SSM

SCUOLA SUPERIORE DELLA MAGISTRATURA

Corso P25019

"LE CRIPTOVALUTE"

Catania, 28 febbraio 2025

Profili di cooperazione internazionale e criticità pratiche nel giudizio

Simona Ragazzi
Giudice Indagini Preliminari
Tribunale Catania
simona.ragazzi@giustizia.it

Caratteristiche delle attività (criminali) nell'universo digitale

- **Rapidità di azioni e transazioni, volatilità**
- **Anonimato degli utenti e facile falsificazione di identità**
- **Transnazionalità, delocalizzazione e non localizzazione fisica di condotte e attori**
- **Crittografia**
- **Tendenza a innovazione e adattamento delle tecniche criminali**
  - **Difficoltà della «*attribution*» a persone fisiche /enti**
  - Possibile **inefficacia dell'*enforcement*** della giurisdizione su fonti di prova, blocco a strumenti di commissione di reati, recupero di guadagni illeciti
  - Ruolo cruciale della **cooperazione internazionale, giudiziaria e di polizia**
  - Necessaria **collaborazione dei prestatori di servizi digitali, che operano fuori Italia** (sia per acquisizione prova sia per esecuzione di sequestro)
  - **Elevata «cifra oscura» del cybercrime** (barriere internazionali alla giurisdizione e capacità degli attori malevoli di bucarle agevolmente)

Strumenti di cooperazione internazionale a fini di indagine o di sequestro su criptovalute (Paesi esteri, providers)

A chi rivolgersi ? Al Ministero della Giustizia? Alla AG di uno Stato estero? A un provider?

Regola basilare - Art. 696 c.p.p. Nei rapporti con gli Stati UE prevale il diritto della UE; in mancanza o se le norme dispongono diversamente, si applicano convenzioni internazionali in vigore per lo Stato e le norme di diritto internazionale generale; con Stati extra-UE si applicano le convenzioni internazionali in vigore per lo Stato e il diritto internazionale generale; in mancanza, le norme del Libro XI c.p.p..

Novità

Cooperazione volontaria e diretta con i Service Providers

(es. social media, app di messaggistica, **exchange di criptovalute**, es. Binance, Coinbase, etc.) molti stabiliti in Irlanda, Paese UE ma estraneo alla Direttiva 2014/41 su OIE

Attuale cooperazione tra AG/PG e Service providers non stabiliti in Italia

- Acquisizione di ***non-content–data (dati estrinseci della comunicazione,*** come i dati identificativi di conti in criptovalute: intestatari, utenze, indirizzi, PIN, Password, etc.) con **cooperazione volontaria e diretta con i service providers di crypto-asset** = richieste della AG o della PG ai portali o a indirizzi di email dei service provider, i quali rispondono e offrono contenuti in base a loro scelte di «policy» e/o al diritto interno dello Stato in cui sono stabiliti. Talvolta chiedono rogatorie (c.d. MLA) o OIE (ambito UE).
- **Criticità**:
  1. approccio non regolato in pressoché alcuno dei Paesi della UE,
  2. Difficoltà di identificare il provider di riferimento o stabilirvi un contatto;
  3. mancanza di collaborazione del service provider per difetto di volontà e/o risorse;
  4. mancanza di quadro giuridico sottostante su obbligo di conservare i dati rilevanti;
  5. tempistiche incerte (e lunghe…), anche per crescita esponenziale di richieste

- Per **dati di contenuto:** il provider può collaborare spontaneamente **oppure** può chiedere di passare da **MLA (atti di mutua assistenza giudiziaria) o OIE (Ordini Europei di Indagine)** alla AG di altro Stato

Modello di policy di un Exchange (fornitore di servizi di portafoglio di criptovalute) in tema di cooperazione volontaria

*L'Exchange con email alla PG comunica di avere sede in *** (Paese extra UE) e di fornire i propri servizi, tra gli altri, attraverso la Società Y con sede in *** (Paese UE);* ***la fornitura di informazioni e collaborazione è volontaria*** *e non soggetta alla giurisdizione italiana e può così proseguire:*

