



STUDIO LEGALE GIAMMATTEO

BLOCKCHAIN

La catena e la prova

Registri distribuiti, smart contract e cripto-attività
nel diritto italiano ed europeo

Avv. Gianluca Giammatteo

PATROCINANTE IN CASSAZIONE

Blockchain. La catena e la prova

Registri distribuiti, smart contract e cripto-attività nel diritto italiano ed europeo.

Autore: Avv. Gianluca Giammatteo, del Foro di Isernia, Patrocinante in Cassazione.

Edizione a cura dello Studio Legale Giammatteo — Via Nicandro Iosso n. 6, 86079 Venafro (IS).

Testo aggiornato al mese di luglio 2026.

L'opera ha finalità informativa e formativa. Non costituisce parere legale, non instaura alcun rapporto professionale e non sostituisce l'esame del caso concreto. I riferimenti normativi e giurisprudenziali sono aggiornati alla data indicata e vanno verificati prima di ogni utilizzo in atti giudiziari; si rinvia alla nota sulle fonti posta in chiusura.

© Studio Legale Giammatteo. Tutti i diritti riservati. È vietata la riproduzione, anche parziale, senza autorizzazione scritta.

Indice

Presentazione	4
PARTE PRIMA — La tecnologia	5
I. Che cosa è la blockchain	6
II. Come funziona: hash, chiavi, consenso	8
III. Famiglie di registri e tipologie di token	11
IV. Smart contract e organizzazioni decentralizzate	13
PARTE SECONDA — Il quadro normativo	16
V. Il diritto dell'Unione europea	17
VI. Il diritto italiano	19
VII. Il regime fiscale delle plusvalenze	21
PARTE TERZA — Diritto sostanziale e prova	23
VIII. La qualificazione giuridica delle cripto-attività	24
IX. Il contratto e la responsabilità dei prestatori	26
X. Il valore probatorio della registrazione	28
XI. Blockchain e protezione dei dati personali	30
PARTE QUARTA — Il processo	32
XII. Il processo civile e l'esecuzione	33
XIII. Il processo penale	35
XIV. La tutela della vittima di frode	37
XV. Cripto-attività, crisi d'impresa e insolvenza	39
XVI. Conclusioni	41
L'autore	42
Nota sulle fonti e avvertenze	44

Presentazione

Questo scritto nasce da una constatazione ricorrente nella pratica professionale: la blockchain viene descritta, quasi sempre, o con l'entusiasmo di chi la vende o con il sospetto di chi la teme, e quasi mai con il linguaggio sobrio del giurista, che è poi l'unico linguaggio utile quando una controversia arriva davanti a un giudice.

Lo Studio Legale Giammatteo si occupa da anni di cripto-attività, di frodi commesse per il tramite di piattaforme di scambio, di sequestri e di recuperi, di procedure di sovraindebitamento nelle quali compaiono portafogli digitali, di compliance in materia di responsabilità amministrativa degli enti. Da questa esperienza deriva la convinzione che il problema principale, oggi, non sia comprendere la tecnologia — che è, nella sua struttura essenziale, molto più semplice di quanto la divulgazione lasci intendere — ma collocarla correttamente entro categorie giuridiche che le preesistono e che, nella maggior parte dei casi, sono perfettamente in grado di governarla.

Il volume è costruito in quattro parti. La prima descrive la tecnologia con il grado di dettaglio necessario a un giurista, senza indulgere in tecnicismi superflui ma senza neppure quelle semplificazioni che, trasferite in un atto, generano errori. La seconda ricostruisce il quadro normativo europeo e nazionale, oggi profondamente mutato per effetto del regolamento europeo sulle cripto-attività e del decreto legislativo di adeguamento dell'ordinamento nazionale al regolamento europeo. La terza affronta i profili civilistici e, in particolare, il tema decisivo dell'efficacia probatoria della registrazione su registro distribuito. La quarta è dedicata al processo: al processo civile, al processo esecutivo, al processo penale e alla tutela concreta di chi sia rimasto vittima di una frode.

Un'avvertenza è doverosa e viene ripetuta in chiusura. La materia è in rapidissima evoluzione normativa e interpretativa. Le indicazioni contenute in questo volume sono aggiornate alla data indicata nel colophon e non costituiscono parere legale né possono sostituire l'esame del caso concreto. Ogni riferimento normativo deve essere verificato alla data di redazione dell'atto.

Avv. Gianluca Giammatteo Patrocinante in Cassazione

PARTE PRIMA

La tecnologia

CAPITOLO I

Che cosa è la blockchain

Un registro senza custode

La blockchain è, prima di ogni altra cosa, un registro. Non un registro qualsiasi: un registro contabile che annota in sequenza degli eventi — tipicamente trasferimenti di unità di valore — e che presenta due caratteristiche congiunte, difficilmente presenti insieme negli archivi tradizionali. La prima è che il registro non è custodito da un soggetto determinato, ma è replicato in modo identico presso una molteplicità di nodi indipendenti. La seconda è che le annotazioni, una volta consolidate, possono essere aggiunte ma non modificate né sopprese senza che l'alterazione risulti immediatamente rilevabile.

L'archivio giuridicamente tradizionale — il registro immobiliare, il registro delle imprese, il libro giornale, il conto corrente bancario — poggia su un custode: un ufficio pubblico, un notaio, un intermediario, la cui affidabilità è garantita dall'ordinamento attraverso regole di responsabilità, vigilanza e sanzione. La blockchain sostituisce la fiducia nel custode con la fiducia in un procedimento: un insieme di regole matematiche e di incentivi economici che rendono, per chi volesse alterare il registro, l'alterazione più costosa del vantaggio che se ne trarrebbe.

Da qui discende l'espressione, spesso abusata, di «macchina della fiducia». È espressione da maneggiare con prudenza, perché descrive bene ciò che la tecnologia effettivamente fa e descrive malissimo ciò che non fa. Su questo punto occorre essere netti fin da subito, perché è il punto dal quale dipende la maggior parte degli equivoci giudiziari.

Ciò che la blockchain garantisce e ciò che non garantisce

La blockchain garantisce l'integrità e la sequenza cronologica del dato registrato. Consente cioè di affermare, con un grado di attendibilità tecnica assai elevato, che una determinata stringa di dati era presente nel registro a partire da un certo blocco e che da quel momento non è stata modificata. Consente inoltre di affermare che l'annotazione è stata autorizzata da chi disponeva di una determinata chiave crittografica privata.

La blockchain non garantisce, invece, nulla di ciò che sta al di fuori del registro. Non garantisce che il dato registrato sia veritiero; non garantisce che chi ha utilizzato la chiave privata ne fosse il legittimo titolare; non garantisce che la merce descritta in un certificato annotato sulla catena esista, sia conforme o sia stata consegnata; non garantisce che il soggetto identificato da un indirizzo alfanumerico sia una determinata

persona fisica. La registrazione di una falsità su blockchain produce una falsità perfettamente conservata e cronologicamente certa.

È il problema che la letteratura tecnica chiama *oracle problem*: la catena è impermeabile all'alterazione interna, ma dipende integralmente dalla qualità dei dati che vi vengono immessi dall'esterno. Per il giurista la conseguenza è immediata: la registrazione su blockchain è idonea a provare l'esistenza e l'antiorità di un documento informatico, non la verità del fatto che quel documento rappresenta. È esattamente la stessa distinzione che l'ordinamento conosce da sempre in tema di atto pubblico, dove la fede privilegiata copre ciò che il pubblico ufficiale attesta essere avvenuto in sua presenza e non la veridicità delle dichiarazioni rese dalle parti.

La definizione normativa

Il legislatore italiano ha fornito una definizione positiva. Il cosiddetto decreto semplificazioni definisce le tecnologie basate su registri distribuiti come «le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturealmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili».

La definizione è tecnicamente accettabile e giuridicamente neutra: descrive un genere — i registri distribuiti — di cui la blockchain in senso stretto, ossia il registro organizzato in blocchi concatenati, costituisce una specie. Nel prosieguo i due termini saranno usati in modo tendenzialmente equivalente, salvo dove la distinzione assuma rilievo.

CAPITOLO II

Come funziona: hash, chiavi, consenso

La funzione di hash

Il primo mattone è una funzione matematica chiamata funzione di hash crittografica. Essa riceve in ingresso una qualsiasi sequenza di dati — un carattere, un contratto, un film — e restituisce in uscita una stringa di lunghezza fissa, l'impronta. La funzione possiede tre proprietà rilevanti. È deterministica: al medesimo ingresso corrisponde sempre la medesima impronta. È sensibile: la modifica di un solo bit dell'ingresso produce un'impronta completamente diversa. È praticamente irreversibile: dall'impronta non è possibile risalire al documento di origine.

