

## Utilizzi a scopi illeciti delle criptovalute: recenti profili giurisprudenziali e normativi italiani ed internazionali e riferimenti al mercato degli NFT.

di **Nicola Mainieri e Nico Di Gabriele** <sup>1</sup>

**Sommario.** **1.** Premessa. - **2.** Il processo legislativo europeo in corso: Regolamento MiCA e *Single Rule Book AML*. - **3.** La recente giurisprudenza statunitense – il tema degli NFT. - **4.** La giurisprudenza di legittimità italiana – note a sentenze di Cassazione n. 2868 del 7 ottobre 2021 e n. 45397 del 9 dicembre 2021. - **5.** Le novità regolamentari italiane: il decreto M.E.F. del 13 gennaio 2022. - **6.** Conclusioni

### 1. Premessa.

La Direzione Investigativa Antimafia, nella sua recente relazione al Parlamento, ha sottolineato come dalle indagini emerge sempre di più l'interesse della criminalità organizzata alle più moderne tecnologie e in particolare a tutti gli strumenti che permettono un rapido e invisibile passaggio di denaro "con ricorso a pagamenti effettuati con criptovalute" <sup>2</sup>. Su altro fronte, nello scorso aprile, la Commissione Europea, dopo aver ancora una volta ribadito come - per via delle transazioni in gran parte anonime - le criptovalute siano ampiamente utilizzate per attività criminali, ha sottolineato che, sulla scia della guerra in Ucraina, i paesi dell'Unione Europea hanno limitato il commercio di criptovalute da utilizzare in Russia o con entità russe <sup>3</sup>. La Commissione ha inoltre fornito agli operatori chiarimenti in merito all'estensione alle criptovalute in tema di sanzioni alla Russia per l'invasione dell'Ucraina, stabilendo che le criptovalute sono comprese nelle sanzioni alla Russia ed evidenziando come - nel regolamento (UE) n. 269/2014 <sup>4</sup> - le definizioni a carattere non esaustivo di "fondi" e di

---

<sup>1</sup> Le opinioni espresse sono a titolo esclusivamente personale e non riflettono necessariamente quelle dell'Istituzione di provenienza.

<sup>2</sup> Direzione Investigativa Antimafia – DIA, 26 marzo 2022, *Relazione del Ministro dell'Interno al Parlamento I Semestre 2021*, pagg. 401 e segg.

<sup>3</sup> Commissione Europea "I rischi delle criptovalute e i vantaggi della legislazione UE" 6 aprile 2022

<sup>4</sup> Regolamento n. 269/2014 del 17 marzo 2014 "Misure restrittive relative ad azioni che compromettono o minacciano l'integrità territoriale, la sovranità e l'indipendenza dell'Ucraina"



“risorse economiche” coprano anche le cripto<sup>5</sup>. Il Comitato ECON del Parlamento Europeo<sup>6</sup> ha recentemente osservato che le cripto-attività supportano l’adozione di aggressivi schemi di pianificazione fiscale e ostacolano l’accertamento degli imponibili fiscali<sup>7</sup> e ha pertanto invitato ad una forte cooperazione tra gli Stati Membri e a livello internazionale<sup>8</sup> per prevenire l’evasione fiscale.

Le criptovalute o “valute virtuali” costituiscono la principale espressione del sistema della *blockchain*, e fanno parte di quell’ormai vastissimo fenomeno formatosi senza una guida centralizzata negli anni successivi al 2008 che sconta l’assenza di una qualsivoglia attività di vigilanza ma è in costante espansione: la loro capitalizzazione complessiva è attualmente pari a circa 1.300 miliardi di dollari<sup>9</sup> e sono scambiati da oltre 300 milioni di persone, mentre - secondo il World Economic Forum - entro il 2025 il 10% del PIL mondiale transiterà su tecnologia *blockchain*<sup>10</sup>.

Come ricordato dalla Banca d’Italia, le nuove tecnologie possono indubbiamente offrire vantaggi al consumatore ma l’adozione da parte degli intermediari di innovazioni tecnologiche improntate a maggiore efficienza non deve prescindere dai requisiti di affidabilità e sicurezza che concorrono a mantenere la fiducia del pubblico nella moneta e la stabilità finanziaria. A questi si affiancano quelli della tutela dell’utenza - nuovi servizi o prodotti devono assicurare relazioni corrette fra la clientela e gli intermediari - e della lotta al riciclaggio dei profitti illeciti e al finanziamento del terrorismo, a fronte delle potenziali vulnerabilità a cui essi possono esporre il sistema

---

<sup>5</sup> “le criptovalute sono coperte dalle disposizioni sul congelamento dei beni e sul divieto di mettere fondi o risorse economiche a disposizione di persone oggetto di misure sanzionatorie. Tutte le transazioni vietate nei Regolamenti sono vietate anche se effettuate in criptovalute”

<sup>6</sup> Bozza di ‘rapporto sull’impatto delle nuove tecnologie sulla tassazione: cripto e blockchain’ [https://www.europarl.europa.eu/doceo/document/ECON-AM-731829\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/ECON-AM-731829_EN.pdf)

<sup>7</sup> Al riguardo si noti che solo 5 dei 27 Stati Membri hanno stabilito un quadro regolamentare per la tassazione delle cripto-attività.

