Lotta alle frodi e alle falsificazioni di mezzi di pagamento diversi dai contanti, tra diritto alla privacy e diritto di difesa del cittadino

Alberto Liguori*

Ricevuto 22 dicembre 2025 – Accettato 26 gennaio 2026

Sommario

L'autore analizza la disciplina sanzionatoria, nazionale ed europea, relativa alle frodi e alle falsificazioni dei mezzi di pagamento diversi dal denaro contante, partendo dalla constatazione del crescente interesse delle organizzazioni criminali per il mercato finanziario delle monete digitali. Codeste organizzazioni sono in grado di trasformare capitali acquisiti illecitamente in criptovalute, le quali rendono molto difficile la tracciabilità. L'autore rileva le difficoltà del sistema processualpenalistico a fronteggiare tali illeciti, soprattutto con riguardo alla ricerca dei mezzi di prova, e auspica un intervento maggiormente incisivo da parte del legislatore, anche a livello europeo, che garantisca un maggiore spazio di intervento del Pubblico Ministero nel corso delle indagini.

Parole chiave: criptovalute, blockchain, privacy, intelligenza artificiale, frode, falsificazione

* Procuratore della Repubblica presso il Tribunale di Civitavecchia. alberto.liguori@giustizia.it.

De Iustitia et Iure (ISSNe 3103-2761), 2/2025
DOI: 10.3280/ius2025oa21755

Combating fraud and counterfeiting of non-cash means of payment: between the right to privacy and the citizen's right of defence

Abstract

The author examines the national and European sanctioning framework governing fraud and the counterfeiting of non-cash payment instruments, in light of the growing interest shown by criminal organizations in the digital currency financial market. Such organizations are capable of converting illicitly acquired capital into cryptocurrencies, thereby rendering traceability significantly more difficult. The author highlights the challenges faced by the criminal procedural system in tackling these illicit activities, particularly concerning the gathering of evidence, and advocates for more robust legislative intervention, including at the European level, to grant the Public Prosecutor broader investigative powers.

Keywords: cryptocurrencies, blockchain, privacy, artificial intelligence, fraud, counterfeiting

1. Premessa

Nel corso del corrente anno, la Direzione Investigativa Antimafia ha confermato anche per l'anno 2024 il crescente interesse delle organizzazioni criminali per il mercato finanziario delle monete digitali in ragione della convenienza offerta dal regime di semianonimato che governa il settore: l'archivio digitale delle transazioni è condiviso tra i soli utenti, accessibile a mezzo chiavi di accesso crittografate dei portafogli elettronici (wallet). Completa il quadro la visibilità pubblica delle operazioni, ma senza possibilità alcuna di essere collegate a persone fisiche o giuridiche. Il meccanismo negoziale incontra il *favor* criminale visto come strumento utile per la lavanderia di capitali illecitamente acquisiti trasformati in criptovalute, delocalizzati, le cui movimentazioni sfuggono alla tracciabilità.

2. La disciplina europea e nazionale vigente

L'aumento e l'intensificazione degli scambi commerciali in via digitale viaggia di pari passo con l'aumento dei rischi di frodi e

falsificazioni informatiche. Di recente, il mercato digitale delle criptovalute ha ricevuto un potenziamento normativo europeo grazie al REG UE 1114/2023, ratificato nel nostro Paese con il DLGS 129/2024, nel tentativo di armonizzare il settore, individuando nella Banca d'Italia e nella Consob i due organismi nazionali deputati alla vigilanza e al controllo, in specie in vista della cooperazione amministrativa transfrontaliera, munendoli di poteri d'indagine, cautelari e sanzionatori per il perseguimento degli obblighi di trasparenza richiesti agli operatori finanziari, obbligandoli alla licenza d'esercizio. Rafforza l'apparato normativo la recente L 90/2024 che fortifica la cybersicurezza inasprendo le pene per i reati informatici e conferendo la competenza penale alla Procura distrettuale. Già in precedenza, con la L 184/2021 il Legislatore è intervenuto nel settore del diritto penale sostanziale: a) con l'intervento sul CP 493 *ter* aggiungendo, all'indebito utilizzo di carte di credito o di pagamento, qualsiasi altro strumento diverso dai contanti e punendo anche il falsificatore o alteratore come il possessore, il cedente o acquirente di tali strumenti o documenti di provenienza illecita; b) con la previsione del CP 493 *quater* che offre la definizione dei dispositivi o altri mezzi progettati per commettere uno dei reati riguardanti strumenti di pagamento diverso dai contanti; c) con l'intervento sul CP 640 *ter* (la frode informatica). La novella aggiunge al secondo comma una nuova circostanza aggravante quando la condotta incriminata produce un trasferimento di danaro, di valore monetario o di valuta virtuale; d) con l'intervento sul DLGS 231/2001. Si arricchisce il catalogo dei reati commessi nell'interesse o a vantaggio di una persona giuridica inserendo quelli commessi con mezzi di pagamento diversi dal contante, con responsabilità amministrativa diretta dell'ente.