Il rilievo giuridico è evidente. L'impronta consente di dimostrare l'identità di un documento senza rivelarne il contenuto. È possibile depositare su un registro pubblico l'impronta di una scrittura riservata, di un progetto industriale, di un'opera dell'ingegno, e conservare il documento presso di sé: la corrispondenza tra il documento esibito in giudizio e l'impronta registrata sarà verificabile da chiunque, mentre il contenuto resterà segreto fino all'esibizione.

La catena

I dati non vengono registrati singolarmente, ma raggruppati in blocchi. Ogni blocco contiene, oltre alle transazioni, l'impronta del blocco immediatamente precedente. Ne deriva una concatenazione: modificare una transazione contenuta in un blocco remoto muterebbe l'impronta di quel blocco, e quindi renderebbe incoerente il blocco successivo, e così via fino all'ultimo blocco prodotto. Per rendere credibile la falsificazione occorrerebbe ricalcolare l'intera catena a valle e imporla alla maggioranza dei nodi, operazione che nelle reti pubbliche di maggiori dimensioni richiede risorse computazionali ed energetiche proibitive.

All'interno di ciascun blocco le transazioni sono ordinate in una struttura ad albero, detta albero di Merkle, che consente di verificare l'appartenenza di una singola transazione al blocco senza dover scaricare l'intero blocco. È il meccanismo che rende possibile, in concreto, la verifica giudiziale di una singola operazione contestata.

Chiavi, firme e portafogli

L'autorizzazione delle operazioni si fonda sulla crittografia asimmetrica. Ogni utente dispone di una coppia di chiavi matematicamente correlate: una chiave privata, che deve restare segreta, e una chiave pubblica, dalla quale si deriva l'indirizzo, cioè la stringa che identifica la posizione sul registro. Chi vuole disporre delle unità associate a un indirizzo firma la transazione con la chiave privata; chiunque può verificare, con la sola chiave pubblica, che la firma è autentica.

Occorre disfarsi di una rappresentazione diffusa e inesatta: il portafoglio digitale non contiene monete. Le unità esistono soltanto come annotazioni sul registro. Il portafoglio contiene chiavi. La conseguenza pratica è di enorme rilievo giuridico e processuale: chi detiene la chiave privata dispone effettivamente del valore, chiunque sia il titolare formale; e chi perde la chiave privata perde irreversibilmente la disponibilità, senza che alcuna autorità possa ripristinarla. Non esiste, nelle reti pubbliche, un potere di annullamento o di storno equiparabile a quello dell'intermediario bancario.

Da questa struttura discende anche la distinzione fondamentale tra custodia diretta, nella quale l'utente conserva personalmente le chiavi, e custodia presso terzi, nella quale le chiavi sono detenute da una piattaforma di scambio o da un prestatore di servizi di custodia. Nella seconda ipotesi — di gran lunga la più diffusa — l'utente non ha alcun potere tecnico diretto sul registro: vanta un diritto di credito, o comunque una pretesa restitutoria, nei confronti del prestatore. È un dato che condiziona interamente la scelta dello strumento di tutela.

Il consenso e la finalità

Poiché nessun soggetto ha l'ultima parola, la rete deve dotarsi di un procedimento per stabilire quale sia la versione valida del registro. È il meccanismo di consenso. Nelle reti che adottano la prova di lavoro i nodi competono nella soluzione di un problema computazionale la cui risoluzione richiede consumo di energia; in quelle che adottano la prova di partecipazione il diritto di proporre il blocco è attribuito in funzione del capitale vincolato a garanzia, che viene decurtato in caso di comportamento sleale. In entrambi i casi il risultato è che l'attacco costa più di quanto renda.

Ne consegue un'osservazione rilevante per il consulente tecnico: nelle reti a prova di lavoro la definitività dell'annotazione non è immediata ma probabilistica. La probabilità che un blocco venga sostituito decresce esponenzialmente con il numero di blocchi successivi, ma non si annulla mai in senso matematico. Le perizie che descrivano la registrazione come «immutabile» in senso assoluto sono, dal punto di vista tecnico, imprecise, e possono essere aggredite in contraddittorio. La formulazione corretta è che l'annotazione è, decorso un congruo numero di conferme, praticamente irreversibile.

Pseudonimato, non anonimato

Un ultimo chiarimento, decisivo per la materia delle frodi. Le reti pubbliche non sono anonime: sono pseudonime. Ogni transazione è pubblica, permanente e consultabile

da chiunque; ciò che non compare è il collegamento tra l'indirizzo e l'identità anagrafica del titolare. Tale collegamento, però, tende a emergere nei punti di contatto con il sistema finanziario tradizionale, cioè presso le piattaforme di scambio, che sono soggette a obblighi di adeguata verifica della clientela.

È su questa asimmetria che si fonda l'intera tecnica investigativa dell'analisi della catena: seguire il flusso dei fondi da indirizzo a indirizzo, raggruppare gli indirizzi riconducibili a un medesimo soggetto e individuare il punto in cui il valore entra in un servizio regolamentato, dal quale è possibile ottenere, con provvedimento dell'autorità, i dati identificativi. È il motivo per cui, nella pratica, il tempo è la variabile decisiva.

CAPITOLO III

Famiglie di registri e tipologie di token

Registri aperti e registri chiusi

La distinzione più rilevante attiene alla possibilità di partecipare alla rete. Nei registri permissionless chiunque può leggere il registro, inviare transazioni e concorrere alla validazione, senza autorizzazione preventiva e senza identificazione. Nei registri permissioned l'accesso, in tutto o in parte, è riservato a soggetti identificati e ammessi secondo regole di governance predeterminate; è la struttura tipica dei consorzi tra imprese, delle filiere logistiche e delle applicazioni della pubblica amministrazione.

La differenza non è tecnica soltanto. Nel registro chiuso esiste un soggetto o un insieme di soggetti identificabili che determinano le finalità e i mezzi del funzionamento del sistema: esiste, quindi, un centro di imputazione di responsabilità, un titolare del trattamento ai sensi del regolamento europeo sulla protezione dei dati personali, un contraddittore processuale. Nel registro aperto tale centro manca, ed è questa mancanza a generare i problemi più seri, dalla individuazione del legittimato passivo alla esecuzione dei provvedimenti giudiziali.

Da un punto di vista strettamente probatorio, peraltro, i due modelli non si equivalgono. Il registro aperto offre garanzie di resistenza all'alterazione più robuste, ma non offre alcuna garanzia sull'identità dei partecipanti. Il registro chiuso offre identità certe, ma la sua integrità dipende dalla governance del consorzio, e dunque, in ultima analisi, dalla fiducia in soggetti determinati: il che lo rende, dal punto di vista dell'efficacia probatoria, più simile a un archivio informatico affidabile che a un registro autonomamente attendibile.

I token e la loro classificazione

Sul registro possono essere rappresentate entità diverse, genericamente denominate token. La distinzione tecnica primaria è tra token fungibili, reciprocamente sostituibili e frazionabili, e token non fungibili, ciascuno dotato di identificativo unico e perciò infungibile.

La distinzione giuridicamente decisiva è però funzionale e attiene alla causa concreta dell'operazione. Si distinguono così, in via descrittiva, i token di pagamento, concepiti come mezzo di scambio; i token di utilizzo, che attribuiscono il diritto di accedere a un bene o a un servizio offerto dall'emittente; i token di investimento, che incorporano di-

ritti di natura patrimoniale o partecipativa assimilabili a quelli tipici degli strumenti finanziari; i token collegati ad attività e i token di moneta elettronica, che mirano a mantenere un valore stabile mediante ancoraggio a una o più attività di riferimento o a una valuta avente corso legale.

Le ultime due categorie hanno oggi definizione normativa espressa nel regolamento europeo sulle crypto-attività. Le prime tre restano categorie descrittive: la qualificazione giuridica di un token di investimento come strumento finanziario, o comunque come prodotto finanziario, discende non dal nome che gli attribuisce l'emittente ma dalla struttura dell'operazione, secondo un criterio funzionale ormai affermato: impiego di capitale, aspettativa di rendimento di natura finanziaria, assunzione di un rischio direttamente connesso a quell'impiego.