<sup>8</sup> Si è recentemente conclusa la fase di pubblicazione consultazione sul Crypto-asset reporting framework (CARF) promosso dall’Organizzazione per la cooperazione e lo sviluppo economico (OCSE) e finalizzato all’avvio di un meccanismo per lo scambio di informazioni su base internazionale relativo alle transazioni in cripto-attività e finalizzato a contrastare l’evasione fiscale. Infatti, l’esistente ‘Common reporting standard – CRS’ si applica esclusivamente alle fiat *currency* e alle ‘tradizionali’ attività.

<sup>9</sup> Vedi: <https://coinmarketcap.com/it/charts>, dati al 24 maggio 2022

<sup>10</sup> Vedi [https://www3.weforum.org/docs/WEF\\_Building-Blockchains.pdf](https://www3.weforum.org/docs/WEF_Building-Blockchains.pdf)

finanziario <sup>11</sup>. D'altro canto, l'utilizzo di nuove tecnologie, in particolare l'Intelligenza Artificiale, potrebbe in un futuro sempre più prossimo essere d'ausilio all'amministrazione della giustizia ed al *criminal law enforcement*, nel rispetto di requisiti stringenti, come indicati nella proposta normativa della Commissione Europea dell'aprile 2021 <sup>12</sup>.

Pur tuttavia, la mancanza di un corso legale delle cripto - non emesse o garantite da una banca centrale o da un'autorità pubblica - non solo le priva di quel vincolo di legge che possa renderle obbligatoriamente accettate per l'estinzione delle obbligazioni pecuniarie, ma rende ancor più stringente la necessità di rendere il loro vasto mercato per quanto possibile indenne da fenomeni di riciclaggio e/o finanziamento del terrorismo. Risulta per questo essenziale seguire lo sviluppo della regolamentazione AML/CFT sul versante internazionale e nazionale, nonché quello della giurisprudenza, oramai anche di legittimità, che si sta formando sul punto: l'obiettivo principale è proprio quello di "creare un contesto di regole che identifichino bene i prodotti e consentano di creare un regime di controllo che presidi i rischi e sviluppi l'innovazione"<sup>13</sup>.

## **2. Il processo legislativo europeo in corso: Regolamento MiCA e *Single Rule Book AML*.**

Il quadro regolamentare europeo in materia di contrasto al riciclaggio a mezzo di cripto-attività è ancora in addivenire poiché, benché la Commissione Europea abbia presentato già il 20 settembre 2020 la proposta per il c.d. *Digital Finance Package*<sup>14</sup> e il 20 luglio 2021 la proposta di *Single Rule Book AML*<sup>15</sup>, l'iter approvativo non è ancora concluso.

Le due iniziative legislative presentano diverse interconnessioni poiché il *Single Rule Book AML* rinvia, tra gli altri, in materia di definizioni al

---

<sup>11</sup> Vedi in proposito Banca d'Italia "La tecnologia blockchain: nuove prospettive per i mercati finanziari - Roma, 21 giugno 2016"

<sup>12</sup> Commissione Europea "Proposta di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale" 21 aprile 2021

<sup>13</sup> Massimo Doria, Capo Servizio della Banca d'Italia, Convegno su "Criptovalute, Nft e Metaverso: una guida semplice alla realtà virtuale" - 17 marzo 2022

<sup>14</sup> Ne fanno parte una proposta di: (i) regolamento per il mercato delle cripto-attività (MiCA), (ii) regolamento per la resilienza operativa (DORA), (iii) regolamento per un regime pilota per l'infrastruttura di mercato basata sulla tecnologia del registro distribuito. Il testo di cui al punto iii è stato approvato separatamente dagli altri e pubblicato sulla Gazzetta ufficiale della UE il 30 maggio 2022.

<sup>15</sup> Per approfondimenti si veda 'Antiriciclaggio: la proposta di single rule book della Commissione europea' di N. Mainieri - N. Di Gabriele, luglio 2021. Diritto Bancario web.



