

INDAGINI PENALI, *BLOCKCHAIN ANALYSIS* E CRIPTO-ATTIVITÀ: *PRIVACY* E GIUSTO PROCESSO IN PROSPETTIVA COMPARATA TRA EUROPA E USA*

di Lorenzo Farneti
(Dottorando di ricerca in procedura penale,
Università di Bologna)

Il contributo esamina l'impiego investigativo e probatorio della *blockchain analysis* in prospettiva comparata tra ordinamento statunitense ed europeo. Dopo aver ricostruito la metodologia investigativa e le principali tecniche, l'indagine si articola lungo due direttrici: la tutela della riservatezza e le garanzie del giusto processo, per poi verificare l'adeguatezza del sistema processuale penale italiano e delineare possibili soluzioni. Ne emerge l'inadeguatezza delle categorie probatorie vigenti e la necessità di un intervento legislativo.

This paper examines the use of blockchain analysis for investigative and evidential purposes from a comparative perspective between the US and European legal systems. After outlining the investigative methodology and key techniques, the study follows two main lines of inquiry: respect for privacy and the guarantees of fair trial, before assessing the adequacy of the Italian criminal procedure system and outlining possible solutions. This reveals the inadequacy of the current categories of evidence and the need for legislative action.

Indagini penali, blockchain analysis, criptovalute, riservatezza, giusto processo
Criminal investigations, blockchain analysis, cryptocurrencies, privacy, fair trial

Sommario: 1. Introduzione. - 2. *Blockchain forensics*, *blockchain analysis* e tecniche investigative. - 2.1 La tecnologia *blockchain*: nozioni essenziali. - 2.2 *Blockchain analysis* e tecniche investigative. - 2.3 La *blockchain analysis* in pratica: l'esempio degli strumenti di Chainalysis. - 3. La *blockchain analysis* e il diritto alla *privacy*. - 3.1 La prospettiva statunitense: dati pubblici e *third-party doctrine*. - 3.2 La prospettiva europea: proporzionalità e *data retention*. - 4. La *blockchain analysis* e il diritto al giusto processo. - 4.1 L'approccio statunitense: ammissibilità secondo i criteri *Daubert*. - 4.2 L'approccio europeo: giusto processo e parità delle armi. - 5. La *blockchain analysis* nella procedura penale italiana. - 6. Prospettive di riforma e soluzioni emergenti. - 7. Conclusioni.

1. L'integrazione delle criptovalute nel sistema finanziario globale ha proceduto a un ritmo che ha ampiamente superato la capacità degli ordinamenti giuridici di apprestare strumenti adeguati di regolazione e contrasto. Sebbene Bitcoin e le criptovalute successive siano stati apprezzati per il loro potenziale innovativo, le rispettive caratteristiche strutturali – in particolare lo pseudonimato degli utenti, la

* Il presente elaborato si inserisce nell'ambito del progetto "PRIN 2022 PNRR – Progetto: CRYPTOSAFE (Towards a safe seizure and confiscation of crypto-assets in criminal proceedings)". Codice progetto P2022HW85A; CUP D53D23022280001. Principal Investigator: Prof. Jacopo Della Torre.

decentralizzazione e la vocazione transnazionale – ne hanno al contempo favorito l'impiego in una pluralità di attività illecite, dal riciclaggio di denaro al finanziamento del terrorismo, sino alle truffe. Tali caratteristiche hanno posto i sistemi di giustizia penale di tutto il mondo di fronte a sfide senza precedenti.

Una delle ragioni di tale difficoltà risiede nella complessità tecnica dello strumento in oggetto: le criptovalute si fondano sulla tecnologia *blockchain*, un'infrastruttura decentralizzata che, per sua stessa architettura, prescinde dall'intervento di un'autorità o di un intermediario centrale ai fini della validazione delle transazioni. L'accesso a tale ecosistema, tuttavia, avviene, nella maggior parte dei casi, attraverso gli *exchange*, ovvero le piattaforme che costituiscono i principali punti di raccordo tra il mondo delle cripto-attività e il sistema finanziario tradizionale, consentendo la conversione reciproca tra valuta legale e le criptomonete. È proprio in corrispondenza di tali snodi che l'attività pseudonima registrata sulla *blockchain* può essere ricondotta, attraverso ulteriori elementi informativi, a soggetti determinati o determinabili. Tale circostanza assume un rilievo centrale, come si vedrà, tanto sotto il profilo investigativo quanto ai fini della qualificazione giuridica delle tecniche di *blockchain analysis*.

Si comprende bene, quindi, come le autorità di contrasto¹ abbiano dovuto progressivamente affinare le proprie tecniche investigative, ricorrendo in misura crescente agli strumenti di *blockchain forensics* e ai software di *blockchain analysis*. Con quest'ultima espressione si designa, in particolare, l'insieme delle metodologie utilizzate per ricostruire i flussi transazionali iscritti sulla *blockchain* e individuare correlazioni tra indirizzi, trasformando ampie masse di dati in elementi conoscitivi suscettibili di assumere rilievo probatorio nel procedimento penale, anche riconducendo tali transazioni a persone fisiche². La *blockchain forensics* rinvia invece a una nozione più ampia, che non si esaurisce nell'analisi dei dati, ma ne comprende l'inserimento in un contesto investigativo, procedurale e probatorio, nonché l'elaborazione di metodi per l'estrazione, la conservazione e la presentazione in giudizio della prova digitale. In definitiva, la *blockchain forensics* rappresenta la cornice metodologica che presiede all'identificazione, all'acquisizione, all'analisi e

¹ Il termine è qui impiegato, per comodità espositiva, nell'accezione fatta propria dal diritto dell'Unione: v. dir. 27.4.2016 n. 2016/680/UE, art. 3 n. 7, che definisce «autorità competente» qualsiasi autorità pubblica competente per la prevenzione, l'indagine, l'accertamento o il perseguimento di reati o l'esecuzione di sanzioni penali, ovvero qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare pubblici poteri e prerogative pubbliche a tali fini.

² A. Balaskas, V.N.L. Franqueira, *Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges*, in *IEEE Access* 2022 (17), 13879, 13880.

all'interpretazione dei dati registrati sulla *blockchain* a fini probatori³.

È in questo contesto che il presente lavoro indaga la tensione tra l'impiego investigativo della *blockchain analysis* e le garanzie fondamentali, articolandosi attorno a tre questioni di fondo: cosa si intenda per *blockchain analysis* quale metodologia investigativa e quali informazioni le autorità di contrasto possano estrarre attraverso tali strumenti; in che misura tali tecniche risultino compatibili con la tutela della riservatezza e con le garanzie del giusto processo; e, infine, se e a quali condizioni il diritto processuale penale italiano offra oggi una cornice normativa e probatoria adeguata al loro impiego. Lo studio muove, in questo senso, da un approccio comparato e fondato sui diritti fondamentali: approfondisce la *blockchain analysis* quale specifica metodologia investigativa e ne saggia la legittimità confrontando, sui medesimi nodi problematici, l'esperienza statunitense e quella europea per misurare, alla luce di tale confronto, l'adeguatezza dell'ordinamento italiano.

In verità, molte delle criticità analizzate nel presente contributo non costituiscono un tratto esclusivo delle cripto-attività, ma si collocano nel più ampio dibattito relativo alla prova digitale e, più in generale, all'impiego di strumenti tecnologici e algoritmici nell'accertamento giudiziario. In questo più ampio contesto, infatti, l'utilizzo di strumenti fondati sulla raccolta, sull'aggregazione e sull'elaborazione automatizzata di dati solleva interrogativi di carattere generale, che attingono tanto la tutela dei diritti fondamentali quanto le garanzie proprie del procedimento penale. Da un lato, l'ampiezza delle informazioni potenzialmente ricavabili dall'analisi delle transazioni *blockchain* pone questioni in ordine alla proporzionalità delle attività di acquisizione e trattamento dei dati rispetto al diritto alla vita privata dei soggetti coinvolti nelle indagini. Dall'altro lato, il ricorso agli specifici strumenti analitici impiegati in questo settore, connotati da un elevato grado di opacità tecnica e, talvolta, dalla natura proprietaria degli algoritmi solleva criticità rispetto ai principi di legalità processuale, trasparenza e contraddittorio, soprattutto laddove gli esiti di tali analisi siano destinati ad assumere rilievo probatorio.

La tecnologia *blockchain* e le peculiarità delle cripto-attività imprimono tuttavia a tali problematiche una fisionomia propria, tale da giustificare, come si vedrà, un esame autonomo della *blockchain analysis* quale metodologia investigativa.

Il contributo è strutturato come segue. La sezione § 2 ricostruisce le tecniche di *blockchain analysis*, offrendo un inquadramento tecnicamente fondato e illustrando il

³ H.F. Atlam e altri, *Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions*, in *Electronics* 2024 (13), 3568.

funzionamento concreto dei principali software impiegati dalle autorità di contrasto. La sezione § 3 esamina, in prospettiva comparata tra ordinamento statunitense ed europeo, l'interazione tra le tecniche di indagine descritte e il diritto alla privacy, al fine di valutare se il loro impiego integri un'ingerenza nella vita privata meritevole di tutela anche sul piano procedurale. La sezione § 4 affronta, con il medesimo approccio comparato, le problematiche che emergono allorché i risultati della *blockchain analysis* siano acquisiti come prova nel procedimento penale, concentrandosi sulla compatibilità con le garanzie del giusto processo a fronte dell'opacità algoritmica e del regime proprietario dei software impiegati. La sezione § 5 trae le conseguenze della ricostruzione comparata sul piano dell'ordinamento italiano, verificando se il codice di procedura penale offra una base legale e garanzie difensive adeguate. La sezione § 6 delinea le possibili risposte alle criticità individuate, distinguendo tra interventi di riforma strutturale e garanzie immediatamente azionabili. La sezione § 7, infine, raccoglie le conclusioni, evidenziando come le categorie processuali attualmente vigenti risultino inadeguate a governare la prova fondata su *blockchain analysis* e come un intervento legislativo si imponga ormai come necessario.

2. Per cogliere le implicazioni probatorie delle attività di indagine tipicamente dispiegate in materia di criptovalute, occorre anzitutto ricostruire i fondamenti tecnologici e operativi della *blockchain forensics* e il ruolo che essi rivestono nelle indagini penali contemporanee. La presente sezione illustra prima l'architettura di base delle *blockchain* pubbliche, chiarendo i meccanismi di registrazione delle transazioni, i tratti di pseudonimato degli utenti, la trasparenza e tracciabilità che ne connotano il funzionamento.

L'analisi si concentra successivamente sulla *blockchain analysis* quale specifica metodologia investigativa. La natura pubblica e immutabile dei dati iscritti nel registro distribuito, infatti, ha favorito lo sviluppo di tecniche e strumenti forensi specializzati, in grado di raccogliere, aggregare ed elaborare sistematicamente ingenti quantità di informazioni. Essi consentono agli investigatori di ricostruire flussi finanziari, individuare schemi ricorrenti nelle transazioni e, a determinate condizioni, formulare ipotesi attributive volte a ricondurre l'attività registrata sulla *blockchain* a soggetti identificabili.

La ricostruzione che segue offre il substrato fattuale e tecnologico necessario a valutare se, e a quali condizioni, l'impiego di simili metodologie investigative possa ingenerare interferenze o violazioni dei diritti fondamentali dei soggetti attinti dalle

indagini.

2.1 Nella sua essenza, una *blockchain* è un registro digitale distribuito (*distributed ledger*): un sistema di tenuta dei dati che, a differenza di un database tradizionale, governato da un solo soggetto (una banca, un'autorità pubblica), è condiviso e mantenuto simultaneamente dagli utenti della rete. Allo stesso tempo, anziché essere custoditi in un'unica sede centrale, i dati sono replicati presso tutti i partecipanti, sicché nessun utente può, da solo, controllarne o modificarne il contenuto. Ciascuna registrazione è aggregata in un "blocco" (*block*) e i blocchi si concatenano in ordine cronologico a formare una "catena" (*chain*) – da cui il termine "*blockchain*": un registro sequenziale che contiene l'intera storia transazionale della rete.

L'avvento della tecnologia *blockchain* e delle criptovalute ha ridisegnato le modalità di registrazione, circolazione e accessibilità dei dati finanziari. Questi ultimi, una volta iscritti nel registro, sono infatti tipicamente pubblici e consultabili da chiunque; restano celate, per contro, le identità dei soggetti che effettuano le transazioni. Tale mutamento ha eroso il ruolo di vigilanza sui flussi finanziari tradizionalmente affidato agli intermediari e ha ridefinito le nozioni stesse di accessibilità e tracciabilità del dato finanziario⁴. Nel campo dell'antiriciclaggio, questo sviluppo è stato descritto come il «*blockchain paradox*»: a differenza di quanto accade nei sistemi centralizzati, nel caso delle criptovalute l'azione di contrasto deve misurarsi con una conoscenza imperfetta delle identità dei soggetti coinvolti nelle transazioni, potendo però giovare di una conoscenza perfetta di tutte le transazioni⁵. È precisamente questa combinazione di trasparenza e pseudonimato a rendere i sistemi basati su *blockchain* al contempo attraenti per chi cerca riservatezza finanziaria e permeabili allo scrutinio investigativo.

Sotto un diverso profilo, il fatto che le *blockchain* siano strutturalmente decentralizzate fa sì che la validazione delle transazioni, la manutenzione del registro e il funzionamento della rete siano rimessi collettivamente ai singoli nodi, secondo un modello *peer-to-peer*. Ne discende che, per un verso, la decentralizzazione accresce la resilienza del sistema; per altro verso, mancando un'autorità centrale con poteri di vigilanza e controllo sugli utenti della rete, non è possibile ricorrere ai tradizionali strumenti di regolamentazione e di *enforcement* in caso di dubbi o irregolarità⁶.

⁴ C. Rueckert, *Cryptocurrencies and Fundamental Rights*, in *Journal of Cybersecurity* 2019 (5), 1, 3.

⁵ M. Campbell-Verduyn, *Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance*, in *Crime, Law and Social Change* 2018 (69), 283 s.

⁶ *Ibid.*

Nelle transazioni in criptovaluta, la *blockchain* serve a registrare, verificare e conservare in modo permanente il trasferimento di *asset* digitali tra i partecipanti, senza che lo scambio debba essere validato o supervisionato da un'autorità centrale. Per operare con cripto-attività occorre anzitutto disporre di un "portafoglio" (*wallet*), ossia dello strumento che custodisce le chiavi crittografiche necessarie a eseguire le transazioni. Sul piano tecnico, le transazioni si fondano su uno schema di crittografia asimmetrica, che prevede l'impiego congiunto di due distinte tipologie di chiavi: una "chiave pubblica", visibile da chiunque e impiegata per generare l'indirizzo al quale sono accreditati gli *asset* digitali, e una "chiave privata", di esclusiva disponibilità dell'utente e necessaria per autorizzare e firmare digitalmente la transazione⁷.

Per trasferire valore sulla rete, quindi, è sufficiente conoscere la chiave pubblica del destinatario e autorizzare l'operazione mediante la chiave privata, senza che occorra l'intervento di un intermediario centrale. La transazione, codificata in una struttura dati che specifica l'importo trasferito e gli indirizzi coinvolti, viene trasmessa ai nodi della rete. I partecipanti alla rete (comunemente denominati "*miners*") forniscono la capacità computazionale necessaria a elaborare e aggregare in un blocco le transazioni pendenti e a verificarne la validità, così da assicurare la coerenza di ciascuna nuova operazione con lo storico del registro. Validato il nuovo blocco, questo viene aggiunto alla catena esistente⁸.

Non tutte le *blockchain* presentano, tuttavia, le medesime caratteristiche architettureali⁹. Le *blockchain* più diffuse – tra cui quella di Bitcoin – rientrano nella categoria delle *blockchain* pubbliche, governate da protocolli fondati sull'apertura della partecipazione, sul consenso distribuito e sulla trasparenza del registro¹⁰. Il

⁷ Le moderne criptovalute basate su *blockchain* traggono origine dalla pubblicazione del *white paper* di S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, in <https://bitcoin.org/bitcoin.pdf>. Ad oggi, Bitcoin rimane il principale punto di riferimento teorico nelle discussioni sulle criptovalute e il più grande *crypto-asset* per capitalizzazione di mercato.

⁸ C.A. Pelker, C.B. Brown, R.M. Tucker, *Using Blockchain Analysis from Investigation to Trial*, in *Department of Justice Journal of Federal Law and Practice* 2021 (69), 59, 60 s.

⁹ R. Verma, N. Dhanda, *Blockchain Types: A Characteristic View*, in *Distributed Computing to Blockchain: Architecture, Technology, and Applications*, a cura di A. Khanna e altri, Amsterdam 2023, 69 ss.

¹⁰ Tra le varie tipologie di *blockchain*, meritano una menzione specifica le *blockchain* a privacy potenziata, sebbene esse esulino dall'ambito della presente analisi. Tali sistemi si caratterizzano per un allontanamento dal modello di trasparenza proprio delle *blockchain* pubbliche: la loro architettura protocollare integra tecnologie di rafforzamento della privacy volte a limitare la visibilità e la tracciabilità dei dati transazionali registrati sul registro distribuito. Per un'analisi più approfondita v. N. Pocher, *Crypto-Asset Ecosystems and the EU Anti-Money Laundering Framework*, Cham 2025, 105 ss.; C. Harvey, I. Branco-Illodo, *Why Cryptocurrencies Want Privacy: A Review of Political Motivations and Branding Expressed in "Privacy Coin" Whitepapers*, in *Journal of Political Marketing* 2020 (19), 107; Y. Li e altri, *Traceable Monero: Anonymous Cryptocurrency with Enhanced Accountability*, in *IEEE Transactions on Dependable and Secure Computing* 2021 (18), 679.

presente contributo si concentra su questa categoria di *blockchain*, di cui occorre ora esaminare le principali caratteristiche strutturali, preliminari all'analisi delle relative implicazioni giuridiche e investigative¹¹.

Le *blockchain* pubbliche si contraddistinguono anzitutto per l'immutabilità: una volta iscritti nel registro, i dati non possono essere alterati o rimossi unilateralmente. Tale integrità è garantita attraverso un meccanismo di consenso decentralizzato (nel caso di Bitcoin il cd. *Proof of Work*) atto a validare le transazioni e ad accodare nuovi blocchi alla catena, il quale esige la maggioranza della potenza computazionale della rete. Inoltre, la replicazione del registro presso tutti i nodi rende sostanzialmente irrealizzabile una manomissione coordinata e neutralizza rischi quali la doppia spesa del medesimo valore (il cd. *double-spending*)¹².

Un ulteriore tratto delle *blockchain* pubbliche è la piena pubblicità e trasparenza. Ogni transazione – e i relativi metadati, come l'importo trasferito, la data, l'orario e gli indirizzi pubblici coinvolti – è annotata in un registro liberamente consultabile da chiunque. Una simile architettura aperta fa della *blockchain* una fonte di informazioni privilegiata a fini investigativi e probatori, consentendo agli investigatori di ricostruire flussi finanziari con un elevato grado di dettaglio¹³.