- *sull'account ID *** sono presenti *** bitcoin, alla data odierna equivalenti ad € *****, somma che potrebbe diminuire qualora subentrassero altre richieste di sequestro da parte di forze di polizia;*
- *l'esecuzione del sequestro sarà soggetta ai seguenti vincoli: a) l'Autorità Giudiziaria dovrà concedere all'indagato/titolare delle criptovalute sequestrate l'opportunità di ricorrere avverso il sequestro dinanzi a un organo giudicante e di essere sentito prima che i fondi vengano trasferiti alla presunta vittima; b) nessuna obiezione ad autorizzare l'Exchange a comunicare al titolare dell'account che i fondi sono stati sequestrati da un'autorità di polizia in tutto o in parte; c) nessuna obiezione a condividere informazioni e documenti, incluso il provvedimento di sequestro, così da consentire al titolare del wallet di contestare il sequestro dopo che lo stesso sia stato eseguito e di avere la possibilità di contattare direttamente chi ha operato il sequestro; d) l'Exchange deve essere autorizzato a trattenere le fees (commissioni); e) la politica dell'Exchange prevede la possibilità di sbloccare l'account dopo l'avvenuto sequestro, sulla base di accertamenti interni condotti dallo stesso Exchange.*

Protocollo addizionale n. 2 alla Convenzione di Budapest sul cybercrime

Adottato il 17/11/2021, aperto alla firma il 12/5/2022, ha ad oggi 47 Stati Parte (ultimo il Paraguay, settembre 2024); entrerà in vigore dopo cinque ratifiche (allo stato, sono due: Serbia e Giappone).

Il protocollo (https://www.coe.int/en/web/cybercrime/second-additional-protocol), tra l'altro, istituisce e regola **forme di cooperazione diretta tra autorità competenti e fornitori di servizi** (service providers) collocati nel territorio di altri Stati Parte a fini di acquisizione di prove elettroniche.

- **Art. 6 - Richiesta di informazioni sulla registrazione di nomi di dominio e Art. 7 - Divulgazione delle informazioni relative agli abbonati:** le autorità competenti di ogni Stato parte possono chiedere a fornitori di tali servizi digitali di altro Stato parte informazioni in loro possesso o sotto il loro controllo, atte a identificare o contattare il titolare di un nome di dominio o emettere ordini per acquisire dai fornitori informazioni su abbonati [….]
- **Art. 8** - le autorità competenti possono essere autorizzate a emettere un **ordine** da presentare a un'altra Parte al fine di imporre a un prestatore di servizi sul territorio della Parte richiesta di divulgare dati su **abbonati** e **dati di traffico**.

«EU E-evidence Package»: Regolamento 2023/1543 e Direttiva 2023/1544 del 12.7.23

- Quadro giuridico che definisce, con regole certe e uniformi, la **cooperazione diretta tra «autorità di contrasto»** (autorità giudiziarie o inquirenti autorizzate a raccogliere prove) e «**fornitori di servizi di comunicazioni elettroniche**», ai fini della produzione e della conservazione provvisoria di prove elettroniche, sulla base di decisioni giudiziarie veicolate da «certificati» dal contenuto definito (Certificato di ordine europeo di produzione, EPOC, e Certificato di ordine europeo di conservazione, EPOC-PR), obblighi di risposta da parte dei fornitori, motivi di eventuale rifiuto codificati, tempistiche certe, e ciò attraverso una piattaforma di comunicazione sicura (Sistema Informatico Decentrato) per gli scambi digitali e le comunicazioni tra AG.

- **Cosa è in concreto?** con **ordine europeo di produzione o un ordine europeo di conservazione** l'Autorità di uno Stato UE - nell'ambito di un **procedimento penale** ovvero per **l'esecuzione di pena** o misura di sicurezza detentiva di almeno 4 mesi a seguito di procedimento penale non in contumacia se la persona condannata è latitante - **ingiunge** a un prestatore di servizi che offre servizi nell'Unione e che è stabilito in un altro Stato membro o, alternativamente, rappresentato da un rappresentante legale in un altro Stato membro, di produrre o conservare prove elettroniche, indipendentemente dall'ubicazione dei dati.

- **Sarà applicata dal 18 agosto 2026**

E-evidence: Chi sono i prestatori di servizi? vi rientrano i prestatori di servizi di moneta virtuale?

(considerando 27-30 e art. 3 n. 4)

Prestatore di servizi ai fini del Regolamento UE 1543/2023 è….