Una precisazione sui token non fungibili

Merita un chiarimento la posizione dei token non fungibili, spesso presentati come strumenti di circolazione di opere dell'ingegno. Il token registrato sulla catena non incorpora l'opera: contiene, di regola, un riferimento a una risorsa esterna, sovente conservata su un server ordinario. L'acquisto del token non comporta, salvo specifica pattuizione, alcun trasferimento dei diritti di utilizzazione economica dell'opera ai sensi della legge sul diritto d'autore. Chi acquista acquista, in mancanza di diversa previsione contrattuale, una posizione registrata su un registro, non un diritto d'autore. È un equivoco che ha già generato contenzioso e che va prevenuto in sede di redazione delle condizioni di vendita.

CAPITOLO IV

Smart contract e organizzazioni decentralizzate

Una definizione ingannevole

Il medesimo decreto definisce lo smart contract come «un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse».

La denominazione è infelice, perché lo smart contract non è un contratto e non è intelligente. Non è intelligente perché si limita a eseguire in modo deterministico un'istruzione condizionale predisposta dai programmatori. Non è un contratto perché non è una manifestazione di volontà, ma uno strumento di esecuzione automatica di un regolamento negoziale che le parti hanno formato altrove, con le regole ordinarie.

La distinzione è tutt'altro che teorica. Il contratto resta soggetto alle regole sulla formazione dell'accordo, sulla causa, sull'oggetto, sui vizi del consenso e sull'invalidità; il programma è la modalità con cui l'esecuzione avviene. Che l'esecuzione sia automatica non sottrae il rapporto al sindacato del giudice: se il presupposto del trasferimento era viziato, il trasferimento eseguito dal programma è ripetibile secondo le regole ordinarie, secondo la disciplina della ripetizione dell'indebito, e ciò a prescindere dalla circostanza che la catena non consenta di annullare l'operazione.

Il nodo della forma scritta

La medesima disposizione prosegue stabilendo che gli smart contract soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dall'entrata in vigore della legge di conversione. Una ulteriore previsione rimette all'Agenzia l'individuazione degli standard tecnici necessari a produrre gli effetti sopra descritti.

Allo stato delle verifiche condotte, tali linee guida non risultano adottate. Il termine, fissato a novanta giorni dall'entrata in vigore della relativa legge di conversione, è ampiamente decorso; un gruppo di lavoro fu istituito presso l'Agenzia nel 2019 e un testo risulta essere stato predisposto, senza che sia seguita l'adozione formale. La conseguenza è che la disposizione, nella parte in cui subordina l'effetto all'intervento amministrativo, non ha ricevuto attuazione.

Ne discende una conclusione operativa che va assunta con chiarezza nella redazione degli atti: allo stato non è predicabile, in via automatica, né l'equivalenza dello smart contract alla forma scritta, né l'attribuzione alla registrazione su registro distribuito degli effetti della validazione temporale elettronica qualificata. Chi voglia conseguire con certezza tali effetti deve ricorrere agli strumenti previsti dal regolamento europeo in materia di identificazione elettronica e servizi fiduciari e dal codice dell'amministrazione digitale, eventualmente combinandoli con la registrazione su catena, che opera allora come elemento di rafforzamento e non come fonte autonoma dell'effetto.

AVVERTENZA OPERATIVA

La registrazione su blockchain non sostituisce, allo stato, la firma elettronica qualificata né la marca temporale qualificata. È consigliabile associare alla registrazione su catena una sottoscrizione digitale conforme al regolamento europeo sui servizi fiduciari e, ove opportuno, la conservazione a norma del documento.

Oracoli e patologie

Poiché il programma opera solo sui dati presenti nella catena, l'esecuzione condizionata a fatti del mondo esterno richiede un oracolo, cioè un servizio che immetta il dato esterno. L'oracolo è, giuridicamente, il punto debole dell'intera costruzione: è un terzo, la cui attività è fonte di responsabilità contrattuale o extracontrattuale, e la cui eventuale corruzione o malfunzionamento determina un'esecuzione conforme al programma ma difforme dal regolamento negoziale.

Le patologie ricorrenti sono essenzialmente tre. La prima è la divergenza tra il testo del contratto e il codice che dovrebbe eseguirlo: in tal caso prevale il regolamento negoziale, da ricostruire secondo i criteri ermeneutici dettati in materia di interpretazione del contratto, e l'esecuzione difforme genera obbligo restitutorio o risarcitorio. La seconda è il difetto del programma, che può integrare inadempimento del predisponente o responsabilità del produttore del software. La terza è la sopravvenienza, che il programma per definizione non contempla: eccessiva onerosità, impossibilità, mutamento normativo. È buona tecnica redazionale prevedere espressamente meccanismi di sospensione o disattivazione del programma e la designazione di un soggetto legittimato ad attivarli, poiché l'assenza di tali previsioni non elimina il diritto ma ne rende costosissima l'attuazione.

Le organizzazioni autonome decentralizzate

Un cenno meritano le cosiddette organizzazioni autonome decentralizzate, strutture nelle quali le decisioni sono assunte mediante votazione dei portatori di token e attuate da programmi. In assenza di un tipo legale che le contempli, il rischio che la fattispecie sia ricondotta alla società di fatto, con conseguente responsabilità illimitata e

solidale dei partecipanti, non è affatto teorico. La costituzione di un veicolo societario di diritto positivo, che agisca quale involucro dell'organizzazione, resta la soluzione prudentiale.

PARTE SECONDA

Il quadro normativo

CAPITOLO V

Il diritto dell'Unione europea

Il regolamento europeo sulle crypto-attività

Il quadro europeo è stato ridisegnato dal regolamento europeo relativo ai mercati delle crypto-attività, comunemente indicato con la sigla MiCAR. Il regolamento è applicabile dal 30 dicembre 2024, mentre le disposizioni dei Titoli III e IV, relative ai token collegati ad attività e ai token di moneta elettronica, si applicano dal 30 giugno 2024.

L'impianto è articolato su tre direttrici. La prima riguarda l'emissione e l'offerta al pubblico di crypto-attività diverse dai token collegati ad attività e dai token di moneta elettronica, subordinata alla pubblicazione di un documento informativo — il *white paper* — redatto secondo un contenuto minimo predeterminato e notificato all'autorità competente. La seconda concerne le due categorie speciali di token stabili, per le quali è prevista una disciplina più stringente, che include l'autorizzazione dell'emittente, la costituzione e la gestione della riserva di attività, il diritto di rimborso dei possessori e poteri di intervento delle autorità di vigilanza. La terza attiene ai prestatori di servizi per le crypto-attività, che possono operare soltanto previa autorizzazione e che sono assoggettati a requisiti organizzativi, patrimoniali e di condotta modellati su quelli dell'intermediazione finanziaria, ivi compresi obblighi di custodia e segregazione delle attività della clientela.

Il regolamento introduce inoltre una disciplina degli abusi di mercato riferita alle crypto-attività ammesse alla negoziazione, con divieti di abuso di informazioni privilegiate, di comunicazione illecita e di manipolazione. Va segnalato che l'ambito di applicazione presenta esclusioni rilevanti: restano fuori, in particolare, le crypto-attività che siano qualificabili come strumenti finanziari, soggette alla disciplina propria, nonché i token non fungibili unici e non fungibili tra loro, salvo il ricorrere di condizioni che ne rivelino la natura sostanzialmente seriale.

Il regime pilota per le infrastrutture di mercato

Con il regolamento europeo sul regime pilota per le infrastrutture di mercato basate su registri distribuiti il legislatore europeo ha istituito un regime pilota per le infrastrutture di mercato basate sulla tecnologia a registro distribuito, consentendo, entro limiti quantitativi e con esenzioni temporanee da specifici obblighi della disciplina sui mercati finanziari, la negoziazione e il regolamento di strumenti finanziari emessi in forma tokenizzata. Si tratta di uno strumento di sperimentazione regolamentata, la cui rilevanza pratica per la clientela ordinaria è al momento limitata, ma che segnala con

chiarezza la direzione: la tokenizzazione degli strumenti finanziari, e non la creazione di attività alternative, è il terreno sul quale la tecnologia è destinata a incidere maggiormente sull'ordinamento.

Identità digitale e validazione temporale

Il regolamento europeo in materia di identificazione elettronica e servizi fiduciari disciplina l'identificazione elettronica e i servizi fiduciari. Ai fini che qui interessano rileva in particolare la disposizione che attribuisce alla validazione temporale elettronica qualificata la presunzione di accuratezza della data e dell'ora indicate e di integrità dei dati associati, e le disposizioni relative alla firma elettronica qualificata, equiparata alla firma autografa. Il quadro è stato modificato dal successivo intervento europeo in materia di identità digitale, che ha introdotto il portafoglio europeo di identità digitale e ampliato il catalogo dei servizi fiduciari qualificati, includendovi, tra l'altro, i registri elettronici.