Dalla trasparenza del registro discende poi la piena tracciabilità delle transazioni. Poiché ciascuna di esse è concatenata informaticamente alle precedenti, è possibile ricostruire l'intera cronologia di un determinato *asset* dalla sua origine al suo stato attuale. Questa caratteristica, come vedremo, costituisce il presupposto tecnico dei principali strumenti di *blockchain analysis* impiegati dalle autorità di contrasto. Si tratta di un profilo che distingue nettamente le transazioni in criptovaluta da quelle tradizionali, nelle quali il passaggio dei fondi attraverso giurisdizioni non cooperative interrompe, di regola, la ricostruzione dei flussi.

¹¹ Il criterio classificatorio rilevante è quello del regime di autorizzazione all'accesso e alla partecipazione al processo di validazione delle transazioni. Le *blockchain* pubbliche (o *permissionless*), oggetto della presente indagine, consentono a chiunque di leggere il registro e di proporre nuove transazioni, senza necessità di autorizzazione da parte di un ente abilitante. Le *blockchain* private (o *permissioned*) riservano invece tale facoltà a soggetti preventivamente identificati e autorizzati da un ente, o da un gruppo di enti preventivamente individuati. Si tratta di tecnologie tipicamente impiegate in contesti aziendali o istituzionali, strutturalmente estranee al fenomeno investigativo e penalistico qui esaminato che presuppone per definizione l'assenza di un ente centrale abilitante; esse restano pertanto fuori dall'ambito della presente trattazione. Per approfondimento si veda R. Verma, N. Dhanda, op. cit., 73 ss.

¹² H.F. Atlam e altri, op. cit., 4.

¹³ P. Tippie, C. Deckers, *Unmixing the Mix: Patterns and Challenges in Bitcoin Mixer Investigation*, in *Forensic Science International: Digital Investigation* 2025 (52, supp.), 2 s.

Le *blockchain* pubbliche, da ultimo, offrono un certo grado di pseudonimato, ma non un anonimato pieno e autentico. Come si è detto, le transazioni sono associate ad indirizzi alfanumerici (chiavi pubbliche) e non a nomi reali. Tali identificativi, nondimeno, possono essere ricondotti a identità concrete mediante euristiche di raggruppamento, correlazione dei metadati e dati *off-chain* – indirizzi IP, cronologie di navigazione, informazioni trasmesse dagli *exchange*, elementi acquisiti da dispositivi sequestrati – in un processo noto come de-anonimizzazione¹⁴. Superare lo pseudonimato è, del resto, la principale sfida investigativa nel contrasto penale alle cripto-attività.

Prima di occuparsi di tali aspetti più nel dettaglio, però, è opportuno volgere l'attenzione alle modalità con cui le caratteristiche delle *blockchain* pubbliche sono concretamente sfruttate, nelle indagini penali, attraverso le tecniche di *blockchain analysis*.

2.2 Come si è osservato in precedenza, la diffusione capillare delle cripto-attività ha introdotto sfide significative per le indagini penali, imponendo alle autorità inquirenti l'adozione di metodi e strumenti tecnicamente specializzati per acquisire ed elaborare le informazioni estraibili dalla *blockchain*.

Tali attività si inscrivono nel più ampio campo della *blockchain forensics*¹⁵. Come per tutte le indagini digitali, questo è un contesto nel quale gli standard di *digital forensics* riconosciuti a livello internazionale – segnatamente il *framework* ISO/IEC 27037:2012 – assumono particolare rilievo, in quanto forniscono un parametro metodologico per l'identificazione, l'acquisizione, la conservazione e l'analisi della prova digitale. Tuttavia, la loro rilevanza nel contesto della *blockchain forensics* resta limitata: da un lato, come la totalità degli standard in materia di prova digitale, si tratta di strumenti di *soft law*, dall'altro, e soprattutto, non sono stati concepiti per misurarsi

¹⁴ P. Tippie, C. Deckers, op. cit., 2; N. Furneaux, *Investigating Cryptocurrencies: Understanding, Extracting, and Analysing Blockchain Evidence*, Hoboken 2018, 239; A. Balaskas, V.N.L. Franqueira, op. cit., 5.

¹⁵ H.F. Atlam e altri, op. cit., 5 ss. Secondo gli autori, la *blockchain forensics* può essere ricostruita come un processo articolato in sei fasi, secondo uno schema che ricalca quello della *digital forensics* in senso lato: (i) *identification*, diretta a individuare i dati *blockchain* rilevanti; (ii) *collection*, relativa alla loro acquisizione sistematica, con garanzia di integrità; (iii) *preservation*, volta ad assicurare l'immutabilità della prova nonché l'integrità e la verificabilità della catena di custodia; (iv) *analysis*, nella quale i dati raccolti vengono elaborati mediante tecniche analitiche, anche di *clustering*, al fine di ricostruire flussi transazionali e relazioni; (v) *examination*, che colloca i risultati nel più ampio contesto investigativo e li confronta con fonti informative esterne; (vi) *reporting*, consistente nella formalizzazione dei risultati in una forma idonea alla loro presentazione in giudizio. Nei casi di monitoraggio *blockchain* in tempo reale o continuativo, le fasi di raccolta e analisi non si svolgono necessariamente in modo sequenziale in ragione della contestualità tra acquisizione dei dati ed elaborazione analitica.

con le peculiarità della prova estratta dalla *blockchain*¹⁶. Entro questo quadro, le attività tecniche più rilevanti riguardano la raccolta dei dati e la loro elaborazione. Quest'ultima costituisce, in particolare, l'oggetto proprio della *blockchain analysis*, quale sottoinsieme specifico della più ampia *blockchain forensics*: essa coinvolge, infatti, principalmente l'impiego, da parte delle autorità di *law enforcement*, di software progettati per estrarre, elaborare e interpretare i dati dalle *blockchain* pubbliche.

Un ulteriore profilo di complessità tecnica deriva dalle modalità con cui la metodologia investigativa in esame – che combina *blockchain forensics* e *blockchain analysis*, definita «*follow the crypto*»¹⁷ – è posta in essere. Sebbene, in linea di principio, l'analisi delle transazioni *blockchain* possa essere condotta manualmente da investigatori specializzati – mediante la consultazione diretta dei registri pubblici e il tracciamento del movimento dei fondi tra gli indirizzi – tale approccio risulterebbe concretamente impraticabile, data la grande mole di dati coinvolti. Infatti, le *blockchain* pubbliche registrano milioni di transazioni, costantemente aggiornate grazie a migliaia di nodi distribuiti. Per far fronte a questa complessità operativa, diverse società private (tra cui Chainalysis, Elliptic e TRM Labs) hanno sviluppato strumenti informatici specializzati di analisi, oggi ampiamente adottati dalle autorità di contrasto a livello globale¹⁸. Il loro impiego si riflette direttamente sulle modalità di conduzione delle indagini e sugli adempimenti di *compliance*, segnatamente in materia di prevenzione del riciclaggio¹⁹.

¹⁶ Come evidenziato da G. Lasagni, *Admissibility of Digital Evidence*, in *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, a cura di V. Franssen e S. Tosza, Cambridge 2025, 126, 132 s., gli standard ISO/IEC costituiscono il quadro internazionale di riferimento per il trattamento della prova digitale. Il processo è articolato in due fasi principali: una fase acquisitiva, nella quale i dati digitali sono identificati, raccolti e preservati, e una fase investigativa, nella quale il materiale viene analizzato in ambiente forense. Per ciascuna fase gli standard individuano i rischi inerenti e le cautele tecniche necessarie a preservare il valore probatorio dei dati. Nel più ampio contesto delle indagini digitali, particolare rilievo assume il ruolo del *digital evidence first responder* (DEFRR), ossia del soggetto che interviene per primo: si tratta di una fase particolarmente delicata, spesso affidata a personale non specialistico, con conseguenti rischi di errore, contaminazione della prova e pregiudizio dei diritti degli interessati. Criticità analoghe possono presentarsi anche in alcune fasi della *blockchain forensics*, in particolare nell'identificazione e nella gestione degli *hardware wallet*, ove un intervento non conforme agli standard tecnici può determinare l'irreversibile alterazione o perdita della prova. Diverso è il caso della *blockchain analysis* in senso stretto, rispetto alla quale tali rischi appaiono più contenuti in ragione della natura pubblica e immutabile dei dati *on-chain*.

¹⁷ J. Della Torre, *Spunti in tema di cripto-attività e procedimento penale*, in www.lalegislazionepenale.eu, 28.2.2025, 318.

¹⁸ Per un'analisi tecnica dettagliata dei principali software di *blockchain analysis*, v. A. Balaskas, V.N.L. Franqueira, op. cit., 3.

¹⁹ Sull'interazione fra regolamentazione antiriciclaggio e prassi investigative e sull'incentivo all'uso di strumenti di *blockchain analytics* da parte delle autorità di vigilanza, v. G. Soana, *The Anti-Money Laundering Regulation*

Le autorità di contrasto sono così poste in condizione di sfruttare i tratti strutturali delle *blockchain* pubbliche per ricostruire il movimento dei fondi e tracciare i proventi di reato. La *blockchain analysis* costituisce, tuttavia, una categoria ampia, che raccoglie una pluralità di tecniche diversificate quanto a complessità e potenzialità investigativa²⁰.

La tecnica più elementare è il *tracing*, consistente nel seguire il movimento di criptovaluta da un indirizzo all'altro attraverso l'analisi dei registri della *blockchain*. Essa consente di ricostruire il flusso dei fondi sospetti, individuare trasferimenti occultati e stabilire connessioni nel tempo. Poiché tutte le transazioni sono pubbliche e registrate in modo immutabile, gli strumenti di *blockchain analysis* permettono alle autorità di contrasto di seguire la circolazione degli asset digitali attraverso la rete sino a un punto di contatto con *exchange* regolamentati o ad altri punti di uscita verso il sistema finanziario tradizionale²¹. Il metodo sconta tuttavia limiti strutturali, poiché anche un utente mediamente avveduto può eludere la tracciabilità utilizzando indirizzi multipli o altri sistemi di offuscamento come *bridge* o *mixer*²².

Per ovviare a tale debolezza, sono state elaborate tecniche più avanzate. Il *clustering*, in particolare, consente agli investigatori di attribuire insieme di indirizzi *blockchain*, su base probabilistica, a una singola entità controllante. Tale processo si fonda su euristiche comportamentali²³, ad esempio l'euristica "*common-input*" (o euristica "*co-spending*"), la quale assume che tutti gli indirizzi utilizzati congiuntamente come *input* in una singola transazione appartengano allo stesso utente. Un'altra euristica comunemente utilizzata è la cosiddetta euristica "*change address*": quando una transazione spende una quantità di criptovaluta inferiore all'importo totale fornito dagli *input* del mittente, il saldo residuo – denominato "*change*" – viene tipicamente inviato a un nuovo indirizzo anch'esso controllato dal mittente. Ove tale *change address* possa essere identificato con sufficiente affidabilità, gli investigatori possono inferire che tanto il *change output* quanto tutti gli *input*

of *Crypto-Assets in Europe*, Padova 2024, 227 ss.

²⁰ Per un approfondimento delle varie tecniche di *blockchain analysis* si veda J. Della Torre, *Cripto-attività e giustizia penale*, Milano 2026, 253 s.

²¹ C.A. Pelker, C.B. Brown, R.M. Tucker, op. cit., 61 s.

²² Per *bridge* si intende un protocollo o servizio che consente di trasferire *crypto-asset* da una *blockchain* a un'altra, con l'effetto di rendere più complessa la ricostruzione lineare dei flussi. Per *mixer*, invece, si intende uno strumento volto a mescolare fondi provenienti da utenti diversi, così da ostacolare l'identificazione del nesso tra indirizzo di provenienza e indirizzo di destinazione. Per approfondimenti v. G. Soana, op. cit., 234.

²³ Un metodo euristico è un approccio alla soluzione di problemi fondato su ragionamento inferenziale, contesto fattuale ed esperienza pregressa in luogo di procedure algoritmiche deterministiche.

coinvolti nella transazione siano verosimilmente controllati dalla stessa entità²⁴. In questo modo il *clustering* permette di ricomporre in capo a un unico soggetto la sua attività finanziaria altrimenti frammentata.

Trattandosi, tuttavia, di metodi euristici fondati su inferenze probabilistiche, i risultati ottenuti non sono assistiti da certezza dimostrativa, né può escludersi il rischio di attribuzioni erronee²⁵. Le relative inferenze muovono dall'osservazione di comportamenti tipici degli utenti e presentano, sul piano epistemologico, la struttura propria delle massime di esperienza di matrice tecnica, più che quella delle leggi scientifiche in senso stretto²⁶. Proprio per ciò, come si dirà, la loro qualificazione assume particolare rilievo ai fini del regime probatorio dei relativi *output*.

Un'ulteriore tecnica è la "*pattern analysis*"²⁷, che si distingue dalle tecniche precedenti in quanto non presuppone la previa identificazione di un indirizzo sospetto, mirando piuttosto a rilevare comportamenti transazionali anomali sintomatici di attività illecite. A differenza del *tracing* e del *clustering* – che richiedono la previa individuazione di un indirizzo sospetto o di un'entità nota come punto di partenza – essa consente di estrarre informazioni direttamente dal registro e dalle dinamiche della rete²⁸. La tecnica in questione è volta a identificare «*red flag*» e ad assegnare punteggi di rischio agli indirizzi coinvolti attraverso l'analisi della tempistica delle transazioni, della frequenza, della dispersione del valore e degli schemi

²⁴ Per un'analisi più dettagliata delle varie euristiche impiegate nella *blockchain analysis*, v. A. Balaskas, V.N.L. Franqueira, op. cit., 2; C.A. Pelker, C.B. Brown, R.M. Tucker, op. cit., 62.

²⁵ Y. Gong e altri, *Analyzing the Error Rates of Bitcoin Clustering Heuristics*, in *Advances in Digital Forensics XVIII*, a cura di G. Peterson e S. Sheno, Cham 2022, 187 ss., ove si rileva che le euristiche *multi-input* e *change-address* presentano tassi di errore medi rispettivamente del 63,46% e del 92,66%, mentre la loro applicazione combinata riduce il tasso medio di errore al 57,47%. Più di recente, v. Y. Gong, K.P. Chow, S. Mingyiu, *Improved Bitcoin Simulation Model and Address Heuristic Method*, in *Forensic Science International: Digital Investigation* 2025, 1 ss.; H. Schnoering, P. Porthaux, M. Vazirgiannis, *Assessing the Efficacy of Heuristic-Based Address Clustering for Bitcoin*, in *arXiv*, 4.3.2024.

²⁶ Sulla qualificazione delle euristiche di *blockchain analysis* come massime di esperienza di matrice tecnica, e non come leggi scientifiche in senso proprio, v. diffusamente J. Della Torre, *Cripto-attività e giustizia penale*, cit., 352-356. La distinzione è cruciale: mentre una legge scientifica, anche di tipo probabilistico, si fonda su un processo di validazione sistematica che assicura replicabilità e quantificazione del margine di errore, la massima di esperienza resta ancorata all'*id quod plerumque accidit*, priva di quel grado di generalità e di stabilità che consentirebbe di inferire relazioni al di là dei casi osservati. Le euristiche impiegate nella *blockchain analysis* hanno infatti a oggetto comportamenti umani ritenuti sintomatici di condotte sospette e pertanto per loro natura suscettibili di essere smentite nel caso concreto.

²⁷ J. Hirshman, Y. Huang, S. Macke, *Unsupervised Approaches to Detecting Anomalous Behavior in the Bitcoin Transaction Network*, CS229 Project, Stanford University 2013, in cs229.stanford.edu/proj2013/HirshmanHuangMacke-UnsupervisedApproachesToDetectingAnomalousBehaviorInTheBitcoinTransactionNetwork.pdf, 21.3.2026.

²⁸ G. Soana, op. cit., 236; per un'analisi dell'interazione fra *pattern analysis* e tecniche di *clustering*, v. J. Hirshman, Y. Huang, S. Macke, op. cit.

transazionali e strutturali ricorrenti. Tra questi ultimi rilevano in particolare le “*peeling chains*”²⁹, ossia sequenze di *output* di basso valore indicative di tecniche di offuscamento, e la “*taint analysis*”³⁰, che traccia la propagazione di fondi illeciti verso indirizzi a valle contrassegnandoli come potenzialmente compromessi. Le informazioni così estratte possono valere tanto a orientare il prosieguo delle indagini, quanto – ove ne ricorrano le condizioni di legge – a essere utilizzate come elementi di prova in giudizio. La corretta individuazione e applicazione delle disposizioni rilevanti presuppone, del resto, la previa comprensione delle modalità con cui simili attività investigative sono concretamente condotte.

Va rilevato che le funzioni più avanzate di *blockchain analysis* – segnatamente i modelli euristici di *clustering* e il riconoscimento dei *pattern* transazionali – si fondano in misura crescente su sistemi di intelligenza artificiale, che consentono di elaborare grandi volumi di dati transazionali e di affinare le proprie prestazioni nel tempo attraverso algoritmi di *machine learning*³¹. Piattaforme commerciali come Chainalysis ed Elliptic integrano modelli di questo tipo per automatizzare il *clustering* e la valutazione del rischio sulla base di tipologie comportamentali e *pattern* ricorrenti³²; strumenti come “Blockchain Inspector”, sviluppato dalla stessa Chainalysis, li impiegano altresì per la profilazione comportamentale degli utenti³³. Ne consegue che, mentre i dati transazionali sottostanti restano, in linea di principio, verificabili all’interno dei singoli registri pubblici, gli output inferenziali prodotti dai modelli automatizzati si sottraggono a una verifica metodologica piena. Si tratta di una circostanza che, come si vedrà, non è priva di implicazioni sul piano processuale.

Taluni degli strumenti di *blockchain analysis* offrono, inoltre, funzionalità di monitoraggio in tempo reale, che consentono alle autorità di contrasto di intercettare e analizzare transazioni pendenti prima ancora della loro conferma da parte della rete³⁴. Si tratta di funzionalità diverse e qualitativamente distinte rispetto alle precedenti: anziché limitarsi a ricostruire flussi di valore già avvenuti, consentono una sorveglianza continuativa e prospettica dell’attività sulla *blockchain*, con un potenziale di monitoraggio – e, corrispondentemente, una capacità investigativa – significativamente superiori rispetto agli strumenti confinati all’analisi *ex post*.

²⁹ P. Tippie, C. Deckers, op. cit., 5.

³⁰ *Ibid.*

³¹ N. Pocher, op. cit., 119 ss.

³² LCX Team, *Brief Introduction to Blockchain Analytics*, in www.lcx.com/nl/brief-introduction-to-blockchain-analytics, 4.8.2023.

³³ A. Balaskas, V.N.L. Franqueira, op. cit., 3.