- Persona fisica o giuridica che fornisce nell'Unione Europea una o più delle seguenti categorie di servizi, ad **eccezione dei servizi finanziari ex art. 2, par. 2, b) Dir. 2006/123/CE**: a) **servizi di comunicazione elettronica** (art. 2 n. 4) dir. UE 2018/1972); b) **servizi di nomi di dominio internet e di numerazione IP**, quali l'assegnazione indirizzi IP, servizi di registri di nomi di dominio, di registrar di nomi di dominio e i servizi per la privacy o proxy connessi ai nomi di dominio; c) **altri servizi della società dell'informazione** (dir. UE 2015/1535) che consentono ai loro utenti di comunicare fra di loro; oppure che rendono possibile la conservazione o il trattamento di dati per conto degli utenti ai quali è fornito il servizio, quando la conservazione dei dati è una componente propria del servizio fornito all'utente.
- **Art. 2, par. 2, b) Direttiva 123/2006**: ….. i servizi finanziari quali l'attività bancaria, il credito, l'assicurazione e la riassicurazione, le pensioni professionali o individuali, i titoli, gli investimenti, i fondi, i servizi di pagamento e quelli di consulenza nel settore degli investimenti, compresi i servizi di cui all'allegato I della Direttiva 2006/48/CE;

Servizi fin. di cui all'allegato I della direttiva 2006/48/CE

- 1. Raccolta di depositi o di altri fondi rimborsabili 2. Operazioni di prestito, in particolare: credito al consumo, credito con garanzia ipotecaria, factoring, cessioni di credito pro soluto e pro solvendo, credito commerciale (compreso il forfaiting) 3. Leasing finanziario 4. "Servizi di pagamento" quali definiti all'articolo 4, punto 3, della direttiva 2007/64/CE del Parlamento europeo e del Consiglio, del 13 novembre 2007, relativa ai servizi di pagamento nel mercato interno 5. Emissione e gestione di altri mezzi di pagamento (travellers cheque e lettere di credito) nella misura in cui quest'attività non rientra nel punto 4
- 6. Rilascio di garanzie e di impegni di firma 7. Operazioni per proprio conto o per conto della clientela in: a) strumenti di mercato monetario (assegni, cambiali, certificati di deposito, ecc.) b) cambi c) strumenti finanziari a termine e opzioni d) contratti su tassi di cambio e tassi d'interesse e) valori mobiliari 8. Partecipazioni alle emissioni di titoli e prestazioni di servizi connessi 9. Consulenza alle imprese in materia di struttura finanziaria, di strategia industriale e di questioni connesse e consulenza nonché' servizi nel campo delle concentrazioni e della rilevazione di imprese 10. Servizi di intermediazione finanziaria del tipo money broking. 11. Gestione o consulenza nella gestione dei patrimoni 12. Custodia e amministrazione di valori mobiliari 13. Servizi di informazione commerciale 14. Locazione di cassette di sicurezza.
- I servizi e le attività di cui all'allegato I, sezioni A e B, della direttiva 2004/39/CE del Parlamento europeo e del Consiglio del 21 aprile 2004 relativa ai mercati degli strumenti finanziari sono soggetti al mutuo riconoscimento ai sensi della presente direttiva quando hanno ad oggetto gli strumenti finanziari di cui all'allegato I, sezione C di tale direttiva.
- 15. Emissione di moneta elettronica (introdotto da art. 20 Direttiva UE 2009/110)

Criptovalute e sequestro - Reati più comuni configurabili

- **Truffa** (appropriazione di denaro conseguito prospettando lauti guadagni tramite investimento in criptovalute) art. 640 c.p.
- **Frode informatica (640-ter c.p.);**
- **Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche** (Art. 617 sexies c.p.)
- **Abusivo esercizio di attività finanziaria** (art. 166, comma 1, lett. a) e c) D. Lgs 58/1998 sul presupposto che le valute virtuali possono essere usate come mezzo di investimento: Cass. Sez. II, sez. II, 17/09/2020, n. 26807**;** Sez. V, n. 37767/23 e n. 29649/24)
- **Autoriciclaggio:** impiego dei proventi di delitti (es. truffa) nell'acquisto di criptovalute su conto intestato alla piattaforma di scambio tramite portafoglio virtuale crittografato, non immediatamente riconducibile agli agenti, meccanismo idoneo a rendere difficile se non impossibile la tracciabilità (v. Cass. sez II, 28279/2023)

