può ottimizzare le risorse e garantire sia una comprensione diffusa tra gli agenti in prima linea, sia lo sviluppo di unità multidisciplinari avanzate. Le unità avanzate non solo possono affrontare i casi più complessi, ma possono anche svolgere un ruolo prezioso nel supervisionare la formazione e il trasferimento delle conoscenze a un gruppo più ampio di colleghi. Sviluppare, in modo capillare, la capacità di tracciare, congelare e confiscare criptovalute porterà solo vantaggi in termini di efficienza e, in ultima analisi, giustizia.

Il personale potrà essere formato attraverso la frequenza di corsi specialistici progettati e realizzati in collaborazione con i poli universitari, privilegiando, in via prioritaria, le Università insistenti sul territorio di riferimento qualora dispongano di comprovate competenze scientifiche e infrastrutturali nelle aree di interesse (informatica forense, *cybersecurity*, crittografia applicata, *data analytics*, diritto dell'informatica e diritto processuale penale). In un'ottica di razionalizzazione dell'offerta formativa, omogeneizzazione degli *standard* didattici e massimizzazione dell'efficienza organizzativa, potrà, altresì, essere individuata una rete di strutture universitarie di riferimento articolata su base macro-regionale, con più poli dedicati rispettivamente al Nord, al Centro, al Sud e alle Isole, deputati alla programmazione e all'erogazione di moduli formativi integrati e progressivi. Tale assetto consentirebbe, da un lato, di assicurare uniformità metodologica e coerenza dei contenuti su tutto il territorio nazionale mediante *syllabi* condivisi, criteri di valutazione comparabili e attività laboratoriali standardizzate, e, dall'altro, di valorizzare le specializzazioni distintive dei singoli atenei,

promuovendo sinergie interdipartimentali e accesso a laboratori e piattaforme di ricerca avanzate. La formazione dovrà essere finalizzata all'acquisizione di competenze processuali-investigative e informatiche indispensabili per la conduzione di indagini nel settore delle criptovalute, con particolare riferimento alle tecniche di tracciamento dei flussi *on-chain* e *off-chain*, alle metodologie di de-anonimizzazione mediante correlazione di dati e analisi dei *cluster*, nonché alle procedure operative e giuridiche per l'adozione di misure di sequestro e preservazione della prova digitale, inclusa la gestione delle chiavi crittografiche, dei *wallet* e delle evidenze estratte da dispositivi e servizi correlati.

2.3. Riorganizzazione interna della polizia giudiziaria.

Le strutture delle forze dell'ordine potrebbero richiedere un adeguamento organizzativo e funzionale al fine di fronteggiare in modo più efficace l'incremento dei procedimenti e degli interventi operativi connessi all'impiego di criptovalute e, più in generale, di strumenti basati su tecnologie di registro distribuito. In tale prospettiva, appare opportuno prevedere l'istituzione di nuclei, gruppi o sezioni a elevata specializzazione tecnico-investigativa, dotati di competenze multidisciplinari (giuridiche, informatiche, contabili e di *digital forensics*) e di strumenti idonei all'analisi delle transazioni *on-chain* e *off-chain*, al tracciamento dei flussi finanziari e alla cooperazione con soggetti istituzionali e privati, nazionali e internazionali.

Una possibile opzione organizzativa consiste nell'articolare tali unità su base territoriale, con presidi distribuiti almeno a livello di capoluogo di regione, così da assicurare prossimità operativa, tempestività d'azione e omogeneità di risposta, integrandoli in un modello di *governance* a regia centrale incaricato di definire *standard*, procedure, indirizzi investigativi, programmi formativi e meccanismi di coordinamento interforze.

La configurazione concreta dovrebbe essere calibrata sulle specificità ordinarie, sulle catene di comando e sulle competenze istituzionali proprie di ciascuna forza di polizia, in modo da garantire interoperabilità, razionalizzazione delle risorse e continuità informativa, minimizzando al contempo frammentazioni e disallineamenti tra livelli periferici e centro.

2.4. Potenziamento di strumenti e risorse tecnologiche.

Chiaramente, per rendere più efficace l'attività investigativa in un mondo così peculiare è necessario potenziare le risorse tecnologiche dedicate al settore, dotando la polizia giudiziaria di infrastrutture *hardware* adeguate e performanti e di applicativi *software* specifici, dedicati alla *blockchain analysis*,

per analizzare, tracciare e visualizzare le transazioni di criptovalute, collegandole a entità reali, che permettano di impostare avvisi (*alert*) per nuove transazioni collegate a entità a rischio.

