

FOCUS

***SEQUESTRO DI CRIPTO-ATTIVITÀ: L'ATTUAZIONE
DELLA DIRETTIVA (UE) 2024/1260***



PREMESSA

Nell'estate del 2026, **due percorsi normativi in materia di crypto-attività**, formalmente autonomi ma strettamente connessi sul piano sistematico, hanno finito per intrecciarsi.

Il 30 giugno è scaduto il regime transitorio previsto dall'art. 45 del d.lgs. 5 settembre 2024, n. 129 – la disciplina nazionale di adeguamento al regolamento (UE) 2023/1114, il c.d. MiCA – nel testo da ultimo modificato dal decreto-legge n. 95 del 30 giugno 2025. Da tale data, **l'offerta di servizi per le crypto-attività è riservata ai soli soggetti autorizzati** e, secondo il comunicato congiunto reso da Consob e Banca d'Italia proprio il 30 giugno, i soggetti abilitati in Italia sono soltanto nove: otto prestatori di servizi e un intermediario bancario ⁽¹⁾.

Due settimane più tardi, il 14 luglio, il Consiglio dei ministri ha approvato in esame preliminare lo schema di decreto legislativo di attuazione della direttiva (UE) 2024/1260 del 24 aprile 2024, riguardante il recupero e la confisca dei beni; il testo è stato trasmesso alle Camere per il parere il 23 luglio, ove è iscritto come Atto del Governo sottoposto a parere parlamentare n. 431. Fra le sue disposizioni figura un intero Titolo – il IV, articoli 12, 13 e 14 – dedicato proprio alle crypto-attività, che introduce **per la prima volta nel nostro ordinamento una disciplina delle *modalità esecutive del sequestro*** avente ad oggetto questa categoria di beni ⁽²⁾.

Fra i due provvedimenti non corre alcun rapporto di causa ed effetto; corre però un rapporto di **dipendenza sistematica**, ed è quello da cui muove questo Focus. La nuova disciplina del sequestro non contiene infatti alcuna definizione autonoma dell'oggetto su cui incide: rinvia a MiCA per la nozione di crypto-attività e individua nel prestatore di servizi uno dei destinatari cui il provvedimento di sequestro va comunicato, «*ove identificabili*».

La conseguenza è duplice. Quanto più ampia sarà la casistica in cui le crypto-attività saranno detenute da prestatori autorizzati e identificabili, tanto più la nuova disciplina potrà trovare applicazione nella sua forma piena. Per tutte le ipotesi residue – ad es., crypto-attività custodite direttamente dal titolare, o affidate a operatori stabiliti fuori dall'Unione – occorrerà ricorrere alle modalità alternative che la disciplina stessa contempla, con le difficoltà applicative di cui si dirà.

Una precisazione di metodo. Il testo qui esaminato è ancora uno schema: i pareri delle Commissioni parlamentari non sono ancora stati resi, il termine di recepimento della direttiva scade il 23 novembre 2026 e l'articolo è suscettibile di modifiche. Le considerazioni che seguono si muovono

⁽¹⁾ Comunicato stampa congiunto Consob – Banca d'Italia del 30 giugno 2026: i prestatori di servizi per le crypto-attività autorizzati risultano otto (CheckSig S.r.l., Conio S.r.l., CryptoSmart S.p.A., Hercle S.r.l., Hodlie S.r.l., Olliv Italia S.r.l., Riv Digital S.r.l., Young Platform S.p.A.), cui si aggiunge un intermediario bancario (Banca Sella S.p.A.). Il dato riguarda le sole autorizzazioni rilasciate in Italia e non fotografa l'insieme degli operatori che servono la clientela italiana, poiché i prestatori autorizzati in altri Stati membri possono operare in regime di libera prestazione di servizi.