Caso pratico: truffa in criptovalute

- Alfa e Beta (di Paesi extra-UE) contattano telefonicamente Mario (res. Italia) tramite segretaria, qualificandosi [fittiziamente] come consulenti/broker di *trading* della società ***Coinmarket*** proponendogli investimento online in criptovalute varie; lo inducono a creare un account su due siti web ("www.coinmarket.cc" e www.coinbase.com), il secondo finalizzato ad acquistare e convertire euro in criptomonete, da riversarsi successivamente sulla prima piattaforma, nella quale dovevano operare Alfa e Beta: rassicurano che sarebbero stati loro due a trasformare gli euro in Bitcoin (o altra c.v.), nonché, a trasferire le criptovalute create sulla piattaforma di trading raggiungibile dal sito www.coinmarket.cc;
- La p.o. esegue vari bonifici istantanei (per un totale di decine di mig. €) a favore di Coinbase.com (Coinbase Ireland Ltd.), ove acquista le criptovalute;
- Alfa e Beta trasferiscono con due transazioni le criptovalute comprate dalla p.o. su *wallet* a ciascuno di loro due intestati; ossia: i soldi versati dalla p.o. su Coinbase venivano riversati su wallet in mano ai due, che gli facevano credere di stare spostando queste somme sulla piattaforma di trading sito www.coinmarket.cc; ma tale sito era una *finta* piattaforma di trading sulla quale i criminali muovevano i grafici e operavano a piacimento, riuscendo a far falsamente credere alla vittima che stava ottenendo dei profitti dall'investimento effettuato;
- Coinbase *è* uno dei siti di Exchange di criptovaluta più importanti, da luglio 2022 anche iscritto anche all'Organismo Agenti e Mediatori (OAM) in Italia, dunque legalmente operante;

- **La PG** chiede informazioni all'Exchange **Coinbase** (dove la p.o. comprava le criptovalute), la quale rivela che i conti-wallet (Portafoglio digitale utilizzato per memorizzare, inviare e ricevere criptovalute) ove sono transitate le somme derivanti dalle transazioni della p.o. non sono radicati presso di sé, ma presso l'**Exchange Binance**, ove erano confluiti su appositi wallet.
- **Binance,** previo **decreto GIP ex art. 132 D.Lgs. 196/2003**, fornisce alla PG i dettagli sui wallet ove sono stati depositati i fondi prelevati alla p.o. (bilancio del conto, storia degli ordini, dei depositi e dei prelievi, identità degli ordinanti, dispositivi approvati per l'accesso alla piattaforma e documenti forniti per l'attivazione del conto); dagli accertamenti sulla blockchain delle criptovalute si ricava che: a) **il wallet 1** risulta registrato con la mail: crypto***@yahoo.com in data ***2020, e intestato a **ALFA;** b) dalla data di apertura alla consegna delle informazioni, vi sono transitati fondi per milioni di euro e al momento si trova la disponibilità di diverse cripto-valute (alla data dell'accertamento la parte più consistente è rappresentata dalla criptovaluta USDT; c) nella lista degli accessi (access logs) si rileva che ALFA fa accesso a Binance da Paese UE 2, Paesi extra UE 1 e 2.
- **GIP**: qualificazione, giurisdizione, competenza → sequestro ex art. 321, co. 1 e 2, cpp di: a) fondi di cripto-valute, riferibili alla p.o. e gestiti dagli indagati; b) somme su wallet, conti, depositi o su qualsiasi tipo di rapporto ove le dette criptovalute fossero state trasferite, fino alla somma integrante profitto del reato, con trasferimento su altro account dell'Exchange intestato al proc. pen.

…. CRITICITÀ IN ESECUZIONE DI SEQUESTRO 1/2

1. Mancanza di norme o linee guida a PG e AG sulle modalità esecutive del sequestro di criptovalute

Non potrebbero essere soddisfacenti le norme sul **Fondo Unico Giustizia** (istituito da art. 61, co. 23, DL 112/2008 conv. L. 133/2008 e regolato da art. 2 L. 143/2008, conv. L. 181/2008): **Modalità di afflusso FUG delle risorse sequestrate:** L'Autorità che ha eseguito il sequestro (PG) deve versare banconote e monete sequestrate in euro sul conto corrente postale n. ……, intestato "Fondo Unico Giustizia", mediante il bollettino postale allegato alla Convenzione del 2 ottobre 2013, senza oneri di versamento.