Regolamento sul mercato in cripto-attività o *Markets in Crypto-Assets - MiCA*. Per esempio, la definizione di 'fornitore di servizi in cripto-attività' (acronimo in inglese 'CASP') è offerta dall'articolo 3 della MiCA, il quale lo identifica con il soggetto (sia esso persona fisica o giuridica) che fornisce su base professionale servizi di custodia, ricezione e trasmissione di ordini, scambio e consulenza in materia di cripto-attività.

Tra gli obiettivi perseguiti con il regolamento MiCA si annoverano la tutela di consumatori e investitori la tutela dell'integrità del mercato e la stabilità finanziaria. Risulta evidente come solo l'efficace contrasto all'utilizzo delle cripto-attività da parte di operatori criminali possa consentire il raggiungimento dei fini prefissati dal legislatore euro-unitario. A tal fine, per effetto del combinato disposto della MiCA e del *Single Rule Book AML*, i CASP saranno soggetti obbligati ai fini antiriciclaggio e i componenti dei loro organi amministrativi dovranno soddisfare requisiti di onorabilità e professionalità. I soci che, direttamente o indirettamente, detengono diritti di voto o una partecipazione al capitale sociale pari o superiore al 20% saranno altresì soggetti a requisiti di onorabilità. La MiCA attribuisce alle autorità di vigilanza (sia essa europea o nazionale) il potere di revocare la licenza concessa a un CASP in caso di violazioni della disciplina antiriciclaggio.

I requisiti di onorabilità troveranno applicazione anche in capo al personale e amministratori di ogni emittente di "token collegato ad attività" (*asset-referenced token - ART* - anche detti *stablecoin*) e così pure ai loro soci qualificati.

Le autorità di vigilanza potranno rigettare l'istanza di acquisizione di una partecipazione qualificata in un CASP o emittente di *asset-referenced-token* ove esse abbiano "motivi ragionevoli per sospettare che, in relazione al progetto di acquisizione, sia in corso o abbia avuto luogo un'operazione o un tentativo di riciclaggio".

Nel rapporto congiunto delle autorità di supervisione europea - ESAs - pubblicato il 31 maggio 2022 si sottolinea l'esigenza che il Regolamento MiCA integri opportunamente la tematica antiriciclaggio nella disciplina della vigilanza prudenziale dei CASP. L'analisi condotta dalle ESAs evidenzia un approccio molto frastagliato nei paesi della UE in materia di poteri conferiti alle autorità per la revoca della licenza dei CASP: emerge in primis che in diversi paesi "probabilmente" c'è l'assenza di competenza in materia, in altri il potere di revoca è attribuito ad autorità differenti (e.g. FIU, agenzia fiscale e delle dogane, ministero degli interni). Considerando che la revoca della licenza è un potente deterrente contro le condotte illecite, sarebbe auspicabile un tempestivo allineamento degli Stati Membri.

I tempi di approvazione del nuovo quadro regolamentare hanno subito una certa dilatazione per via delle intense negoziazioni tra i tre attori del processo legislativo. Di particolare rilievo per lo scopo di questo articolo è la posizione assunta dal Parlamento Europeo il quale ha chiesto delle modifiche sostanziali alla proposta di emendamento del Regolamento 2015/847 in materia di trasferimento fondi<sup>16</sup>. Nello specifico, il Parlamento vorrebbe l'abolizione della soglia di esenzione di 1.000 euro per l'applicazione della c.d. *travel rule*: in sostanza per tutti i trasferimenti di fondi, a prescindere all'importo, gli intermediari coinvolti dovrebbero trasmettere/acquisire informazioni sul mittente e destinatario. Si aggiunge a ciò l'applicazione della *travel rule* anche ai trasferimenti da/verso i c.d. *'un-hosted wallet'*. Da ultimo, il Parlamento chiede che sia istituito e gestito dall'Autorità Bancaria Europea un elenco dei CASP che non sono conformi alla legislazione europea. Tale registro dovrebbe essere interrogato dagli intermediari prima di accreditare al beneficiario le cripto-attività oggetto del trasferimento. L'accredito non dovrebbe essere eseguito nel caso l'intermediario mittente sia soggetto a "misure restrittive" oppure via siano "rischi di riciclaggio o finanziamento del terrorismo".

Gli operatori del settore hanno manifestato una forte opposizione all'applicazione senza soglie della *travel rule* argomentando che si tratti una misura "sproporzionata" e che si voglia istituire "un regime di sorveglianza" sui CASP che stroncherebbe l'innovazione e forzerebbe gli intermediari ad abbandonare l'Europa.

L'irrigidimento delle regole ha avuto un ampio supporto da parte dei membri dei Comitati ECON e LIBE che hanno richiesto l'adozione della procedura rapida (c.d. *fast track*) per l'adozione degli emendamenti al Regolamento 2015/847.