⁽²⁾ La relazione illustrativa colloca le disposizioni in materia di crypto-attività all'«*articolo 11 dello schema di decreto legislativo*», mentre nel testo trasmesso alle Camere esse figurano agli articoli 12, 13 e 14: la relazione risulta evidentemente tarata su una precedente versione dell'articolo.

perciò, dichiaratamente, sul terreno del *de iure condendo*, nella consapevolezza del carattere provvisorio del quadro normativo di riferimento.

1. CHE COSA SI SEQUESTRA: LA NOZIONE DI CRIPTO-ATTIVITÀ E I SUOI CONFINI

Il legislatore delegato non ha coniato una nozione autonoma di cripto-attività agli effetti delle misure ablativo. La nuova disciplina rinvia all'art. 3, paragrafo 1, punto 5), del regolamento MiCA, che definisce la cripto-attività come «*una rappresentazione digitale di un valore o di un diritto che può essere trasferito e memorizzato elettronicamente, utilizzando la tecnologia a registro distribuito o una tecnologia analoga*»; la relazione illustrativa affianca a tale definizione la nozione onnicomprensiva di bene dell'art. 810 c.c., osservando che il coordinamento si è reso necessario proprio «*tenuto conto della definizione onnicomprensiva di "bene" presente nell'ordinamento*».

La tecnica del rinvio è, in sé, coerente con l'esigenza di uniformità terminologica fra disciplina regolamentare e disciplina processuale. Merita però attenzione la precisazione contenuta in nota nella relazione illustrativa, secondo cui «*il richiamo alla definizione di cripto-attività contenuta nel Regolamento MiCA ha **funzione descrittiva**, non impedendo il sequestro anche [di] cripto-attività che, pur essendo negoziate al di fuori dei mercati regolamentati, rientrano nella più ampia nozione di beni digitali elaborata a livello internazionale*».

La precisazione produce un effetto di non poco rilievo: **il perimetro dell'apprensione risulta deliberatamente più esteso di quello della vigilanza**. Vi rientrano, infatti, anche cripto-attività che MiCA esclude dal proprio ambito di applicazione – segnatamente quelle uniche e non fungibili – o che circolano interamente al di fuori di infrastrutture vigilate.

L'intento di effettività è comprensibile, e anzi condivisibile: un perimetro cautelare modellato su quello regolamentare sarebbe stato aggirabile con un semplice spostamento di piattaforma. Resta però che, per questa via, l'individuazione dell'oggetto del vincolo cautelare viene affidata a un rinvio cui la stessa relazione attribuisce «*funzione descrittiva*» e a una «*più ampia nozione*» di elaborazione internazionale, cioè a una categoria priva di confini normativi definiti. Non è una questione teorica: stabilire che cosa sia stato appreso, e a quale titolo giuridico, è il primo terreno su cui si misura la legittimità della misura.

Vale la pena ricordare, per completezza, che il quadro sanzionatorio in cui la nozione si inserisce è già operativo. Il d.lgs. n. 129 del 2024 presidia con sanzione penale l'esercizio non autorizzato dei servizi per le cripto-attività ⁽³⁾, fattispecie che, chiusosi il regime transitorio, ha smesso di essere un'ipotesi di scuola; e la giurisprudenza di legittimità aveva già chiarito che, «*ove le monete virtuali vengano utilizzate come strumenti di*

⁽³⁾ Art. 30 del d.lgs. n. 129 del 2024, che configura le fattispecie di abusivismo in materia di cripto-attività – tra cui la prestazione di servizi in mancanza dell'autorizzazione prevista dall'art. 59 MiCA – punite con la reclusione da sei mesi a quattro anni e con la multa da euro 2.066 a euro 10.329.

investimento finanziario, la negoziazione è soggetta al rispetto delle norme in materia di intermediazione finanziaria, ivi compresa la necessaria abilitazione del soggetto intermediario» (così Cass. pen., sez. III, 15 gennaio 2025, n. 1760, che richiama Cass. pen., sez. II, 17 settembre 2020, n. 26807). Il punto merita di essere tenuto presente, perché è proprio da procedimenti di questo genere che origina, in concreto, il patrimonio digitale poi sottoposto a sequestro.