In caso di **sequestro di valuta diversa dall'euro**, l'Autorità che ha eseguito il sequestro deve negoziare la valuta stessa e versare il controvalore con le stesse modalità previste per il versamento del contante sequestrato in euro e poi versare su conto intestato FUG.

Non si tratta, infatti, di valuta diversa dall'euro (v. Cass. **Cass. 20.11.2024, dep. 15.1.2025 n. 1760/25**: il reinvestimento in criptovalute del profitto del reato (es. tributario) non implica che queste siano profitto diretto del reato, perché le criptovalute non sono «valuta». L'eventuale sequestro/confisca sarebbe qui per equivalente (diverso in caso di truffa diretta in criptovalute).

…. CRITICITÀ IN ESECUZIONE DI SEQUESTRO 2/2: PRASSI APPLICATIVE

- **OPZIONE 1:** su disposizione del PM, la PG chiede al provider il blocco dei conti («Wallet») intestati agli indagati ove sono allocate le criptovalute provento di reato; e su indicazione dell'Exchange la PG acquista un hardware Wallet Nano X-Ledger configurando una chiavetta (creazione di codice PIN, parole chiave -c.d. parole di recupero in caso di smarrimento della chiavetta o del codice PIN); procedura (buste sigillate, plurimi operatori, etc.) sottoposta a videoripresa. All'esito il provider trasferisce agli indirizzi memorizzati nel Wallet hardware configurato criptovalute per complessivi euro XXX sotto forma di Bitcoin, Ethereum, etc. provenienti dal conto dell'indagato. Il provider poi informa i titolari dei wallet colpiti da sequestro.

- **OPZIONE 2.** spossessamento del titolare del wallet sospetto, con cambio password e sua gestione dinamica (investimenti nomina amministratore);

- **OPZIONE 3 (eventualmente passo successivo a 1)**: conversione delle criptovalute ad opera di piattaforma di Exchange italiano, nominato ausiliario di P.G. (es. Young Platform), che acquisterà criptovalute restituendo in cambio euro che potranno confluire al FUG, vincolate fino all'esito del proc. pen.. Ma a che data? Per quale valore? L'avente diritto può lamentare misura della conversione in caso di successivo rialzo?

…. CRITICITÀ NEL GIUDIZIO 1/3

Esercizio dell'azione penale nei confronti dei ritenuti autori delle condotte illecite

Spunti di riflessione:

- **Giurisdizione** (affermazione di giurisdizione italiana ex art. 6, comma 2, c.p. e possibili confitti con altri Stati che hanno casi sovrapponibili)
- **Identificazione** degli imputati/notifica atti giudiziari (possibile necessità di rogatoria)
- **Cooperazione** con Paesi extra UE, etc.
- Qualificazione e ammissibilità delle **prove** acquisite mediante cooperazione volontaria con i providers

Cass. su competenza terr.: utile descrizione della dimensione virtuale, ma soluzione difficile da adattare a condotte tenute nel cyberspazio e non localizzabili

Corte di cassazione -Sezioni Unite (n. 17325/2015 del 26.3.2015, dep. 24.4.2015), su competenza (interna allo Stato) per accesso abusivo a sistema informatico ex art. 615-ter c.p. (caso con dimensione solo nazionale):

*la "**dimensione virtuale o smaterializzata**" è concretamente distinta dalla dimensione spaziale classica, perché non è possibile vi sia né coincidenza né concreta individuazione del luogo in cui i dati, sotto forma di impulsi elettronici, vengono scambiati e circolano fisicamente. Non si può infatti dire che i dati circolino soltanto ove è posto il server o il sistema informatico. Il server, data la complessità anche solo potenziale dei vari elementi di cui si compone, non è individuabile in un solo luogo secondo criteri fisici.*

*Nel cyberspazio i dati, pur essendo archiviati in uno spazio fisico (il **server**), circolano e vengono messi a disposizione di chi li consulta. Costituiscono quindi un flusso caratterizzato dall'ubiquità e dalla diffusione dei dati stessi. Non è giusto dunque ritenere che tali dati si trovino soltanto all'interno del server a cui si accede. Le prove inerenti ai flussi di scambio, poi, non sono soltanto rinvenibili all'interno dei server ove tali dati sono conservati, ma sono anche ben rintracciabili attraverso l'analisi dell'elaboratore o della postazione attraverso la quale l'agente abbia effettuato il proprio accesso; tale elaboratore è anche definito "**client**" in contrapposizione al "server" cui si accede*.