³⁴ A. Balaskas, V.N.L. Franqueira, op. cit., 4.

Un'ulteriore tecnica, verosimilmente la più rilevante sul piano investigativo, è la de-anonimizzazione, ossia la riconduzione di indirizzi di portafoglio pseudonimi a identità reali. Essa consente infatti di identificare i soggetti sottostanti alle transazioni sospette e costituisce, pertanto, un passaggio essenziale per l'adozione di misure cautelari conservative e, in ultima analisi, per l'accertamento della responsabilità in giudizio. La de-anonimizzazione è generalmente realizzata acquisendo informazioni identificative dai *crypto-asset service provider* (CASP). Si tratta dei soggetti autorizzati, ai sensi degli artt. 3, par. 1, punto 15, e 59 del regolamento (UE) 2023/1114 (MiCA), a prestare professionalmente uno o più servizi relativi alle cripto-attività, tra cui la custodia, la negoziazione e lo scambio. Tali informazioni possono essere acquisite anche nell'ambito degli obblighi previsti dalla normativa antiriciclaggio³⁵. Inoltre, qualora il CASP detenga le chiavi private a titolo di custodia, il suo coinvolgimento può consentire il diretto congelamento dei fondi.

Tale attività si colloca all'intersezione tra *blockchain analysis* e *digital forensics* in senso ampio. Essa mira, infatti, a combinare le informazioni ottenute attraverso i software di *blockchain analysis* con dati esterni (*off-chain*) – quali indirizzi IP, informazioni ricavate da dispositivi sequestrati, *open-source intelligence* o registri KYC (*Know your customer*) raccolti dai CASP – al fine di sviluppare ipotesi attributive, ricondurre indirizzi sospetti a soggetti identificabili e orientare il prosieguo delle indagini³⁶.

Le capacità di aggregazione e correlazione proprie di tali strumenti schiudono implicazioni giuridiche rilevanti. Il trattamento su larga scala di dati pseudonimi, specialmente se combinati con informazioni esterne idonee a identificare gli interessati, consente infatti la ricostruzione di profili economici e comportamentali che trascende la mera consultazione del registro pubblico. Come si vedrà nella sezione seguente, la sola tracciabilità delle transazioni su una *blockchain* pubblica, in assenza

³⁵ Sull'interazione fra regolamentazione antiriciclaggio e prassi investigative nel settore dei *crypto-asset*, gli obblighi imposti ai CASP – in particolare gli obblighi di adeguata verifica della clientela e i requisiti KYC (*Know your customer*) – svolgono un ruolo decisivo nel processo di de-anonimizzazione, nella misura in cui impongono agli intermediari regolamentati di raccogliere e conservare dati identificativi a cui le autorità di *law enforcement* possono successivamente accedere per collegare indirizzi *blockchain* pseudonimi a individui identificabili. Sul punto, v. J. Della Torre, G. Pontepino, *Commento al d.lgs. 129 del 2024 di attuazione del Regolamento UE sui mercati delle cripto-attività: le novità sul versante penalistico e amministrativo punitivo*, in www.lalegislazionepenale.eu, 18.2.2025, 249 s.

³⁶ C.A. Pelker, C.B. Brown, R.M. Tucker, op. cit., 62. Sull'interazione fra metodi di *clustering* e de-anonimizzazione, v. M.A. Harlev e altri, *Breaking Bad: De-anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning*, in *Proceedings of the 51st Hawaii International Conference on System Sciences*, 2018.

di collegamenti con persone identificabili, non determina di regola un'interferenza con la vita privata di intensità comparabile a quella che si produce quando i dati *on-chain* vengano associati a informazioni *off-chain* idonee a identificare gli interessati: è proprio in quest'ultima fase, infatti, che le questioni di tutela dei dati personali e della privacy assumono rilievo.

Tratteggiate le principali tecniche investigative entro il perimetro della *blockchain analysis*, conviene ora, prima di passare all'analisi giuridica, riportare quanto detto in termini generali a un esempio concreto, utile a chiarire le modalità con cui le indagini penali sono implementate attraverso i software commerciali di *blockchain analysis*.

2.3 Chainalysis è la società che oggi produce alcuni tra i software di *blockchain analysis* più diffusamente impiegati nelle indagini in materia di *crypto-asset*, concedendone la licenza d'uso ad agenzie governative, autorità di *law enforcement* e operatori regolamentati del settore crypto³⁷. Sul piano operativo, le autorità investigative se ne avvalgono per ricostruire i flussi transazionali, raggruppare indirizzi correlati e ricondurre l'attività di portafogli pseudonimi a servizi o entità identificabili, segnatamente là dove le transazioni interessino intermediari regolamentati. Tali strumenti trovano attualmente applicazione nelle indagini condotte dalle autorità federali statunitensi³⁸, sono integrati nelle attività analitiche e operative di Europol³⁹ e adottati in misura crescente dalle autorità di contrasto nazionali in ambito europeo. In Italia, ad esempio, l'Unità di Informazione Finanziaria e la Guardia di Finanza fanno già oggi ampio ricorso a strumenti di analisi della *blockchain*⁴⁰.

Chainalysis, in particolare, offre un'ampia gamma di applicativi di *blockchain analysis*, tra i quali i due di maggior rilievo e diffusione sono Rapid e Reactor.

Chainalysis Rapid è impiegato a supporto delle fasi iniziali delle indagini su *crypto-asset*, in particolare laddove le autorità investigative dispongano di elementi di partenza limitati, quali un indirizzo di portafoglio o un *hash* transazionale⁴¹. Lo strumento elabora dati *on-chain* pubblici per ricostruire e visualizzare i flussi di *crypto-*

³⁷ T. van Roomen, *Cross-Border Evidence Gathering in Criminal Crypto Investigations: A Case Study of the Netherlands*, in *Tilburg Law Review* 2025 (30), 126. Tra gli altri strumenti di *blockchain analytics* comunemente utilizzati nella prassi si annoverano, *inter alia*, TRM Labs, Elliptic e CipherTrace.

³⁸ C.A. Pelker, C.B. Brown, R.M. Tucker, op. cit., 63.

³⁹ Europol, *Europol and Chainalysis Reinforce Their Cooperation in Fight Against Cybercrime*, in www.europol.europa.eu/media-press/newsroom/news/europol-and-chainalysis-reinforce-their-cooperation-in-fight-against-cybercrime, 19.2.2016.

⁴⁰ È emerso con chiarezza dagli incontri e dalle interviste condotte nell'ambito del progetto di ricerca PRIN 2022 PNRR: CRYPTOSAFE.

⁴¹ Chainalysis, *Rapid*, in www.chainalysis.com/product/rapid, 21.3.2026.

asset attraverso la *blockchain* mediante tecniche automatizzate di analisi dei grafi transazionali, evidenziando percorsi transazionali, controparti e sequenze temporali. Esso integra componenti basati sull'intelligenza artificiale che generano sintesi automatizzate, indicazioni di priorità e indicatori di rischio, organizzando gli *output* analitici sulla scorta dei dataset di attribuzione esistenti. Tali esiti hanno natura probabilistica e classificatoria e valgono a fornire un primo orientamento investigativo. Gli *output* così prodotti – essenzialmente visualizzazioni dei flussi transazionali, sintesi contestuali e valutazioni indicative del rischio – possono essere esportati o utilizzati come base per analisi più approfondite mediante strumenti investigativi avanzati. Mentre i dati transazionali sottostanti restano, in linea di principio, verificabili rispetto al registro pubblico, i risultati interpretativi – in particolare quelli relativi all'associazione con entità identificabili o tipologie criminali – derivano da euristiche proprietarie ed elaborazioni assistite dall'intelligenza artificiale la cui logica sottostante non è resa pubblica.

Chainalysis Reactor è il principale strumento investigativo della società, progettato per l'analisi forense delle transazioni in criptovaluta nell'ambito delle indagini penali⁴². Esso consente di tracciare il flusso degli *asset* digitali applicando tecniche euristiche di *clustering* – tra cui il menzionato rilevamento del *co-spending* – e di integrare dati *on-chain* con informazioni *off-chain* acquisite attraverso *open-source intelligence*, consentendo così la ricostruzione di un quadro probatorio più articolato⁴³. La piattaforma può operare in tempo reale, permettendo il monitoraggio dinamico dei movimenti degli *asset* e il rilevamento di *pattern* comportamentali e connessioni di rete. Reactor incorpora inoltre algoritmi di intelligenza artificiale a sostegno della classificazione e della prioritizzazione degli indirizzi sulla base di valutazioni probabilistiche del rischio. La sua interfaccia visuale agevola la predisposizione di diagrammi dei flussi transazionali esportabili in formati standardizzati, impiegabili nel procedimento penale tanto a fondamento di misure cautelari quanto a fini probatori.

Nonostante il ricorso a tali strumenti sia ormai generalizzato tra le autorità di contrasto a livello mondiale, per ragioni di segreto industriale la società non rende accessibile il proprio codice sorgente – ossia l'insieme delle istruzioni informatiche che ne determinano il funzionamento – a terzi, ivi comprese le autorità governative. A queste ultime è concesso l'accesso esclusivamente all'interfaccia utente e agli *output*

⁴² Chainalysis, *Reactor*, in www.chainalysis.com/product/reactor, 21.3.2026.

⁴³ Chainalysis, *Preventing Crypto Fraud with Off-Chain and On-Chain Data*, in www.chainalysis.com/blog/preventing-crypto-fraud-with-off-chain-on-chain-data, 21.3.2026.

standard – quali visualizzazioni dei flussi transazionali, *clustering* degli indirizzi e rapporti investigativi – mentre gli algoritmi e le euristiche sottostanti restano inaccessibili. Ne consegue che investigatori e pubblici ministeri possono fare affidamento sugli *output* e sui rapporti generati dal software, ma ne ignorano la logica interna di funzionamento. Come si dirà, tale opacità algoritmica solleva questioni di non lieve momento sul piano della spiegabilità e della verificabilità della prova: anche là dove gli *output* del software siano acquisiti come elementi di prova, la logica inferenziale sottostante resta sottratta a qualsiasi forma di scrutinio⁴⁴.

3. Delineate le caratteristiche tecniche e operative delle indagini sulla *blockchain*, se ne può ora definire con maggiore precisione la struttura investigativa essenziale. Come si è anticipato, le tecniche investigative descritte si svolgono, di regola, attraverso un procedimento che prende avvio dall'acquisizione massiva dei dati. Tale fase implica la raccolta sistematica di informazioni ricavate dai registri delle *blockchain* pubbliche (dati *on-chain*) – quali cronologie transazionali, indirizzi, *timestamp* e collegamenti tra transazioni – e si estende frequentemente a dati provenienti da una pluralità di fonti esterne (dati *off-chain*), tra cui registri degli *exchange*, *open-source intelligence* e ulteriori elementi contestuali idonei a integrare e rendere intelligibile il quadro investigativo.

La prima questione giuridica da prendere in considerazione, quindi, concerne la tutela del diritto alla privacy. Si tratta di un profilo che potrebbe apparire, a prima vista, controintuitivo, dal momento che i dati registrati sulla *blockchain* sono, in linea di principio, pubblicamente accessibili. Resta però da verificare se tale accessibilità pubblica sia di per sé sufficiente a escludere ogni ingerenza nella vita privata, o se anche dati singolarmente pubblici possano, se acquisiti e correlati sistematicamente, dar luogo a una simile ingerenza. Sulla questione si tornerà più diffusamente nei paragrafi seguenti.

In via preliminare, occorre chiarire che non ogni attività di accesso o analisi dei dati *blockchain* integra, di per sé, un'ingerenza in tale diritto. È necessario distinguere,

⁴⁴ Peraltro, una componente di particolare rilievo operativo per le autorità di *law enforcement* è costituita dai database proprietari già nella disponibilità delle società private: come riporta J. Della Torre, *Cripto-attività e giustizia penale*, cit., 285 s., la sola Chainalysis dichiara di aver raggruppato in *cluster* oltre un miliardo di indirizzi, collegandoli a più di 55.000 tra servizi, *wallet* e protocolli. Questi archivi si alimentano attraverso un meccanismo circolare e le autorità investigative, acquistando le licenze d'uso del software, contribuiscono a loro volta al costante aggiornamento del database e delle relative attribuzioni.

almeno sul piano concettuale, tra il tracciamento isolato di singole transazioni e l'aggregazione massiva e la correlazione di dati idonee a generare una profilazione dell'individuo interessato. Se il primo, isolatamente considerato, determina un'interferenza nella sfera privata che risulta però chiaramente recessiva rispetto alle esigenze della repressione penale – pur richiedendo, in ogni caso, una base giuridica idonea a legittimarla –, le seconde impongono invece una verifica più approfondita circa la loro capacità di dar luogo a forme di intrusione suscettibili di incidere in modo significativo sulla vita privata dei soggetti coinvolti. Si tratta, tuttavia, di una distinzione che, pur risultando lineare in astratto, presenta margini applicativi assai meno netti nella prassi⁴⁵. L'analisi che segue è dunque circoscritta a quegli impieghi della *blockchain analysis* connotati da carattere massivo e sistematico, che ne costituiscono l'utilizzo maggiormente problematico.

3.1 Una prima questione giuridica da prendere in esame è se le attività di *blockchain analysis* siano idonee a integrare un'ingerenza nel diritto alla riservatezza. La risposta non è univoca. Come si è già osservato, le informazioni registrate sulle *blockchain* pubbliche sono, per loro natura, pubblicamente disponibili e accessibili a una pluralità indeterminata di soggetti, senza necessità di autorizzazioni né di canali di accesso privilegiati⁴⁶. Di conseguenza, si potrebbe sostenere che, rispetto a simili informazioni, gli individui non possano vantare una ragionevole aspettativa di riservatezza⁴⁷. Da

⁴⁵ Al riguardo, v. M. Bedi, *Social Network, Government Surveillance, and the Fourth Amendment Mosaic Theory*, in *Boston University Law Review* 2014 (94), 1813, 1845, dove l'autore evidenzia espressamente la presenza di «significant practical hurdles» nell'individuare il punto in cui le prassi di sorveglianza si trasformano da osservazione isolata a monitoraggio prolungato. Merita osservare che la distinzione tra sorveglianza occasionale e sistematica ha già trovato riconoscimento normativo in alcuni ordinamenti, con corrispondenti differenze nelle garanzie procedurali. Il diritto processuale penale olandese, ad esempio, disciplina espressamente l'esercizio della sorveglianza sistematica da parte delle autorità di *law enforcement* mediante strumenti digitali. Ai sensi dell'art. 126g del Codice di Procedura Penale olandese, il Pubblico Ministero ha la facoltà di autorizzare attività di osservazione sistematica, anche nell'ambiente digitale. La norma impone che l'autorizzazione sia redatta in forma scritta e ne definisce rigorosamente i contenuti: la durata massima (tre mesi), la fattispecie di reato contestata e le specifiche modalità d'esecuzione. Per un'analisi dettagliata, v. B.J. Koops, *Police Investigations in Internet Open Sources: Procedural-Law Issues*, in *Computer Law & Security Review* 2013 (29), 654.

⁴⁶ La questione si inserisce nel più ampio quadro dell'*open-source intelligence* (OSINT). V. B.J. Koops, op. cit., 655; A. Lyle, *Legal Considerations for Using Open Source Intelligence in the Context of Cybercrime and Cyberterrorism*, in *Open Source Intelligence Investigation: From Strategy to Implementation*, a cura di B. Akhgar, P.S. Bayerl e F. Sampson, Cham 2016, 277; A. Shere, *Reading the Investigators Their Rights: A Review of Literature on the General Data Protection Regulation and Open-Source Intelligence Gathering and Analysis*, in *The New Collection* 2020 (3), 1.

⁴⁷ In tal senso, v. S. Signorato, *Le indagini digitali*, Torino 2018, 83, la quale osserva che laddove un soggetto comunichi volontariamente informazioni a persone sconosciute all'interno di un ambiente digitale aperto al pubblico, egli non può successivamente dolersi del fatto che tali informazioni siano visualizzate e acquisite dalle autorità di *law enforcement* a fini investigativi. V. altresì, in senso analogo, N. Petrashek, *The Fourth Amendment*

questo punto di vista, la mera acquisizione e analisi dei dati *blockchain* non integrerebbe, di per sé, un'interferenza nella sfera privata; ne deriverebbe, sul piano applicativo, la possibilità per le autorità di *law enforcement* di accedere a tali dati e di trattarli senza che trovino applicazione specifiche garanzie procedurali.

Questa linea argomentativa è stata espressamente avallata dalla giurisprudenza federale statunitense in tema di tutela della riservatezza⁴⁸. In *United States v. Gratkowski* (2020)⁴⁹, in particolare, la *Court of Appeals for the Fifth Circuit* è stata chiamata a stabilire se l'impiego, da parte del governo, di software specializzati per l'analisi delle transazioni in Bitcoin integrasse una perquisizione (*search*) ai sensi del Quarto Emendamento e richiedesse, pertanto, un'autorizzazione giudiziaria. In assenza di pronunce della Corte Suprema sul punto, la decisione del *Fifth Circuit* resta ad oggi il precedente più autorevole in materia, ed è assunta come riferimento nella ricostruzione che segue.

L'imputato sosteneva che la *blockchain analysis*, in ragione del suo carattere investigativo e della sua capacità ricostruttiva e retrospettiva, costituisse una forma di attività intrusiva al punto da richiedere l'operatività della garanzia costituzionale invocata.

I giudici del *Fifth Circuit* hanno disatteso questa impostazione. Il nucleo della motivazione ruotava attorno alla distinzione tra dati *on-chain* e dati *off-chain*, distinzione che impone percorsi argomentativi diversi che convergono, tuttavia, verso la medesima conclusione: l'inapplicabilità delle garanzie del Quarto Emendamento.

Quanto ai dati *on-chain*, la Corte ha affermato che «non sussiste alcun interesse alla riservatezza nelle informazioni conservate nella *blockchain* di Bitcoin, in quanto sono informazioni pubblicamente accessibili a qualsiasi utente»⁵⁰; ha inoltre valorizzato il carattere volontario dell'esposizione, osservando che «il trasferimento e la ricezione di Bitcoin richiedono un atto affermativo da parte del titolare dell'indirizzo Bitcoin»⁵¹. Su

and the Brave New World of Online Social Networking, in *Marquette Law Review* 2010 (93), 1522.

⁴⁸ Per una discussione più approfondita di tale questione, si può fare rinvio alla letteratura statunitense sviluppata in materia: Y. Kogan, *The Privacy Limits of Transacting in Bitcoin*, in *Columbia Business Law Review* 2022 (1), 506; V. Lark, *Building Blocks of Privacy: Why the Third-Party Doctrine Should Not Be Applied to Blockchain Transactions*, in *Federal Communications Law Journal* 2022 (3), 353; N. Lesiuk, *Ushering in a New Era: Assessing the Reasonable Expectation of Privacy vis-à-vis Cryptocurrency and Blockchain Data*, in *Manitoba Law Journal* 2024 (5), 1; C.A. Pelker, C.B. Brown, R.M. Tucker, op. cit., 59; D. Penn, *The Fifth Circuit, Fourth Amendment, and the Third-Party Doctrine: Two Takeaways from the Court's First Ruling on Bitcoin Privacy*, in *SMU Science and Technology Law Review* 2021 (1), 125; M. Wostbrock, *Miller in a Cashless Society: Financial Surveillance and the Fourth Amendment*, in *Columbia Business Law Review* 2023 (2), 1015.