2. COME SI ESEGUE IL SEQUESTRO: LA NUOVA LETTERA E-TER) DELL'ART. 104 DISP. ATT. C.P.P.

L'art. 104 delle disposizioni di attuazione del codice di procedura penale è rubricato «*Esecuzione del sequestro preventivo*» e disciplina, per categorie determinate di beni, il modo in cui il vincolo va materialmente eseguito su aziende, società, beni immobili e mobili registrati, crediti, titoli, quote. **Nulla, sino ad oggi, per le cripto-attività.** Si badi, la lacuna non ha impedito l'applicazione del sequestro – che trova comunque fondamento nelle norme generali – ma ha lasciato alla prassi la parte più delicata dell'operazione, ossia le modalità concrete della sua esecuzione. Da qui una casistica disomogenea e non di rado fonte di contenzioso.

L'art. 12 dello schema colma tale lacuna inserendo nell'art. 104, comma 1, una nuova lettera e-ter), a norma della quale il sequestro preventivo si esegue «*sulle cripto-attività [...] mediante trasferimento delle stesse e, ove possibile, dei relativi mezzi di accesso, ivi incluse le chiavi crittografiche private*», nel Fondo unico giustizia di cui all'art. 61, comma

23, del d.l. 25 giugno 2008, n. 112, «*ovvero, in caso di impossibilità tecnica, mediante ogni altra procedura idonea ad assicurare la custodia ed il controllo esclusivi sulla cripto-attività da parte dell'autorità procedente*».

La norma prosegue disponendo che il provvedimento sia comunicato, «*ai fini dell'adozione delle misure necessarie all'esecuzione del sequestro*», al soggetto che ha emesso le cripto-attività e al prestatore di servizi eventualmente incaricato, dal destinatario del sequestro, della loro custodia e amministrazione, «*ove identificabili*».

Completano il Titolo IV due disposizioni di corredo.

L'art. 13 estende alle cripto-attività il perimetro del Fondo unico giustizia, intervenendo sull'art. 2, comma 2, lett. c), del d.l. 16 settembre 2008, n. 143.

L'art. 14 istituisce presso il Fondo «*un servizio apposito per l'attività di gestione del portafoglio delle cripto-attività sottoposte a sequestro*» – che, nella lettura della relazione illustrativa, configura uno specifico servizio di custodia, un *wallet*, gestito da Equitalia Giustizia S.p.A. – e rimette a un decreto del Presidente del Consiglio dei ministri, da adottarsi su proposta dei Ministri dell'economia e della giustizia, di concerto con il Ministro dell'interno e sentita l'Agenzia per la cybersicurezza nazionale, la disciplina dei termini e delle modalità «*per la vendita disposta, anche d'urgenza, dal giudice delle criptoattività sequestrate*», dei requisiti delle infrastrutture digitali e delle misure di sicurezza necessarie a garantire «*autenticità,*

integrità, accessibilità e trasferibilità» dei beni appresi.

Una notazione sulla rubrica normativa. Il Titolo IV è intitolato «*Disposizioni in materia di confisca di cripto-attività*», ma il suo contenuto attiene, per intero, all'esecuzione del sequestro e alla gestione dei beni sequestrati. Non è un rilievo formale: la confisca delle cripto-attività resta governata dalle regole generali, e la scelta di intervenire a monte – sull'apprensione e sulla custodia – è la più significativa dell'intero Titolo. Del resto, è lì, e non nel momento finale della confisca, che si gioca l'effettività.