*Laddove la comunicazione avviene attraverso lo scambio di impulsi elettronici sotto forma di bit, rileva il luogo di **interazione dell'umano con il sistema informatico*** **(= luogo dal quale l'utente autore dell'accesso abusivo si è connesso).**

Si possono qualificare gli elementi ottenuti dai Cryptoassets Service Providers con collaborazione volontaria come scambio spontaneo di informazioni?

- **art. 9 D. Lgs. 52/2017** (recepisce art. 7 Convezione MAP UE 29/5/2000): 1. E' consentito, nell'ambito di un procedimento penale ….lo scambio diretto e spontaneo di informazioni utili e di atti con l'autorità competente di altro Stato Parte. Le informazioni e gli atti ricevuti sono utilizzabili nel rispetto dei limiti indicati dall'autorità competente dello Stato Parte. Resta fermo quanto disposto dall'articolo 78 disp. att. C.p.p. (NB riguarda collaborazione tra AG)
- **Art. 26 della Convenzione di Budapest** sul ***Cybercrime*** **trasmissione spontanea di informazioni tra Parti** (sia tra AG e sia tra PG)

- **Scambio spontaneo di informazioni tra forze di polizia** (Direttiva UE 2023/977 del 10.5.2023 – Art. 7 – recepita con D. Lgs. 12.11.2024 n. 181)

- **Cass. Pen., S.1, 354/2023, Rv.283864-01** (già Cass. pen., VI, n. 9960/2005): *In tema di rapporti giurisdizionali con autorità straniere, le informazioni e gli atti trasmessi autonomamente dall'Autorità giudiziaria di uno Stato estero sono utilizzabili nel procedimento penale, non essendo, in tali casi, applicabile in via estensiva o analogica la disciplina speciale ex art. 729, co. 1, c.p.p. per le rogatorie dall'estero*.

- N.B.: fermi gli **artt. 729-bis c.p.p**. (Acquisizione di atti e informazioni da autorità straniere: 1. La documentazione di atti e informazioni spontaneamente trasmessi dall'autorità di altro Stato è acquisita al fascicolo del Pubblico Ministero. 2. L'autorità giudiziaria è vincolata al rispetto delle condizioni eventualmente poste all'utilizzabilità…) e, ai fini della utilizzazione processuale, **238 c.p.p. e 78 disp. Att. C.p.p**. (utilizzazione su consenso o dopo esame)

…. CRITICITÀ NEL GIUDIZIO 2/3

Corte di Appello del Cantone di Berna (Svizzera)

Decisione del 4/12/2023 sulla **legittimità della cooperazione diretta con il provider di criptovalute**

Blocking of a cryptocurrency exchange account, following an order from the public prosecutor that was sent directly to Binance.

The court considered that: *in contrast to conventional fiat currencies, cryptocurrencies are not stored locally at a specific location but are stored in a decentralized or location-independent manner on a blockchain. In addition, the Binance cryptocurrency exchange does not have a fixed location and only appears to be accessible via the internet. Against this background, no request for MLA [mutual legal assistance] can be made to another State and the public prosecutor's office does not violate the principle of territoriality by contacting the cryptocurrency exchange Binance directly or without a prior request for MLA to block the account of the accused person.*

Corte di Appello del Cantone di Berna (Svizzera), 4.12.2023

Diversamente dalle monete tradizionali, le criptovalute non sono conservate in una specifica sede fisica bensì in una maniera decentralizzata o comunque indipendente da una location specifica su una blockchain. In aggiunta l'exchange di criptovalute BINANCE non ha una sede fissa ed è accessibile soltanto via Internet. In questo contesto non può essere formulata alcuna richiesta di mutua assistenza giudiziaria all'autorità di un altro Stato e l'ufficio del Pubblico Ministero non viola il principio di territorialità contattando *direttamente* l'exchange BINANCE senza una previa richiesta di mutua assistenza giudiziaria per congelare il conto della persona indagata.

…. CRITICITÀ IN RESTITUZIONE DEL PROFITTO ALLA P.O.

3. È possibile la restituzione «anticipata» alla p.o. del profitto del reato o comunque procedervi in mancanza di condanna? (es. archiviazione/sentenza ex art. 420-quater c.p.p.)