Quest'ultimo dato merita attenzione: la valorizzazione del registro elettronico quale servizio fiduciario qualificato apre una prospettiva nella quale la registrazione su registro distribuito, se effettuata da un prestatore qualificato secondo standard armonizzati, potrà conseguire effetti probatori presuntivi in tutto lo spazio europeo. È la strada attraverso la quale, verosimilmente, verrà colmata la lacuna lasciata aperta dalla mancata attuazione di tale previsione.

Antiriciclaggio e tracciabilità dei trasferimenti

Il regolamento europeo sui trasferimenti di fondi e di cripto-attività ha esteso ai trasferimenti di cripto-attività la disciplina già prevista per i trasferimenti di fondi, imponendo ai prestatori di servizi l'obbligo di accompagnare l'operazione con i dati identificativi dell'ordinante e del beneficiario: è la cosiddetta *travel rule*, che costituisce, sul piano investigativo, lo strumento più efficace di ricostruzione dei flussi.

A ciò si aggiunge il pacchetto normativo del 2024, composto dal regolamento europeo in materia di prevenzione del riciclaggio in materia di prevenzione dell'uso del sistema finanziario a fini di riciclaggio e finanziamento del terrorismo, dal regolamento istitutivo dell'Autorità europea antiriciclaggio istitutivo dell'Autorità europea antiriciclaggio e dalla direttiva europea in materia di prevenzione del riciclaggio, che disegnano un assetto armonizzato di obblighi e una vigilanza sovranazionale. Sul versante fiscale, la direttiva europea sullo scambio automatico di informazioni estende lo scambio automatico di informazioni ai prestatori di servizi per le cripto-attività, riducendo drasticamente l'opacità delle posizioni detenute all'estero.

CAPITOLO VI

Il diritto italiano

La norma di principio e la sua attuazione mancata

Come già osservato, l'ordinamento italiano ha anticipato il legislatore europeo con una norma di principio. La disposizione contiene anzitutto le definizioni; attribuisce poi alla memorizzazione di un documento informatico mediante tecnologie basate su registri distribuiti gli effetti giuridici della validazione temporale elettronica; e subordina tale effetto all'individuazione, da parte dell'Agenzia per l'Italia digitale, degli standard tecnici che le tecnologie devono possedere.

La struttura della norma è quella di una previsione a efficacia condizionata. Poiché gli standard non risultano essere stati adottati, la tesi preferibile — e quella che appare più difendibile in giudizio — è che l'effetto legale tipico non si sia ancora prodotto in via generale. Ciò non significa che la registrazione su catena sia processualmente irrilevante: significa che essa non gode di un effetto presuntivo automatico e va valutata dal giudice secondo le regole ordinarie in tema di prova documentale e di prova atipica, delle quali si dirà nel capitolo X.

Il decreto di adeguamento nazionale

L'adeguamento dell'ordinamento nazionale al regolamento europeo sulle crypto-attività è stato realizzato con il decreto legislativo di adeguamento dell'ordinamento nazionale al regolamento europeo. 215 del 13 settembre 2024 ed entrato in vigore il giorno successivo.

Il decreto designa la Consob e la Banca d'Italia quali autorità nazionali competenti, ripartendo le attribuzioni secondo il criterio delle finalità: alla Consob la trasparenza e la correttezza dei comportamenti, la tutela degli investitori e l'ordinato svolgimento delle negoziazioni; alla Banca d'Italia la sana e prudente gestione, l'adeguatezza patrimoniale, il contenimento del rischio e la stabilità. Alle autorità sono attribuiti poteri regolamentari, informativi, ispettivi, cautelari e di intervento sui prodotti. Il decreto disciplina altresì la separazione patrimoniale delle crypto-attività e dei fondi della clientela, profilo di rilievo decisivo in caso di insolvenza del prestatore.

Sul piano sanzionatorio l'impianto è prevalentemente amministrativo, con sanzioni pecuniarie di importo assai elevato per le persone giuridiche. È prevista tuttavia una fattispecie penale per l'esercizio abusivo delle attività riservate, punita con la reclusione da sei mesi a quattro anni e con la multa: si tratta di disposizione destinata ad assumere rilievo crescente nel contenzioso, poiché consente di contestare l'abusivismo a chi

presti servizi in cripto-attività senza autorizzazione, senza dover previamente dimostrare la natura di prodotto finanziario del bene negoziato.

Antiriciclaggio e registro OAM

Prima dell'entrata in vigore del quadro europeo, l'ordinamento italiano aveva assoggettato a obblighi antiriciclaggio i prestatori di servizi relativi all'utilizzo di valuta virtuale e i prestatori di servizi di portafoglio digitale, mediante la normativa antiriciclaggio, più volte modificata in sede di recepimento delle direttive europee. La normativa di settore ha imposto l'iscrizione in una sezione speciale del registro tenuto dall'Organismo degli agenti e dei mediatori, con modalità e tempistiche definite dal decreto ministeriale attuativo.

L'iscrizione costituiva condizione per l'esercizio legittimo dell'attività sul territorio nazionale. Con l'applicazione del regolamento europeo sulle cripto-attività e del decreto di adeguamento nazionale il regime è destinato a essere assorbito dal sistema autorizzatorio europeo, secondo le previsioni transitorie applicabili agli operatori già attivi. Nel contenzioso in corso, tuttavia, la disciplina previgente conserva rilievo per i fatti anteriori, ed è dato spesso decisivo per fondare la contestazione di abusivismo o per allegare la responsabilità dell'intermediario che abbia operato in violazione degli obblighi di adeguata verifica.

Il monitoraggio fiscale

Le cripto-attività detenute sono oggetto di obblighi dichiarativi ai fini del monitoraggio fiscale, mediante indicazione nel quadro RW della dichiarazione dei redditi, ed è dovuta l'imposta sul valore delle cripto-attività introdotta dalla legge di bilancio che ha introdotto il regime impositivo delle cripto-attività. L'omissione espone a sanzioni autonome e, in presenza di plusvalenze non dichiarate, può integrare gli estremi dei reati tributari. Trattandosi di materia di stretta competenza del consulente fiscale, ci si limita in questa sede alla segnalazione, con l'avvertenza che il quadro sanzionatorio e dichiarativo è stato più volte modificato.

CAPITOLO VII

Il regime fiscale delle plusvalenze

L'assetto vigente

Il regime impositivo delle plusvalenze da cripto-attività è stato introdotto dalla legge di bilancio che ha introdotto il regime impositivo delle cripto-attività, che ha inserito nel testo unico delle imposte sui redditi la disposizione che qualifica come redditi diversi le plusvalenze e gli altri proventi realizzati mediante rimborso, cessione a titolo oneroso, permuta o detenzione di cripto-attività. La plusvalenza è determinata quale differenza tra il corrispettivo percepito e il costo o valore di acquisto documentato, secondo le regole ordinarie.

Nell'assetto originario l'imposizione operava con aliquota del ventisei per cento e con una soglia di rilevanza di duemila euro. La successiva legge di bilancio è intervenuta due volte: ha eliminato la soglia, con decorrenza dal 1° gennaio 2025, e ha elevato l'aliquota al trentatré per cento per le plusvalenze e gli altri proventi realizzati a decorrere dal 1° gennaio 2026.

Da ultimo, la più recente legge di bilancio ha introdotto un'eccezione: restano soggetti all'aliquota del ventisei per cento i redditi derivanti da operazioni di detenzione, cessione o impiego di token di moneta elettronica denominati in euro secondo la definizione accolta dal regolamento europeo, intendendosi per tali i token il cui valore è stabilmente ancorato all'euro e le cui riserve sono integralmente detenute in attività denominate in euro presso soggetti autorizzati nell'Unione. La medesima disposizione precisa che non costituisce realizzo la mera conversione tra euro e token di moneta elettronica denominati in euro, né il rimborso in euro del valore nominale.

Alcune implicazioni pratiche

Tre indicazioni meritano di essere evidenziate, per la frequenza con cui il tema si presenta nella pratica difensiva.

La prima riguarda le permuta. Lo scambio tra cripto-attività aventi medesime caratteristiche e funzioni non è, secondo l'impostazione accolta, fiscalmente realizzativo, mentre lo è la conversione in valuta avente corso legale o in cripto-attività di natura diversa. La corretta ricostruzione dello storico delle operazioni è quindi indispensabile e va documentata mediante estrazione integrale dei registri della piattaforma.

La seconda riguarda l'onere documentale. In assenza di documentazione del costo di acquisto, l'amministrazione tende ad assumere valore nullo, con conseguente tassa-

zione dell'intero corrispettivo. La conservazione dei rendiconti, delle conferme d'ordine e degli estratti conto bancari collegati è, sotto questo profilo, un adempimento difensivo prima ancora che contabile.

