"FOLLOW THE VIRTUAL MONEY": EVOLUZIONI DELLE STRATEGIE DI CONTRASTO E NUOVI AFFARI DELLE MAFIE 4.0 (*)

VINCENZO MUSACCHIO (**)

Negli ultimi anni, la strategia investigativa inventata da Giovanni Falcone del "follow the money" si dovrà evolvere giocoforza in una nuova dimensione: quella digitale. Con la diffusione delle criptovalute e dei sistemi finanziari decentralizzati, le tecniche di indagine antimafia dovranno comprendere nei fatti il sistema del "follow the virtual money". Questo cambiamento non riguarda solo la tecnologia, ma anche il modo in cui le organizzazioni criminali — dalle storiche mafie italiane come Cosa Nostra, 'Ndrangheta e Camorra — operano e riciclano capitali illeciti. La transizione dal contesto fisico a quello digitale richiede un necessario ripensamento degli schemi investigativi consolidati e una revisione delle tecniche di indagine finanziaria, poiché le modalità di occultamento, trasferimento e integrazione dei proventi illeciti mutano in ragione delle caratteristiche intrinseche degli asset digitali.

Il riciclaggio di denaro tradizionalmente avveniva attraverso circuiti bancari, società di copertura o investimenti immobiliari, processi che lasciavano tracce documentali, circuiti contabili e responsabilità giuridiche in grado di essere analizzate e perseguite. Oggi, invece, le criptovalute come *bitcoin* o *ethereum* offrono nuovi strumenti: trasferimenti rapidi,

(*) Intervention at the conference entitled "Emerging Cybercrime Trends and Threats" - February 11, 2026, New York University (NYU) School of Law, New York City (USA).

(**) Professore di strategie di contrasto della criminalità organizzata – Associato al Rutgers Institute on Anti-Corruption Studies (RIACS) - Rutgers University Newark (USA).

pseudonimato e assenza di intermediari. Queste peculiarità determinano un profilo di rischio differente per le forze dell'ordine. Una transazione con bitcoin, ad esempio, può essere confermata in pochi minuti e inoltrata istantaneamente a controparti in altre giurisdizioni, rendendo inefficaci le tradizionali misure cautelari basate su procedimenti giudiziari ordinari. La possibilità di convertire fondi in stablecoin, token non fungibili (NFT) o di utilizzare protocolli di finanza decentralizzata (DeFi), inoltre, introduce ulteriori livelli di complessità nel tracciamento e nella valutazione del valore reale dei proventi.

Le "nuove mafie" hanno dimostrato una grande capacità di adattamento nei mercati globali, per cui se un tempo utilizzavano paradisi fiscali e società offshore, oggi si avvalgono di wallet digitali, exchange e piattaforme decentralizzate per spostare fondi in modo più difficile da intercettare. Esempi concreti includono l'uso di account su exchange centralizzati con KYC falsificati, la creazione di reti di wallet controllati da terzi per spezzare le catene di transazione e l'impiego di marketplace on-chain per riciclare valore. Questi adattamenti si affiancano a strategie tradizionali: investimenti immobiliari ed economici nel mondo reale rimangono strumenti fondamentali per "ripulire" capitali, spesso integrati in strutture ibride che combinano flussi fiat e cripto.

Le criptovalute attraggono la criminalità organizzata poiché le caratteristiche delle valute virtuali le rendono particolarmente appetibili per vari motivi. Le transazioni non sono direttamente collegate all'identità reale. Pur non garantendo anonimato assoluto, la pseudonimia può ostacolare l'identificazione del reale beneficiario se non si adottano metodologie investigative adeguate. Le monete virtuali consentono di attuare trasferimenti immediati oltre confine. Questa caratteristica facilita il frazionamento dei flussi e la dispersione geografica del valore, complicando le attività di sequestro e confisca. Sono difficilmente sequestrabili senza accesso alle chiavi private, i fondi restano irraggiungibili. Il controllo delle chiavi rappresenta il fulcro del possesso. La loro custodia in dispositivi

hardware o in servizi con custodia esterna può determinare la perdita definitiva dell'accesso da parte delle autorità.

Questi elementi favoriscono attività come il riciclaggio, il finanziamento illecito e persino il pagamento di riscatti nel cyberspazio. Nel fenomeno dei ransomware, ad esempio, si osserva una diffusione delle richieste di pagamento in criptovaluta: studi e rapporti di agenzie specializzate hanno evidenziato come una quota significativa dei riscatti sia stata richiesta e, in parte, corrisposta in bitcoin o in altre monete digitali. Analogamente, il traffico di stupefacenti e il commercio illecito online si sono evoluti su mercati darknet che spesso accettano criptovalute come mezzo di scambio primario.