3. QUANDO IL TRASFERIMENTO NON È POSSIBILE: I LIMITI DEL «CONTROLLO ESCLUSIVO»

Il passaggio più delicato dell'intera disciplina è quello che accosta il «*trasferimento [...] ove possibile*» dei mezzi di accesso all'ipotesi della «*impossibilità tecnica*». È il legislatore stesso ad ammettere, in una norma di attuazione, che la modalità piena di apprensione potrà non essere praticabile. La relazione illustrativa ne indica espressamente la ragione: «*in considerazione della eterogeneità delle modalità di custodia delle cripto-attività (custodial wallet, self-custody wallet, hardware wallet, paper wallet, ecc.), si è previsto che il trasferimento delle chiavi avvenga "ove possibile"*».

Conviene distinguere le due situazioni, perché conducono a esiti opposti.

Quando il trasferimento è possibile, il controllo dell'autorità è effettivamente esclusivo. Le cripto-attività vengono spostate su un

indirizzo del Fondo unico giustizia, le cui chiavi sono nella sola disponibilità del custode istituzionale: la circostanza che il destinatario del sequestro conservi memoria delle proprie credenziali originarie è, a quel punto, irrilevante, perché l'indirizzo cui esse davano accesso è vuoto. Il modello è pienamente efficace, e replica quello bancario: quando le cripto-attività sono detenute presso un prestatore di servizi esiste un terzo cui notificare il provvedimento e che può darvi esecuzione, esattamente come accade per un conto corrente.

Quando invece il trasferimento non è possibile, il problema si sposta sul piano della tecnica e non è superabile in via giuridica. Le chiavi private di un portafoglio auto-custodito sono tipicamente ricostruibili da una sequenza di parole, la c.d. *seed phrase*, che non è una cosa ma un'informazione: sequestrare il dispositivo o il supporto cartaceo su cui è annotata non ne cancella la conoscenza, e chiunque la conosca può rigenerare il portafoglio su un qualsiasi altro dispositivo, ovunque nel mondo. Né la *seed phrase* può essere «*cambiata*»: l'unico modo per neutralizzare credenziali compromesse è trasferire le disponibilità su un nuovo portafoglio, che è esattamente l'operazione che, per ipotesi, non è stata possibile.

Esiste una via alternativa, ma copre solo una parte del fenomeno, ed è precisamente quella che la norma contempla quando prescrive la comunicazione al soggetto emittente. Per le cripto-attività dotate di un emittente identificabile e tecnicamente in grado di intervenire sul *token* – si pensi ai *token* di moneta elettronica e a quelli collegati ad attività, i cui emittenti dispongono di norma di

funzioni di blocco – la comunicazione ha un destinatario capace di dare esecuzione al vincolo anche senza trasferimento. Di converso, per una crypto-attività nativa di un registro *permissionless*, priva di emittente e di amministratore, non vi è nessuno cui rivolgersi e nulla da bloccare.

Ne discende un interrogativo che il testo non affronta: in che senso il controllo dell'autorità procedente possa dirsi «*esclusivo*» nella seconda ipotesi. Se inteso in senso funzionale – ossia come capacità dell'autorità di disporre del bene – il requisito può ritenersi integrato anche in tale evenienza. Se, invece, inteso in senso pieno – quale esclusione di ogni possibilità di disposizione da parte di terzi – essa descrive un obiettivo, non un risultato garantito.

La distinzione non è meramente teorica: l'art. 104 disp. att. c.p.p. detta modalità esecutive, e quando la modalità concretamente prescelta non assicura l'esclusività che la norma richiede, è sull'idoneità di quella modalità che potrà concentrarsi il sindacato in sede di riesame.