La terza riguarda i rapporti tra pretesa tributaria e sequestro penale. Come si vedrà nel capitolo XIII, l'apprensione di cripto-attività quale profitto di un reato tributario incontra limiti significativi, che discendono proprio dalla circostanza che esse non costituiscono moneta avente corso legale.

AVVERTENZA

La materia fiscale è stata modificata in tre esercizi consecutivi. Ogni valutazione va condotta con riferimento alla data di realizzo e previa verifica della normativa e della prassi vigenti, in raccordo con il consulente fiscale.

PARTE TERZA

Diritto sostanziale e prova

CAPITOLO VIII

La qualificazione giuridica delle crypto-attività

Non sono moneta

Il punto di partenza è negativo e sufficientemente consolidato: le crypto-attività non costituiscono moneta avente corso legale. Non sono emesse da un'autorità monetaria, non hanno efficacia solutoria imposta dall'ordinamento, non liberano il debitore se non in forza di accordo delle parti. Ai soli fini dell'imposta sul valore aggiunto è riconosciuta, in ambito europeo, la loro assimilazione ai mezzi di pagamento, con conseguente esenzione delle operazioni di cambio; ma si tratta di qualificazione funzionale e settoriale, non estensibile senza cautela ad altri ambiti.

Tale carattere assume rilievo anche in sede penale, e in particolare in materia di sequestro: le crypto-attività non svolgono le funzioni tipiche della moneta avente corso legale e sono soggette a continue fluttuazioni di valore, sicché la loro apprensione non può essere trattata come se avesse a oggetto denaro.

Sono beni

Escluso il carattere monetario, resta da stabilire che cosa siano. L'impostazione preferibile le riconduce alla categoria dei beni immateriali suscettibili di formare oggetto di diritti: entità dotate di autonomo valore economico, individuabili, trasferibili e aggredibili dai creditori. Il regolamento europeo sulle crypto-attività, del resto, adotta una definizione che ne presuppone la natura di rappresentazione digitale di valore o di diritti trasferibile e memorizzabile elettronicamente mediante tecnologia a registro distribuito.

Dalla qualificazione come bene discendono conseguenze pratiche di rilievo. Le crypto-attività rientrano nella garanzia patrimoniale generica e sono aggredibili in executivis. Cadono in successione, con il problema, tutt'altro che teorico, della trasmissione delle chiavi private agli eredi. Ricadono nella comunione legale tra coniugi secondo le regole ordinarie sugli acquisti. Devono essere inventariate nelle procedure di regolazione della crisi e dell'insolvenza. Possono formare oggetto di conferimento, di pegno e di patti di garanzia, con le difficoltà esecutive che la particolare natura del bene comporta.

Quando diventano prodotto finanziario

La qualificazione muta, e con essa il regime applicabile, quando l'operazione presenta la struttura dell'investimento finanziario. Ove la vendita di valute virtuali sia reclamizzata quale vera e propria proposta di investimento, l'attività è soggetta agli adempimenti previsti dal testo unico della finanza, la cui omissione integra il reato di abusivismo finanziario.

Il criterio adottato è funzionale e coincide con quello elaborato in tema di prodotto finanziario atipico: impiego di capitale, aspettativa di rendimento di natura finanziaria, assunzione di un rischio direttamente connesso all'impiego del capitale. Ricorrendo tali elementi, la causa concreta dell'operazione attrae il bene nella nozione di prodotto finanziario del testo unico, con l'intero corredo di obblighi informativi, di prospetto e di riserva di attività.

Per il difensore della persona offesa da una frode il rilievo è considerevole: consente di affiancare alla contestazione di truffa quella di abusivismo, che ha struttura di pericolo e non richiede la prova degli artifici, e di attivare i poteri di intervento della Consob. Per il difensore dell'operatore, per converso, il terreno di difesa è la ricostruzione della causa concreta e delle modalità di offerta.

CAPITOLO IX

Il contratto e la responsabilità dei prestatori

Il rapporto con la piattaforma

Nella grande maggioranza dei casi il rapporto giuridicamente rilevante non intercorre tra l'utente e la catena, ma tra l'utente e una piattaforma di scambio. La qualificazione di tale rapporto è controversa e va condotta caso per caso sulla base delle condizioni generali: possono ricorrere elementi del mandato, del deposito, della commissione e del contratto di custodia, spesso combinati.

Il dato decisivo è che l'utente, nella custodia presso terzi, non ha alcuna disponibilità tecnica diretta: vanta una pretesa restitutoria. Ne discende che, in caso di insolvenza del prestatore, la sorte della pretesa dipende dall'effettiva segregazione delle attività della clientela. Il regolamento europeo sulle cripto-attività e il decreto di adeguamento nazionale impongono oggi obblighi espressi di detenzione e segregazione: la loro violazione, oltre a fondare responsabilità dell'operatore, costituisce elemento centrale nella ricostruzione delle pretese in sede concorsuale.

Clausole, consumatore e giurisdizione

Le condizioni generali predisposte dalle piattaforme presentano con frequenza clausole di limitazione o esonero di responsabilità, clausole di deroga alla giurisdizione e alla legge applicabile, clausole arbitrali e clausole di modifica unilaterale.

Tali previsioni vanno vagliate con rigore. Le clausole che escludono o limitano preventivamente la responsabilità per dolo o colpa grave sono nulle. Ove l'utente rivesta la qualità di consumatore, opera la disciplina del codice del consumo, con presunzione di vessatorietà per le clausole che sanciscono deroghe alla competenza dell'autorità giudiziaria del luogo di residenza del consumatore, e trova applicazione, nei rapporti transfrontalieri all'interno dell'Unione, la disciplina protettiva del regolamento europeo sulla competenza giurisdizionale e sul riconoscimento delle decisioni in materia civile e commerciale, che consente al consumatore di agire davanti al giudice del proprio domicilio. La legge applicabile è individuata secondo il regolamento europeo sulla legge applicabile alle obbligazioni contrattuali, con il limite delle disposizioni imperative di protezione.

L'esperienza professionale insegna che la contestazione della clausola di deroga è, nella pratica, il primo vero scoglio del contenzioso contro piattaforme estere, ed è ter-

reno sul quale conviene investire argomentazione fin dall'atto introduttivo.

La responsabilità del prestatore

Le fattispecie ricorrenti sono sostanzialmente quattro: la sottrazione di fondi per effetto di accesso abusivo all'account dell'utente; la perdita di disponibilità per violazione dei sistemi della piattaforma; l'esecuzione di ordini non autorizzati; l'omesso o inesatto adempimento degli obblighi di adeguata verifica e di segnalazione, che abbia consentito il transito dei proventi di una frode.

Nelle prime tre ipotesi la responsabilità si atteggia in termini contrattuali, secondo le regole ordinarie in tema di inadempimento e onere del prestatore di provare che l'inadempimento è dipeso da causa a lui non imputabile; assume rilievo centrale l'adeguatezza delle misure di sicurezza, valutabile anche alla luce degli obblighi imposti dal regolamento europeo sulla protezione dei dati personali e, per gli operatori vigilati, dalle disposizioni di settore. Nella quarta ipotesi la responsabilità è tipicamente extracontrattuale nei confronti del terzo danneggiato, e va costruita sul nesso tra la violazione della regola cautelare e il danno, con le difficoltà probatorie che ciò comporta. È materia ancora in assestamento, nella quale l'esito dipende in misura decisiva dalla qualità della ricostruzione tecnica.

CAPITOLO X

Il valore probatorio della registrazione

Documento informatico e riproduzioni

La registrazione su registro distribuito è, dal punto di vista processuale, un documento informatico. Il regime è quello dettato dal codice dell'amministrazione digitale, e dalle norme del codice civile in tema di riproduzioni meccaniche.

Il documento informatico sottoscritto con firma elettronica qualificata o digitale ha l'efficacia propria della scrittura privata riconosciuta. Il documento informatico privo di sottoscrizione qualificata è liberamente valutabile dal giudice, tenuto conto delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità. Il codice civile attribuisce alle riproduzioni informatiche piena efficacia rappresentativa dei fatti e delle cose rappresentate se colui contro il quale sono prodotte non ne disconosce la conformità.

Su quest'ultimo punto occorre precisione, perché è il terreno su cui si gioca la maggior parte delle controversie. Il disconoscimento non è una formula di stile: perché sia efficace la contestazione deve essere chiara, circostanziata ed esplicita, e indicare in modo specifico gli aspetti di difformità rispetto all'originale, non essendo sufficiente una negazione generica. Il difensore che intenda contestare una registrazione deve dunque indicare che cosa non corrisponde, e non limitarsi a negare.