Tuttavia, tale incremento di capacità tecnico-operative deve essere bilanciato, sul piano delle scelte regolative e delle concrete modalità d'impiego, con esigenze attinenti al rispetto del principio di parità delle parti, poiché si pone il problema di come la difesa possa accedere a strumenti e competenze idonei a verificare, replicare e contestare le inferenze e le ricostruzioni probatorie fondate su analisi algoritmiche dei flussi *on-chain* presentate dall'accusa. In questa prospettiva, assumono rilievo sia il profilo della trasparenza "algoritmica" – considerato che numerosi applicativi sono di natura proprietaria e rendono difficoltosa la conoscibilità, nei dettagli, delle euristiche, delle soglie di rischio e dei criteri di ricerca, aggregazione e attribuzione che ne orientano il funzionamento – sia quello dell'affidabilità, intesa come robustezza metodologica e controllabilità empirica dei risultati, alla luce del rischio di errori di attribuzione, falsi positivi/negativi e opacità delle catene inferenziali, con conseguente necessità di garantire tracciabilità delle operazioni, auditabilità, documentazione tecnica e, ove possibile, verificabilità indipendente degli esiti, così da preservare l'equilibrio del contraddittorio e la qualità epistemica dell'accertamento.

2.5. Protocolli di collaborazione.

La sinergia è fondamentale per sviluppare soluzioni previsionali e affrontare le sfide globali legate alle cripto-attività con competenze specialistiche e strumenti avanzati, uniti alla necessaria cooperazione internazionale. La proposta a più voci riguarda tre ambiti di collaborazione.

Collaborazione tra agenzie nazionali: le indagini in materia spesso abbracciano le responsabilità di diverse agenzie. Ad esempio, le unità di *intelligence* finanziaria dovrebbero fornire alle agenzie investigative informazioni chiare e utilizzabili, basate sull'analisi dei dati provenienti dai fornitori di servizi patrimoniali virtuali.

Collaborazione con le controparti internazionali: in ragione della natura intrinsecamente transnazionale e "senza confini" delle cripto-attività, il contrasto ai fenomeni di criminalità economico-finanziaria e di riciclaggio richiede un assetto cooperativo sovranazionale idoneo ad assicurare il coordinamento tra autorità competenti operanti in giurisdizioni differenti. In tale prospettiva, organismi quali *Europol* ed *Eurojust*, nell'ambito dell'architettura dell'Unione, nonché *Interpol* sul piano globale, assumono rilievo dirimente nel favorire la circolazione delle informazioni, la tempestiva attivazione dei canali di cooperazione e l'armonizzazione operativa delle iniziative

investigative, anche in funzione dell'individuazione, tracciamento e ricostruzione dei flussi finanziari in ambiente digitale.

Un rafforzamento della collaborazione internazionale specificamente orientata alle cripto-attività può, altresì, agevolare una più fluida e celere trasmissione di dati e segnalazioni tra autorità, in considerazione delle caratteristiche della tecnologia *blockchain*, la cui dimensione pubblica e globale consente, in particolare alle giurisdizioni dotate di maggiore maturità investigativa e capacità di *blockchain analysis*, di rilevare indicatori di rischio, identificare *pattern* di movimentazione sospetta e allertare le controparti estere circa possibili condotte illecite, in un'ottica di prevenzione e repressione integrate.

Le procedure di cooperazione previste in ambito unionale, ivi incluse quelle attivabili mediante l'Ordine Europeo di Indagine, sebbene concepite per semplificare e rendere più efficiente l'acquisizione transfrontaliera di prove e informazioni, nel concreto possono determinare dilazioni incompatibili con l'esigenza di immediatezza che connota le indagini su cripto-attività, nelle quali la rapidità di trasferimento e la possibile dissimulazione della disponibilità dei fondi (anche tramite conversioni, passaggi su più *wallet* o impiego di strumenti di anonimizzazione) espongono al rischio di irreversibile dispersione delle utilità oggetto di accertamento.

Ne consegue l'esigenza di prevedere e consolidare protocolli operativi e canali di interlocuzione con *exchange* autorizzati a operare nell'Unione Europea e in Italia, tali da garantire tempi di riscontro e di esecuzione compatibili con la volatilità e la mobilità degli *asset* digitali, così da rendere realmente praticabili, con adeguata tempestività, gli accertamenti propedeutici e l'adozione di provvedimenti di congelamento delle cripto-attività prima che l'indagato possa trasferirle, occultarle o renderle di fatto indisponibili.

Collaborazione tra pubblico e privato: impegnarsi in partenariati strutturati pubblico-privato, come gruppi di lavoro e *task force* che combinano professionisti del settore, specialisti legali ed esperti accademici, per migliorare la condivisione delle informazioni e la consapevolezza degli sviluppi illeciti del mercato *crypto*.

2.6. Sollecitare un'implementazione del Regolamento MiCAR.

Il nuovo Regolamento UE non affronta in modo organico alcuni settori emergenti del mondo delle cripto-attività, come *NFT*, finanza decentralizzata (DeFi) e il metaverso. L'evoluzione costante e velocissima della tecnologia apre alla criminalità nuovi spazi virtuali per i propri guadagni illeciti e risulta fondamentale colmare queste lacune.