⁴⁹ *United States v. Gratkowski*, 5th Cir. 2020.

⁵⁰ *Ibid.*

⁵¹ *Ibid.*

tale base, essa ha concluso che gli utenti Bitcoin «hanno scarse ragioni di attendersi che le informazioni pubblicate sulla *blockchain* di Bitcoin saranno mantenute riservate»⁵², con conseguente esclusione di una legittima aspettativa di riservatezza.

Un esito analogo è stato raggiunto con riguardo ai dati *off-chain* acquisiti presso gli *exchange* di criptovalute. A tal proposito la Corte ha ritenuto che i registri detenuti da Coinbase – un *exchange* che consente agli utenti di acquistare, vendere e detenere criptovalute attraverso un account collegato alla propria identità reale – siano sostanzialmente assimilabili ai tradizionali registri bancari e ricadano, pertanto, nell'ambito applicativo della *third-party doctrine*⁵³. In questa prospettiva, i giudici hanno osservato che gli utenti «hanno la possibilità di mantenere un elevato livello di riservatezza effettuando transazioni senza un intermediario»⁵⁴, ma che, scegliendo di operare tramite un *exchange* come Coinbase, accettano consapevolmente di «sacrificare una parte della propria riservatezza»⁵⁵ in cambio della maggiore comodità del servizio. Ne consegue che, rispetto ai dati *off-chain* detenuti dall'intermediario, non può riconoscersi alcuna ragionevole aspettativa di riservatezza.

Tale impostazione è stata in larga parte ribadita in *Harper v. Werfel* (2024)⁵⁶. In quel caso, la *Court of Appeals for the First Circuit* è stata chiamata a valutare la legittimità di un ordine emesso dall'*Internal Revenue Service* statunitense anch'esso nei confronti dell'*exchange* Coinbase, per ottenere informazioni sugli account relativi a un ampio numero di utenti. La controversia investiva esclusivamente l'accesso a dati *off-chain* detenuti dall'*exchange*. Anche in questa occasione la Corte ha escluso l'operatività delle tutele apprestate dal Quarto Emendamento, rilevando che l'appellante «non aveva un'aspettativa ragionevole di riservatezza nelle informazioni che aveva volontariamente comunicato a Coinbase»⁵⁷.

Con riguardo ai dati *off-chain*, dunque, entrambe le pronunce applicano un consolidato orientamento interpretativo del diritto del Quarto Emendamento: la *third-party doctrine*, secondo cui non sussiste alcuna aspettativa ragionevole di riservatezza con riguardo a informazioni volontariamente comunicate a un terzo, poiché si assume che l'interessato abbia accettato il rischio che il destinatario le trasmetta, a sua volta, alle autorità pubbliche. Sviluppata originariamente in relazione ai registri bancari e

⁵² *Ibid.*

⁵³ *United States v. Miller*, 425 US 435 (1976); *Smith v. Maryland*, 442 US 735 (1979).

⁵⁴ *United States v. Gratkowski*, *cit.*

⁵⁵ *Ibidem*. Per una revisione critica di tale ragionamento, v. Y. Kogan, *op. cit.*, 540.

⁵⁶ *Harper v. Werfel*, 1st Cir. 2024.

⁵⁷ *Ibid.*

ai dati telefonici, tale dottrina è stata successivamente estesa – non senza contestazioni – a un’ampia gamma di intermediari digitali e finanziari, una traiettoria in cui sono oggi ricompresi anche gli *exchange* centralizzati di criptovalute quali Coinbase⁵⁸.

Merita tuttavia attenzione un passaggio della motivazione che, pur non incidendo sull’esito del giudizio, ne segnala un possibile limite. In *obiter dictum* del caso *Harper*, infatti, la Corte ha riconosciuto che gli utenti che operano direttamente sulla *blockchain* possono «mantenere [un] elevato livello di riservatezza»⁵⁹, ancorché a fronte di maggiori oneri tecnici e operativi. L’osservazione è rilevante perché lascia intravedere, sia pure in forma non decisiva, che il giudizio sull’esistenza di una ragionevole aspettativa di riservatezza non sia necessariamente uniforme, ma possa variare in funzione della natura del dato e, soprattutto, del contesto in cui esso viene generato o detenuto: presso un intermediario, nel caso dei dati *off-chain*; direttamente sulla *blockchain*, nel caso dell’operatività *on-chain*.

Quanto ai dati *on-chain* – vale a dire alle informazioni registrate direttamente sul registro della *blockchain*, tra cui informazioni transazionali, indirizzi coinvolti e *timestamp* – la questione si presenta più complessa. A prima vista, il ragionamento sviluppato dalla Corte sembrerebbe difficilmente contestabile: poiché i dati registrati sulla *blockchain* sono, per definizione, pubblici, ritenerli estranei a qualunque ragionevole aspettativa di riservatezza potrebbe apparire una conclusione lineare. Tale impostazione si presta, nondimeno, a rilievi critici ove si prenda seriamente in considerazione il funzionamento concreto della tecnologia *blockchain* e le reali potenzialità degli strumenti di *blockchain analysis*.

L’accessibilità pubblica dei dati registrati sulla *blockchain*, infatti, non equivale, di per sé, a una rinuncia agli interessi di riservatezza. Come si è già osservato, la trasparenza costituisce un elemento strutturale dei registri distribuiti pubblici, in quanto funzionale a garantire integrità, verificabilità e affidabilità del sistema. A tale trasparenza, tuttavia, si affianca lo pseudonimato, cioè il principale meccanismo tecnico di preservazione della riservatezza degli utenti. Detto altrimenti, chiunque consulti la *blockchain* di Bitcoin «può vedere che qualcuno sta inviando un importo a qualcun altro, ma senza informazioni che collegano la transazione a qualcuno»⁶⁰.

⁵⁸ Per un’analisi approfondita della *third-party doctrine*, v. O. Kerr, *The Case for the Third-Party Doctrine*, in *Michigan Law Review* 2009 (107), 561; e, con specifico riferimento alla sua applicazione alle transazioni in criptovaluta, v. la dottrina statunitense già richiamata *supra* a nota n. 49.

⁵⁹ *Harper v. Werfel*, cit.

⁶⁰ S. Nakamoto, *Bitcoin*, cit., 6.

Ne deriva che la pubblicità del dato transazionale non implica, sul piano sostanziale, l'accettazione della piena identificabilità del soggetto che lo ha generato. Gli utenti della *blockchain*, infatti, possono ben essere consapevoli della visibilità pubblica delle transazioni senza, per ciò solo, potersi attendere che da esse sia possibile risalire alla loro identità personale. Tutelare quest'ultimo profilo non richiede di postulare un autonomo "diritto a transazioni anonime": esso discende direttamente dall'architettura pseudonima della rete stessa, che rende visibile la transazione trattenendo, al contempo, qualsiasi collegamento con l'identità delle parti coinvolte.

È precisamente in questo snodo che l'approccio delle corti statunitensi mostra il proprio limite nella misura in cui sovrappone la formale accessibilità del dato al contenuto informativo che può essere ricavato soltanto mediante successive operazioni di correlazione, aggregazione e inferenza analitica. Si tratta, infatti, di piani distinti. Una cosa è la mera visibilità di una sequenza di indirizzi e trasferimenti; altra cosa è la possibilità di trasformare quel materiale grezzo in un patrimonio informativo idoneo a ricostruire identità, relazioni economiche e, più in generale, abitudini di vita⁶¹.

Sotto questo profilo, l'impiego di indirizzi alfanumerici in luogo di identificativi riferibili alla persona fisica non esprime affatto una tacita rinuncia alla riservatezza. Al contrario, è espressione di una precisa scelta architetture (e degli utenti che aderiscono a questi sistemi di pagamento) volta a separare la validazione pubblica delle transazioni dall'immediata identificazione dei soggetti coinvolti. Pertanto, assimilare la disponibilità pubblica dei dati *blockchain* a una generale rinuncia alla riservatezza è una soluzione che, nella migliore delle ipotesi, riflette un fraintendimento della logica tecnologica sottesa al sistema.

3.2 I profili critici sin qui richiamati assumono un rilievo particolarmente accentuato se esaminati nel contesto europeo. Specie rispetto al diritto alla riservatezza e alla tutela dei dati, infatti, il diritto europeo poggia su presupposti valoriali e normativi profondamente diversi da quelli che connotano il contesto statunitense appena descritto. Pur in assenza, ad oggi, di precedenti europei, tanto della Corte di giustizia dell'Unione europea quanto della Corte europea dei diritti dell'uomo, specificamente riferiti all'impiego investigativo di strumenti di analisi della *blockchain*, è nondimeno possibile ricavare alcune coordinate interpretative dai principi già consolidati nella

⁶¹ J. Della Torre, *Spunti in tema di cripto-attività*, cit., 318.

giurisprudenza relativa a tecniche investigative idonee a determinare un'apprezzabile ingerenza nella vita privata.

Nel contesto europeo, come noto, il riferimento centrale è dato dall'art. 8 Cedu e dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, che tutelano rispettivamente il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali. Entro tale assetto, la configurabilità di un'ingerenza non dipende né dalla natura pubblica o privata delle informazioni acquisite dalle autorità di *law enforcement*, né dall'esistenza di una *reasonable expectation of privacy* nei termini propri del diritto statunitense. Ciò che rileva, come si vedrà, è se l'attività investigativa, per le modalità concrete e per gli effetti che la caratterizzano, sia idonea a incidere in modo significativo sulla sfera privata dell'individuo⁶². Da questa prospettiva, la mera accessibilità pubblica dei dati non vale, di per sé, a escludere l'operatività delle garanzie convenzionali ed eurounitarie, ove le tecniche di acquisizione, aggregazione e analisi consentano una penetrazione apprezzabile nella vita privata dell'interessato⁶³.

Questa impostazione affonda le proprie radici nella giurisprudenza della Corte europea dei diritti dell'uomo, che ha progressivamente precisato l'estensione della nozione di vita privata ai sensi dell'art. 8 Cedu. Nell'orientamento ormai consolidato della Corte, questa nozione non si esaurisce nelle informazioni segrete o strettamente riservate, ma costituisce piuttosto «un termine ampio non suscettibile di definizione esaustiva»⁶⁴, capace di oltrepassare la sfera meramente intima e di «comprendere anche il diritto di condurre una vita sociale privata»⁶⁵. Inoltre, la Corte ha chiarito espressamente che la tutela della vita privata non resta esclusa per il solo fatto che «le attività abbiano luogo in un contesto pubblico»⁶⁶. Ne consegue che, ai fini che qui interessano, la mera accessibilità di un'informazione nel dominio pubblico, al pari dello svolgimento in un contesto pubblico della condotta cui essa si riferisce, non vale, di per sé, a escludere l'applicabilità delle garanzie derivanti dall'art. 8 Cedu.

Muovendo da tale premessa, la Corte europea ha costantemente affermato che la tutela apprestata dall'art. 8 Cedu si estende anche ad attività di carattere economico e

⁶² Sul punto, per tutti, v. V. Mitsilegas, *The Transformation of Privacy in an Era of Pre-emptive Surveillance*, in *Tilburg Law Review* 2015 (20), 35, 53 s.

⁶³ Come precisamente rilevato da T. van Roomen, op. cit., 141, negli Stati Uniti la verifica dell'ingerenza nella privacy ruota intorno al *reasonable expectation of privacy test*, e dunque all'aspettativa di riservatezza del soggetto nel caso concreto; nei sistemi europei, invece, la valutazione si fonda su un'impostazione *rights-based*, imperniata sull'art. 8 Cedu e sulla portata dell'ingerenza nel diritto alla vita privata nel caso concreto.

⁶⁴ C. eur., 4.7.2023, *Glukhin c. Russia*, ric. n. 11519/20, § 64.

⁶⁵ *Ibid.*

⁶⁶ *Ibid.*

finanziario. Costituisce, infatti, principio consolidato quello per cui «non vi è ragione di principio per cui tale concezione della nozione di “vita privata” debba escludere attività di natura professionale o commerciale»⁶⁷. Questa impostazione è stata espressamente ribadita con specifico riguardo alle informazioni finanziarie, avendo la Corte precisato che «le informazioni tratte da documenti bancari configurano indubbiamente dati personali relativi a un individuo, a prescindere dal fatto che si tratti o meno di informazioni sensibili»⁶⁸. Ne deriva che i dati relativi ad attività economiche e finanziarie rientrano nell’ambito di tutela dell’art. 8 Cedu⁶⁹. Per le medesime ragioni, anche i dati registrati sulle *blockchain* pubbliche, così come i dati trattati dai CASP, possono ragionevolmente essere ricondotti alla nozione di dati personali ai fini dell’art. 8 Cedu, nella misura in cui siano suscettibili di essere collegati a individui identificabili.

Quanto alla soglia di ingerenza rilevante ai sensi dell’art. 8 Cedu, la Corte di Strasburgo ha affermato che «la conservazione da parte di un’autorità pubblica di informazioni relative alla vita privata di un individuo costituisce un’ingerenza ai sensi dell’art. 8»⁷⁰ e che «il successivo uso delle informazioni conservate non incide su tale constatazione»⁷¹. Ne deriva che la raccolta e la conservazione sistematica di dati da parte delle autorità di *law enforcement* integrano un’ingerenza ai sensi dell’art. 8 Cedu, indipendentemente dal carattere pubblicamente accessibile delle informazioni considerate⁷².

Una volta qualificato in questi termini, un atto investigativo del tipo descritto può ritenersi compatibile con la Convenzione solo ove sia assistito da adeguate garanzie sostanziali e procedurali⁷³. Sul primo versante, la disciplina interna deve essere

⁶⁷ C. eur., 16.12.1992, *Niemietz c. Germania*, ric. n. 13710/88, § 29.

⁶⁸ C. eur., 7.7.2015, *M.N. e altri c. San Marino*, ric. n. 28005/12, § 51. In senso convergente, C. eur., 27.4.2017, *Sommer c. Germania*, ric. n. 73607/13, §§ 57-59; C. eur., 1.12.2015, *Brito Ferrinho Bexiga Villa-Nova c. Portogallo*, ric. n. 69436/10, §§ 42-44.

⁶⁹ C. eur., 22.12.2015, *G.S.B. c. Svizzera*, ric. n. 28601/11, § 89.

⁷⁰ C. eur., 16.2.2000, *Amann c. Svizzera*, ric. n. 27798/95, § 69. Nello stesso senso anche C. eur., 4.5.2000, *Rotaru c. Romania*, ric. n. 28341/95, § 43.

⁷¹ *Ibid.*

⁷² La questione era già stata affrontata con lungimiranza da S. Allegrezza, *Giustizia penale e diritto all'autodeterminazione dei dati personali nella regione europea*, in *Protezione dei dati personali e accertamento penale. Verso la creazione di un nuovo diritto fondamentale?*, a cura di D. Negri, Roma 2007, 69, la quale sottolineava che ciò che rileva non è tanto la pubblicità del dato personale, quanto piuttosto la registrazione sistematica o permanente della condotta in questione.

⁷³ Per una approfondita proposta di articolazione delle garanzie su una scala graduata, modulata in funzione dell'intensità dell'ingerenza (analisi isolata di indirizzi on-chain; correlazione sistematica on-chain/off-chain; raccolta massiva e preventiva per la costruzione di database), con corrispondente differenziazione degli standard di tutela, v. J. Della Torre, *Cripto-attività e giustizia penale*, op. cit., 325-328.

accessibile e prevedibile nella sua applicazione e deve delimitare con sufficiente chiarezza l'ampiezza della discrezionalità riconosciuta alle autorità competenti⁷⁴. A tal fine, essa deve prevedere almeno un nucleo minimo di garanzie, comprensivo della natura dei reati e delle categorie di persone rispetto alle quali la misura può essere disposta, dei limiti di durata, delle procedure relative all'esame, all'utilizzo, alla conservazione e alla detenzione dei dati acquisiti, nonché delle condizioni che ne impongono la cancellazione o la distruzione⁷⁵. Sul piano procedurale, è inoltre necessario che l'atto di indagine sia assoggettato a un controllo preventivo da parte di un'autorità indipendente e che all'interessato sia assicurato l'accesso a un ricorso effettivo⁷⁶.

Ulteriore conferma può trarsi dal diritto dell'Unione europea. Le attività di *blockchain analysis* rientrano, infatti, nell'ambito di applicazione della Dir. 2016/680/UE, che disciplina il trattamento dei dati personali da parte delle autorità di contrasto per finalità di prevenzione, indagine e repressione dei reati⁷⁷. Ai sensi dell'art. 3, par. 1, della Direttiva, la nozione di «dati personali» è definita in termini ampi, così da ricomprendere qualsiasi informazione relativa a una persona identificata o identificabile, inclusi i dati che ne consentano un'identificazione indiretta. Entro siffatta cornice definitoria, i dati impiegati nelle attività di *blockchain analysis* possono essere ricondotti a tale nozione nella misura in cui, come si è visto, risultano suscettibili di permettere l'identificazione indiretta degli interessati.

Inoltre, l'impiego di software di *blockchain analysis* può essere qualificato come attività di «profilazione» ai sensi dell'art. 3, par. 4, della medesima Direttiva. Come già rilevato, tali attività non si esauriscono nel tracciamento isolato di singole transazioni, ma si traducono, il più delle volte, in forme di aggregazione massiva, cumulativa e retrospettiva, orientate alla profilazione dei soggetti coinvolti. Attraverso la correlazione strutturata di dati *on-chain* e *off-chain*, le autorità di *law enforcement* sono in grado di ricostruire sequenze transazionali, connessioni relazionali e schemi di comportamento, trasformando registri formalmente pubblici e frammentari in insiemi informativi coerenti e a elevata capacità descrittiva. Un simile trattamento è

⁷⁴ C. eur. GC, 4.12.2015, *Roman Zakharov c. Russia*, ric. n. 47143/06, §§ 228-230.

⁷⁵ *Ibid.*, § 231.

⁷⁶ *Ibid.*, §§ 232-233.

⁷⁷ Per una panoramica completa, v. *inter alia* E. Kosta, F. Boehm, *The EU Law Enforcement Directive (LED)*, Oxford 2024; T. Marquenie, *The Police and Criminal Justice Authorities Directive: Data Protection Standards and Impact on the Legal Framework*, in *Computer Law & Security Review* 2017 (33), 324; J. Sajfert, T. Quintel, *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities*, in *SSRN Electronic Journal* 2017, in www.ssrn.com/abstract=3285873, 4.9.2024.

idoneo a determinare un'ingerenza significativa nella vita privata qualora possa condurre alla ricostruzione della «vita economica»⁷⁸ dell'individuo, rivelandone abitudini di spesa, relazioni finanziarie e *pattern* comportamentali che eccedono ampiamente la singola transazione oggetto di esame⁷⁹.

