Alessandro Lega (*)

Criptovalute e attività illecite: strumenti normativi di contrasto e casi applicativi

PARTE I

La diffusione delle criptovalute e delle tecnologie basate su registri distribuiti ha inciso profondamente sui sistemi finanziari contemporanei. Accanto alle opportunità di innovazione e di efficientamento dei mercati, tali strumenti sono stati impiegati anche per finalità illecite, in particolare nella fase iniziale del loro sviluppo. Riciclaggio di proventi criminali, evasione fiscale, frodi informatiche e ransomware hanno beneficiato della natura transnazionale delle transazioni e della percezione di anonimato associata agli asset digitali[1].

[1] V. FATF, Virtual Assets and Virtual Asset Service Providers, 2019.

(*) Senior Corporate Security Advisor

Nell'Unione Europea il contrasto alle attività illecite in ambito cripto si fonda su un impianto regolatorio armonizzato. Il Regolamento (UE) 2023/1114 **(MiCA) ha introdotto un regime di autorizzazione e vigilanza per i fornitori di servizi in cripto-attività, imponendo requisiti di governance, trasparenza e presidi antiriciclaggio[2].** L'efficacia di tale approccio è emersa in diversi casi concreti, nei quali autorità nazionali di vigilanza hanno disposto la cessazione dell'operatività di exchange extra-UE privi di autorizzazione, accompagnata dal congelamento di fondi riconducibili a transazioni sospette[3]. Sul piano fiscale, la Direttiva (UE) 2023/2226 (DAC8) ha esteso lo scambio automatico di informazioni anche alle criptovalute. A partire **dal 1° gennaio 2026, le autorità fiscali nazionali ricevono dati sistematici sulle transazioni rilevanti** effettuate da residenti UE su piattaforme regolamentate. In più Stati membri, l'applicazione della direttiva ha consentito di individuare contribuenti che avevano accumulato rilevanti patrimoni digitali senza adeguata dichiarazione. In alcuni procedimenti, l'analisi dei flussi verso e da piattaforme regolamentate ha dimostrato la sproporzione tra redditi dichiarati e investimenti in cripto-attività, portando al recupero di imposte e sanzioni[4].

Travel Rule e investigazioni su frodi online in Europa

L'estensione della cosiddetta *Travel Rule* ai trasferimenti di cripto-attività ha inciso profondamente sull'operatività criminale. L'obbligo per gli intermediari di raccogliere e trasmettere le informazioni identificative di ordinanti e beneficiari ha consentito di ricostruire catene di pagamento complesse.

In un'indagine coordinata a livello europeo, una rete di truffatori attiva tramite falsi portali di investimento è stata smantellata grazie alla ricostruzione dei flussi in criptovalute e al collegamento dei wallet a soggetti identificati attraverso **procedure KYC[5].**

L'approccio statunitense: enforcement penale e sequestri

Negli Stati Uniti il contrasto alle attività illecite legate alle criptovalute si è sviluppato prevalentemente attraverso un approccio di **enforcement penale.** Il Dipartimento di Giustizia, l'FBI e l'IRS Criminal Investigation hanno fatto ampio uso di strumenti di blockchain analytics per ricostruire i flussi finanziari. Un caso emblematico è rappresentato dallo smantellamento di grandi marketplace del dark web, nei quali i pagamenti avvenivano prevalentemente in Bitcoin. In tali indagini, le autorità sono riuscite a identificare i gestori delle piattaforme e a sequestrare criptovalute per valori pari a centinaia di milioni di dollari[6]. Particolarmente rilevante è il contrasto ai ransomware. In una nota operazione federale, il Dipartimento di Giustizia ha annunciato il sequestro di Bitcoin versati come riscatto a un gruppo ransomware, dimostrando come i proventi illeciti possano essere recuperati quando transitano attraverso infrastrutture riconducibili a soggetti identificabili[7].