Soprattutto, né il MiCAR (Reg. 2023/1114/UE) né il TFR (*Transfer of Funds Regulation* - Reg. 2023/1113/UE) prevedono un divieto espresso e generalizzato di utilizzo di cripto-attività con funzionalità di anonimizzazione quali Monero o Zcash (“*privacy coin*”), limitandosi rispettivamente a una disciplina di mercato degli operatori e a obblighi di tracciabilità informativa dei trasferimenti. La prima interdizione normativa di carattere specificamente “anti-anonimato” è rinvenibile nel Regolamento (UE) 2024/1624 (*Single Rulebook*), quale divieto in capo ai soggetti obbligati (inclusi i prestatori di servizi su cripto-attività) di offrire o mantenere *asset* e strumenti idonei a incrementare l’opacità o l’anonimato delle transazioni; tuttavia, la differita applicabilità al 2027 determina un significativo periodo transitorio che, in assenza di misure equivalenti immediatamente operative, rischia di compromettere l’effettività dell’azione di contrasto in un settore caratterizzato da rapida evoluzione tecnica e da elevata capacità di elusione.

2.7. Obblighi di collaborazione per i CASPs.

Introdurre un sistema sanzionatorio specificamente rivolto ai *crypto-asset service providers* (CASPs) che, pur risultando formalmente conformi ai requisiti autorizzativi e organizzativi previsti dalla disciplina europea, omettano di dare esecuzione agli ordini dell’Autorità giudiziaria funzionali all’accertamento di reati riguardanti le cripto-attività, significa allineare la dimensione regolamentare-amministrativa e quella giurisdizionale, disincentivando strategie opportunistiche da parte degli operatori ed evitando che l’innovazione tecnologica si traduca in uno spazio di sottrazione alla giurisdizione.

Verrebbe attuato il principio di “convenienza regolatoria”, il quale implica che l’adesione ai circuiti autorizzati e il rispetto delle prescrizioni provenienti dall’autorità giudiziaria risultino economicamente più vantaggiosi rispetto a condotte elusive o dilatorie. Ciò può essere perseguito attraverso un sistema graduato di misure, che comprenda sanzioni pecuniarie commisurate al volume d’affari e alla gravità della violazione, misure interdittive temporanee, fino alla sospensione o revoca dell’autorizzazione nei casi di reiterazione o particolare gravità.

Dal momento che, il più delle volte, sono coinvolti *providers extra UE*, rispetto ai quali l’adempimento alle richieste dell’Autorità giudiziaria italiana risulta incerto, con conseguente compromissione dell’effettività dell’azione investigativa, si potrebbero incentivare accordi bilaterali con le controparti *extra UE* per prevedere un obbligo per tutti i *providers* di eseguire ordini giudiziari validamente emessi dalle autorità degli Stati firmatari per la produzione di dati e informazioni in loro “possesso, custodia o controllo”, nonché per l’esecuzione di ordini di congelamento del *wallet*,

indipendentemente dalla localizzazione fisica dei *server*, purché rilevanti per un'indagine penale relativa a crimini gravi come criminalità organizzata transnazionale, terrorismo, *cybercrime* etc.

3. Proposte in tema di “uso illecito della crittografia”.

In tema di crittografia, le audizioni hanno consentito di apprendere, anzitutto, che la normativa italiana contiene già gli strumenti per intervenire sui servizi OTT (artt. 11 e 57 Codice delle Comunicazioni Elettroniche); a seguire, che alcuni *partner* europei hanno già affrontato il problema introducendo un regime autorizzatorio presidiato da sanzioni penali; e che, in presenza di un quadro giuridico adeguato e di una cooperazione internazionale efficace, è tecnicamente possibile penetrare le piattaforme che offrono servizi di crittografia (come accaduto per le ultime operazioni investigative europee di *EncroChat* e *Sky ECC*).

Sebbene sia chiaro che ogni ritardo amplia il vantaggio tecnologico di cui godono le organizzazioni criminali – le quali dispongono di ingenti risorse finanziarie per accedere agevolmente alle tecnologie più avanzate – e riduce proporzionalmente l'efficacia dell'azione di contrasto dello Stato, le proposte di seguito formulate mirano a recuperare le capacità investigative perdute a causa dell'evoluzione tecnologica, non a creare nuovi poteri di sorveglianza di massa.

L'obiettivo da raggiungere, infatti, non coincide con la neutralizzazione della crittografia, ma con la ridefinizione del modello di sicurezza e di fiducia del sistema, bilanciando obiettivi investigativi e tutela dei diritti fondamentali.

3.1. Obblighi per gli operatori OTT.

Tutte le voci *audite* segnalano la necessità di costruire un'infrastruttura normativa – articolata in obblighi positivi e in un apparato sanzionatorio per l'inadempimento – per consentire all'Autorità giudiziaria di dare esecuzione effettiva ai propri provvedimenti anche in caso di inerzia o rifiuto del fornitore, mantenendo tuttavia un assetto coerente con i principi di minimizzazione, separazione delle funzioni, sicurezza *by design* e tutela della libertà e segretezza delle comunicazioni e della *privacy* degli utenti.