Il nodo della validazione temporale

Si è già osservato che il decreto semplificazioni attribuirebbe alla memorizzazione su registro distribuito gli effetti della validazione temporale elettronica, ma che tale effetto è subordinato all'individuazione di standard tecnici da parte dell'Agenzia per l'Italia digitale, che allo stato non risultano adottati.

La conclusione operativa è duplice. In sede di redazione degli atti è imprudente affermare che la registrazione su blockchain gode ex lege della presunzione riconosciuta alla validazione temporale qualificata: l'affermazione è aggredibile e indebolisce l'intera costruzione difensiva. È invece corretto, e assai più solido, sostenere che la registrazione costituisce documento informatico dotato di elevate caratteristiche oggettive di sicurezza, integrità e immodificabilità, e che tali caratteristiche, tecnicamente dimostrate, orientano la libera valutazione del giudice e possono fondare presunzioni gravi, precise e concordanti.

SINTESI OPERATIVA

La registrazione su blockchain prova l'esistenza e l'anteriorità del dato, non la verità del fatto rappresentato. Non gode automaticamente della presunzione propria della validazione temporale qualificata. Va introdotta in giudizio come documento informatico, corredata di verifica tecnica e catena di custodia.

Come si porta in giudizio una registrazione

Il passaggio dalla catena al fascicolo processuale richiede metodo. L'esperienza suggerisce alcune cautele.

Occorre anzitutto acquisire l'evidenza in modo ripetibile: l'estrazione della transazione da un servizio di consultazione pubblico va documentata con indicazione della data e dell'ora, dello strumento utilizzato e dell'identificativo della transazione, e va accompagnata dal calcolo dell'impronta del file prodotto, così da consentire il successivo controllo di integrità. È buona pratica far eseguire l'acquisizione da un tecnico e formalizzarla in un referto, ovvero, nei casi di maggiore rilievo, in un atto notarile di attestazione.

Occorre in secondo luogo dimostrare la corrispondenza tra il documento e l'impronta registrata, e non limitarsi ad affermarla: è operazione elementare, ma che va compiuta e documentata.

Occorre infine ricostruire il collegamento tra l'indirizzo e la persona. È il punto più delicato: la catena prova che una chiave ha firmato, non chi ne disponeva. Il collegamento si costruisce con elementi esterni — corrispondenza, documentazione della piattaforma, flussi bancari, dati di adeguata verifica — e in giudizio si regge, di regola, su un ragionamento presuntivo. Nel processo penale, dove opera il principio del libero convincimento, la ricostruzione può fondarsi su un compendio indiziario; nel processo civile essa deve confrontarsi con la ripartizione dell'onere della prova.

CAPITOLO XI

Blockchain e protezione dei dati personali

Un'antinomia strutturale

Il regolamento europeo sulla protezione dei dati personali attribuisce all'interessato il diritto alla rettifica e alla cancellazione dei dati e impone al titolare l'obbligo di limitarne la conservazione. La blockchain, per costruzione, non consente la cancellazione. L'antinomia è evidente e non risolvibile in via interpretativa.

Il primo problema è di qualificazione. La chiave pubblica e l'indirizzo costituiscono, di regola, dati personali pseudonimizzati: non rivelano direttamente l'identità, ma consentono l'identificazione mediante l'impiego di informazioni aggiuntive, che nel caso di specie esistono e sono detenute dai prestatori di servizi. La conclusione, sostenuta dalla dottrina prevalente, è che il regolamento si applichi.

Il secondo problema è l'individuazione del titolare del trattamento. Nei registri chiusi il titolare è identificabile nel consorzio o nel soggetto che ne determina finalità e mezzi. Nei registri aperti l'individuazione è problematica, e le soluzioni proposte — contitolarietà dei nodi validatori, responsabilità del soggetto che immette il dato, esclusione del trattamento per finalità esclusivamente personali — sono tutte insoddisfacenti sotto qualche profilo.

Le soluzioni tecniche e la loro tenuta

La prassi ha elaborato accorgimenti che consentono di ridurre la frizione. Il più diffuso consiste nel non registrare sulla catena il dato personale, ma soltanto la sua impronta, conservando il dato in un archivio esterno: la cancellazione del dato esterno rende l'impronta priva di significato, poiché dall'impronta non è possibile risalire al contenuto. Analogo effetto si ottiene con la cifratura del dato registrato e la successiva distruzione della chiave.

Tali soluzioni sono ragionevoli, ma vanno adottate con consapevolezza: la loro tenuta presuppone che l'impronta o il dato cifrato non consentano, con mezzi ragionevolmente disponibili, l'identificazione dell'interessato, valutazione che va condotta in concreto e documentata. La progettazione dell'architettura secondo i principi di protezione dei dati fin dalla fase di ideazione, imposta dalla disciplina europea, non è dunque un adempimento formale ma la sede propria in cui il problema va risolto, prima che il sistema entri in esercizio. Rimediare dopo, su una catena in funzione, è tecnicamente

impossibile.

PARTE QUARTA

Il processo

CAPITOLO XII

Il processo civile e l'esecuzione

L'onere della prova e l'istruttoria

Nel giudizio civile la ripartizione dell'onere probatorio resta governata dalla regola generale del codice civile, senza deroghe. Chi agisce per la restituzione di cripto-attività o per il risarcimento del danno deve provare il titolo, l'avvenuto trasferimento e la riferibilità dell'operazione alla controparte; chi eccepisce l'adempimento o l'esistenza di una causa giustificativa deve provarla.

La difficoltà pratica si concentra sulla riferibilità soggettiva. Nella custodia presso una piattaforma il problema è attenuato, perché il rapporto è documentato e l'operatore detiene i dati di adeguata verifica; nel trasferimento diretto tra indirizzi la ricostruzione è affidata a un ragionamento presuntivo, che deve poggiare su elementi gravi, precisi e concordanti.

Sul piano degli strumenti, l'istanza di esibizione, rivolta al terzo prestatore di servizi, è lo strumento naturale per acquisire lo storico delle operazioni e i dati identificativi; la richiesta di informazioni alla pubblica amministrazione può risultare utile ove pendano parallelamente accertamenti dell'autorità di vigilanza. Va tenuto presente che l'ordine di esibizione ha efficacia limitata nei confronti di soggetti stabiliti fuori dall'Unione, e che in tali ipotesi la via penale, con i suoi strumenti di cooperazione, risulta di regola più efficace.

La consulenza tecnica

La consulenza tecnica d'ufficio è, in questa materia, pressoché indispensabile. La qualità del quesito determina la qualità dell'accertamento; è opportuno che il quesito chieda al consulente di verificare l'esistenza e il contenuto delle transazioni indicate, di ricostruire il flusso dei trasferimenti a partire dagli indirizzi individuati, di accertare l'eventuale riconducibilità di più indirizzi a un medesimo soggetto secondo le tecniche di raggruppamento comunemente adottate, di individuare i servizi regolamentati di destinazione e di quantificare i valori alle date rilevanti, precisando il criterio di conversione adottato.

Ove sussista pericolo di dispersione dell'evidenza, l'accertamento tecnico preventivo consente di cristallizzare la situazione e, al contempo, di tentare la composizione della lite. La nomina di un consulente tecnico di parte, in ogni caso, non è un lusso: l'analisi della catena è disciplina specialistica e il contraddittorio tecnico è la sede in cui si formano gli errori più costosi.

Cautela ed esecuzione

Sul versante cautelare, il sequestro conservativo può avere a oggetto le cripto-attività detenute presso un prestatore identificato, che assume la posizione di terzo custode. Nei confronti delle piattaforme è talora praticabile il ricorso d'urgenza per ottenere il blocco temporaneo dell'account, misura la cui efficacia dipende dalla localizzazione dell'operatore e dalla sua disponibilità a dare esecuzione spontanea.

Sul versante esecutivo, lo strumento naturale è il pignoramento presso terzi, dove terzo è il prestatore di servizi presso il quale le cripto-attività risultano detenute. La ricerca dei beni con modalità telematiche può fornire, attraverso i flussi bancari, l'indicazione della piattaforma utilizzata. È utile che l'atto di pignoramento e la dichiarazione richiesta al terzo siano formulati in modo da comprendere tanto i saldi in valuta avente corso legale quanto le cripto-attività, indicate per denominazione e quantità, e da imporre al terzo il divieto di disporre.