Genius Act

Un'ultima novità, approvata nel corso del 2025 negli USA, è il Genius act[8], che ha una applicazione graduale partita nel 2025 e che proseguirà fino al 2028. È una reazione al

---

[2] Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio.

[3] ESMA, Supervisory actions against unauthorized crypto-asset service providers, 2023–2024.

[4] Consiglio dell'UE, Direttiva (UE) 2023/2226 (DAC8).

[5] Europol, Internet Organised Crime Threat Assessment, edizioni recenti.

[6] U.S. Department of Justice, Press releases on darknet marketplace seizures.

[7] U.S. Department of Justice, Seizure of cryptocurrency linked to ransomware attacks.

[8] La differenza sostanziale può essere riassunta così: il MiCA è un codice onnicomprensivo nato per proteggere i consumatori e il mercato, mentre il GENIUS Act è una legge mirata nata per istituzionalizzare il dollaro digitale e rafforzare l'egemonia finanziaria statunitense.

MiCA introdotto in Europa alla quale gli Stati Uniti hanno reagito per contrastare il successo europeo, visto che stava attirando capitali e aziende grazie a regole chiare. **Il Genius act è intervenuto a difesa del Dollaro.** C'era infatti il timore che, senza una legge federale, le stablecoin potessero diventare uno strumento per l'evasione delle sanzioni o, al contrario, che stablecoin non denominate in dollari potessero minare l'egemonia del biglietto verde nel commercio digitale. Un altro modo per difendere l'economia USA.

DeFi, NFT e nuove frontiere dell'illecito

La finanza decentralizzata e il mercato degli NFT presentano profili di rischio emergenti sia in Europa sia negli Stati Uniti. Fenomeni di *wash trading* e *rug pull* hanno causato perdite rilevanti agli investitori. In alcune indagini statunitensi, l'analisi dei contratti intelligenti ha consentito di dimostrare la premeditazione delle condotte fraudolente, collegando più progetti apparentemente distinti agli stessi sviluppatori[9]. Analogamente, in Europa tali condotte iniziano a essere contestate sulla base delle norme in materia di frode e abuso di mercato.

Cooperazione internazionale e conclusioni

La dimensione globale delle criptovalute rende imprescindibile una cooperazione internazionale strutturata. Operazioni congiunte tra autorità europee e statunitensi, spesso coordinate da Europol, hanno dimostrato l'efficacia del partenariato transatlantico. I casi analizzati mostrano come l'idea delle criptovalute quali strumenti intrinsecamente anonimi risulti oggi superata. **L'integrazione tra regolazione, tecnologia investigativa e cooperazione internazionale ha progressivamente ridotto gli spazi di utilizzo illecito,** delineando un ecosistema in cui innovazione e legalità possono coesistere.

[9] SEC, Enforcement actions involving digital assets and DeFi, 2022–2024.

Riferimenti internazionali

Council of the European Union. (DAC8 del 2023)
https://eur-lex.europa.eu/eli/dir/2023/2226/oj

Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA)
https://eur-lex.europa.eu/eli/reg/2023/1114/oj

Supervisory actions against unauthorized crypto-asset service providers (2023-2024)
https://www.esma.europa.eu/market-analysis/financial-innovation-and-crypto-assets

Europol. (2022–2024). Internet organised crime threat assessment (IOCTA)
https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta

Federal Bureau of Investigation. (2021–2024). Internet crime report FBI
https://www.ic3.gov

Guidance for a risk-based approach. FATF.
https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

Bitcoin and cryptocurrency technologies: A comprehensive introduction
https://press.princeton.edu/books/hardcover/9780691171692/bitcoin-and-cryptocurrency-technologies

U.S. Department of Justice. (2020). Cryptocurrency enforcement framework
https://www.justice.gov/archives/ag/page/file/1326061/download

Press releases on cryptocurrency and ransomware cases. U.S. Department of Justice
https://www.justice.gov/opa/pr

U.S. Securities and Exchange Commission (2022–2024)
https://www.sec.gov/spotlight/cybersecurity-enforcement-actions