Vi è poi un secondo profilo, che il decreto lascia aperto e che – se la formulazione rimarrà quella attuale – è destinato a occupare la giurisprudenza. Nella seconda ipotesi, ottenere le chiavi private significa, nella grande maggioranza dei casi, ottenere una **collaborazione attiva del destinatario del provvedimento**, eppure nessuna tecnica

investigativa consente di estrarre da un soggetto una sequenza mnemonica. È qui che **il sequestro delle crypto-attività si allontana dal modello ordinario, nel quale l'esecuzione prescinde dalla volontà di chi la subisce**, perché la polizia giudiziaria apprende materialmente e coattivamente la cosa. E il nostro ordinamento, a differenza di altri ⁽⁴⁾, non conosce alcuna norma che imponga all'indagato di consegnare credenziali di accesso né alcuna sanzione per il rifiuto: la facoltà di non rispondere di cui all'art. 64, comma 3, lett. b), c.p.p. e il principio *nemo tenetur se detegere* restano invero intatti.

Diversa è la posizione del terzo che detenga le credenziali per conto altrui – tipicamente il prestatore di servizi – al quale la norma indirizza appunto la comunicazione «*ai fini dell'adozione delle misure necessarie all'esecuzione del sequestro*». Lo schema non affronta il punto, e difficilmente avrebbe potuto farlo entro i limiti dell'oggetto della delega; ma la questione si porrà, prevedibilmente, già nei primi casi applicativi.

Va per contro riconosciuto che la novità è meno dirompente di quanto la formulazione lasci intendere. La figura del custode professionale di chiavi crittografiche private esiste nel nostro ordinamento almeno dal 2019, in ambito antiriciclaggio ⁽⁵⁾, ed era già stata presa in considerazione dalla giurisprudenza di legittimità (Cass. pen., sez. II, 26 ottobre 2022, n. 44378). Ciò che cambia

⁽⁴⁾ Altri ordinamenti hanno compiuto la scelta opposta: nel Regno Unito la Parte III del *Regulation of Investigatory Powers Act 2000* consente di ordinare la comunicazione delle chiavi di cifratura e sanziona penalmente l'inottemperanza. L'ordinamento italiano non conosce un istituto equivalente.

⁽⁵⁾ La nozione è quella dell'art. 1, comma 2, lett. ff-*bis*), del d.lgs. n. 231 del 2007, introdotta dal d.lgs. 4 ottobre 2019, n.

125, che definisce il prestatore di servizi di portafoglio digitale come chi fornisce a terzi, a titolo professionale, «*servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*».

non è la figura: è che, per la prima volta, quel ruolo viene assunto dallo Stato.

Resta infine la questione posta in premessa, quella del destinatario della comunicazione. La norma la risolve con un inciso – «*ove identificabili*» – che ne segna insieme la praticità e il limite. Là dove il prestatore sia autorizzato e riconoscibile, l'esecuzione è agevole. Là dove operi in regime di libera prestazione di servizi da altro Stato membro, occorrerà passare per gli strumenti di cooperazione, e in particolare per il regolamento (UE) 2018/1805 sul reciproco riconoscimento dei provvedimenti di congelamento e di confisca. Là dove, infine, il prestatore sia stabilito fuori dall'Unione o non sia identificabile affatto, la comunicazione non ha destinatario. Il numero dei soggetti autorizzati in Italia, ricordato in apertura, non misura dunque la capacità del sistema: ne misura soltanto la parte più semplice.

4. DAL SEQUESTRO ALLA CONFISCA: VALORE EQUIVALENTE, VOLATILITÀ E VENDITA ANTICIPATA

Sul versante della confisca, il decreto non detta previsioni specifiche per le crypto-attività: interviene con disposizioni di ordine generale, che, su questa categoria di beni, producono però effetti particolarmente sensibili. Conviene muovere dalla già citata sentenza 15 gennaio 2025, n. 1760: pur riguardando un sequestro, essa restituisce con nitidezza il problema di fondo – destinato a ripresentarsi identico in sede di confisca – del **rapporto tra il bene digitale e il profitto del reato**.

Con la citata pronuncia, la Terza Sezione penale della Corte di cassazione ha annullato con rinvio l'ordinanza con cui il Tribunale del riesame di Firenze aveva confermato la convalida del sequestro probatorio di 1,88805294 bitcoin, per un controvalore di euro 120.638,20 corrispondente all'imposta ritenuta evasa, in un procedimento per dichiarazione infedele ex art. 4 d.lgs. n. 74 del 2000 relativa a plusvalenze da operazioni di *trading*.