Restano fuori dalla portata dell'esecuzione, di fatto, le cripto-attività detenute in autocustodia: senza la chiave privata nessun ausiliario può disporre del bene. In tali ipotesi lo strumento residuo è l'ordine giudiziale di consegna delle credenziali rivolto al debitore, con le conseguenze processuali e, ove ne ricorrano i presupposti, penali dell'inottemperanza. È terreno ancora poco battuto nella pratica, e va affrontato con argomentazione accurata.

CAPITOLO XIII

Il processo penale

Le fattispecie ricorrenti

Le condotte illecite realizzate mediante cripto-attività si distribuiscono su un numero contenuto di fattispecie. La truffa copre la generalità degli schemi fondati su artifici o raggiri, dalle finte piattaforme di investimento alle promesse di rendimento garantito. La frode informatica e l'accesso abusivo a sistema informatico ricorrono nelle sottrazioni realizzate mediante violazione di credenziali. La sostituzione di persona accompagna con frequenza le condotte realizzate su piattaforme di messaggistica e social network.

Sul versante finanziario, l'abusivismo e l'abusiva attività finanziaria si affiancano oggi alla fattispecie di esercizio abusivo introdotta dal decreto di adeguamento nazionale. Sul versante della circolazione dei proventi vengono in rilievo la ricettazione, il riciclaggio, l'impiego e l'autoriciclaggio, quest'ultimo di particolare rilievo perché la conversione in cripto-attività dei proventi di un delitto costituisce condotta idonea a ostacolarne l'identificazione.

Nelle vicende di maggiori dimensioni, caratterizzate da una struttura promozionale organizzata, la contestazione associativa consente di aggregare posizioni altrimenti frammentate e di attivare strumenti investigativi più incisivi.

Le indagini e l'acquisizione della prova

L'attività investigativa si articola su due piani. Il primo è l'analisi della catena, che consente di seguire il flusso dei valori a partire dall'indirizzo di destinazione dei fondi della persona offesa, di raggruppare gli indirizzi riconducibili al medesimo soggetto e di individuare il punto di ingresso in un servizio regolamentato. Il secondo è l'acquisizione, presso tale servizio, dei dati identificativi e della documentazione di adeguata verifica.

Gli strumenti sono quelli ordinari: gli accertamenti tecnici, il sequestro probatorio, e in particolare il sequestro di dati informatici presso i fornitori di servizi, introdotto in attuazione della Convenzione di Budapest dalla legge di ratifica della Convenzione di Budapest. Nei rapporti con operatori stabiliti in altri Stati membri l'ordine europeo di indagine penale è la via ordinaria; il quadro è destinato a essere integrato dalla disciplina europea sulle prove elettroniche, che introduce ordini di produzione direttamente indirizzabili ai prestatori di servizi.

Un'osservazione di metodo: la tempestività è il fattore critico. I proventi vengono di regola movimentati e frazionati entro poche ore, e ogni giorno trascorso riduce la probabilità di intercettare il valore in un punto aggredibile. La denuncia va dunque presentata immediatamente e corredata fin da subito degli identificativi delle transazioni, senza attendere la ricostruzione completa della vicenda.

Sequestro e confisca

Il sequestro preventivo può avere a oggetto cripto-attività, tipicamente mediante ordine rivolto alla piattaforma che le detiene ovvero mediante apprensione delle chiavi private e trasferimento a un portafoglio nella disponibilità dell'autorità giudiziaria.

Esiste però un limite significativo, che la difesa può utilmente valorizzare. Sequestrare una quantità di cripto-attività corrispondente per controvalore alla somma costituente profitto del reato non equivale a sequestrare il profitto diretto: significa, in realtà, procedere a un sequestro per equivalente avente a oggetto non moneta avente corso legale, bensì un bene digitale privo delle funzioni tipiche della moneta e soggetto a continue fluttuazioni di valore. Ne discende un più rigoroso onere di motivazione sul nesso di derivazione fra il bene appreso e il reato, che va sollecitato e, ove mancante, censurato.

Restano poi i problemi, tutt'altro che marginali, della custodia e della gestione: la volatilità del bene rende la conservazione in natura una scelta gestoria con conseguenze patrimoniali, e la conversione anticipata solleva questioni di legittimità e di responsabilità. È materia nella quale la prassi è ancora in formazione e nella quale il difensore può utilmente intervenire con istanze specifiche.

CAPITOLO XIV

La tutela della vittima di frode

Le prime quarantotto ore

La fase iniziale è decisiva e va gestita con freddezza. Occorre interrompere immediatamente ogni ulteriore versamento; conservare integralmente le evidenze, comprese le conversazioni, le schermate, i messaggi di posta elettronica con le intestazioni complete, le ricevute dei bonifici e gli identificativi delle transazioni; raccogliere gli indirizzi di destinazione dei fondi.

Se il trasferimento è avvenuto da un conto corrente, va immediatamente sollecitata alla banca l'attivazione delle procedure di richiamo dell'operazione; se è avvenuto con carta di pagamento, va verificata la percorribilità della procedura di contestazione presso l'emittente, nei termini contrattuali. Se le somme risultano transitate su una piattaforma identificata, la segnalazione all'operatore, corredata degli identificativi, può condurre al congelamento del conto di destinazione: molte piattaforme vi provvedono in via cautelativa in attesa del provvedimento dell'autorità.

Va infine detto con chiarezza ciò che non va fatto. Non va dato seguito alle offerte di recupero che pervengono, spesso a breve distanza dalla denuncia, da sedicenti società specializzate che richiedono il pagamento anticipato di somme a titolo di sblocco, di imposte o di spese: si tratta, nella quasi totalità dei casi, di una seconda frode ai danni della medesima vittima, condotta da soggetti che dispongono degli elenchi dei danneggiati.

La strategia

La denuncia-querela deve essere costruita, non compilata. Deve contenere la ricostruzione cronologica e discorsiva dei fatti, l'indicazione puntuale delle somme e delle date, gli identificativi delle transazioni e degli indirizzi, la documentazione dei rapporti con la piattaforma, l'indicazione delle norme che si assumono violate e la richiesta di adozione dei provvedimenti cautelari urgenti, oltre alla richiesta di essere informati dell'eventuale richiesta di archiviazione. Va presentata nel termine di legge, tenendo conto della disciplina della procedibilità applicabile alle singole fattispecie.

Sul piano civile, l'azione risarcitoria può essere proposta autonomamente ovvero mediante costituzione di parte civile nel processo penale, con i vantaggi propri di quest'ultima soluzione in termini di accesso al compendio investigativo e di possibile provvisorio. Ove siano identificati beni aggredibili, il sequestro conservativo penale e quello civile vanno valutati con urgenza.

L'azione collettiva

Nelle frodi seriali, che coinvolgono decine o centinaia di danneggiati, l'aggregazione delle posizioni produce vantaggi concreti: consente di ricostruire lo schema nella sua interezza, di dimostrare la sistematicità della condotta e quindi il dolo, di ripartire i costi della consulenza tecnica, di conferire alla vicenda il rilievo necessario a ottenere un'assegnazione investigativa adeguata.

Lo Studio Legale Giammatteo ha maturato in questo ambito un'esperienza consolidata, avendo curato querele collettive con decine di querelanti in vicende di rilievo nazionale relative a piattaforme di scambio e a schemi di investimento in cripto-attività, con attività di tracciamento dei flussi e di individuazione dei servizi di destinazione. L'organizzazione dell'azione richiede rigore: raccolta uniforme della documentazione, ordinamento alfabetico delle posizioni, quantificazione individuale del danno, unitarietà della ricostruzione giuridica.

CAPITOLO XV

Cripto-attività, crisi d'impresa e insolvenza

L'attivo che non si vede

La presenza di cripto-attività nel patrimonio di un debitore assoggettato a una procedura di regolazione della crisi o dell'insolvenza pone problemi peculiari. Il codice della crisi d'impresa e dell'insolvenza impone al debitore obblighi di informazione e di consegna dei beni, e attribuisce agli organi della procedura poteri di apprensione. Ma l'apprensione di un bene che esiste soltanto come annotazione su un registro e la cui disponibilità dipende dal possesso di una chiave privata non è operazione materialmente eseguibile senza la collaborazione del debitore.

Ne discende che il tema si sposta sul piano dei doveri di collaborazione e delle conseguenze della loro violazione: sul piano processuale, in termini di valutazione della meritevolezza e di accesso al beneficio dell'esdebitazione; sul piano penale, in termini di eventuale rilevanza delle condotte di sottrazione o occultamento dell'attivo.