N.B.: **art. 420-quater, comma 7, c.p.**: «In deroga a quanto disposto dagli articoli 262, 317 e 323 [c.p.p.], gli effetti dei provvedimenti che hanno disposto il sequestro probatorio, il sequestro conservativo e il sequestro preventivo permangono fino a quando la sentenza non è più revocabile ai sensi del comma 6».

→ dunque non si può disporre la confisca del profitto del reato. E la restituzione del profitto alla vittima di condotte malevole?

Restituzione profitto alla p.o. vs. confisca

Cass., S. II, 15218/2014, Gavagin, "Con la restituzione alla persona offesa delle somme -profitto del reato viene meno sia l'oggetto su cui dovrebbe cadere la confisca sia lo scopo della confisca (impedire che l'impiego dei beni di provenienza delittuosa possa consentire al colpevole di garantirsi il vantaggio cui mirava il suo disegno). Ne consegue, una volta che l'imputato ha restituito alla persona offesa le somme profitto del reato, che il giudice non può disporre la confisca di altra somma corrispondente a tale profitto, che costituirebbe una inammissibile duplicazione sanzionatoria a carico del reo« (idem Sez. III, n. 44446 del 15/10/2013**;** Sez. II, n. 36444/2015 ; Sez. II, n. 20749/2021).

Cass. Sez. Un. sent. 26.6. 2015 n. 31617 Lucci : "Il giudice, nel dichiarare la estinzione del reato per intervenuta prescrizione, può applicare, a norma dell'art. 240, comma 2, n. 1, cod. pen., la confisca del prezzo del reato e, a norma dell'art. 322-ter cod. pen., la confisca del prezzo o del profitto del reato sempre che si tratti di confisca diretta e vi sia stata una precedente pronuncia di condanna, rispetto alla quale il giudizio di merito permanga inalterato quanto alla sussistenza del reato, alla responsabilità dell'imputato ed alla qualificazione del bene da confiscare come profitto o prezzo del reato".

Ratio: **confisca diretta** non è pena/sanzione afflittiva (come confisca per equivalente), ma **misura di sicurezza**, dunque non presuppone un giudicato di condanna.

SPUNTI APERTI DI RIFLESSIONE

- **Rispetto del contraddittorio e rapporto con la «Policy» del provider**
- **Sfide alla professionalità di PG e AG in vari settori di reati commessi con modalità telematiche e in «cyberspazio»** (inclusi spesso i reati afferenti a criptovalute)
- **Pensare alla concentrazione della competenza in pochi uffici giudiziari e corpi di polizia?**
- **Verso una nuova giurisdizione «senza giudizio»?** (rischio di non perseguire e di non «assicurare alla giustizia» gli autori di fatti gravi ovvero comunque di non accertarne la responsabilità in modo pieno)

Strumenti operativi utili in ambito europeo

- **EUROPOL (EC3) - Cryptocurrency Services Review 2023** (disponibile anche alle forze di polizia tramire Ufficio italiano presso Europol): elenco e valutazione dei vari CASPs nella cooperazione con PG/AG
- **EUROJUST *Cybercrime Judicial Monitor* (CJM)** (criptovalute (v. Issue 9, pag. 27-31): rassegna del quadro normativo e giurisprudenziale nei Paesi EU e oltre
- **EUROJUST Report on Money Laundering** (2022, pag. 15-17)

Spunti utili

1. Fondazione Vittorio Occorsio - CRIMINALITÀ INFORMATICA E INTELLIGENZA ARTIFICIALE - Quaderno della Rivista Trimestrale della Scuola di Perfezionamento per le Forze di Polizia, II/2022 (scaricabile da internet)
2. Accinni, *Cybersecurity e criptovalute. profili di rilevanza penale dopo la quinta direttiva* , in Sistema Penale 2020
3. De Flammineis, *Le sfide della prova digitale: sequestri, chat, processo penale telematico e intelligenza artificiale* in Sistema Penale, 2024
4. Croce, *Cyberlaundering e valute virtuali*. […], Sistema penale, 4/2021
5. EUROPOL – EC3 - Cryptocurrency Services Review 2023
6. EUROJUST *Cybercrime Judicial Monitor* 2023
7. Decreto sequestro preventivo GIP Catania 24/3/2023
8. EUCRIM, n. 2/2023, pag. 143-144 e 169-229
9. Sentenze Corte di Cassazione pen. 2023-2025 citate