Paradossalmente, la tecnologia alla base delle criptovalute, la blockchain, è anche uno strumento investigativo potente. Ogni transazione è registrata in modo permanente e pubblico. Questo significa che, con le giuste competenze e strumenti di analisi adeguati, è possibile ricostruire i movimenti di denaro virtuale, identificare pattern transazionali ripetuti e collegare indirizzi apparentemente scollegati. Strumenti di analytics on-chain consentono di individuare schemi di smurfing (frazionamento di transazioni), identificare ponti tra blockchain (cross-chain bridges) e riconoscere l'uso di servizi di conversione in fiat mediante exchange.

Nascono così nuove figure professionali: analisti blockchain, esperti in cyber intelligence e forze dell'ordine altamente specializzate. Organismi europei come Eurojust, Europol, Eppo e la Direzione Investigativa Antimafia in Italia, stanno investendo in tecnologie avanzate per seguire le tracce digitali del denaro. L'adozione di tecniche di data science, machine learning e analisi di rete permette di estrarre segnali utili da grandi volumi di transazioni. Allo stesso tempo, è necessario integrare tali capacità con competenze giuridiche e operative per tradurre le evidenze tecniche in prove ammissibili in sede processuale.

Le nuove sfide determinate dal passaggio al "virtual money" pongono diverse criticità. Un problema particolarmente

complesso e di difficile soluzione sono le normative non uniformi tra i diversi Paesi: la mancanza di standard internazionali armonizzati su antiriciclaggio, identificazione dei clienti (KYC) e condivisione di informazioni ostacola di fatto le indagini transfrontaliere. Molto critica è anche la situazione relativa agli exchange non regolamentati che operano in giurisdizioni opache. Tali piattaforme possono fungere da punti di ricongiunzione per fondi illeciti se non soggette a controlli stringenti. La criminalità organizzata, inoltre, utilizza tecniche avanzate come mixer e privacy coin per offuscare le transazioni mediante servizi di mixing, coinjoin e criptovalute progettate per la privacy che rendono più complesso il recupero della catena di transazione.

Per contrastare queste minacce, è fondamentale una cooperazione internazionale più stretta e un aggiornamento continuo delle competenze investigative e giudiziarie. Occorre promuovere accordi di mutua assistenza più rapidi ed efficaci, definire standard internazionali per la due diligence e investire nella formazione di operatori giudiziari e tecnici. È utile, inoltre, sviluppare partnership pubblico-privato con operatori del settore cripto: exchange regolamentati, custodi e società di analytics possono fornire dati e insight cruciali per le indagini.

Le contromisure efficaci combinano strumenti tecnologici, strumenti normativi e approcci preventivi. A livello tecnologico, l'adozione di piattaforme di analisi on-chain, la condivisione di threat intelligence e l'impiego di tecniche forensi per il recupero delle chiavi private o la compromissione di infrastrutture di custodialità possono contribuire al sequestro dei fondi. A livello normativo, l'estensione delle normative antiriciclaggio alle entità che forniscono servizi cripto, l'obbligo di reporting delle transazioni sospette e l'introduzione di limiti e controlli sui servizi anonimi sono leve importanti. Sul piano preventivo, la promozione dell'educazione finanziaria digitale e la trasparenza nelle operazioni commerciali che coinvolgono asset digitali riducono le superfici di rischio.

Benché la regolamentazione possa limitare gli usi illegittimi, è necessario bilanciare le misure con la tutela della privacy e dell'innovazione tecnologica. Un'eccessiva rigidità normativa rischia di soffocare l'adozione legittima delle tecnologie blockchain e di trasferire attività lecite verso giurisdizioni meno regolamentate. Le politiche degli Stati devono essere calibrate, basate su analisi di rischio e promuovere standard di trasparenza che non impediscano lo sviluppo economico.

Numerosi casi investigativi recenti mostrano sia la crescente adozione delle tecnologie digitali da parte delle organizzazioni criminali sia l'efficacia di approcci investigativi moderni. Operazioni coordinate a livello internazionale hanno permesso il sequestro di wallet contenenti cripto-asset di valore significativo e lo smantellamento di reti che impiegavano mixer. Se da un lato tali successi dimostrano la fattibilità di interventi mirati, dall'altro mettono in luce la necessità di procedure accelerate per la conversione e la conservazione degli asset sequestrati, nonché di competenze tecniche negli uffici giudiziari per valutare correttamente la prova digitale.

Il principio del "follow the virtual money" rappresenta oggi una delle frontiere più avanzate nella lotta alle nuove mafie. Se da un lato le organizzazioni criminali sfruttano le innovazioni tecnologiche per evolversi, dall'altro anche gli strumenti di contrasto stanno diventando sempre più sofisticati. La sfida è aperta: in un mondo sempre più digitale, la capacità di tracciare il denaro — anche quando è "invisibile" ai metodi tradizionali — sarà decisiva per combattere l'enorme potere economico delle mafie. Per conseguire risultati duraturi è indispensabile un approccio integrato che combini competenze tecniche, adeguamenti normativi, cooperazione internazionale e partnership tra settore pubblico e privato, nonché investimenti continui in formazione e ricerca applicata. Solo così si potrà sperare di riportare efficacia all'azione investigativa nel contesto di un ecosistema finanziario sempre più complesso e interconnesso a livello globale.