Va detto subito, per evitare l'equivoco in cui sono incorsi alcuni commentatori, che **la Corte non ha affermato l'insequestrabilità delle cryptovalute**. L'annullamento è intervenuto per vizio di motivazione: da un lato per la carenza di argomentazione sulla finalità probatoria perseguita, dall'altro perché il riesame, affermando il nesso di derivazione fra i bitcoin e un profitto consistente in un'imposta evasa quantificata in euro, aveva finito «*con il legittimare un sequestro probatorio del profitto del reato non diretto, ma per equivalente*». È un rilievo di coerenza interna, non una preclusione: ma è un rilievo che ogni difensore avrà interesse a riproporre ogniqualvolta l'oggetto appreso non dovesse coincidere con il profitto come giuridicamente individuato.

Ciò che, ai fini del presente Focus, la sentenza offre di più rilevante sta però in un passaggio ricostruttivo. La Corte osserva che le valute virtuali non sono emesse da una banca centrale, che per esse «*non vige il principio nominalistico*», che non svolgono le funzioni tipiche della moneta e che, in ragione dell'estrema volatilità, «*non vi è chi possa stabilizzarne in via autoritaria i corsi e da qui discendono le oscillazioni del cambio che*

generano incertezze in sede di conversione». È la Corte, dunque, a qualificare l'incertezza in sede di conversione come dato strutturale del bene: ed è esattamente il dato con cui le nuove disposizioni dovranno misurarsi.

La **prima di tali novità** è il **nuovo art. 536-bis c.p.p.**, introdotto dall'art. 3 dello schema, a norma del quale, in tutti i casi in cui debba essere disposta la confisca per equivalente, il giudice *«con la sentenza di condanna, individua specificamente i beni di valore equivalente assoggettati a confisca oppure determina la somma di denaro di valore equivalente oggetto della confisca»*. La disposizione risponde a **un'esigenza reale di determinatezza** del vincolo ablativo e merita adesione. Applicata a un bene privo di principio nominalistico, però, l'alternativa che essa disegna assume conseguenze di rilievo.

Le due opzioni, sul piano applicativo, conducono a esiti opposti.

Se il giudice individua specificamente la cripto-attività, l'oggetto della confisca è certo ma il suo valore no: fra la sentenza e l'esecuzione, infatti, il controvalore può mutare sensibilmente, in eccesso o in difetto rispetto alla stima.

Se, invece, il giudice determina una somma di denaro equivalente, è il valore a essere certo, ma cristallizzato a una data che l'andamento del mercato renderà presto superata, con la conseguenza che le cripto-attività da liquidare per soddisfarlo potranno risultare, al momento dell'esecuzione, più o meno di quelle considerate in sentenza.

In sintesi, **nessuna delle due opzioni è neutra, e la norma non offre criteri per orientarne la scelta**.

La **seconda novità** attiene alla **vendita anteriore alla confisca**, ed è utile tenere distinti i due piani su cui essa si articola.

Sul piano generale, l'art. 10 dello schema introduce nel **testo unico delle spese di giustizia** l'**art. 151-bis**, che consente al giudice di disporre la vendita dei beni sequestrati che *«non possono essere custoditi senza pericolo di deterioramento o di rilevanti diseconomie»*.

La disposizione non è dettata per le cripto-attività, ma detta un modello procedimentale garantito: informazione del pubblico ministero e dell'interessato, facoltà per quest'ultimo di chiedere di essere sentito entro quindici giorni a pena di decadenza, trasferimento del vincolo cautelare sulla somma ricavata, appellabilità a norma dell'art. 322-bis c.p.p. dell'ordinanza con cui è disposta la vendita, con appello che *«non sospende l'esecuzione del provvedimento»* salvo diversa determinazione del giudice per il caso di grave e irreparabile danno.