Con riferimento al *Single Rule Book AML* il Parlamento Europeo ha proposto ulteriori rafforzamenti dei presidi, con particolare riguardo agli operatori in cripto-attività. Le richieste di modifica di maggior rilievo formulate dal Parlamento sono le seguenti.

- Conferimento all'autorità europea AML della responsabilità di supervisione sui CASP più significativi.
- Incarico all'autorità europea AML di definire la lista dei dati e informazioni utili per la valutazione della rischiosità dei soggetti vigilati.
- Riduzione ad euro 5.000 del limite per le transazioni in contanti (euro 10.000 nella proposta della Commissione).

---

<sup>16</sup> Quest'ultimo fa parte del *Single Rule Book AML*.



- Divieto di intrattenere relazioni con CASP non conformi alla normativa (trattandoli, pertanto, alla stregua delle *'shell bank'*).
- Obbligo per l'ente che offre conti di corrispondenza in cripto-attività di tipo *nested/pass-through*<sup>17</sup> di verificare l'adeguatezza delle misure antiriciclaggio poste in essere dalla controparte, cioè l'ente autorizzato ad usare il conte come *'rispondente'*.
- Le partecipazioni superiori al 5% (anziché attuale 25%) devono essere oggetto di valutazione per l'identificazione dei titolari effettivi.
- Divieto di utilizzo di strumenti al portatore (anziché la mera applicazione di misure di contrasto all'abuso).

Gli emendamenti proposti dal Parlamento Europeo appaiono idonei a serrare le maglie di un sistema di contrasto al crimine che purtroppo spesso progredisce con una velocità inferiore a quella con cui evolvono le competenze il settore degli operatori illeciti. Negli ultimi due anni le relazioni di Europol hanno ricordato come gli operatori criminali abbiano saputo sfruttare a pieno le potenzialità offerte dal progresso tecnologico e attuato anche nuove condotte illecite del tipo *'crime-as-a-service'*. In sostanza, operatori criminali offrono a terzi servizi illeciti basati sull'utilizzo di nuove tecnologie (e.g. *software* per sottrarre dati o attuare *ransoware*) in cambio di una percentuale dei proventi generati con il loro sfruttamento (le potremmo definire *royalty* criminali).

### **3. La recente giurisprudenza statunitense – il tema degli NFT.**

Gli Stati Uniti sono stati storicamente il paese guida per l'innovazione nel settore delle cripto-attività e più recentemente, a seguito del bando introdotto dalle autorità cinesi<sup>18</sup>, la maggiore piazza (virtuale) di scambio. L'attivismo sul versante tecnologico e transazionale è accompagnato un crescente volume di condotte illecite sulle quali le autorità federali (siano

---

<sup>17</sup> Trattasi di conti a cui hanno accesso diretto i clienti del *respondent*. Vedi FATF Guidance - Correspondent banking services, ottobre 2016 <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf>

<sup>18</sup> Il 24 settembre 2021 la banca centrale cinese (PBOC), assieme a nove agenzie governative, ha emanato una circolare che sancisce il divieto di condurre qualsiasi operazione connessa a valute virtuali. La circolare, altresì, stabilisce che la fornitura di servizi in valute virtuali in favore di persone residenti in Cina costituisce attività illegale. La circolare della PBOC fornisce una definizione di valuta virtuale degna di menzione: non emesse da un'autorità monetaria, basate sulla crittografia, DLT o tecnologie similari e aventi natura digitale. <http://www.pbc.gov.cn/en/3688253/3689012/4353814/index.html>



essere investiti di poteri di giustizia criminale ovvero amministrativa) concentrano l'attenzione.

Negli ultimi mesi sono comparse pronunce di corti penali federali relative a reati perpetrati a mezzo di cripto-attività taluni dei quali relativi alla violazione dei programmi sanzionatori, nonché richieste di rinvio a giudizio formulate dal Dipartimento della Giustizia a fronte di *'insider trading'* e riciclaggio sempre connessi alle cripto-attività.

Di particolare interesse è il rinvio a giudizio, deciso da un giudice federale di Washington D.C., a carico di un cittadino americano accusato dal Dipartimento di Giustizia di aver trasferito Bitcoin per un controvalore di oltre 10 milioni di dollari su piattaforme di scambio riconducibili a paesi oggetto di sanzioni (Cuba, Iran, Corea del Nord, Siria e Russia). Il giudice ha rigettato l'obiezione della difesa secondo la quale le monete virtuali non sono soggette alla disciplina USA in materia di sanzioni poiché esse sono 'emesse e circolano all'esterno del sistema finanziario'. Il giudice, aderendo alla posizione espressa dall'Ufficio per il controllo delle attività estere (OFAC<sup>19</sup>) nelle linee guida<sup>20</sup> emanate il 15 ottobre 2021, ha sostenuto che il Dipartimento di Giustizia può perseguire le violazioni dei programmi sanzionatori OFAC anche in riferimento a violazioni commesse solo a mezzo di 'valute virtuali'.