3. Mezzi di ricerca della prova e limiti della legge processuale penale italiana per contrastare gli investimenti della criminalità comune ed organizzata in criptovalute. L'assenza di una disciplina processuale

Moneta elettronica e moneta virtuale offrono il vantaggio di consentire pagamenti a distanza ma è, soprattutto, la seconda a garantire forme di anonimato circa l'identità dei protagonisti dell'operazione finanziaria confidando sullo sfruttamento della crittografia che usa specifici algoritmi matematici per creare una raccolta di dati in continua crescita, i quali possono unicamente essere aggiunti ma non rimossi. Il blockchain è un registro digitale che contiene dati condivisi da vari blocchi (ledgers) e gestito da una rete di server, detti nodes. Nel meccanismo si inserisce il wallet (il detentore del portafoglio) che ha disposto o ricevuto l'operazione che rimane noto, mentre rimane anonimo il possessore, come avviene per la moneta contante o elettronica. Il protocollo della Blockchain (catena di nodi) non richiede per i Bitcoin alcuna identificazione e verifica dei partecipanti, né fornisce uno storico dei movimenti avvenuti, collegati a soggetti necessariamente esistenti nel mondo reale. La criminalità organizzata da tempo ha intuito i vantaggi di un sistema che garantisce una sorta di semianonimato, luogo ideale per investire proventi illeciti, consapevoli delle difficoltà investigative in fase di tracciamento dei movimenti finanziari.

La consapevolezza di muoversi in una sorta di zona franca aumenta allorquando si è costretti a constatare come in realtà nel nostro sistema europeo, e italiano in particolare, se da una parte la legislazione penale sostanziale ha cercato di tipizzare il fenomeno coprendo l'intera fenomenologia, dall'altra manca completamente la normativa processuale volta a regolamentare le modalità di identificazione di conti in criptovalute, spesso accesi all'estero, per svelare l'identità dei protagonisti dell'operazione negoziale, rivelandone indirizzi, Pin, PW, anche per poi procedere alla c.d. ablazione dei portafogli digitali e alla conseguente monetizzazione del valore solo virtuale. In mancanza di apposito Regolamento europeo, l'unico strumento di lavoro rimane il CPP 696 avente ad oggetto i rapporti giurisdizionali con autorità straniere e che affida al diritto unionale la disciplina di quelli tra i Paesi UE,

mentre deve far ricorso alle convenzioni internazionali per i rapporti con i Paesi extra UE e a quelle convenzionali bilaterali ove esistenti.

Le indagini preliminari aventi ad oggetto fattispecie delittuose commesse con l'uso di moneta digitale devono confrontarsi, quindi, con le difficoltà di identificazione del provider, di eventuale mancanza di collaborazione del service provider, di quadro giuridico vigente nel Paese richiesto, in materia di conservazione dei dati. Il tutto condito con il limite temporale della durata delle indagini preliminari che in Italia oscilla da un anno e sei mesi a due anni. In questo arco temporale le inchieste avviate devono concludersi. Con questo scenario e con gli strumenti processuali messi a disposizione del P.M., occorre avventurarsi e provare che un wallet sia di natura mafiosa per poi successivamente tentare di sequestrare un valore digitale che non ha né una banca né sportelli. Sul tavolo del pubblico ministero, il procedimento penale, di norma, nasce da una c.d. S.O.S., segnalazione di operazione sospetta, veicolata dall'U.I.F. della Banca d'Italia per il tramite della Guardia di Finanza. Normalmente l'operazione sospetta è intestata ad un soggetto incensurato, amministratore di una società che presenta elevati indici di rischio. Da una parte, manca una sede operativa, non esiste un deposito e i dipendenti sono irreperibili, dall'altra, vi è emissione di numerose fatture a fronte di movimenti finanziari inesistenti; in sintesi la classica cartiera che apre conti correnti in criptovalute, all'interno dei quali far transitare capitali illecitamente acquisiti per poi sparire nell'arco di 12/18 mesi. Le mafie si trasformano passando dalle armi ai bonifici. A questo punto, con quali armi è possibile fronteggiare i cybercriminali?