Per l'organo della procedura è dunque essenziale che l'attività di ricerca sia condotta con metodo fin dall'inizio: esame dei conti correnti alla ricerca di bonifici verso piattaforme di scambio, richieste agli operatori identificati, esame della documentazione fiscale e in particolare del quadro relativo al monitoraggio, verifica delle dichiarazioni rese dal debitore. L'omessa indicazione di posizioni in cripto-attività è oggi, statisticamente, una delle ipotesi più frequenti di incompletezza dell'inventario.

Sovraindebitamento e composizione negoziata

Nelle procedure che riguardano il consumatore e il debitore civile, la presenza di perdite subite in operazioni su cripto-attività si presenta con frequenza crescente e pone un problema di valutazione della colpa nella formazione dell'indebitamento. La linea difensiva va costruita con attenzione: occorre distinguere la scelta di investimento imprudente, che non esclude di per sé la meritevolezza, dalla condotta gravemente colposa consistita nel contrarre debiti per alimentare operazioni speculative in assenza di ogni ragionevole prospettiva di rimborso. La documentazione del contesto — in particolare l'eventuale ricorrere di una condotta fraudolenta altrui ai danni del debitore — è spesso decisiva.

Nella composizione negoziata e negli strumenti di regolazione della crisi d'impresa, per converso, la presenza di cripto-attività nell'attivo richiede una valutazione pruden-

ziale del valore, ancorata a criteri dichiarati e a date certe, e la predisposizione di presidi che evitino che la volatilità del bene comprometta l'attendibilità del piano.

CAPITOLO XVI

Conclusioni

Chi si avvicini alla materia con l'aspettativa di trovare un ordinamento nuovo resterà deluso. La tecnologia dei registri distribuiti non ha creato uno spazio esente dal diritto: ha creato un modo diverso di conservare informazioni, al quale l'ordinamento applica, con gli aggiustamenti necessari, categorie che gli preesistono. Il contratto resta il contratto, la proprietà resta la proprietà, la prova resta soggetta alle regole della prova.

Tre indicazioni conclusive riassumono quanto precede.

La prima è che la blockchain prova l'integrità e l'anteriorità del dato, non la verità del fatto rappresentato né l'identità di chi ha operato. Ogni ricostruzione difensiva che confonda questi piani è destinata a essere smontata in contraddittorio.

La seconda è che il quadro normativo è oggi, per la prima volta, sufficientemente definito: il regolamento europeo sulle cripto-attività e il decreto di adeguamento nazionale hanno ricondotto la prestazione di servizi in cripto-attività entro un sistema di riserva di attività e di vigilanza, e ciò muta radicalmente il terreno del contenzioso, rendendo contestabile in via diretta l'esercizio abusivo. Resta invece irrisolto, sul piano interno, il nodo dell'efficacia probatoria, per effetto della mancata attuazione di tale previsione.

La terza è che, nella tutela della vittima, il fattore determinante non è la sofisticazione dell'argomentazione ma la tempestività dell'intervento e il rigore nella raccolta e nella conservazione delle evidenze. È in quelle prime ore che si decide, nella maggior parte dei casi, se il valore sarà recuperabile.

L'autore

Avv. Gianluca Giammatteo

Gianluca Giammatteo, nato a Venafro (IS) l'8 luglio 1972, è avvocato del Foro di Isernia, iscritto all'albo tenuto dal Consiglio dell'Ordine degli Avvocati di Isernia dal dicembre 2002, e patrocinante dinanzi alla Corte di cassazione e alle altre giurisdizioni superiori.

Esercita la professione presso lo Studio Legale Giammatteo, con sede in Venafro (IS) alla via Nicandro Iosso n. 6, assistendo privati, professionisti e imprese in Molise, nel basso Lazio e, per le materie di specializzazione, su tutto il territorio nazionale. L'operatività ordinaria copre i circondari di Isernia, Campobasso, Cassino e Frosinone, con attività di udienza e domiciliazione senza costi di trasferta a carico del cliente.

Le aree di attività

L'attività professionale si è progressivamente concentrata su alcune direttrici. La prima è la difesa penale, nella fase delle indagini e nel giudizio dinanzi a ogni autorità giudiziaria, tanto per l'indagato e l'imputato quanto per la persona offesa e la parte civile. La seconda è il contenzioso civile, in materia di contratti, responsabilità, recupero del credito e responsabilità civile da sinistro stradale. La terza è la tutela delle vittime di frodi in crypto-attività, con attività di ricostruzione dei flussi, individuazione dei prestatori di servizi di destinazione e coordinamento di azioni collettive. La quarta è la tutela della reputazione digitale, che comprende la rimozione di contenuti diffamatori, la deindicizzazione dai motori di ricerca, il diritto all'oblio e l'azione risarcitoria per il danno all'immagine.

A queste si affiancano la consulenza in materia di responsabilità amministrativa degli enti, con predisposizione e aggiornamento dei modelli di organizzazione, gestione e controllo, e l'assistenza nelle procedure di regolazione della crisi e dell'insolvenza disciplinate dal codice della crisi d'impresa, ivi comprese le procedure di composizione della crisi da sovraindebitamento e l'esdebitazione.

L'esperienza in materia di crypto-attività

Nel settore delle frodi realizzate mediante crypto-attività lo Studio ha maturato un'esperienza consolidata, occupandosi da anni di assistenza alle vittime, anche in vicende di rilievo internazionale, e curando querele collettive con decine di danneggiati, con attività di tracciamento dei trasferimenti, di individuazione dei servizi regolamentati di destinazione e di interlocuzione con l'autorità giudiziaria procedente. È da tale

esperienza che nasce il presente volume.

Il metodo

Tre criteri orientano l'attività dello Studio. Il fascicolo è seguito direttamente dall'avvocato, e non da un ufficio: il cliente sa sempre con chi parla e a che punto si trova il procedimento. Il preventivo precede il conferimento dell'incarico, con indicazione di ciò che è compreso e di ciò che dipende dall'andamento del giudizio. La strategia è preceduta dall'ascolto del caso e da una valutazione realistica delle prospettive, anche quando questa comporti sconsigliare l'azione.

CONTATTI

Studio Legale Giammatteo — Via Nicandro Iosso n. 6, 86079 Venafro (IS). Tel. 0865.1945640 — Mobile 348.0359103. studiolegale@giammatteo.it — studiolegale@pec.giammatteo.it — www.giammatteo.it

Nota sulle fonti e avvertenze

Il presente volume ha finalità divulgativa e formativa. Non costituisce parere legale, non instaura alcun rapporto professionale e non può sostituire l'esame del caso concreto da parte di un professionista abilitato.

Per scelta redazionale il volume non riporta citazioni puntuali: né di decisioni giurisdizionali, né di norme individuate per numero, data o articolo. Le fonti sono richiamate per denominazione e per contenuto, in forma discorsiva. La ragione è pratica. La disciplina delle cripto-attività è mutata più volte in pochi anni e gli orientamenti interpretativi sono in movimento: un riferimento numerico stampato in un volume divulgativo invecchia rapidamente e rischia di essere invocato quando non è più attuale.

Ne discende un'avvertenza che va presa alla lettera. Le indicazioni qui contenute servono a orientare, non a fondare un atto. Prima di ogni utilizzo in sede giudiziaria o stragiudiziale gli estremi delle norme e delle pronunce vanno ricostruiti e verificati sulle fonti ufficiali, con l'assistenza di un professionista abilitato.

Si segnala inoltre che l'affermazione relativa alla mancata adozione, da parte dell'Agenzia per l'Italia digitale, delle linee guida e degli standard tecnici previsti dal decreto semplificazioni riflette le verifiche condotte alla data di redazione e non risulta smentita da fonti ufficiali; se ne raccomanda comunque l'aggiornamento, poiché su di essa poggia la conclusione esposta nel capitolo X in tema di efficacia probatoria.

La materia è in rapida evoluzione. Ogni riferimento va verificato alla data di utilizzo.



Studio Legale Giammatteo

Avv. Gianluca Giammatteo — Patrocinante in Cassazione

Foro di Isernia

Via Nicandro Iosso n. 6 — 86079 Venafro (IS)

Tel. 0865.1945640 — Mobile 348.0359103

studiolegale@giammatteo.it

studiolegale@pec.giammatteo.it

www.giammatteo.it

P.IVA 00412250946 — C.F. GMMGLC72L08L725M

AREE DI ATTIVITÀ

Frodi in cripto-attività e recupero — azioni collettive

Compliance D.Lgs. 231/2001 — modelli organizzativi

Crisi d'impresa e sovraindebitamento (CCII)

Contenzioso civile e difesa penale — reputazione digitale

Il presente volume ha finalità informativa e non costituisce parere legale.

© Studio Legale Giammatteo — Tutti i diritti riservati