Ne deriva che i requisiti posti dagli artt. 4 e 8 della Dir. 2016/680/UE dovrebbero trovare applicazione anche in questo ambito, con particolare riferimento ai profili concernenti la liceità del trattamento e la necessità di una base giuridica chiara, precisa e sufficientemente determinata, idonea a garantire il rispetto delle garanzie in materia di protezione dei dati previste dalla Direttiva⁸⁰.

Nella misura in cui i software di *blockchain analysis* si fondano su tecniche automatizzate o basate sull'intelligenza artificiale per il *clustering* e il riconoscimento di *pattern*, essi potrebbero altresì rientrare nell'ambito di applicazione del Regolamento (UE) 2024/1689 (AI Act). Tali impieghi risultano suscettibili di essere classificati come "ad alto rischio" ai sensi dell'art. 6 e dell'allegato III, punto 6, che riguarda i sistemi di IA impiegati dalle autorità di *law enforcement* per la profilazione delle persone fisiche nell'ambito di indagini penali⁸¹. Così inquadrati, questi strumenti sarebbero assoggettati agli obblighi che il Capo III, Sezione 2, del Regolamento pone a carico dei sistemi ad alto rischio – tra i quali i requisiti di corretta governance dei dati, documentazione tecnica e tracciabilità delle operazioni, di trasparenza verso il *deployer* e necessaria sorveglianza umana – obblighi destinati a cumularsi a quelli già discendenti dalla Dir. 2016/680/UE. Come si vedrà, tale classificazione solleva ulteriori questioni interpretative quanto alle sue implicazioni pratiche.

⁷⁸ J. Della Torre, *Spunti in tema di cripto-attività*, cit., 318.

⁷⁹ C. Rueckert, op. cit., 6, il quale osserva che la mera consultazione di dati presenti sulla *blockchain* non integra, di per sé, un'ingerenza nel diritto alla protezione dei dati personali. Diverso è il caso in cui autorità investigative, pubblici ministeri o autorità di regolamentazione procedano alla raccolta, conservazione o elaborazione sistematica di dati *blockchain*: in tale ipotesi l'ingerenza diviene configurabile.

⁸⁰ Gli artt. 4 e 8 della dir. 2016/680/UE articolano un insieme coerente di garanzie sostanziali e procedurali che disciplinano il trattamento dei dati personali da parte delle autorità competenti. L'art. 4 enuncia i principi fondamentali in materia di protezione dei dati, prescrivendo che i dati personali siano trattati in modo lecito e corretto, raccolti per finalità determinate e legittime, e limitati a quanto adeguato, pertinente e non eccedente rispetto a tali finalità. Esso impone inoltre obblighi di esattezza, limitazione della conservazione e sicurezza, circoscrivendo ogni successivo trattamento per finalità diverse ai casi in cui esso sia autorizzato dalla legge e dimostrabilmente necessario e proporzionato. Tali principi sono completati dal requisito di responsabilizzazione (*accountability*), che pone in capo al titolare del trattamento l'onere di garantire e dimostrare la conformità. L'art. 8 rafforza tali garanzie ancorando la liceità del trattamento a un compito svolto da un'autorità competente sulla base del diritto dell'Unione o degli Stati membri, il quale deve a sua volta definire, come minimo, gli obiettivi, le finalità e le categorie di dati personali interessati.

⁸¹ L'allegato III n. 6 lett. *d-e* dell'AI Act si riferisce, rispettivamente, ai sistemi di IA impiegati per valutare il rischio che una persona fisica commetta reati o li reiteri, e ai sistemi di IA impiegati per la profilazione nel corso di attività di individuazione, indagine o perseguimento di reati ai sensi dell'art. 3 n. 4 dir. 2016/680/UE.

Non da ultimo, la valutazione dell'intensità dell'ingerenza prodotta da simili forme di trattamento deve essere condotta alla luce dei criteri elaborati dalla Corte di giustizia nella propria giurisprudenza in materia di accesso ai dati personali. Come noto, la C.G.U.E ha più volte affermato che l'accesso a dati personali deve considerarsi grave quando, «nel loro complesso, [i dati] possono permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati»⁸², integrando così un'ingerenza nei diritti garantiti dagli artt. 7 e 8 della Carta⁸³. Ne consegue che ogni interferenza nella vita privata, per risultare compatibile con tali disposizioni, deve poggiare su una base giuridica adeguata, perseguire finalità legittime connesse alla prevenzione e alla repressione dei reati e, soprattutto, rispettare il principio di proporzionalità. In questo contesto, la Corte ha ritenuto indispensabile che l'accesso ai dati trovi fondamento in una disciplina normativa chiara, idonea ad assicurare un insieme di garanzie sostanziali e procedurali, tra le quali assume particolare rilievo l'assoggettamento dell'accesso a un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente⁸⁴.

Al contempo, sul piano procedurale, la violazione delle garanzie poste a tutela della riservatezza non comporta automaticamente l'inutilizzabilità della prova nel procedimento penale. Secondo la Corte di giustizia, infatti, il giudice nazionale è tenuto a escludere i dati illegittimamente acquisiti solo al ricorrere di due condizioni cumulative: in primo luogo, che le persone interessate «non siano in grado di prendere efficacemente posizione su tali informazioni ed elementi di prova»; in secondo luogo,

⁸² C.G.U.E, 2.10.2018, *Ministerio Fiscal*, C-207/16, § 54; C.G.U.E, 8.4.2014, *Digital Rights Ireland*, cause riunite C-293/12 e C-594/12, § 27.

⁸³ Per un'analisi dettagliata, v. I. Neroni Rezende, *Criminal Justice and Data Protection: Communication Metadata under EU Human Rights Law*, Torino-Londra 2026, 138.

⁸⁴ V., *inter alia*, C.G.U.E, *Digital Rights Ireland*, cit.; C.G.U.E, 21.12.2016, *Tele2 Sverige e Watson*, cause riunite C-203/15 e C-698/15; C.G.U.E, *Ministerio Fiscal*, cit.; C.G.U.E, 6.10.2020, *Privacy International*, C-623/17; C.G.U.E, 6.10.2020, *La Quadrature du Net*, cause riunite C-511/18, C-512/18 e C-520/18; C.G.U.E, 2.3.2021, *H.K. c. Prokuratuur*, C-746/18; C.G.U.E GS, 30.4.2024, *M.N.*, C-670/22; C.G.U.E, 4.10.2024, *Bezirkshauptmannschaft Landeck*, C-548/21. Come è noto, il nucleo della giurisprudenza della Corte in materia di *data retention* risiede nel requisito secondo cui le ingerenze gravi negli artt. 7 e 8 della Carta devono essere assistite da garanzie particolarmente rigorose. Oltre all'esistenza di una base giuridica chiara e prevedibile e al perseguimento di finalità legittime connesse alla lotta contro la criminalità grave, il diritto dell'Unione richiede un insieme di garanzie procedurali. Tra queste rientrano, *inter alia*, l'autorizzazione preventiva da parte di un giudice o di un'autorità amministrativa indipendente, limitazioni rigorose concernenti le categorie di dati accessibili, le persone interessate e l'ambito temporale dell'accesso, nonché norme precise sui periodi di conservazione, la custodia sicura e la cancellazione irreversibile dei dati una volta venuta meno la necessità. Tali requisiti sono strettamente connessi all'idea che la proporzionalità debba essere valutata alla luce del potenziale informativo complessivo generato dall'attività di trattamento, piuttosto che con riferimento a singoli dati considerati isolatamente.

che le medesime informazioni «provengano da un settore che esula dalla competenza dei giudici e possano influenzare in maniera preponderante la valutazione dei fatti»⁸⁵.

Muovendo da tali premesse, vi sono solide ragioni per ritenere che le garanzie elaborate dalla giurisprudenza della Corte di Giustizia in materia di *data retention* possano estendersi anche alle attività investigative di *blockchain analysis* volte alla de-anonimizzazione degli indirizzi. Sebbene i due contesti differiscano quanto alla natura del dato trattato – tabulati e metadati di comunicazioni elettroniche, da un lato; dati transazionali *on-chain* e informazioni *off-chain*, dall'altro – ciò che li accomuna, e che giustifica l'applicazione delle medesime garanzie, è la natura del trattamento e il suo effetto complessivo.

Un'estensione di questo tipo non è priva di precedenti: sia la Corte EDU sia la C.G.U.E hanno già applicato, a dati finanziari detenuti da terzi, garanzie concepite per i dati di comunicazione, riconoscendo a tali dati una tutela comparabile proprio in ragione della loro capacità di rivelare scelte, abitudini e relazioni dell'individuo. La medesima logica giustifica l'estensione di tali garanzie alla *blockchain analysis*⁸⁶. In entrambi i casi, infatti, la raccolta sistematica, cumulativa e retrospettiva di informazioni atomisticamente innocue è in grado di generare profili individualizzati precisi, rivelatori di abitudini, relazioni e comportamenti che l'interessato non ha mai inteso rendere conoscibili come insieme coerente.

In quest'ottica, la *blockchain analysis* deve essere ricondotta all'ambito applicativo delle garanzie sancite dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, nonché dall'art. 8 Cedu. L'ingerenza nella vita privata, infatti, non discende dalla consultazione isolata di singoli dati transazionali, bensì dalla loro raccolta, aggregazione e analisi in forma massiva, sistematica e retrospettiva⁸⁷. Proprio per tali caratteristiche, essa è idonea a produrre effetti comparabili, quanto a intensità, a quelli che la Corte di giustizia ha qualificato come ingerenze gravi, nella misura in cui i dati,

⁸⁵ C.G.U.E, *La Quadrature du Net* (2020), cit., § 227; C.G.U.E, *H.K. c. Prokuratuur*, cit., § 44. Sul tema, v. *inter alia* G. Lasagni, *Admissibility of Evidence in Criminal Proceedings: Lessons (and Problems) from the "Data Retention Saga"*, in *Admissibility of Evidence in EU Cross-Border Criminal Proceedings*, a cura di L. Bachmaier Winter e F. Salimi, Oxford 2024, 35; M. Panzavolta, E. Maes, *Exclusion of Evidence in Times of Mass Surveillance: In Search of a Principled Approach to Exclusion of Illegally Obtained Evidence in Criminal Cases in the European Union*, in *The International Journal of Evidence & Proof* 2022 (26), 204; I. Neroni Rezende, op. cit., 260.

⁸⁶ Come rilevato da G. Lasagni, *Banking Supervision and Criminal Investigation. Comparing the EU and US Experiences*, Torino 2019, 337, questa giurisprudenza segna un distacco rispetto alla più ristretta concezione della riservatezza finanziaria prevalente negli Stati Uniti a partire da *United States v. Miller*, cit.

⁸⁷ In senso analogo v. T. van Roomen, op. cit., 141; J. Della Torre, *Cripto-attività e giustizia penale*, cit., 315 s.

nel loro complesso, possono consentire di trarre conclusioni precise sulla vita privata delle persone interessate⁸⁸.

In conclusione, il potenziale marcatamente intrusivo che le tecniche di *blockchain analysis* dispiegano allorché siano impiegate per costruire profili individualizzati e inferenze di de-anonimizzazione impone di subordinarne la compatibilità con il diritto alla riservatezza all'esistenza di una base normativa chiara e sufficientemente precisa. Una simile disciplina dovrebbe tradurre in prescrizioni operative le garanzie sin qui richiamate, fissando limiti predeterminati alla raccolta, alla correlazione e alla conservazione dei dati, obblighi di documentazione e forme di autorizzazione giudiziaria. In difetto, l'impiego di software di *blockchain analysis* resta estraneo agli standard di tutela della vita privata elaborati in sede convenzionale ed eurounitaria.

4. L'impiego probatorio della *blockchain analysis* solleva questioni che eccedono il piano della tutela della riservatezza. Quando gli *output* di software analitici proprietari sono introdotti come prova nel procedimento penale, emerge un ulteriore ordine di problemi relativo alla loro compatibilità con il diritto al giusto processo. Come già rilevato, i dati raccolti mediante attività di *blockchain forensics* sono elaborati e interpretati attraverso software specializzati che combinano tecniche automatizzate di *clustering*, modelli di *pattern recognition* ed euristiche probabilistiche, al fine di individuare relazioni tra indirizzi, ricostruire flussi transazionali e formulare ipotesi attributive. Tali operazioni si fondano su algoritmi proprietari la cui logica interna, i cui parametri applicativi e i cui criteri decisionali, come già illustrato, di norma non sono accessibili all'esterno. Ne deriva una sostanziale opacità del funzionamento di questi strumenti, che investe non soltanto la difesa, ma, in diversa misura, anche le stesse autorità inquirenti e il giudice, per effetto del concorso tra proprietà intellettuale e segreto commerciale.

L'opacità incide direttamente su due profili, distinti ma strettamente connessi.

Il primo concerne l'affidabilità della prova. Quando l'enunciato probatorio si fonda su inferenze mediate dal software, l'assenza di accesso alla logica del sistema, alle

⁸⁸ Va osservato che non tutte le ingerenze negli artt. 7 e 8 della Carta presentano la medesima gravità. La C.G.U.E ha elaborato un approccio graduato, distinguendo tra ingerenze particolarmente gravi – come la conservazione e il trattamento dei dati di traffico e di localizzazione, che consentono di trarre conclusioni precise sulla vita privata degli interessati – ingerenze gravi – come la conservazione indiscriminata degli indirizzi IP – e limitazioni meno severe, come l'accesso ai dati anagrafici dei titolari di schede SIM. La gravità dell'ingerenza dipende sia dall'ampiezza della misura sia dalla profondità del profilo informativo che essa consente di estrarre. Per un'analisi dettagliata, v. I. Neroni Rezende, op. cit., 138 s.

euristiche impiegate e ai relativi processi di validazione impedisce una verifica effettiva della solidità metodologica dell'*output*. Diviene così difficile accertare se il procedimento analitico sia stato corretto, se le euristiche adottate siano empiricamente fondate e se i risultati ottenuti siano riproducibili.

Il secondo profilo riguarda, invece, l'effettiva possibilità per la difesa di esaminare e contestare la prova. L'opacità del software, infatti, non limita soltanto lo scrutinio delle conclusioni offerte dall'accusa, ma investe anche il percorso inferenziale che ha condotto alla loro formulazione.

4.1 Le corti federali statunitensi sono state le prime a misurarsi direttamente con i problemi delineati nel contesto di eccezioni relative all'ammissibilità della prova fondata su strumenti di *blockchain analysis* alla luce delle *Federal Rules of Evidence*. Allo stato, l'unico precedente sul tema è *United States v. Sterlingov* (2024), deciso dalla *District Court for the District of Columbia*⁸⁹. In quel procedimento, Sterlingov era accusato, tra l'altro, di associazione finalizzata al riciclaggio di denaro mediante l'impiego di criptovalute, e l'impianto probatorio dell'accusa si fondava, in parte, su risultati generati da Chainalysis Reactor.

La difesa aveva sostenuto che tali prove dovessero essere escluse in quanto incompatibili con la *Federal Rule of Evidence* 702(c), sul rilievo che Chainalysis Reactor costituirebbe «*junk science*»⁹⁰: un metodo non scientificamente affidabile, non sottoposto a *peer review* e privo di un tasso di errore noto, sicché le deposizioni fondate su Reactor non sarebbero frutto di principi e metodi affidabili.

La Corte ha disatteso questo argomento e, all'esito di una serie di udienze *Daubert*⁹¹, ha ritenuto affidabile il software. Il percorso argomentativo seguito dal giudice si è sviluppato attorno a una pluralità di elementi convergenti. In primo luogo, è stato valorizzato il fatto che gli esiti restituiti da Chainalysis Reactor trovassero riscontro in ulteriori prove ritualmente acquisite. In secondo luogo, la Corte ha attribuito rilievo all'esperienza professionale degli agenti che avevano condotto le indagini, i quali

⁸⁹ *United States v. Sterlingov*, D.D.C. 2024.

⁹⁰ *Ibid.*

⁹¹ A partire dalla sentenza cardine *Daubert v. Merrell Dow Pharmaceuticals Inc.*, 509 US 579 (1993), le cosiddette *Daubert hearings* sono udienze sull'ammissibilità della prova in cui il giudice del merito svolge una funzione di *gatekeeping* sulla prova scientifica, valutando se questa soddisfi la *Federal Rule of Evidence* 702, in particolare se sia «il prodotto di principi e metodi affidabili e se tali metodi siano stati applicati in modo affidabile ai fatti». I criteri *Daubert* sono gli indicatori di affidabilità della prova scientifica individuati dalla Corte Suprema: (a) verificabilità; (b) *peer review* e pubblicazione; (c) tasso di errore noto o potenziale; (d) accettazione generale nella comunità scientifica di riferimento.

hanno dichiarato di avere già utilizzato con successo il software in precedenti occasioni operative. Da ultimo, il giudice ha richiamato anche una forma di validazione incrociata, rilevando come i risultati prodotti da Chainalysis Reactor fossero stati in larga parte confermati mediante l'impiego di un diverso strumento di *blockchain analysis*, sviluppato da una società concorrente, vale a dire CipherTrace. Sulla base di tali elementi, la Corte ha quindi concluso che «quantomeno per come è stato impiegato nel presente caso e come confermato dagli ulteriori elementi probatori acquisiti dalla Corte [...] Chainalysis Reactor è affidabile»⁹².

La Corte, inoltre, non ha limitato il proprio scrutinio al solo caso concreto, ma ha ritenuto di affrontare la questione, più generale, se Chainalysis Reactor sia, in quanto tale, conforme ai requisiti di affidabilità scientifica richiesti dallo standard *Daubert*. In un successivo *obiter dictum*, la Corte ha formulato una valutazione di portata più ampia, dichiarandosi «convinta che la *blockchain analysis* in generale, e Reactor in particolare, non costituiscano *junk science*»⁹³. Nel procedere, poi, all'applicazione dei singoli criteri *Daubert*, la Corte ha preliminarmente osservato che l'individuazione di «ragionevoli parametri di affidabilità in un caso specifico»⁹⁴ integra una valutazione rispetto alla quale il giudice del merito dispone di «un ampio margine di apprezzamento»⁹⁵, per passare quindi all'esame autonomo di ciascun parametro.

Sul criterio della *testability*, ossia la possibilità che la teoria o la tecnica siano state effettivamente sottoposte a test, la Corte ha ritenuto che «il *clustering* di Reactor può essere testato, ed è stato effettivamente testato»⁹⁶, attribuendo particolare rilievo alla circostanza che tale metodologia risulta replicabile sia mediante software concorrenti, sia, su scala più contenuta, attraverso verifiche manuali.