Il 15 ottobre 2021 l'OFAC aveva anche aggiornato le sue *Frequent Asked Question (FAQ)*<sup>21</sup> stabilendo che le "valute digitali" sono soggette ai programmi sanzionatori e che la definizione di "valuta digitale" comprende 'cripto valute emesse da stati sovrani', 'valute virtuali' e 'rappresentazioni digitali di valute aventi corso legale'<sup>22</sup>. L'OFAC chiarisce che una valuta digitale è una rappresentazione di valore e che essa svolge tutte e tre le classiche funzioni della moneta: mezzo di scambio, unità di conto e riserva di

---

<sup>19</sup> L'OFAC è incardinato presso il Dipartimento del Tesoro ed è competente per l'amministrazione e l'applicazione dei programmi di sanzioni economiche contro paesi e gruppi di individui (e.g. terroristi, narcotrafficienti).

<sup>20</sup> *Sanctions compliance guidance for the virtual currency industry* [https://home.treasury.gov/system/files/126/virtual\\_currency\\_guidance\\_brochure.pdf](https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf)

<sup>21</sup> L'OFAC pubblica sulla sua pagina web le risposte a quesiti sottoposti in merito ai programmi sanzionatori. Le risposte sono intese solo come informazioni generali per aiutare le persone soggette alla giurisdizione degli Stati Uniti a conformarsi ai requisiti legali e per facilitare la comprensione della portata e delle finalità dei programmi sanzionatori. L'OFAC chiarisce che fatti specifici possono alterare un'analisi e, poiché ogni programma riflette contesti unici di politica estera e sicurezza nazionale, una risposta particolare non sarà sempre applicabile a tutti i programmi o in ogni momento.

<sup>22</sup> <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/559>



valore. Considerando l'estrema volatilità e assenza di valore intrinseco della maggior parte delle valute digitali – fattispecie ripetutamente riconosciute da esponenti apicali delle principali autorità monetarie mondiali<sup>23</sup> – la posizione dell'OFAC che riconosce la funzione di unità di conto e riserva di valore alle valute digitali potrebbe essere considerata strumentale allo scopo sanzionatorio. Ne è riprova il fatto che nella campagna di contrasto alle condotte criminali in cripto-attività, le autorità inquirenti americane stanno adottando in via analogica disposizioni di diritto statunitense relative agli strumenti finanziari (cfr. infra).

Il 12 aprile 2022 uno dei personaggi chiave per lo sviluppo di Ethereum<sup>24</sup> è stato condannato da una corte federale<sup>25</sup> a una pena detentiva di 63 mesi e una pecuniaria di 100.000 dollari dopo essersi dichiarato colpevole di aver violato la normativa federale che proibisce l'esportazione di tecnologie in Corea del Nord in assenza di un'autorizzazione dell'OFAC<sup>26</sup>. Il condannato, nonostante il diniego al rilascio del permesso di viaggio in Corea del Nord opposto dalle autorità USA, aveva raggiunto nell'aprile 2019 il paese sanzionato e fornito illecitamente consulenza tecnica per lo sviluppo dell'infrastruttura tecnologica idonea all'utilizzo di cripto-attività per fini di riciclaggio e di circonvenzione delle sanzioni. Lo stesso, inoltre, aveva fornito suggerimenti per l'utilizzo di *smart contract*<sup>27</sup> basati sulla *distributed ledger*

---

<sup>23</sup> Tra gli altri la banca centrale USA – Federal Reserve – ha pubblicato il 2 giugno 2022 i risultati della sua indagine sul crollo di alcuni stablecoins e ha concluso dicendo che alcuni stablecoins non sono affatto stabili, soprattutto nella prospettiva dei piccoli investitori (*"our results serve as useful reminder that some stablecoins are not stable at all, particularly for the users of smaller accounts who bought into the falling knife when IRON was tumbling."*) <https://www.federalreserve.gov/econres/notes/feds-notes/runs-on-algorithmic-stablecoins-evidence-from-iron-titan-and-steel-20220602.htm>

<sup>24</sup> Ethereum è la seconda cripto-attività in termini di capitalizzazione di mercato preceduta da Bitcoin. La progettazione e sviluppo di Ethereum è stata curata dall'omonima fondazione di cui il reo è stato uno degli artefici.