4. Le banche dati e i diritti fondamentali della privacy e della difesa. Il ruolo dell'intelligenza artificiale

Forte è l'impegno delle Forze dell'ordine nell'attuale fase di creazione e alimentazione di banche dati, in grado di studiare il mercato digitale alla ricerca di informazioni utili per poi incrociarle e ricostruire attorno ai movimenti finanziari il legame che lega taluni soggetti. Ma queste operazioni incontrano il limite della c.d. pesca a

strascico: non è consentita la raccolta di dati indistinti, perché è concreto il rischio di minare diritti fondamentali dei sospettati, quali il diritto alla privacy. Insegna la giurisprudenza europea CEDU e CGUE che per de-anonimizzare le transazioni economiche e finanziarie serve rispettare CEDU 8 e Carta di Nizza 7 e 8; l'autorità giudiziaria deve assicurare lo standard minimo di garanzie delle persone e per fare questo serve: a) l'intervento normativo primario del Legislatore che disciplini tempi e modalità dei poteri intrusivi cautelari del P.M.; b) la consumazione di un reato di criminalità organizzata; c) il potere cautelare deve essere motivato espressamente e guidato dal principio di proporzionalità nella scelta delle misure da mettere in campo. Legittima la lettura europea il nostro sistema processuale penale previsto da CPP 189 e 348 e 234 *bis*.

Anche l'I.A. incontra i medesimi limiti del potere cautelare; la raccolta dei dati e la creazione di software di intelligence investigativa scontano la mancanza di una normativa processuale che legittimi il ricorso all'I.A. nel campo delle indagini preliminari. Non c'è alcuna fonte che disciplini la fase di formazione della banca dati e dell'algoritmo che la governa, con conseguente impossibilità dell'interessato di poter svolgere il controllo sull'esattezza delle informazioni raccolte e con patente violazione di COST. 24 declinata in CPP 189 e 19. Insomma, la mancanza di una regolamentazione primaria dello strumento dell'intelligenza artificiale rende concreto il pericolo di cultura investigativa votata al sospetto. Le S.O.S. risentono di questo clima: l'iscrizione è curata nel registro degli atti non costituenti reato, senza termini per il compimento delle indagini preliminari e con la messa a disposizione del P.M. di documentazione amministrativa di varia natura, il quale è, poi, onerato di delegare la polizia giudiziaria operante per la ricerca all'interno del software di elementi utili per la lo sviluppo di spunti investigativi, con l'unico limite del divieto di svolgere atti istruttori che prevedano la partecipazione del difensore. La possibilità di variare l'iscrizione al registro delle notizie di reato da fatti non reato a fatti reato è resa ancor di più impervia in ragione della riforma Cartabia che ha rivisto CPP 335: l'iscrizione a registro notizie di reato a carico di noti, richiede la comunicazione da parte della p.g. operante di un fatto determinato attribuibile oggettivamente e soggettivamente

ad un determinato soggetto, attinto da un convergente quadro indiziario. Serve un qualcosa in più di una serie di dati incrociati per passare dal sospetto all'indizio, anche per un'eventuale iscrizione a Registro ignoti, utile per un'eventuale attività intrusiva nella vita delle persone. Ma anche laddove si addivenisse ad una tale trasformazione, il P.M. vedrebbe limitato il suo potere d'azione in quanto, per il potere di sequestro e di confisca di monete virtuali, la nostra legge processuale penale non prevede le modalità di acquisizione–ablazione. Sul punto la DIR. UE 2014/1260 rimette la questione al potere degli Stati membri e lo Stato italiano non vi ha provveduto. E, infine, anche per l'utilizzo del trojan attraverso l'inoculazione nello smartphone o in un PC di un virus per favorire con microfono e fotocamera conversazioni e digitazioni di PW/PIN per decodificare un wallet crittografato, serve l'intercettazione ambientale che per i reati ordinari presuppone che l'attività criminosa sia in corso, con oggettiva impossibilità di provare la circostanza con gli ordinari poteri istruttori.

5. Criptovalute: rilevanza fiscale e tributaria

L'inquadramento fiscale delle criptovalute e dei redditi ad esse correlate concorrono alla formazione della base imponibile delle imposte sui redditi e pertanto la relativa non dichiarazione può comportare, nel caso in cui vengano superate le soglie di rilevanza, la configurazione dei reati tributari. Sottosoglia l'illecito avrà natura amministrativa. Discorso diverso per l'imposta sul valore aggiunto, dove i redditi relativi alla conversione o scambio di criptovalute rientra tra le operazioni esenti.