Con riferimento, invece, alla *peer review* – vale a dire alla sottoposizione del metodo a revisione tra pari e a pubblicazione scientifica – la Corte ha riconosciuto che «Chainalysis Reactor non è stato, di per sé, sottoposto a *peer review*»⁹⁷, ma ha reputato tale dato né inatteso né decisivo. Al riguardo, essa ha osservato che l'euristica del *co-spend*, posta a fondamento dello strumento, aveva già ottenuto ampio riconoscimento in ambito scientifico e che la *peer review* rappresenterebbe un «*odd fit*»⁹⁸ rispetto a un

⁹² *United States v. Sterlingov*, cit.

⁹³ *Ibid.*

⁹⁴ *Ibid.*

⁹⁵ *Ibid.*

⁹⁶ *Ibid.*

⁹⁷ *Ibid.*

⁹⁸ *Ibid.*

prodotto di questa natura. In sostanza, l'assenza di una formale revisione paritaria non è stata considerata un indice contrario all'affidabilità del software.

Quanto, poi, al criterio concernente la conoscibilità del tasso di errore del software, la Corte ha preso atto del fatto che Chainalysis non avesse mai effettuato indagini o pubblicato dati circa falsi positivi o falsi negativi. Ciononostante, ha concluso che la «assenza di una rilevazione sistematica del tasso di errore»⁹⁹ non incidesse, di per sé, sulla valutazione finale di affidabilità di Reactor, in quanto l'investigatore «ha reso una testimonianza persuasiva circa l'assenza di falsi positivi sulla base della sua ampia esperienza nell'utilizzo di Reactor»¹⁰⁰.

Infine, con riguardo alla *general acceptance* – ossia alla verifica che la teoria o la tecnica godano di generale accettazione nella comunità scientifica di riferimento – la Corte ha valorizzato il fatto che il *blockchain tracing* «è ampiamente utilizzato tanto dalle autorità di *law enforcement* quanto dagli operatori economici»¹⁰¹, aggiungendo che Chainalysis, in particolare, «è considerato uno strumento standard nel settore»¹⁰².

Tale decisione risulta persuasiva solo in parte, poiché il ragionamento della Corte appare significativamente influenzato dalle peculiarità del caso concreto. Il giudice, infatti, sottolinea che, nella fattispecie esaminata, non sussistevano ragioni serie per dubitare dell'affidabilità degli esiti prodotti da Chainalysis Reactor, in quanto trovavano conferma in ulteriori prove ritualmente acquisite, provenivano dall'impiego dello strumento da parte di investigatori esperti ed erano stati, in larga misura, oggetto di validazione incrociata attraverso un diverso software. Sotto questo profilo, la conclusione secondo cui Reactor fosse affidabile nel caso di specie appare, nel complesso, convincente.

Meno persuasivo è, invece, l'ulteriore passaggio che conduce dall'accertamento dell'affidabilità nel caso concreto all'enunciazione di una più generale validità scientifica di Chainalysis Reactor. I fattori valorizzati dalla Corte – ossia la corroborazione offerta da ulteriori elementi di prova, l'esperienza degli investigatori e la validazione incrociata mediante uno strumento concorrente – non integrano, infatti, una verifica sul piano propriamente metodologico. Non viene in rilievo alcun parametro tra quelli abitualmente ritenuti significativi nel giudizio di affidabilità scientifica di uno strumento tecnologico, quali la trasparenza dei protocolli di verifica, l'accertamento indipendente del tasso di errore e la conoscibilità della logica

⁹⁹ *Ibid.*

¹⁰⁰ *Ibid.*

¹⁰¹ *Ibid.*

¹⁰² *Ibid.*

algoritmica sottostante. Inoltre, la Corte ha ampiamente sottovalutato due criteri che costituiscono l'essenza stessa della scientificità: la sottoposizione a *peer review* e la quantificazione del tasso di errore. Come rilevato, infatti, le euristiche a supporto di Reactor non presentano la struttura delle leggi scientifiche, bensì quella delle massime di esperienza di matrice tecnica: una qualificazione che impone di verificare la correttezza dell'inferenza nel caso concreto, attraverso riscontri specifici, piuttosto che in termini di affidabilità generale dello strumento¹⁰³.

Ne emerge, in definitiva, una pronuncia che, pur legittimando l'impiego dello strumento nel peculiare contesto probatorio del caso esaminato, non sembra ancora offrire coordinate sufficientemente solide per fondarne l'affidabilità in termini generali. È proprio in questo scarto tra validazione situata e affidabilità metodologica generale che si manifesta il limite teorico della decisione. Uno standard di affidabilità costruito essenzialmente sulle circostanze del caso, e quindi sulla presenza di riscontri esterni e sull'esperienza degli operatori, difficilmente può proiettarsi oltre il singolo giudizio e sorreggere, in via generale, un'affermazione di affidabilità dello strumento, tanto più nei procedimenti in cui gli esiti della *blockchain analysis* non si limitino a corroborare l'ipotesi accusatoria ma ne costituiscano il fulcro probatorio.

4.2 Il quadro giuridico europeo si confronta con le medesime questioni muovendo da premesse profondamente diverse. Ne consegue che, anche sotto questo profilo, il ragionamento sviluppato oltreoceano difficilmente può essere assunto quale precedente suscettibile di trasposizione negli ordinamenti europei, per una pluralità di ragioni. Le criticità che vengono qui in rilievo si iscrivono, del resto, nella più ampia problematica della prova algoritmica, dalla quale mutuano i medesimi principi di riferimento; la loro concreta declinazione applicativa risente, tuttavia, delle specificità tecniche e operative della *blockchain analysis*.

Anzitutto, l'AI Act ha espressamente portato al centro dell'attenzione l'impiego di sistemi di intelligenza artificiale nel settore delle attività di *law enforcement*, anche con riguardo alla raccolta e alla valutazione della prova, nonché al rispetto dei diritti fondamentali della persona coinvolta¹⁰⁴. Alla luce delle caratteristiche tecniche dei

¹⁰³ Sul punto, diffusamente, J. Della Torre, *Cripto-attività e giustizia penale*, cit., 353-358.

¹⁰⁴ Al riguardo, è importante ricordare che il considerando n. 27 dell'AI Act rinvia agli *Ethics Guidelines for Trustworthy AI* del 2019, elaborati dal gruppo indipendente di esperti ad alto livello sull'intelligenza artificiale (AI HLEG) nominato dalla Commissione. Inoltre, il considerando n. 59 affronta i rischi per i diritti fondamentali garantiti dalla Carta derivanti dall'uso di sistemi di IA da parte delle autorità di *law enforcement*, sottolineando che tali sistemi devono soddisfare requisiti adeguati in termini di prestazioni, accuratezza e robustezza, e devono essere sufficientemente trasparenti, spiegabili e documentati. In una prospettiva critica sulla capacità dell'AI Act

principali software di *blockchain analysis*, già ricostruite *supra* (§§ 2.2 e 2.3), tali strumenti sembrano poter essere ricondotti alla categoria dei sistemi «ad alto rischio» ai sensi dell'art. 6, in combinato disposto con l'allegato III, punto 6, lett. c) ed e), dell'AI Act. Depone in tal senso, in particolare, l'impiego sistematico di modelli di machine learning per l'automazione del *clustering*, per l'attribuzione di punteggi di rischio e per la profilazione comportamentale degli utenti. Si tratta, infatti, di strumenti utilizzati per assistere le autorità competenti nella «valutazione dell'affidabilità degli elementi probatori» nel corso del procedimento penale.

Una simile qualificazione comporta che tali strumenti debbano essere progettati e sviluppati con un grado di trasparenza sufficiente a consentire ai *deployer* di interpretare correttamente gli esiti del sistema e di farne un uso appropriato (art. 13, par. 1, AI Act), nonché in modo da rendere possibile un'effettiva sorveglianza umana durante il loro impiego (art. 14, par. 1, AI Act)¹⁰⁵. In questa prospettiva, la trasparenza *by design* diventa un presupposto necessario affinché possa esservi contraddittorio effettivo¹⁰⁶. In mancanza di caratteristiche progettuali idonee a rendere il funzionamento del sistema controllabile e verificabile, la difesa potrebbe infatti non essere posta in condizione di esaminare efficacemente né il metodo né il risultato del procedimento algoritmico-probatorio, con il concreto rischio che il sistema operi come una *black box*, vale a dire un «sistema in cui *input* e *output* sono osservabili, mentre il funzionamento interno resta oscuro persino ai suoi stessi programmatori»¹⁰⁷. Va tuttavia precisato che l'AI Act non si spinge fino a ricollegare all'inosservanza di tali requisiti di trasparenza l'inutilizzabilità della prova così ottenuta: il regolamento, infatti, non detta regole di natura processuale-penalistica di questo tipo, sicché le conseguenze sul piano probatorio di un'eventuale violazione restano affidate alla disciplina nazionale.

di affrontare le preoccupazioni legate alla trasparenza, v. M. Anastasopoulou, *Exploring Algorithmic Governance: The AI Act and New Realities for Criminal Justice and Fundamental Rights*, in *New Journal of European Criminal Law* 2025 (16), 176, 190, la quale osserva che «sebbene nel regolamento vi siano numerosi riferimenti ai diritti fondamentali, manca un meccanismo o una metodologia sufficienti per valutare cosa costituisca un rischio per i diritti fondamentali, e se o quando una violazione/ingerenza possa essere giustificabile».

¹⁰⁵ Per un approfondimento sull'impatto dell'AI Act sul procedimento penale italiano si veda N. Gibelli, *AI Act e procedimento penale italiano: una valutazione d'impatto*, in *DPenCont* 2025, 90 s.

¹⁰⁶ Come correttamente affermato da S. Quattrocchio, *Artificial Intelligence, Computational Modelling and Criminal Proceedings*, Cham 2020, 94, la trasparenza, nel contesto del diritto delle prove, dovrebbe tradursi alternativamente nell'imposizione di standard idonei a garantire sempre, *ex ante*, la possibilità del *reverse engineering*, oppure nella predisposizione di modelli di revisione capaci di offrire, *ex post*, una validazione dell'affidabilità dei dati generati automaticamente e ammessi come prova in giudizio.

¹⁰⁷ G. Lasagni, G. Contissa, *When It Is (also) Algorithms and AI that Decide on Criminal Matters: In Search of an Effective Remedy*, in *European Journal of Crime, Criminal Law and Criminal Justice* 2020 (28), 280, 281.

Questo grado di opacità incide direttamente sulle garanzie del giusto processo e, in particolare, sul principio di parità delle armi. Secondo un orientamento costante della Corte EDU, il principio in parola richiede che accusa e difesa siano poste in condizione di conoscere la prova introdotta dalla controparte e di svolgere un contraddittorio effettivo¹⁰⁸. Pertanto, se strumenti di IA concorrono alla ricostruzione dei fatti, il loro impiego esclusivo da parte dell'accusa può determinare un'asimmetria epistemica difficilmente compatibile con un contraddittorio realmente equilibrato. Ne consegue che la parità delle armi richiede che la difesa sia posta in condizione di conoscere, in modo sufficientemente dettagliato, il funzionamento del software, così da poter contestare efficacemente la prova ottenuta tramite il suo impiego, anche sotto il profilo dell'affidabilità e della scientificità.

Il diritto a un giusto processo implica, in linea di principio, la *disclosure* di tutto il materiale investigativo «anche se non preso in considerazione o non ritenuto rilevante dall'accusa»¹⁰⁹. Ciò comporta che l'accesso difensivo non possa limitarsi ai soli dati in ingresso e ai risultati sui quali si fonda l'impostazione accusatoria, ma debba estendersi anche ai presupposti metodologici del sistema, alle euristiche impiegate, ai dati di addestramento, ove pertinenti, nonché alle procedure di validazione. Solo a queste condizioni la difesa può contestare in modo effettivo non soltanto il valore probatorio dell'elemento così acquisito, ma anche l'affidabilità scientifica del metodo che ne ha reso possibile la produzione. In mancanza, il contraddittorio rischia di ridursi a una garanzia meramente apparente. Poiché, inoltre, gli strumenti di IA non sono esenti da

¹⁰⁸ C. eur., 16.2.2000, *Rowe e Davis c. Regno Unito*, ric. n. 28901/95, § 60, dove la Corte ha affermato che «è un aspetto fondamentale del diritto a un equo processo che il procedimento penale, ivi compresi gli elementi di tale procedimento che attengono alla procedura, sia in contraddittorio e che vi sia parità delle armi tra l'accusa e la difesa. Il diritto a un processo in contraddittorio implica, nell'ambito di un procedimento penale, che tanto l'accusa quanto la difesa devono avere la possibilità di prendere conoscenza e di formulare osservazioni sulle memorie presentate e sulle prove addotte dalla controparte, che l'accusa comunichi alla difesa tutto il materiale probatorio in suo possesso a favore o a carico dell'accusato»; nello stesso senso v. C. eur., 28.8.1991, *Brandstetter c. Austria*, ric. nn. 11170/84, 12876/87 e 13468/87, §§ 66-67. Più in generale, i principi di parità delle armi e del contraddittorio costituiscono due espressioni complementari della più ampia garanzia del giusto processo ai sensi dell'art. 6 § 1 Cedu: il primo esige che ciascuna parte del procedimento penale disponga di una ragionevole possibilità di presentare la propria causa in condizioni che non la pongano in una posizione di svantaggio rispetto alla controparte (C. eur. GC, 12.5.2005, *Öcalan c. Turchia*, ric. n. 46221/99, § 140); il secondo esige che tanto l'accusa quanto la difesa abbiano la possibilità di prendere conoscenza e di formulare osservazioni su tutte le memorie e le prove addotte dalla controparte (C. eur., 26.3.1996, *Doorson c. Paesi Bassi*, ric. n. 20524/92, §§ 70-72). Per un'analisi più approfondita del principio di parità delle armi e della prova digitale, v. S. Quattrocchio, op. cit., 73.

¹⁰⁹ C. eur., 26.9.2023, *Yüksel Yalçınkaya c. Turchia*, ric. n. 15669/20, § 327; C. eur., 25.7.2019, *Rook c. Germania*, ric. n. 1586/15, § 58.

margin di errore, l'assenza di adeguate condizioni di conoscibilità e verificabilità finisce inevitabilmente per riflettersi sull'affidabilità stessa della prova¹¹⁰.

Il diritto di accesso, nondimeno, non riveste carattere assoluto. La mancata divulgazione di determinate informazioni può ritenersi ammissibile solo nella misura in cui sia strettamente necessaria alla tutela di interessi contrapposti di particolare rilievo – quali la sicurezza nazionale, l'incolumità di terzi o il segreto dei metodi investigativi – e sempre che le limitazioni imposte all'accesso della difesa alla prova siano assoggettate al controllo di un'autorità giudiziaria¹¹¹. In ogni caso, ove venga sottratto alla conoscenza della difesa materiale ad essa rilevante, devono essere predisposte adeguate misure compensative, idonee a garantire che il procedimento, considerato nel suo complesso, resti conforme alle esigenze del giusto processo ai sensi dell'art. 6 Cedu¹¹².

¹¹⁰ Per un'ampia panoramica e classificazione delle fonti di errore nella prova generata dall'IA ai fini della determinazione della colpevolezza o dell'innocenza, distinguendo tra *input* umani erronei (come dati obsoleti, incompleti o distorti), errori della macchina, errori analitici derivanti da eccessiva semplificazione, errori analitici derivanti da errori di programmazione o da presupposti errati, errori del *machine learning* e acquiescenza all'automazione si veda A. Roth, *The Use of Algorithms in Criminal Adjudication*, in *The Cambridge Handbook of the Law of Algorithms*, a cura di W. Barfield, Cambridge 2020.

¹¹¹ Sul punto, va precisato che tale bilanciamento non può essere delegato interamente all'accusa: laddove un giudice ometta di esaminare il materiale non divulgato, di motivare adeguatamente sulla mancata divulgazione e di valutarne l'importanza per la difesa, un'esclusione generalizzata di informazioni rilevanti si pone in contrasto con i requisiti dell'art. 6 Cedu (C. eur., *Yüksel Yalçınkaya c. Turchia*, cit., § 331). Il controllo giudiziario così configurato, del resto, non può nemmeno risolversi in una verifica meramente formale della sussistenza dell'interesse contrapposto invocato dall'accusa. Al contrario, è necessario che il giudice sia posto concretamente in condizione di apprezzare, sia pure in via riservata e senza *disclosure*, la reale rilevanza del materiale non divulgato per la difesa. Da questo punto di vista è interessante notare che, seppur in un ambito distinto (in materia di valutazione creditizia, c.d. *credit scoring*) la Corte di giustizia ha di recente affermato che l'interessato ha diritto a una spiegazione idonea a garantire una comprensione "significativa" della procedura e dei principi effettivamente applicati dallo strumento automatizzato (C.G.UE, 27.2.2025, *Dun & Bradstreet Austria*, C-203/22). Come rilevato da M. Caianiello, *Il controllo umano della decisione: IA, spiegabilità e giustizia penale*, in *OIDU 2026* (in corso di pubblicazione), tale statuizione attribuisce alla spiegabilità una dimensione giuridica autonoma, distinta sia dalla trasparenza tecnica del sistema sia dalla sua mera intelligibilità. Sebbene, come detto, resa in un contesto regolatorio diverso da quello processuale penale, tale standard costituisce un utile parametro di riferimento anche ai fini del sindacato giudiziario sulla *non-disclosure*: se in sede di *credit scoring* una comprensione effettiva del funzionamento dello strumento automatizzato costituisce il presupposto perché l'interessato possa esercitare i propri diritti, a maggior ragione un simile, se non superiore, grado di comprensione dovrebbe guidare il giudice penale nel valutare se il materiale sottratto alla conoscenza della difesa sia effettivamente rilevante per quest'ultima.

¹¹² Al riguardo, la sentenza della Grande Camera in *Yüksel Yalçınkaya c. Turchia*, cit., offre indicazioni rilevanti rispetto alla necessità di prevedere misure compensative necessarie per salvaguardare i diritti della difesa nelle indagini *data-driven*, in particolare laddove la mancata divulgazione riguardi elementi tecnici essenziali per la comprensione e la contestazione delle prove presentate dall'accusa. La *ratio* sottesa a tali misure compensative è quella di assicurare che la difesa sia coinvolta quanto più possibile nel processo decisionale e tenuta all'oscuro soltanto nella misura in cui ciò sia strettamente necessario. Di conseguenza, una restrizione al diritto di accesso è compatibile con l'art. 6 Cedu soltanto laddove la decisione sia soggetta al controllo di un'autorità giudiziaria e la limitazione che ne derivi per la difesa sia ridotta al minimo necessario. Secondo la Corte, la natura e

Trasposti al contesto specifico dei software di *blockchain analysis*, gli standard delineati appaiono in larga parte disattesi. Quanto agli strumenti maggiormente diffusi, le informazioni pubblicamente accessibili sui tassi di errore empiricamente validati, sui dataset e sui processi di addestramento che sorreggono i modelli analitici, nonché sulle garanzie predisposte per prevenire impieghi impropri dei dati personali, risultano spesso limitate, se non del tutto assenti. A ciò si aggiunga che i software sono normalmente commercializzati a costi elevati e resi accessibili, in via principale, alle autorità di *law enforcement* sulla base di accordi istituzionali. Ne deriva che la difesa solo eccezionalmente può disporre di risorse tecnologiche comparabili. Un simile squilibrio economico è suscettibile di tradurre il vantaggio tecnologico dell'accusa in un corrispondente vantaggio processuale, con conseguente aggravamento delle criticità in punto di parità delle armi¹¹³. Tali problematiche risultano ancor più marcate ove non siano predisposte adeguate misure compensative idonee a preservare l'equità complessiva del procedimento, lasciando la difesa priva di strumenti per comprendere la genesi della prova e poterla efficacemente contestare.