<sup>25</sup> <https://www.justice.gov/opa/pr/us-citizen-who-conspired-assist-north-korea-evading-sanctions-sentenced-over-five-years-and>

<sup>26</sup> L'[Ordine Esecutivo presidenziale 13466](#) del 26 giugno 2008, emesso in forza della legge 'Poteri a fronte di emergenze economiche internazionali' - [International Emergency Economic Powers Act](#) (IEEPA) – sancisce il divieto di esportare beni, servizi e tecnologie in favore della Corea del Nord in assenza di un'apposita autorizzazione da parte dell'OFAC. Violazioni dello IEEPA possono essere punite con pena detentiva fino a 20 anni e pecuniaria fino a 1 milione di dollari.

<sup>27</sup> Gli *smart contract* sono programmi informatici che operano su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli *smart contract* permettono

*technology*<sup>28</sup> – DLT - con la finalità di favorire il regime di Pyongyang nelle negoziazioni con il governo USA in materia di armi nucleari. In aggiunta, l'imputato aveva predisposto e posto in esecuzione piani per facilitare l'impiego di cripto-attività di proprietà del regime nordcoreano.

Sempre in tema di uso delle cripto-attività per aggirare i divieti imposti dal programma di sanzioni a carico della Corea del Nord è da rilevare la sanzione irrogata il 6 maggio 2022 dall'OFAC a carico della società *Blender.io* che gestisce un *mixer*<sup>29</sup> di valute virtuali sulla *blockchain* di Bitcoin. Il procedimento sanzionatorio è a valle dell'attività investigativa condotta in seguito al più grande furto di cripto-attività sinora realizzato. Infatti, il 23 marzo 2022 il *Lazarus Group*, considerato un'organizzazione di *hacker* sponsorizzata dal regime di Pyongyang, ha sottratto cripto-attività per un controvalore di 620 milioni di dollari da un progetto *blockchain* connesso alla piattaforma di giochi *online Axie Infinity*. Circa 20,5 milioni di dollari rinvenienti dal furto sono stati riciclati tramite *Blender.io* che, avvalendosi di

---

l'esecuzione di transazioni (contratti) sulla *blockchain*. Gli *smart contract*, dopo essere stati sviluppati al di fuori della rete (*offline*), sono inseriti nella *blockchain* in genere dallo stesso sviluppatore (identificabile a mezzo di un indirizzo – *address*) e messi in esecuzione sui nodi validatori. Gli *smart contract* possono essere 'scritti' usando diversi tipi di linguaggi di programmazione. Per quanto attiene la rete Ethereum, il codice di ogni *smart contract* è memorizzato sulla *blockchain* e qualsiasi partecipante può esaminarlo accertandosi del suo stato attuale, al fine di verificarne la funzionalità. Ogni computer sulla rete (denominato anche "nodo") memorizza una copia di tutti gli *smart contract* esistenti e del loro stato attuale nella *blockchain*, oltre ai dati delle transazioni. Quando uno *smart contract* riceve fondi da un utente, il suo codice viene eseguito da tutti i nodi della rete, al fine di raggiungere il consenso in merito all'esito e al flusso di valore risultante. Questo meccanismo consente l'esecuzione sicura degli *smart contract*, senza che sia necessaria un'autorità centrale. Per eseguire uno *smart contract* sulla rete Ethereum, è necessario versare una commissione denominata "*gas*" (è chiamata così perché le commissioni consentono alla *blockchain* di funzionare). Anche se esistono alcune eccezioni, in generale, una volta innestati nella *blockchain*, gli *smart contract* non possono più venire modificati, neanche dal loro autore.

<sup>28</sup> Ai sensi della legge n° 12 dell'11 febbraio 2019 – art. 8ter - si definiscono tecnologie basate su registri distribuiti le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetture decentralizzate 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.

<sup>29</sup> Sebbene di per sé l'attività di '*mixing*' (oppure *tumbling*) non è di per sé illecita, è di frequente utilizzata da attori criminali per mascherare l'origine illecita dei fondi e la loro destinazione finale.

un protocollo informatico, combina valute virtuali provenienti da una moltitudine di differenti indirizzi (*wallet*) al fine di offuscare l'origine e la proprietà di detti valori.<sup>30</sup> L'OFAC ha, altresì, accertato che *Blender.io* ha supportato il riciclaggio di proventi illeciti generati dall'attività di *ransomware*<sup>31</sup> di gruppi sponsorizzati dalla Russia (Trickbot, Conti, etc.). A seguito dei risultati dell'attività investigativa l'OFAC ha designato *Blender.io*, ai sensi dell'ordine esecutivo presidenziale 13694<sup>32</sup>, come una "significativa minaccia alla sicurezza nazionale".

Nella campagna di contrasto al crimine le autorità inquirenti americane fronteggiano difficoltà connesse alla qualificazione giuridica di nuove cripto-attività quali, ad esempio, i *non-fungible token* (NFT). Oramai da diversi anni le autorità americane, in particolare la Commissione di vigilanza sui mercati finanziari – SEC<sup>33</sup> – portano avanti una politica di "*regulation by enforcement*" che si basa sull'adozione di una nuova interpretazione della regolamentazione esistente al fine di coprire condotte individuali e strumenti (tecnologici) ancora non '*censiti*' dal diritto.