Resta da esaminare il tema dell'utilizzabilità delle prove digitali nel processo tributario. Sul punto si registra uno scarso utilizzo di detto strumento di prova sia da parte delle Agenzie delle Entrate sia da parte dei contribuenti. Le ragioni risiedono nella prova principe del documento amministrativo (verbale di accertamento/cartella esattoriale) creato dall'agenzia fiscale e sul quale si forma la prova costruita fuori dal processo e non nel processo. Ragioni più strettamente giuridiche ne impediscono il pieno utilizzo, specie per la corrispondenza telematica senza firma digitale, con tutti i problemi di forma che presenta CC

2702: l'efficacia probatoria della scrittura privata è subordinata a requisiti formali tra i quali primeggia la sottoscrizione, superabile, allo stato, solo attraverso la prova testimoniale. Allo stato, messaggistica ed altre forme di scambio di informazioni prive di sottoscrizione, se prodotte innanzi alle commissioni tributarie, sono rimesse al libero giudizio del giudice tributario che potrà utilizzarla quale prova se acquisita con correttezza e con metodo affidabile senza rischi di contaminazione del dato e che ne consenta la ripetizione dell'operazione.

6. Conclusioni

La produzione penale offerta dal Legislatore necessita di maggiore determinatezza, auspicando una maggiore definizione e sottolineando che il mercato delle criptovalute ad oggi non è assistito da apposita regolamentazione, rivelandosi imperfetto un sistema che affida la disciplina al solo aspetto penale, poiché si tratta di materia di rilevanza primariamente di natura civilistica. Lo strumento sanzionatorio, tra pene detentive e sanzioni interdittive, tenuto conto della capacità imprenditoriale di molte società di investire capitali illeciti in valuta virtuale, specie in operazioni fiscali complesse e di difficile accertamento, avrebbe meritato anche altro tipo di sanzione che in Europa ha dimostrato efficacia deterrente, quali le sanzioni reputazionali che incidono sui profitti aziendali con danno all'immagine imprenditoriale. Sul fronte della criminalità comune, è avvertita la necessità di una adeguata formazione della polizia giudiziaria e degli uffici requirenti italiani, alle prese con la complessa acquisizione della prova digitale già sul suolo italico, essendo sufficiente pensare alle modalità complesse di svolgimento di ispezioni (CPP 244), perquisizioni informatiche (CPP 254 *bis*) e acquisizioni documentali all'estero (CPP 234 *bis*), tra genuinità/immodificabilità/conservazione del dato.

Passando al settore dei reati transfrontalieri, il quadro normativo esistente sconta i limiti della ricerca di tracce dei reati spesso contenute in server ubicati all'estero e, se l'acquisizione tra gli Stati aderenti alla Convenzione di Budapest del 2011 sulla criminalità informatica si presenta agevole, il quadro invece si complica allorquando la coopera-

zione giudiziaria intercorre con Stati non aderenti. In questo caso, il successo della prova digitale è su base volontaristica e presuppone il consenso all'acquisizione del dato da parte del legittimo proprietario (CPP 234 *bis*). Sul fronte della criminalizzata, ai limiti sopra esposti del quadro normativo, tenuto conto della professionalità criminale dei colletti bianchi, ancor di più è sentita la necessità di formare polizia giudiziaria in grado di fronteggiare la concorrenza criminale, specie per inseguire investitori all'estero e terroristi finanziati con criptovalute, nonché per smascherare aiuti in criptovalute a Paese sotto embargo per violazioni internazionali.

Infine, il versante fiscale. Se da un lato si perseguono redditi sopra soglia acquisiti tramite criptovalute, dall'altro si considerano le operazioni in valuta virtuale esenti da IVA. Invece, sarebbe prospettabile un sistema di calcolo della criptovaluta come unità di conto, partendo dal valore all'atto del deposito nel portafoglio digitale a quello in uscita. Per il processo tributario, l'attuale sistema probatorio fondato sulla prova documentale formata fuori dal processo (verbali di accertamento e cartelle esattoriali) pone dei limiti alla prova digitale sia per il Fisco sia per il contribuente specie per quelle, come normalmente accade, prive di sottoscrizione. Infatti, le operazioni sottoscritte rientrano a pieno nel regime di CC 2702, diversamente per quelle prive di sottoscrizione, l'ammissione e il valore probatorio delle quali è rimesso alla discrezionalità dell'a.g. che valuterà provenienza, contesto, metodo di acquisizione ripetibile della conversazione o scambio di informazioni del caso.

Infine, serve un forte monito al Legislatore, europeo e nazionale, per dettare le regole processuali di intervento del P.M. nella sfera dei diritti fondamentali dell'uomo, guidato dai principi europei e costituzionali della necessità e della proporzionalità per garantire il giusto equilibrio tra autorità e libertà.

Riferimenti bibliografici

Rogoff K. (2017). *The curse of cash*. Princeton University Press. DOI: 10.1515/9781400888726.