Sul piano speciale, invece, proprio per i beni che di quelle garanzie avrebbero maggiore bisogno – perché il rischio non è il deterioramento fisico, ma l'oscillazione del valore – l'art. 14, comma 2, dello schema rimette termini e modalità della vendita, *«anche d'urgenza»*, a un decreto del Presidente del Consiglio dei ministri, **senza fissare criteri sostanziali** né richiamare il modello procedimentale dell'art. 151-bis.

È il punto su cui, ad avviso di chi scrive, il dibattito in sede di parere parlamentare

potrebbe utilmente concentrarsi. La vendita anticipata di un bene volatile non è soltanto una misura di conservazione del valore: è una conversione irreversibile, che sostituisce all'*asset* una somma di denaro sulla quale il vincolo si trasferisce, riducendo a quella somma l'aspettativa restitutiva di chi la subisce. Se il valore di mercato sale, la restituzione avverrà in euro e sarà, di fatto, parziale; se scende, la vendita avrà protetto l'Erario.

Che una scelta di questo peso sia rimessa integralmente a fonte secondaria è profilo che meriterà, quanto meno, un supplemento di riflessione.

5. LA CORRELAZIONE TEMPORALE: UNA GARANZIA PIÙ AGEVOLE DA VERIFICARE SUL REGISTRO DISTRIBUITO

Il decreto non amplia soltanto i poteri ablativi: ne rafforza anche i presupposti. L'art. 2 inserisce nell'**art. 240-bis c.p.** un comma a norma del quale *«il giudice dispone la confisca quando **accerta la correlazione temporale** tra l'epoca di acquisizione dei beni e quella di svolgimento di attività delittuosa»*; l'art. 9 introduce nel codice antimafia un art. 24-bis di analogo contenuto per la confisca di prevenzione, con obbligo di indicazione specifica nel provvedimento.

La relazione illustrativa ne chiarisce la *ratio* garantistica, recependo l'elaborazione giurisprudenziale sul punto: *«la sproporzione patrimoniale e l'assenza di giustificazione lecita della provenienza dei beni non sono sufficienti, da sole, a fondare l'ablazione»*,

occorrendo accertare che i beni siano stati acquisiti in un periodo temporalmente compatibile con l'attività delittuosa.

Applicata alle cripto-attività, **questa garanzia produce un effetto opposto a quello che ci si attenderebbe**. Si è soliti pensare al patrimonio digitale come al più opaco e al meno ricostruibile: eppure, mentre per i beni tradizionali la data di acquisizione va ricostruita per via documentale, con esiti spesso faticosi e sempre opinabili, per le cripto-attività registrate su un registro distribuito ogni movimento risulta tracciato in un archivio pubblico, ordinato cronologicamente e non modificabile. La data in cui una determinata disponibilità è pervenuta a un determinato indirizzo è dunque verificabile con precisione, con un grado di attendibilità difficilmente raggiungibile mediante l'ordinaria documentazione.

In altri termini, l'argomento della correlazione temporale, che altrove è terreno fertile per sviluppare argomentazioni difensive garantiste, in materia di cripto-attività rischia di ritorcersi contro chi lo prospetta.

6. RIFLESSI OPERATIVI E CONSIDERAZIONI CONCLUSIVE

Tirando le fila, lo schema di decreto compie un passo che l'ordinamento attendeva: sottrae alla prassi la disciplina esecutiva del sequestro delle cripto-attività e la consegna a una previsione normativa, individuando un custode istituzionale e un servizio dedicato. Non è una rivoluzione, e non pretende di

esserlo: come rileva la stessa relazione illustrativa, l'intervento mira «*a colmare spazi residui non disciplinati dalla normativa vigente*». Esso assume tuttavia rilievo perché concentra l'attenzione sul segmento decisivo dell'apprensione e della custodia, vale a dire sul momento in cui si determina, in concreto, l'effettività del vincolo.