---

<sup>30</sup> Come ricostruito dal FinCEN – l'unità di informazione finanziaria degli USA – un *mixer* opera nel seguente modo: (i) i clienti forniscono un indirizzo (*wallet*) sul quale vogliono ricevere le cripto-valute; (ii) il *mixer* indica al cliente un indirizzo al quale i clienti devono trasferire le cripto-valute; (iii) il *mixer* trasmette le cripto-valute dei clienti presso numerosi conti accesi presso piattaforme di conversione di cripto-valute; (iv) il *mixer* preleva altre cripto-valute di cui ha il controllo e le trasferisce su diversi conti; (v) il *mixer* preleva dai conti di cui al punto iv le cripto-valute ai clienti al netto di una commissione per lo svolgimento dei suoi servizi.

<sup>31</sup> Il *ransomware* rientra nella fattispecie giuridica dell'estorsione: l'attore criminale si adopera per infettare con un virus l'infrastruttura informatica della vittima e inibire l'accesso ai dati ivi archiviati. L'attore criminale minaccia la vittima che in assenza del pagamento di un riscatto (*ransom* in inglese) i dati verranno cancellati. Cfr. <https://www.europol.europa.eu/cms/sites/default/files/documents/ransomware-what-you-need-to-know.pdf>

<sup>32</sup> <https://www.govinfo.gov/content/pkg/CFR-2016-title3-vol1/pdf/CFR-2016-title3-vol1-eo13694.pdf>

<sup>33</sup> Securities and Exchange Commission.

La dottrina si è espressa in senso critico sulla "*regulation by enforcement*"<sup>34</sup>, sebbene un approccio diverso potrebbe condurre al non perseguire condotte dannose per la collettività<sup>35</sup>.

I citati NFT, che hanno fatto la loro comparsa tra il 2014 e il 2015, rappresentano ormai una realtà di notevole rilievo in termini economici; infatti nel 2021 risultano trasferiti circa 44,2 miliardi di dollari sugli *smart-contract* di Ethereum associati ai mercati di scambio dei *non-fungible-token*<sup>36</sup>. Gli NFT sono attività digitali negoziabili che rappresentano la registrazione sulla *blockchain* di immagini, suoni o oggetti artistici. Gli NFT appartengono alla categoria concettuale dei '*valueless token*' la cui funzione si esaurisce nella loro stessa titolarità e nella certificazione di autenticità di una attività digitale e, di conseguenza, nella sua infungibilità. Il trasferimento di un NFT viene gestito tramite uno *smart contract* che ne regola le condizioni.<sup>37</sup>

Il caso più recente e senza dubbio estremamente interessante risale al 1° giugno 2022 quando il Dipartimento della Giustizia ha annunciato la richiesta di rinvio a giudizio a carico di un ex dirigente di una primaria società -

<sup>34</sup> Vedi Regulation by Enforcement: Problems with the SEC's Approach to Cryptoasset Regulation. Carol R. Goforth, University of Arkansas - School of Law; 14 aprile 2022 [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4084033](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4084033)

Regulation by Selective Enforcement: The SEC and Initial Coin Offerings. James J. Park and Howard H. Park (UCLA), 21 novembre 2019 <https://corpgov.law.harvard.edu/2019/11/21/regulation-by-selective-enforcement-the-sec-and-initial-coin-offerings/>

<sup>35</sup> Celebre è il caso il contenzioso avviato dalla SEC il 22 dicembre 2020 contro la società Ripple Labs Inc e i suoi fondatori. <https://www.sec.gov/litigation/complaints/2020/comp-pr2020-338.pdf> Nel caso in specie la SEC contestava l'offerta non autorizzata di strumenti finanziari, argomentando che le cripto-attività emesse da Ripple fossero 'contratti di investimento' e pertanto si qualificassero come 'strumenti finanziari' ai sensi della normativa federale. In precedenza, però la SEC aveva affermato che Bitcoin e Ethereum – simili in natura alla cripto-attività di Ripple – non fossero strumenti finanziari. Cfr. Regulation By Enforcement Is Stifling Cryptocurrency, Curt Levey, 29 aprile 2021 <https://fedsoc.org/commentary/fedsoc-blog/regulation-by-enforcement-is-stifling-cryptocurrency>

<sup>36</sup> Il rapporto sul mercato degli NFT pubblicato a inizio giugno 2022 da Chainalysis indica che un gruppo molto ristretto di investitori altamente sofisticati trae la maggior parte dei profitti, nonostante la maggior parte delle transazioni (in media con un controvalore inferiore a 10.000 dollari) sia riconducibile al c.d. *retail*. Chainalysis ipotizza che taluni investitori professionali si avvalgono di tecniche per escludere dalle transazioni più promettenti gli operatori *retail* dopo che questi ultimi hanno pagato commissioni di transazione.