In tale prospettiva, l'intervento normativo non può limitarsi alla sola individuazione dei soggetti obbligati e delle conseguenze dell'inadempimento, ma deve necessariamente investire anche il piano tecnico-organizzativo, disciplinando le modalità attraverso cui i servizi offerti dagli operatori OTT possano essere strutturati in modo da rendere concretamente eseguibili gli obblighi di collaborazione con l'Autorità giudiziaria, secondo soluzioni compatibili con i diritti fondamentali e con i principi di

proporzionalità e necessità. Questo significa fissare requisiti chiari e verificabili, così che l'esecuzione degli ordini non dipenda da scelte discrezionali del fornitore né si traduca in accessi più ampi del necessario.

Sul punto, possono essere menzionate due distinte linee di intervento, funzionalmente orientate alla medesima finalità.

3.1.1. La parificazione regolatoria.

La prima strada percorribile è quella di estendere espressamente agli OTT – basati e non su numerazione – l'applicabilità delle disposizioni contenute negli artt. 11 e 57 Codice delle Comunicazioni Elettroniche, includendoli, a monte, nel perimetro soggettivo del medesimo Codice. In tal modo, gli OTT sarebbero assoggettati al medesimo quadro di obblighi e al medesimo schema di autorizzazione generale già previsto per gli operatori tradizionali.

L'inadempimento – ossia la mancata acquisizione dell'autorizzazione generale (art. 11 c.c.e.) e/o la mancata esecuzione delle prestazioni obbligatorie (art. 57 c.c.e.) – dovrebbe essere adeguatamente presidiato da sanzioni. È chiaramente necessario prevedere che un organo – il MIMIT o altra autorità competente – vigili sulla corretta applicazione degli artt. 11 e 57 del Codice delle Comunicazioni Elettroniche; attualmente, infatti, tale compito di controllo non risulta esercitato da nessun ente.

In particolare, a livello amministrativo si potrebbero prevedere per gli OTT inadempienti la sospensione delle attività, la sanzione amministrativa pecuniaria e, in ultimo l'inibitoria definitiva.

Dal punto di vista penalistico, invece, si potrebbe sanzionare la strumentalizzazione patologica della crittografia, ove risulti essenziale alla commissione di gravi reati, introducendo, con la previsione incriminatrice di fornitura, trasferimento all'interno dell'UE, esportazione e importazione di mezzi o servizi di crittografia non conformi al modello amministrativo delineato, la fattispecie di attività abusive in ordine a mezzi e servizi di crittografia.

In questo scenario, l'effettività degli obblighi di collaborazione presuppone che il servizio offerto dagli OTT sia tecnicamente configurato in modo da consentire, nei soli casi e modi previsti dalla legge e su ordine dell'autorità competente, l'accesso legale alle comunicazioni o ai relativi dati. L'obiettivo non è “rendere leggibile tutto”, ma rendere eseguibile l'ordine in un perimetro strettamente definito, con evidenza documentabile di ciò che viene acquisito e quanto resta escluso.

Nel corso delle audizioni è stato richiamato – a titolo d'esempio – il *LEON - Law Enforcement Operational Needs for lawful access to communications*, ossia il documento strategico, presentato durante la presidenza svedese del Consiglio UE nel 2023, che definisce le esigenze operative delle forze dell'ordine europee (e internazionali) in merito all'accesso legale alle comunicazioni, inclusi i

metadati e i contenuti, in un contesto di crescente cifratura e complessità digitale. È stato proposto di attuare il principio “*Legal Access by Design*” prevedendo un’architettura regolatoria che imponga agli OTT di incorporare sin dalla fase di progettazione dei sistemi crittografici dei meccanismi che rendano possibile l’accesso legale ai contenuti cifrati da parte delle autorità competenti.

Dal momento che creare una “*backdoor*” per le forze dell’ordine potrebbe minare la sicurezza complessiva delle comunicazioni, rendendole vulnerabili anche ad attori malevoli, si potrebbe piuttosto sviluppare un “*Legal Access with Verifiable Minimization*”, cioè un insieme di requisiti architetturali che consentirebbero, solo in presenza di un titolo giudiziario e di un perimetro istruttorio puntualmente definito, l’estrazione mirata di evidenze digitali senza introdurre un meccanismo generalizzato di *bypass* della confidenzialità né indebolimenti strutturali della cifratura.

In questa riformulazione, verrebbero preservate le proprietà di sicurezza per la generalità degli utenti, ammettendo solo eccezioni ad alta soglia, strettamente mirate e tecnicamente rendicontabili, così da ridurre al minimo l’introduzione di vulnerabilità strutturali e l’ampliamento della superficie d’attacco, in linea con la solida giurisprudenza della Corte di giustizia, secondo la quale le misure nazionali incidenti sull’accesso delle autorità pubbliche ai dati di comunicazione devono essere strettamente necessarie, soggette a controllo giurisdizionale effettivo e non possono comportare forme generalizzate e indiscriminate di accesso o indebolimento sistemico della sicurezza delle comunicazioni elettroniche.