Sul piano operativo se ne ricavano, in definitiva, cinque direttrici.

La qualificazione del bene. Data l'ampiezza dichiaratamente «*descrittiva*» del rinvio a MiCA, la verifica che l'*asset* appreso rientri effettivamente nella nozione di cripto-attività, e non in una diversa categoria di beni, costituisce un passaggio argomentativo autonomo e non un presupposto implicito.

Le modalità esecutive. Poiché la norma prescrive il trasferimento «*ove possibile*» e ammette in via subordinata l'«*impossibilità tecnica*», l'autorità dovrà dare conto della via concretamente seguita e della sua idoneità ad assicurare custodia e controllo esclusivi. Laddove il trasferimento non sia avvenuto, il sindacato non potrà che concentrarsi sull'effettiva esclusività del controllo, non già sulla sua mera affermazione formale.

La collaborazione richiesta. Ogni istanza di consegna di chiavi private andrà valutata alla luce del principio *nemo tenetur se detegere*, tenendo presente che quelle chiavi danno accesso non soltanto ai beni oggetto del vincolo ma all'intero storico delle operazioni, e che nessuna norma impone all'indagato di fornirle.

Il valore. La volatilità del bene, che la Corte di cassazione ha qualificato come dato

strutturale, è argomento spendibile tanto sulla proporzionalità del vincolo quanto sulla legittimità della vendita anticipata, specie ove disposta d'urgenza e in assenza di contraddittorio effettivo.

Il profilo transnazionale. L'efficacia dell'esecuzione dipende dall'identificabilità del prestatore: quando questi sia vigilato altrove, il terreno di gioco si sposta sul regolamento (UE) 2018/1805, con i tempi e i filtri che gli sono propri.

Resta, sullo sfondo, un interrogativo di ordine pratico che nessuna norma allo stato è in grado di risolvere. L'art. 16 dello schema reca la consueta clausola di invarianza finanziaria: le amministrazioni provvederanno «*con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri a carico della finanza pubblica*». Si chiede però allo Stato di gestire portafogli digitali istituzionali, custodire chiavi crittografiche private, garantire autenticità, integrità, accessibilità e trasferibilità dei beni appresi e assicurare la tenuta informatica dell'intero sistema. Sono attività che richiedono competenze specialistiche e infrastrutture dedicate, come del resto conferma il coinvolgimento dell'Agenzia per la cybersicurezza nazionale nel procedimento di adozione del decreto attuativo previsto dall'art. 14, comma 2.

La misura del successo di questa riforma, in conclusione, non si coglierà tanto nel testo del decreto legislativo, che nell'impianto appare complessivamente equilibrato, quanto nel decreto che ne dovrà definire i contenuti tecnici e nella capacità dell'apparato applicativo di sostenerne l'attuazione. È un

giudizio che, allo stato, resta necessariamente
sospeso: varrà la pena riprenderlo quando
l'iter parlamentare sarà concluso e il decreto
attuativo adottato.

CONTATTI



Giuseppe Fornari
Founder Partner

g.fornari@fornarieassociati.com



Francesca Procopio
Partner

f.procopio@fornarieassociati.com



Luigi Francesco Corrado
Trainee Lawyer

l.corrado@fornarieassociati.com

Milano

Via Chiossetto 18

T: +39 0254122206

E: milano@fornarieassociati.com

Roma

Piazza Adriana 5

T: +39 0622201000

E: roma@fornarieassociati.com

Bari

Via Principe Amedeo 25

T: +39 080 918 4280

E: bari@fornarieassociati.com

Questa pubblicazione ha lo scopo di fornire informazioni di carattere generale rispetto all'argomento trattato e non deve quindi essere considerata come un parere legale né come una disamina esaustiva di ogni aspetto relativo alla materia oggetto del documento.

Fornari e Associati

www.fornarieassociati.com