I nodi sin qui evocati investono la più ampia questione della prova ottenuta mediante algoritmi e sistemi di intelligenza artificiale, attorno alla quale il dibattito si è fatto sempre più ricco e dinamico, tanto nella letteratura giuridica quanto in quella informatica, ove non sono mancate né la segnalazione dei rischi né la proposta di possibili rimedi¹¹⁴.

l'adeguatezza di tali misure devono essere valutate in proporzione al pregiudizio concretamente subito dalla difesa in ragione della mancata divulgazione (§ 330). Laddove la difesa sia strutturalmente impossibilitata ad accedere direttamente alla prova e a verificarne l'integrità e l'affidabilità in prima persona, ciò «*places a greater onus on the domestic courts to subject those issues to the most searching scrutiny*» (§ 334). I giudici interni non possono limitarsi ad accettare acriticamente gli *output* di tecniche investigative complesse – essi sono piuttosto tenuti a scrutinare attivamente la solidità metodologica del processo attraverso il quale tali *output* sono stati generati. Dalla motivazione della Corte emergono diverse misure compensative. Anzitutto, all'accusato deve essere garantita la possibilità di prendere visione dell'intero materiale che lo riguarda, sì da poter formulare osservazioni e individuare elementi potenzialmente a discarico (§ 335). In secondo luogo, ove la difesa richieda che sia svolta una perizia ai fini dell'acquisizione della prova digitale, i giudici nazionali sono tenuti a motivare adeguatamente l'eventuale rigetto di tale richiesta: la mancata indicazione delle ragioni per cui un simile vaglio non sia ritenuto necessario costituisce di per sé una carenza procedurale suscettibile di pregiudicare l'equità complessiva del procedimento (§ 333). In terzo luogo, il giudice deve assicurarsi che l'accusato sia debitamente informato, ammesso a depositare memorie e a partecipare al processo decisionale nella misura più ampia possibile, affinché la limitazione del diritto di accesso non si traduca in una strutturale incapacità di condurre una difesa effettiva (§ 331).

¹¹³ Per ulteriori considerazioni sul rapporto tra trasparenza e segreti commerciali, v. U.-M. Mylly, *Transparent AI? Navigating Between Rules on Trade Secrets and Access to Information*, in *International Review of Intellectual Property and Competition Law* 2023 (54), 1013; M. Busuioc, D. Curtin, M. Almada, *Reclaiming Transparency: Contesting the Logics of Secrecy Within the AI Act*, in *European Law Open* 2023 (2), 79, 105.

¹¹⁴ Nella dottrina giuridica europea, per un'analisi completa e un insieme di proposte particolarmente stimolanti elaborate nel contesto europeo, v. ad esempio K. Ligeti, *Unpacking AI Evidence and (Re-)Defining Procedural*

In ogni caso, in attesa dell'adozione di soluzioni tecniche e legislative capaci di conciliare efficacemente gli interessi in gioco, è necessario ricercare un rimedio sul piano processuale. In assenza di una sanzione procedurale chiaramente definita, idonea a garantire la corretta formazione di questa tipologia di prove, indicazioni significative possono essere tratte dalla giurisprudenza della Corte di giustizia. Come chiarito in *M.N.*, «per quanto riguarda specificamente il diritto a un equo processo, occorre rilevare in particolare che, se un giudice ritiene che una parte non sia in grado di svolgere efficacemente le proprie osservazioni in merito a un mezzo di prova idoneo ad influire in modo preponderante sull'accertamento dei fatti, detto giudice deve constatare una violazione del diritto a un equo processo ed escludere tale prova al fine di evitare una siffatta violazione»¹¹⁵. Di conseguenza, laddove la difesa non sia in condizione di svolgere efficacemente le proprie osservazioni¹¹⁶ sulla prova derivata dal

Safeguards in Digital Investigations, in *AI Evidence and Criminal Proceedings*, a cura di K. Ligeti, Oxford 2026, 50 s.; v. altresì European Law Institute, *Proposal for a Directive on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings in the EU*, 2023. Soluzioni interessanti emergono anche dal contesto statunitense. In particolare, B.L. Garrett, C. Rudin, *The Right to a Glass Box: Rethinking the Use of Artificial Intelligence in Criminal Justice*, in *Cornell Law Review* 2024 (109), 561, sostengono che dovrebbe essere riconosciuto «a right to glass box AI». Operando una distinzione tra «interpretability» e «explainability», gli autori sostengono che le spiegazioni *ex post* dei sistemi *black-box* sono insufficienti e che soltanto l'*interpretability* può produrre una *glass box*. Una *glass box*, nella loro ricostruzione, richiede modelli la cui logica interna sia direttamente intelligibile, così che la trasformazione degli *input* in *output* possa essere compresa ed efficacemente contestata in giudizio. Gli autori collegano il «right to glass box AI» a concrete garanzie procedurali, tra cui requisiti di validazione e verifica, divulgazione e *discovery* orientate alla difesa, e accesso – mediante *protective orders* – al codice sorgente e alla documentazione di supporto ai fini della revisione indipendente e dello scrutinio in contraddittorio nel caso concreto. Con riguardo alla letteratura tecnica e informatica sul tema, per una ricostruzione sistematica del concetto e una trattazione completa di come la contestabilità dei sistemi di intelligenza artificiale possa essere strutturalmente integrata nelle indagini penali v. S. Maoro, *Contestable AI for Criminal Intelligence Analysis: Improving Decision-Making through Semantic Modeling and Human Oversight*, in *AI and Law* 2023, in doi.org/10.1007/s10506-023-09354-3, 21.3.2026.

¹¹⁵ C.G.U.E, *M.N.*, cit., § 105. Merita rilevare che tale regola di esclusione differisce dall'approccio adottato nella giurisprudenza in materia di *data retention*. In quel contesto, la Corte sembrava condizionare l'esclusione al soddisfacimento di tre requisiti cumulativi, lasciando così un'incertezza laddove uno di essi non risulti soddisfatto. Per contro, nella sentenza *M.N.* il criterio decisivo è se l'accusato sia stato effettivamente posto in condizione di formulare efficacemente osservazioni su una prova idonea ad influire in modo preponderante sull'accertamento dei fatti: in difetto di ciò, l'esclusione si impone.

¹¹⁶ Sebbene il criterio riguardi chiaramente i diritti della difesa e il principio del contraddittorio, la sua reale portata normativa rimane incerta: la C.G.U.E non ha chiarito il contenuto della garanzia insita nel requisito di «essere in condizione di formulare efficacemente le proprie osservazioni», né ha definito le circostanze concrete in cui l'esclusione della prova debba essere disposta, rimettendo entrambe le questioni all'interpretazione dei giudici nazionali. Vale inoltre osservare che la Corte ha deliberatamente preferito il termine «esclusione della prova» a quello di «inammissibilità», verosimilmente per evitare di affrontare direttamente la questione dell'ammissibilità in quanto tale. Per una discussione più dettagliata, v. S. Okunrobo Perez, *Proliferation of e-Evidence: Reliability Standards and the Right to a Fair Trial*, in *European Journal of Crime, Criminal Law and Criminal Justice* 2025 (33), 187, 195 ss.; L. Bernardini, *On Encrypted Messages and Clear Verdicts – the EncroChat Case before the Court of Justice (Case C-670/22, MN)*, in www.eulawlive.com, 21.5.2024.

software ed essa sia idonea ad influire in modo preponderante sull'accertamento dei fatti, una risposta conforme al giusto processo ne impone l'esclusione.

5. La ricostruzione svolta nei paragrafi precedenti permette ora di trasferire l'analisi sul piano dell'ordinamento italiano per verificare se vi sia un fondamento legislativo sufficientemente chiaro, categorie probatorie adeguate e garanzie difensive effettive per l'utilizzo investigativo e probatorio della *blockchain analysis*.

Sotto questo profilo, come spesso accade nell'ambito delle indagini digitali, è evidente il divario tra la prassi delle autorità inquirenti e lo sforzo regolativo del legislatore: alla rapida specializzazione delle forze dell'ordine non ha fatto seguito alcun intervento normativo significativo. Il problema, dunque, è verificare se e in quale misura sia possibile ricondurre queste tecniche entro una cornice legale compatibile con gli standard di tutela dei diritti fondamentali illustrati nelle sezioni che precedono.

Una prima questione riguarda la qualificazione dell'attività investigativa sul piano procedimentale. Occorre distinguere, a tal fine, due livelli che nella prassi si intrecciano, ma che restano concettualmente autonomi: da un lato, l'acquisizione dei dati grezzi dal registro distribuito – indirizzi, *hash*, *timestamp*, importi, sequenze transazionali – dall'altro, le successive elaborazioni prodotte tramite software specializzati¹¹⁷.

I dati *on-chain* sono, per loro natura, informazioni che esistono già prima del procedimento penale e che risultano fissate in un supporto informatico tecnicamente pensato per garantirne pubblicità e attendibilità. Pertanto, essi possono essere agevolmente ricondotti alla categoria della prova documentale di cui all'art. 234 Cpp. La disposizione, com'è noto, abbraccia una nozione ampia del mezzo di prova, ricomprendendo qualunque rappresentazione di fatti, persone o cose formatasi fuori dal processo e utile alla ricostruzione del *thema probandum*¹¹⁸.

Più articolato è il ragionamento allorché si passa alle elaborazioni inferenziali. Nel momento in cui, a partire dal dato grezzo, i software di *blockchain analysis* attribuiscono indirizzi a entità, costruiscono *cluster*, rilevano *pattern*, assegnano punteggi di rischio o procedono a operazioni di de-anonimizzazione, l'oggetto dell'attività probatoria cambia natura: non è più soltanto un dato registrato, ma una ricostruzione tecnica di natura valutativa, basata su inferenze di tipo probabilistico e

¹¹⁷ J. Della Torre, *Cripto-attività e giustizia penale*, cit., 451 s.

¹¹⁸ Per tutti, F. Zacché, *La prova documentale*, Milano 2012, 26 ss.; M. Pittiruti, *Digital evidence e procedimento penale*, Torino 2017, 24 ss.; P. Tonini, *Documento informatico e giusto processo*, in *DPP* 2009, 401 s. Con specifico riferimento ai dati cristallizzati sulla *blockchain*, J. Della Torre, *Cripto-attività e giustizia penale*, cit., 452 s.

che genera informazioni ulteriori rispetto a quelle ricavabili dalla semplice lettura del registro.

Esclusa la riconducibilità degli *output* inferenziali al paradigma documentale, occorre passare in rassegna le categorie codicistiche concettualmente più prossime, per verificare se alcuna di esse possa offrire un adeguato supporto normativo all'attività in esame. L'operazione è, peraltro, tutt'altro che agevole: le tecniche qui considerate sfuggono a una definizione positiva e la loro fisionomia composita e multiforme – in parte accertamento tecnico su dati preesistenti, in parte attività di ricerca della prova – ne rende incerta la collocazione entro l'una o l'altra delle categorie tipiche¹¹⁹.

Innanzitutto, l'assimilazione alle intercettazioni non convince. La nozione accolta dalle Sezioni unite – «captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti che agiscono con l'intenzione di escludere altri e con modalità oggettivamente idonee a tale scopo, attuata da un soggetto estraneo mediante strumenti tecnici di percezione tali da vanificare le cautele ordinariamente poste a protezione del carattere riservato della comunicazione»¹²⁰ – presuppone tre elementi che, nella *blockchain analysis*, risultano strutturalmente assenti: una comunicazione riservata tra soggetti determinati; una volontà esclusiva di quei soggetti di sottrarre lo scambio alla percezione altrui; una sfera di riservatezza protetta che l'atto investigativo violi aggirando cautele predisposte dagli interessati.

Nelle *blockchain* pubbliche, al contrario, la trasparenza è una caratteristica strutturale della rete: l'utente che conduce una transazione non comunica con un altro soggetto in condizioni di segretezza, ma iscrive un'operazione in un registro pubblicamente consultabile. Allo stesso modo, l'investigatore che analizza tali dati non capta una comunicazione altrui, bensì accede a informazioni che la rete stessa rende disponibili a chiunque¹²¹. Inoltre, manca, ancor prima, il presupposto stesso della captazione. La *blockchain analysis* non intercetta un flusso comunicativo in corso ma osserva e ricostruisce dati che, una volta validati, sono registrati permanentemente nel registro distribuito. Pertanto, la nozione di comunicazione non può estendersi alle transazioni in quanto tali: queste ultime non veicolano un contenuto tra interlocutori

¹¹⁹ Sul punto, *amplius*, J. Della Torre, *Cripto-attività e giustizia penale*, cit., 418

¹²⁰ Cass. S.U. 28.5.2003 n. 36747, Torcasio.

¹²¹ Per le difficoltà applicative della nozione di intercettazioni a fronte dell'evoluzione tecnologica, A. Camon, *I confini mobili delle intercettazioni*, in *Indagini e prove nella società digitale*, a cura di G. Di Paolo e L. Pressacco, Padova 2024, 9 ss. Per un'analisi specifica circa l'assimilazione della *blockchain analysis* al regime delle intercettazioni J. Della Torre, *Cripto-attività e giustizia penale*, cit., 419 ss.

determinati sorretto da un intento comunicativo, ma registrano un'operazione di natura economica destinata strutturalmente alla pubblicità.

Non persuade del tutto neppure l'accostamento al monitoraggio bancario e finanziario in tempo reale previsto dall'art. 20 co. 2 d.lgs. 21.6.2017 n. 108. Come indicato dalla dottrina, se una certa affinità funzionale è innegabile, in particolare rispetto ai CASP – che la disciplina antiriciclaggio considera intermediari finanziari – il parallelismo non regge oltre¹²². La *blockchain analysis*, infatti, può avere a oggetto trasferimenti *peer-to-peer* tra privati, senza alcun intermediario vigilato, e il carattere pseudonimo degli indirizzi impedisce di stabilire in anticipo se il *wallet* da analizzare appartenga a un CASP o a un soggetto privato¹²³. Va peraltro osservato come l'art. 20 operi quale disciplina di risposta a un ordine europeo di indagine penale, e non quale base legale generale per le indagini di natura puramente interna: al di fuori del perimetro applicativo della direttiva 2014/41/UE, non risulta rinvenibile, allo stato, una disciplina equivalente¹²⁴. Inoltre, anche ove, in astratto, la disposizione fosse applicabile ai rapporti tra utenti e CASP, essa non offrirebbe copertura giuridica alle operazioni successive di *clustering*, *risk scoring* e de-anonimizzazione, che eccedono la nozione stessa di “monitoraggio finanziario” e costituiscono attività inferenziali autonome.

Neppure convince, infine, l'assimilazione agli accertamenti tecnici ex art. 359 Cpp, che presuppongono un oggetto già determinato sul quale l'esperto si limita a intervenire con competenze specialistiche, senza margini di scelta sul perimetro dell'indagine. Le indagini di cui si tratta procedono, invece, in senso inverso. In un primo momento viene condotta un'attività investigativa volta a scandagliare la rete e il registro *blockchain*: un'attività che va più propriamente assimilata a un mezzo di ricerca della prova. Solo in un secondo momento gli elementi così individuati vengono sottoposti a valutazione tecnica. Le due fasi, tuttavia, non sono scindibili, perché il modo in cui i dati vengono selezionati determina già, a monte, l'esito dell'analisi successiva. Non si può, dunque, ricondurre la *blockchain analysis* nel suo complesso alla figura dell'accertamento tecnico, che ne coglierebbe al più la fase valutativa finale,

¹²² Sull'estensibilità di questo strumento di indagine anche ai procedimenti in cui non viene in rilievo un ordine europeo di indagine penale, v. M. Caianiello, *L'attuazione della direttiva sull'ordine europeo di indagine penale e le sue ricadute nel campo del diritto probatorio*, in CP 2018, 2206; G. Lasagni, *Banking Supervision*, cit., 303.

¹²³ J. Della Torre, *Cripto-attività e giustizia penale*, cit., 422 s., che qualifica l'accostamento come inadeguato, ma non del tutto impraticabile.

¹²⁴ G. Lasagni, *Banking Supervision*, cit., 303.

lasciando priva di base normativa quella, preliminare e non meno rilevante, di individuazione e selezione dei dati¹²⁵.

Esclusa la riconducibilità della *blockchain analysis* alle specifiche categorie legali sin qui esaminate, resta da verificare se una base normativa adeguata possa essere individuata nei poteri investigativi generali che gli artt. 55, 348 e 358 Cpp attribuiscono, rispettivamente, alla polizia giudiziaria e al pubblico ministero.

Il parametro di riferimento è, ancora, il canone di qualità della legge ricostruito *supra* (§ 3.2), nella declinazione che di esso hanno dato le Corti di Strasburgo e di Lussemburgo in materia di sorveglianza e di trattamento sistematico di dati personali per finalità di prevenzione e repressione dei reati. Anche qui la risposta pare essere negativa: si tratta di previsioni che conferiscono ampi poteri di iniziativa, ma non indicano i casi e i modi in cui possono essere svolte specifiche attività investigative, né predispongono altre garanzie procedurali sufficienti. Pertanto, il loro impiego come base normativa sarebbe incompatibile con lo standard ricavabile dagli artt. 8 Cedu e 7 e 8 della Carta.

In assenza di un inquadramento entro categorie tipiche, l'unica opzione rimanente potrebbe essere quella dell'art. 189 Cpp, che disciplina le prove atipiche. La disposizione nasce proprio per consentire al sistema di accogliere le innovazioni tecnologiche senza sacrificare le garanzie difensive¹²⁶ e subordina l'ammissione della prova non regolata dalla legge a tre condizioni: che lo strumento sia idoneo ad accertare i fatti, che non incida sulla libertà morale della persona, che le modalità di assunzione siano discusse nel contraddittorio tra le parti.

Tuttavia, l'utilità della norma rispetto alle attività di analisi della *blockchain* è molto limitata. In termini di garanzia, l'art. 189 Cpp difficilmente supera il vaglio degli artt. 8 Cedu e 7 e 8 della Carta quando queste tecniche sono impiegate per forme di profilazione sistematica: mancano una delimitazione dell'ambito applicativo, una tipizzazione delle ipotesi in cui la misura può essere adottata e una procedura che preveda l'autorizzazione di un giudice¹²⁷.