3.1.2. Introduzione di un nuovo regime d’autorizzazione.

Diversamente, si potrebbe introdurre un regime di autorizzazione o licenza per la fornitura di servizi di comunicazione crittografata offerti da operatori OTT, quale condizione legale per l’accesso al mercato nazionale, con conseguente sottoposizione dell’attività ad un controllo preventivo dell’autorità pubblica finalizzato a verificare il possesso di determinati requisiti tecnici, organizzativi e di sicurezza, puntualmente stabiliti dalla legge.

In tale prospettiva, la disciplina autorizzatoria non dovrebbe limitarsi ad una verifica meramente formale dell’affidabilità soggettiva dell’operatore o della conformità agli *standard* di protezione dei dati personali, ma potrebbe includere, quale requisito essenziale, la predisposizione di soluzioni tecniche e procedurali idonee a consentire, nei soli casi e con le garanzie previste dall’ordinamento processuale, l’effettiva esecuzione dei provvedimenti dell’autorità giudiziaria volti all’acquisizione di comunicazioni o dati comunicativi, anche quando i servizi siano fondati su sistemi di cifratura avanzata o *end-to-end*.

Ne consegue che l'autorizzazione potrebbe essere subordinata alla dimostrazione, da parte dell'operatore OTT, dell'esistenza di meccanismi di cooperazione tecnica qualificata con l'Autorità giudiziaria, consistenti, ad esempio, nella disponibilità di procedure di *lawful access*, nella capacità di fornire metadati e informazioni tecniche utili all'identificazione degli utenti, nonché – entro limiti di stretta proporzionalità, necessità e controllo giurisdizionale – nella predisposizione di soluzioni che rendano tecnicamente possibile l'aggiramento mirato della cifratura in presenza di un ordine dell'Autorità giudiziaria, senza che ciò comporti una vulnerazione generalizzata della sicurezza del sistema o un indebito sacrificio dei diritti fondamentali degli utenti.

Un simile assetto, per risultare compatibile con i principi costituzionali e sovranazionali in materia di segretezza delle comunicazioni, protezione dei dati personali e libertà d'iniziativa economica, dovrebbe essere costruito secondo criteri di stretta legalità, tassatività delle condizioni, controllo giurisdizionale preventivo, tracciabilità delle operazioni e responsabilità dell'operatore, configurando, dunque, un modello di "crittografia regolata" in cui la tutela della riservatezza resta la regola, mentre la possibilità di accesso investigativo rappresenta un'eccezione rigorosamente disciplinata.

Si tratterebbe, dunque, di un intervento normativo di tipo strutturale che incide direttamente sulla libertà di iniziativa economica e sulla configurazione del mercato, giustificabile, tuttavia, alla luce delle esigenze di sicurezza pubblica, di lotta alla criminalità grave e di amministrazione della giustizia, purché rispettoso del principio di proporzionalità e non discriminazione nei confronti degli operatori OTT.

Del resto, la giurisprudenza della Corte di giustizia in materia di regolazione dei servizi digitali e delle comunicazioni elettroniche ha ripetutamente chiarito che sistemi autorizzatori nazionali sono ammissibili solo se fondati su criteri oggettivi, trasparenti, non discriminatori e previamente conoscibili, secondo una logica coerente con la disciplina del mercato interno delle comunicazioni elettroniche.

In quest'ordine di idee, sulla scorta di soluzioni già sperimentate in altri ordinamenti, si potrebbe poi qualificare come illecito penale la fornitura di tali servizi in assenza della prescritta autorizzazione.

Altresì, dovrebbero essere previste sanzioni specifiche nel caso di mancata cooperazione tecnica con l'Autorità giudiziaria o per le ipotesi di implementazione consapevole di soluzioni progettate per impedire, in modo assoluto, qualsiasi forma di esecuzione dei provvedimenti giurisdizionali, assicurando, al contempo, che l'estensione extraterritoriale degli obblighi e delle sanzioni sia compatibile con il diritto dell'Unione e con il principio di territorialità ragionevole.

In tal modo si potrebbe rafforzare l'effettività del sistema e prevenire fenomeni di elusione regolatoria mediante localizzazione estera dell'infrastruttura o offerta transfrontaliera dei servizi digitali, senza

compromettere l'equilibrio complessivo tra esigenze investigative, sicurezza informatica, tutela della concorrenza e protezione dei diritti fondamentali nello spazio giuridico europeo.

3.2. Armonizzazione della normativa europea sugli OTT.

Parallelamente alla definizione di regole interne, sarebbe opportuno che il nostro Paese promuovesse, in sede sovranazionale, un processo di progressiva armonizzazione della normativa europea volto a colmare le attuali asimmetrie regolatorie tra operatori di comunicazioni elettroniche tradizionali e prestatori di servizi digitali transnazionali.

Sarebbe opportuno sostenere l'adozione di un quadro regolatorio uniforme che, nel rispetto dei principi di proporzionalità, necessità e tutela dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea e dalla Convenzione europea dei diritti dell'uomo, introduca obblighi positivi di cooperazione in capo ai fornitori di servizi OTT, prevedendo strumenti procedurali standardizzati per l'esecuzione di ordini dell'Autorità giudiziaria degli Stati membri, nonché modalità tecniche e organizzative idonee a garantire l'accessibilità ai dati legalmente richiesti, anche quando l'architettura del servizio sia caratterizzata da sistemi avanzati di cifratura; fermo restando che tali modalità non devono tradursi in obblighi di indebolimento generalizzato della sicurezza o della cifratura per la generalità degli utenti.

In questa direzione si inserisce la necessità di promuovere un'evoluzione del Codice europeo delle comunicazioni elettroniche affinché la sua sfera applicativa venga esplicitamente estesa ai servizi OTT che svolgono, sotto il profilo funzionale, attività equivalenti alle comunicazioni interpersonali tradizionali, superando l'attuale impostazione fondata su distinzioni tecnologiche ormai recessive rispetto alla sostanza economico-sociale del servizio erogato; tale intervento consentirebbe di assoggettare tali operatori a un regime di responsabilità, tracciabilità e cooperazione comparabile a quello previsto per gli operatori di telecomunicazioni, assicurando uniformità di obblighi in materia di conservazione dei dati, identificazione degli utenti nei limiti consentiti dall'ordinamento europeo, risposta alle richieste giudiziarie e predisposizione di punti di contatto giurisdizionali effettivi all'interno dell'Unione.

Parallelamente, si rende opportuna una più ampia riconsiderazione del sistema europeo dei prestatori di servizi della società dell'informazione operanti sulla rete, mediante una revisione coordinata delle discipline in materia di responsabilità degli intermediari digitali, stabilimento virtuale, criteri di collegamento territoriale e obblighi di rappresentanza legale nell'Unione, al fine di evitare fenomeni di *forum shopping* regolatorio e di garantire che la natura transfrontaliera dell'infrastruttura digitale

non si traduca in una sostanziale immunità rispetto all'esercizio dei poteri pubblici legittimamente fondati.

Un simile percorso normativo, se adeguatamente calibrato, permetterebbe di perseguire un punto di equilibrio tra l'esigenza di preservare l'elevato livello di protezione della riservatezza delle comunicazioni elettroniche e la necessità, parimenti costituzionalmente rilevante, di assicurare l'effettività della tutela giurisdizionale, della sicurezza pubblica e della repressione dei reati, evitando che l'innovazione tecnologica determini zone franche sottratte alla legalità procedurale e alla cooperazione giudiziaria europea.

3.3. Utilizzabilità processuale del materiale probatorio già acquisito all'estero.

Per superare del tutto i problemi legati alla utilizzabilità del materiale probatorio “raccolto” all'estero – oggi gestiti attraverso il combinato disposto di norme di cooperazione, strumenti UE e principi elaborati dalla giurisprudenza di legittimità –, un ulteriore profilo di riforma dovrebbe riguardare il riconoscimento probatorio dei dati acquisiti all'estero mediante operazioni congiunte o tramite autorità straniere, introducendo norme che chiariscano espressamente i criteri di utilizzabilità processuale delle prove digitali ottenute attraverso l'accesso a *server* ubicati fuori dal territorio nazionale, purché l'attività sia stata svolta nel rispetto dei principi fondamentali dell'ordinamento costituzionale, del diritto di difesa e del contraddittorio sulla prova.

In tale prospettiva, sarebbe opportuno prevedere un obbligo di documentazione tecnica integrale delle operazioni di acquisizione, comprensiva delle procedure di decrittazione, delle catene di custodia digitali, degli algoritmi di selezione e delle verifiche di integrità dei dati, così da consentire alla difesa un controllo effettivo sull'affidabilità della prova informatica.

3.4. Istituzione di un centro di competenza nazionale.

Una proposta a più voci riguarda la creazione, anche nel nostro Paese, di un centro nazionale, a composizione mista (istituzioni, magistratura, professori e/o studiosi di comprovata esperienza nel settore, polizia giudiziaria, fornitori dei servizi digitali), per la ricerca delle vulnerabilità dei principali sistemi operativi e delle applicazioni maggiormente utilizzate in ambito criminale, finalizzata all'impiego più efficiente e sicuro dei captatori informatici ai fini investigativi.

L'adozione di tali strumenti, infatti, richiede un punto di equilibrio tra l'esigenza di garantire l'effettività dell'accertamento penale e la tutela dei diritti fondamentali; equilibrio che, nell'attuale contesto, risulta fortemente condizionato dall'asimmetria informativa e tecnica tra soggetti pubblici

chiamati a disporre e controllare l'impiego del mezzo di ricerca della prova e soggetti privati detentori di *know-how*, infrastrutture e servizi digitali.