¹²⁵ Sul punto, *amplius*, J. Della Torre, *Cripto-attività e giustizia penale*, cit., 426 s.

¹²⁶ *Relazione al progetto preliminare del codice di procedura penale*, in G.U. 24.10.1988 n. 250, 121, che qualifica l'art. 189 Cpp come «soluzione intermedia» volta ad aprire il sistema all'innovazione tecnologica senza compromissione delle garanzie difensive.

¹²⁷ J. Della Torre, *Cripto-attività e giustizia penale*, cit., 432 s., che rileva l'insufficienza dell'art. 189 Cpp quale base legale per l'impiego investigativo di strumenti algoritmici ad alta capacità intrusiva. Per uno studio sistematico sul principio di proporzionalità si veda M. Caianiello, *Il principio di proporzionalità nel procedimento penale*, in *DPenCont* 2014, 143 ss., e D. Negri, *Compressione dei diritti di libertà e principio di proporzionalità davanti alle sfide del processo penale contemporaneo*, in *RIDPP* 2020, 3 ss.

Il punto più problematico, però, riguarda i requisiti interni della disposizione. I software commercialmente più diffusi sono applicativi proprietari, protetti dal segreto industriale e caratterizzati da un elevato grado di opacità, tanto nel funzionamento interno quanto nei tassi di errore. Tali caratteristiche si conciliano difficilmente con il requisito di idoneità all'accertamento dei fatti richiesto dall'art. 189 Cpp, la cui verifica compete anzitutto al giudice, chiamato a valutarla quale condizione di ammissibilità della prova atipica. Le stesse caratteristiche si conciliano altrettanto difficilmente con il diritto al *fair trial*: come illustrato *supra* (§ 4.2), la parità delle armi esige che la difesa possa esaminare in modo sufficientemente dettagliato il funzionamento del software, e non i soli *output*. In questa prospettiva si colloca anche la giurisprudenza della Corte di giustizia, che impone al giudice nazionale di escludere dal giudizio la prova digitale rispetto alla quale una parte non sia stata posta in condizione di formulare efficacemente le proprie osservazioni, quando tale prova risulti idonea a influire in modo preponderante sull'accertamento dei fatti.

Ne consegue che, a normativa vigente, la sanzione sul piano processuale non può che essere l'inutilizzabilità *ex art.* 191 Cpp¹²⁸.

Proprio perché prevedibilmente inammissibili in giudizio, nella prassi investigativa le informazioni provenienti dalla *blockchain analysis* sono sovente impiegate come meri spunti investigativi e successivamente riscontrate attraverso atti di indagine tradizionali¹²⁹, quali perquisizioni, sequestri o richieste di dati agli *exchange*.

Gli applicativi operano, così, non come fonti dirette di prova, bensì quali strumenti funzionali a orientare successive attività di indagine formalmente tipiche che finiscono per costituire gli unici elementi utilizzabili in sede processuale, pur restando causalmente dipendenti dall'*output* algoritmico a monte.

Lungi dal risolvere la tensione sottostante, un simile *modus operandi* la rende ancor più evidente. Sul piano della tutela della riservatezza, l'impiego dello strumento a soli fini investigativi non muta i termini della violazione: l'assenza di una base giuridica idonea a disciplinarne condizioni e modalità d'uso determina comunque un'ingerenza nella vita privata contraria agli artt. 8 Cedu e 7-8 della Carta di Nizza, indipendentemente dall'utilizzo che dei relativi dati venga poi fatto in giudizio. Sul piano processuale, il quadro si presenta invece più sfumato, poiché la sanzione dell'inutilizzabilità opera diversamente a seconda che l'elemento raccolto sia destinato

¹²⁸ In questo senso anche J. Della Torre, *Cripto-attività e giustizia penale*, cit., 438 ss.

¹²⁹ Cfr. K. Ligeti, op. cit., 6, ove l'Autrice, con riferimento ai sistemi di intelligenza artificiale impiegati a fini investigativi definisce tale prassi come «*lead-only paradox*».

a un impiego meramente investigativo o a un impiego probatorio in senso proprio. In definitiva, per un verso, tale prassi riduce il potenziale probatorio diretto degli strumenti impiegati, impedendo agli inquirenti di spenderne direttamente gli *output* in sede processuale; per altro verso, in assenza di un quadro regolamentare chiaro, le conseguenze della lacuna legislativa finiscono comunque per scaricarsi sull'accusato, che subisce gli svantaggi derivanti dalla mancata definizione delle condizioni di liceità, trasparenza e contestabilità di tali tecniche¹³⁰.

In conclusione, i dati *on-chain*, se acquisiti con modalità tecnicamente verificabili, possono entrare nel processo come prova documentale *ex art.* 234 Cpp; sensibilmente diversa è la sorte degli *output* dei software di *blockchain analysis*. Infatti, le operazioni di tracciamento sistematico, *clustering* e de-anonimizzazione sollevano tensioni serie con i diritti fondamentali e con le garanzie processuali che conducono all'inutilizzabilità della prova ai sensi del combinato disposto degli artt. 189 e 191 Cpp.

6. Prima di volgere alle conclusioni, conviene delineare alcune possibili risposte ai problemi sin qui esaminati. Le proposte che seguono procedono dalle misure più strutturali e di lungo termine a quelle immediatamente azionabili dagli operatori e dalle corti, rappresentando ovviamente soltanto alcuni dei possibili approcci a un problema ancora in evoluzione. Dall'analisi condotta emergono due esigenze di fondo: da un lato, definire per via legislativa le condizioni di liceità dell'impiego investigativo della *blockchain analysis*, così da renderlo compatibile con gli standard convenzionali ed eurounitari; dall'altro, assicurare che gli esiti inferenziali dei software impiegati siano effettivamente contestabili dalla difesa.

Sul piano interno, la prima e più urgente esigenza di carattere strutturale è l'introduzione di una disciplina legislativa che regoli, in modo specifico, il monitoraggio investigativo della rete *blockchain* e, al suo interno, l'impiego della *blockchain analysis*. Il catalogo delle garanzie che tale disciplina dovrebbe recepire riflette, com'è evidente, il nucleo minimo elaborato dalla giurisprudenza di Strasburgo

¹³⁰ Il ragionamento è svolto, con specifico riguardo alla *blockchain analysis*, da J. Della Torre, *Cripto-attività e giustizia penale*, cit., 438-441, il quale evidenzia come la sopravvivenza di tale prassi dipenda in larga misura dall'accoglimento da parte della giurisprudenza della teoria del *male captum bene retentum*, che, negando la trasmissione del vizio agli atti derivati, depotenzia l'operatività dell'art. 191 Cpp e finisce per legittimare una forma surrettizia di recupero della prova acquisita in violazione di legge. Di qui la necessità che la sanzione dell'inutilizzabilità trovi applicazione già in sede di indagini preliminari, coerentemente con la duplice funzione dell'art. 191 Cpp, chiamato non soltanto a impedire l'ingresso nel procedimento di prove vietate, ma anche a privare di qualsiasi efficacia gli elementi raccolti *contra legem*: diversamente opinando, lo strumento computazionale continuerebbe a orientare l'intera sequenza probatoria, e la sanzione processuale risulterebbe svuotata sul piano applicativo.

e di Lussemburgo in materia di sorveglianza e di trattamento sistematico di dati personali per finalità di prevenzione e repressione dei reati (*supra*, § 3.2). La disciplina dovrebbe prevedere, in particolare: la delimitazione dell'ambito applicativo in funzione della gravità dei reati e delle categorie di soggetti interessati, la fissazione di limiti temporali, la regolamentazione puntuale delle modalità di trattamento e cancellazione dei dati acquisiti, la subordinazione delle tecniche a maggiore invasività all'autorizzazione preventiva dell'autorità giurisdizionale, la predisposizione di un rimedio effettivo in favore dell'interessato per dolarsi di trattamenti illeciti.

Allargando l'angolo visuale, una soluzione percorribile sul lungo periodo consisterebbe nel progressivo abbandono degli strumenti analitici proprietari, controllati da privati, nei contesti di giustizia penale, a vantaggio di software di *blockchain analysis* sviluppati e gestiti da autorità pubbliche¹³¹. Una simile soluzione ridurrebbe la dipendenza dal prodotto proprietario e consentirebbe, almeno in linea teorica, di concepire strumenti trasparenti *by design*¹³², sufficientemente interpretabili e idonei a operare in modo compatibile con i diritti fondamentali delle persone interessate. Il loro sviluppo in mano pubblica varrebbe a superare la specifica criticità rappresentata dal segreto industriale e dall'opacità commerciale, segnando un avanzamento non trascurabile. Si tratta, peraltro, di una prospettiva non priva di ostacoli: la progettazione e la manutenzione di strumenti di questo genere comporterebbero costi rilevanti e richiederebbero competenze tecniche specialistiche che le amministrazioni non sempre possiedono o riescono a conservare nel tempo. Ciò non escluderebbe, inoltre, la possibilità di opporre il segreto di Stato: la delimitazione del relativo ambito applicativo e il suo raccordo con i principi di trasparenza e con le garanzie processuali costituiscono, da questo punto di vista, questioni di particolare delicatezza, meritevoli di autonomo e ulteriore approfondimento.

Peraltro, alla luce della dimensione spiccatamente transnazionale dei *crypto-crime*, l'opzione più appropriata appare quella di sviluppare strumenti di questo tipo su scala europea. Ciò favorirebbe lo sviluppo di standard comuni, almeno a livello investigativo

¹³¹ V. K. Ligeti, op. cit., 32, la quale segnala che software di questo tipo sono già operativi in alcuni contesti europei. Si fa riferimento, ad esempio, all'iniziativa sviluppata dall'Unità di Informazione Finanziaria del Lussemburgo, nonché a NIKI, un sistema di IA sviluppato internamente dalle autorità inquirenti della Bassa Sassonia (Germania) per individuare materiale di abuso sessuale su minori nei dispositivi di memoria sequestrati e nei telefoni cellulari.

¹³² Sul punto, con un giudizio lapidario, J. Della Torre, *Cripto-attività e giustizia penale*, cit., 361, afferma che «dare rilievo a tali istanze di “capitalismo giudiziario” significa rischiare di comprimere principi fondamentali quali il contraddittorio, la parità delle armi e la trasparenza algoritmica, che non possono essere sacrificati sull'altare di meri interessi commerciali o della volontà di preservare il segreto industriale di un applicativo».

e operativo, suscettibili di fungere da premessa alla più ambiziosa elaborazione di standard probatori condivisi a livello sovranazionale, in attuazione dell'art. 82, par. 2, TFUE. In questa direzione, un'ipotesi normativa consisterebbe nel collegare l'ammissibilità della prova digitale alla sua validità scientifica, vincolando così la discrezionalità legislativa e giudiziaria e stabilendo una regola tecnicamente fondata¹³³.

Più in generale, il crescente ricorso a strumenti di *blockchain analysis* richiede un ripensamento dei confini tradizionali della procedura penale. Laddove le informazioni guidino l'attività investigativa, indipendentemente dal fatto che siano poi utilizzate nel processo come prova, il diritto processuale non dovrebbe restare indifferente rispetto a quella fase di elaborazione analitica che, orientando la direzione delle indagini e la scelta degli atti successivi, può avere ripercussioni significative sulla decisione. Sul piano generale, comune a ogni forma di prova algoritmica e *AI generated*, occorre porre le condizioni tecniche e giuridiche che rendano tale prova realmente contestabile. Ciò richiede standard minimi di trasparenza su metodologia e tassi di errore: un chiaro obbligo di documentare in modo esaustivo le attività operative svolte – il software impiegato, le operazioni OSINT, i dataset utilizzati, le ipotesi e gli obiettivi che guidano l'analisi, le autorità coinvolte e le procedure di validazione applicate ai risultati – assicurerebbe un controllo effettivo sulle pratiche di *law enforcement*, prevenendo impieghi tecnologici arbitrari o opachi e consentendo al difensore di comprendere le premesse e lo sviluppo delle ipotesi investigative, salvaguardando così l'effettività del diritto di difesa.

Sul punto, occorre segnalare che nemmeno il recente D. Lgs. 9 settembre 2026 n. 160, volto a adeguare l'ordinamento interno all'AI Act in materia di utilizzo dei sistemi di intelligenza artificiale per l'attività di polizia, offre soluzioni ai temi qui affrontati. L'unica disposizione di respiro generale applicabile ai sistemi di IA impiegati dalle forze di polizia è l'art. 3, co. 4. La norma si limita a richiedere una «revisione umana qualificata dei risultati delle elaborazioni automatiche prima del loro impiego in atti e provvedimenti incidenti sulla sfera giuridica degli interessati», obbligando anche la polizia giudiziaria a «documentar[la] in modo da assicurarne la tracciabilità». Non ne precisa, tuttavia, il contenuto minimo né eventuali sanzioni in caso di inosservanza. Sull'idoneità di tale disposizione a colmare il vuoto normativo segnalato, pertanto, è lecito dubitare.

¹³³ Per un'analisi più approfondita e ulteriori spunti sul tema, v. G. Lasagni, *Admissibility of Digital Evidence*, cit., 148.

In ogni caso, anche in assenza di innovazioni legislative, un miglioramento appare possibile già in via interpretativa, benché di per sé non sufficiente. In particolare, la difesa, unitamente al proprio consulente tecnico, dovrebbe essere posta in condizione di accedere al software a disposizione dell'autorità inquirente e di utilizzarlo, in condizioni controllate¹³⁴. La difesa non dovrebbe essere confinata alla contestazione degli *output* finali, ma dovrebbe poter verificare in modo appropriato le modalità con cui tali *output* sono stati generati¹³⁵. Ciò consentirebbe una forma concreta – seppur, lo si ribadisce, non completamente soddisfacente – di contraddittorio tecnico e contribuirebbe a ridurre l'attuale divario economico e tecnologico. Una simile soluzione, ovviamente, presuppone che alla difesa siano assicurate anche le risorse necessarie per avvalersene, ma può costituire, sin d'ora, un primo punto di partenza.

7. Le riflessioni sin qui condotte convergono verso un'unica conclusione: se i diritti fondamentali nel processo penale meritano di essere presi sul serio, l'impiego investigativo dei software di *blockchain analysis* non può continuare a muoversi in un'area sostanzialmente sottratta alle regole di diritto. L'aggregazione sistematica e su larga scala dei dati, unita all'opacità proprietaria degli strumenti impiegati, reclama un quadro normativo capace di definire tanto le condizioni di liceità del trattamento, quanto le garanzie che ne rendono contestabile l'esito probatorio nel processo.

L'indagine comparata ha rivelato due traiettorie divergenti. La giurisprudenza statunitense ha finora relegato ai margini dell'irrilevanza giuridica sia le implicazioni della *blockchain analysis* sulla riservatezza – attraverso un'applicazione estensiva della *third-party doctrine* – sia le criticità metodologiche dei suoi risultati, filtrate da uno scrutinio *Daubert* condotto con mano leggera. Il diritto europeo muove da premesse opposte: ogni ingerenza qualificata nella sfera privata esige una base legale precisa e

¹³⁴ In senso convergente, con specifica attenzione alla disparità economica che rende tali strumenti spesso inaccessibili persino ai consulenti tecnici della difesa, v. J. Della Torre, *Cripto-attività e giustizia penale*, cit., 380 s.

¹³⁵ Tale possibilità per la difesa, già attuata in vari contesti negli Stati Uniti, è stata nondimeno criticata a causa delle significative limitazioni pratiche imposte al difensore. Ad esempio, ai periti della difesa è tipicamente concesso un accesso *una tantum*, in presenza, presso gli uffici del consulente legale della società, sotto la diretta supervisione di un rappresentante della società stessa. L'accesso è fornito su un *computer* privo di connessione a Internet e alla difesa è normalmente consentito soltanto di prendere appunti durante l'ispezione o di richiedere copie cartacee di porzioni limitate del codice sorgente. In tali condizioni, diversi studiosi e operatori del diritto hanno messo in dubbio l'effettività di tali garanzie, ritenendole in larga misura illusorie. Sul tema v. N. Murphy, *Give Me Liberty or Give Me the Source Code: Challenging a Black-Box Computer Algorithm Under Daubert*, in *Richmond Journal of Law and Technology* 2024 (30), 348.

proporzionata e alla difesa deve essere garantita una possibilità reale di misurarsi con la prova generata da sistemi automatizzati.

In questo confronto, l'ordinamento italiano rivela tutta la propria vulnerabilità. Gli strumenti di analisi della *blockchain* occupano uno spazio normativo rimasto pressoché vuoto, in cui al rapido affinarsi delle prassi investigative non ha fatto seguito alcun intervento legislativo di rilievo.

Se i dati *on-chain* possono ancora trovare cittadinanza nel processo come prova documentale, gli esiti inferenziali dei software di analisi restano privi di un ancoraggio normativo soddisfacente e il richiamo all'art. 189 Cpp si scontra con ostacoli non superabili quando il software si presenta opaco, proprietario e sottratto a un effettivo controllo difensivo, con conseguente inutilizzabilità *ex art.* 191 Cpp.

Fino a quando questa cornice mancherà, la *blockchain analysis* continuerà a produrre ingerenze invasive nella vita privata e compressioni significative del diritto a un giusto processo. Muovendo da queste premesse, un intervento legislativo, nei termini già indicati (*supra*, § 6), non appare più procrastinabile. La sede più naturale resta quella sovranazionale: l'art. 82, par. 2, TFUE abilita l'Unione europea all'adozione di norme minime in materia probatoria e, in un settore intrinsecamente segnato dalla dimensione transfrontaliera del crimine, solo una disciplina comune può garantire prevedibilità degli standard di ammissibilità e circolazione affidabile della prova. Ciò non esclude, beninteso, che il legislatore nazionale possa intervenire in via autonoma, in assenza o in attesa di un'iniziativa europea. L'obiettivo, in ogni caso, resta quello di definire le condizioni di liceità di queste indagini e di garantire che la metodologia sottesa agli esiti inferenziali sia trasparente e verificabile al punto da reggere il vaglio del contraddittorio.

Un quadro legislativo chiaro e coerente è pertanto essenziale per conciliare l'efficienza investigativa con la tutela dei diritti fondamentali. Una regolamentazione adeguata non indebolirebbe l'azione di contrasto; al contrario, la rafforzerebbe, accrescendo l'affidabilità della prova prodotta e la possibilità di circolazione transfrontaliera. Al contempo, garantirebbe che i diritti fondamentali operino come parametri strutturali dell'azione investigativa, e non come limiti residuali invocabili solo *ex post*. In questo modo, l'intervento legislativo realizzerebbe un duplice obiettivo: rafforzare la repressione della criminalità legata alle cripto-attività, elevando al contempo il livello di tutela riconosciuto ai diritti fondamentali delle persone coinvolte.