Tale centro di competenza nazionale potrebbe:

- supportare il legislatore, mediante la produzione di pareri tecnici, linee guida e analisi di impatto, contribuendo a una normazione più consapevole delle implicazioni tecnologiche e più coerente con l'evoluzione dei rischi digitali;
- costituire il punto di contatto con gli OTT per l'erogazione delle prestazioni obbligatorie;
- assistere le forze di polizia e l'Autorità giudiziaria nelle questioni tecniche;
- spiegare agli operatori stranieri cosa fare e come erogare le prestazioni obbligatorie;
- verificare il rispetto degli adempimenti da parte dei soggetti autorizzati;
- definire preventivamente i requisiti tecnici per le prestazioni obbligatorie prima del lancio commerciale di nuovi servizi.

3.5. Estensione delle operazioni sotto copertura.

Sarebbe utile estendere la disciplina del c.d. “*undercover* informatico” al reato di associazione mafiosa.

L'estensione delle operazioni sotto copertura al dominio digitale ad opera della l. 9 ottobre 2023, n. 137 (di conversione del d.l. n. 105/2023) si colloca nel più ampio processo di adeguamento degli strumenti investigativi alla morfologia contemporanea delle minacce cibernetiche, segnate da organizzazioni fluide, transnazionali e ad alta intensità tecnologica.

Se la scelta legislativa ha sinora circoscritto l'operatività dell'agente sotto copertura informatico ai delitti con finalità di terrorismo o di eversione e ai reati informatici in danno di infrastrutture critiche, ciò è avvenuto in ragione dell'elevato grado di offensività e del rischio sistemico che tali fattispecie esprimono; nondimeno, analoghi indici di pericolosità e di compromissione dell'ordine pubblico economico e istituzionale connotano le condotte riconducibili alle associazioni di tipo mafioso, specie ove si consideri la progressiva digitalizzazione delle loro modalità operative.

Pertanto, sarebbe utile consentire l'infiltrazione nelle reti di distribuzione di dispositivi e servizi di comunicazione criptata utilizzati dalla criminalità organizzata mafiosa.

4. Considerazioni conclusive: le mafie sono cambiate. Lo Stato deve cambiare con loro.

Per troppo tempo abbiamo raccontato le mafie con il vocabolario di trent'anni fa. Quel vocabolario serviva a descrivere un nemico che sparava per strada, che intimidiva con la violenza fisica, che lasciava segni visibili. Tutto questo, naturalmente, esiste ancora. Ma accanto a quella mafia, e in larga misura sopra di essa, è cresciuta una mafia diversa: silente, finanziaria, tecnologicamente attrezzata. Una mafia che non ha bisogno di apparire perché ha imparato a operare nei luoghi in cui lo Stato fatica ad arrivare: le piattaforme di comunicazione cifrata, le valute virtuali, le reti decentralizzate.

La Relazione documenta peraltro una trasformazione del modo in cui le mafie si presentano nei luoghi della socialità digitale. Da un lato, accanto al nucleo dirigenziale dei «veterani» che custodisce riti e codici della tradizione, le organizzazioni hanno integrato giovani membri con elevata competenza digitale, capaci di operare nel linguaggio contemporaneo della rete. Si tratta di un «ponte generazionale» che è anche una sfida culturale: difendere le competenze e gli ideali delle nuove generazioni dalla tentazione di metterle al servizio della criminalità organizzata. Dall'altro lato, si registra l'uso crescente, da parte della criminalità organizzata, dell'ecosistema dei videogiochi e delle piattaforme di gioco online come canale di comunicazione riservata. Videogiochi e piattaforme sono diventati ambienti in cui la comunicazione criminale si nasconde proprio perché si confonde con la comunicazione di tutti, e in particolare con quella dei più giovani.

L'inchiesta della Commissione porta ad una considerazione tanto semplice quanto necessaria: non possiamo accettare che esistano zone della vita economica e relazionale in cui le organizzazioni criminali si muovano indisturbate semplicemente perché lo Stato non ha gli strumenti per vedere. La legalità non può fermarsi davanti a una soglia tecnologica.

La dimensione del problema è ormai documentata. Emerge dalla Relazione un dato che dovrebbe scuotere chiunque abbia a cuore la sicurezza nazionale: l'undici per cento degli attacchi informatici gravi a livello mondiale registrati nell'ultimo anno è stato diretto contro obiettivi italiani. Non è una percentuale residuale: è la conferma che il nostro Paese è uno dei terreni di prova privilegiati della nuova criminalità tecnologica, e che la risposta dello Stato non può più essere differita.

Nessuna delle proposte qui contenute mira a indebolire la crittografia di uso comune, nessuna chiede di introdurre *backdoor* sistemiche, nessuna intende sacrificare la riservatezza dei cittadini onesti per inseguire i criminali. L'obiettivo è esattamente il contrario: tutelare i cittadini onesti facendo in modo che le mafie non abbiano più nessuno strumento privilegiato di occultamento.

Le garanzie processuali, le tutele della Convenzione europea dei diritti dell'uomo, il sindacato della Corte costituzionale non sono — non sono mai stati — ostacoli sulla strada dell'azione dello Stato.

Sono la cornice che dà a quell'azione legittimità democratica. La Relazione si muove dentro questa cornice e propone strumenti che dentro questa cornice possano operare. È la cifra di un'antimafia ferma sui principi e rigorosa sui mezzi, quella che da sempre l'Italia ha saputo esprimere.

L'Italia non è un Paese qualsiasi, su questo terreno. È il Paese che ha pagato in vite umane il prezzo di una lezione che il mondo intero ha poi imparato da noi. I magistrati Giovanni Falcone, Paolo Borsellino, Rocco Chinnici, Gaetano Costa, Rosario Livatino, Cesare Terranova, Giangiacomo Ciaccio Montalto. Il generale Carlo Alberto Dalla Chiesa. Il parlamentare Pio La Torre, che insieme al ministro Virginio Rognoni ha dato all'ordinamento la legge che ancora oggi è il pilastro della legislazione antimafia. E con loro gli uomini delle forze dell'ordine caduti al loro fianco. Sono nomi che appartengono alla storia della Repubblica e che continuano a indicare la direzione. La determinazione delle nostre istituzioni democratiche — magistrati, forze di polizia, Direzione Nazionale Antimafia e Antiterrorismo, Direzioni Distrettuali Antimafia, Direzione Investigativa Antimafia, Polizia di Stato, Arma dei Carabinieri, Guardia di Finanza, Polizia Penitenziaria — ha consegnato all'Italia un patrimonio di esperienza, di strumenti normativi, di prassi operative che nessun altro Paese può vantare.

Questo patrimonio, oggi, è chiamato a misurarsi con la trasformazione digitale del fenomeno mafioso. Le indagini più recenti dimostrano che la strada è praticabile. L'arresto in Brasile di Rocco Morabito, capo della 'ndrangheta latitante da anni e considerato uno dei più pericolosi narcotrafficienti italiani all'estero, è stato reso possibile dall'operazione internazionale ANØM coordinata dalle autorità americane e australiane, che ha consentito di penetrare un sistema di comunicazione cifrata utilizzato dalle organizzazioni criminali in tutto il mondo. È la dimostrazione concreta che la tecnologia investigativa, quando le forze dell'ordine ne dispongono e quando la cooperazione internazionale funziona, non lascia spazio nemmeno ai latitanti più protetti.

E l'Italia, come è sempre accaduto, non può permettersi di subire questa trasformazione: deve guidarla. Le proposte della Relazione vanno lette in questa chiave. Costruire un Fondo Unico Giustizia capace di custodire criptovalute con tecnologie all'altezza del compito; tipizzare procedure di sequestro che oggi gli inquirenti adattano a fatica al codice di rito; rafforzare la cooperazione internazionale; riservare alle forze dell'ordine italiane gli strumenti tecnologici già da tempo nelle disponibilità di altre democrazie occidentali. Non è arretrare: è tornare a essere all'avanguardia, che è la posizione che l'Italia, sul terreno antimafia, ha occupato per quarant'anni e merita di continuare a occupare.

Del resto la sfida del cyberspazio e delle criptovalute non si combatte dentro i confini di un solo Stato. La Relazione lo riconosce con chiarezza, e indica nell'Unione europea il livello istituzionale al quale molte delle questioni qui poste devono trovare risposta: dal regime degli operatori *Over-The-Top* alla

disciplina antiriciclaggio armonizzata, dal Regolamento DORA al Cyber Resilience Act, dal nuovo Regolamento antiriciclaggio del 2024 al documento *LEON* — le « Esigenze operative delle forze dell'ordine per l'accesso legale alle comunicazioni » presentato durante la presidenza svedese del Consiglio dell'Unione europea nel 2023. L'Italia partecipa a questi tavoli, e deve continuare a parteciparvi con il peso che le compete.

Ma il contributo italiano non è quello di un Paese in attesa di essere istruito. È quello di un Paese che porta nei consessi europei un'esperienza che gli altri non hanno avuto.

Le proposte normative contenute nella Relazione meritano tempestive strategie d'intervento, in considerazione dell'estrema mutevolezza dei contesti tecnologici di riferimento.

La Commissione, per quanto la riguarda, consegna al Parlamento un importante contributo di proposte. Continuerà ad accompagnare il loro percorso, vigilare sulla loro coerenza e contribuire al loro affinamento. Lo deve a quei magistrati e a quegli uomini in divisa che, ogni giorno, in silenzio, fanno il mestiere più difficile di tutti: garantire la sicurezza di chi non sa di essere in pericolo.

Continuerà a farlo con il rispetto delle regole, con la determinazione delle istituzioni, con la fedeltà alla Repubblica e alla Costituzione.



190230206630