<sup>37</sup> Cfr. NFT – L'arte e il suo doppio. F. Annunziata, A. Conso, novembre 2021, Montabone Editore

*OpenSea*<sup>38</sup> - attiva nella commercializzazione di NFT per frode perpetrata con strumenti di comunicazione (c.d. *'wire fraud'*<sup>39</sup>) e riciclaggio. Il Dipartimento della Giustizia ha contestato all'indagato l'acquisto di 45 NFT prima che gli stessi venissero pubblicizzati sulla pagina *web* della *OpenSea* e, pertanto, prima che il loro prezzo di mercato crescesse significativamente. L'indagato avrebbe frodato il suo datore di lavoro con l'uso indebito di informazioni confidenziali cui aveva accesso in ragione del suo ruolo di incaricato della gestione delle aste di NFT. Il Dipartimento della Giustizia non ha potuto qualificare il reato presupposto del riciclaggio come *'insider trading'* poiché gli NFT non sono (ancora) considerati uno strumento finanziario nel diritto statunitense<sup>40</sup>. La qualificazione degli NFT come strumenti finanziari avrebbe, invece, consentito di formulare l'accusa di frode in titoli<sup>41</sup> e di denunciare la condotta anche alla SEC la quale è competente per perseguire i casi di *insider trading*. L'indagato avrebbe attuato le condotte di *fraudolente* per un periodo di circa tre mesi – da giugno a settembre 2021 – e svolto l'attività di riciclaggio dei proventi illeciti accendendo ad-hoc portafogli virtuali anonimi ed eseguendo multipli trasferimenti di cripto-attività Ethereum tra gli stessi. È interessante osservare che la proposta di regolamento MiCA licenziata dalla Commissione Europea esclude dal suo perimetro di applicazione gli NFT e pertanto, la disciplina di contrasto dell'*insider trading* non troverebbe applicazione per gli stessi<sup>42</sup>. La circostanza ha sollevato critiche in dottrina<sup>43</sup>

<sup>38</sup> Ozone Networks, Inc. d/b/a OpenSea gestisce la più grande piattaforma virtuale per la commercializzazione di NFT.

<sup>39</sup> Ai sensi del paragrafo 1343 dello U.S. Code of law è la frode perpetrata a mezzo di false o fraudolente dichiarazioni, pretese o promesse trasmesse o generate per il tramite di cavi, radio, o televisione in ambito interstatale o internazionale. La pena massima edittale è di 20 anni, incrementata ad anni 30 in presenza di aggravanti. Lo U.S. Code of law è la raccolta codificata e ufficiale delle leggi generali e in vigore aventi validità a livello federale. Il codice è predisposto dall'Ufficio del consiglio per la revisione della legge del Congresso. <https://uscode.house.gov/>

<sup>40</sup> Va osservato che nella richiesta di rinvio a giudizio il procuratore federale pur qualificando il reato come frode a mezzo di strumenti di comunicazione lo descrive come *'insider trading in non-fungible-token'*. (cfr. <https://www.justice.gov/usao-sdny/press-release/file/1509701/download> capo di accusa n. 1)

<sup>41</sup> La frode in titoli è un reato a livello statale e federale con pene massime edittali molto severe: 20 anni di reclusione (5 anni nel caso di reato non di rilievo federale) e 10 milioni di dollari di pena pecuniaria accessoria.

<sup>42</sup> L'articolo 4(2) del regolamento prevede la non applicabilità alle attività digitali che sono uniche e non fungibili.

<sup>43</sup> Cfr. Non-fungible tokens: NFTs and the silence of the EU legislator. Hogan Lovells – FinTech Perspectives 28 ottobre 2021 <https://www.engage.hoganlovells.com/knowledgeservices/news/non-fungible->

e il Parlamento Europeo, a marzo 2022, ha proposto delle modifiche al fine di assicurare che le frazioni di un NFT suscettibili di trasferimento a terzi siano disciplinate dalla MiCA.<sup>44</sup>

In base al Codice delle leggi degli Stati Uniti<sup>45</sup> le 'attività digitali' come Bitcoin e altre 'valute virtuali' sono considerate *commodity* alla stregua dei metalli preziosi e del petrolio e da ciò discende la competenza della Commissione di vigilanza sui derivati (Commodity Futures Trading Commission – CFTC)<sup>46</sup> ad autorizzare i contratti derivati su tali attività. Alla luce di ciò va esaminata la procedura avviata il 2 giugno 2022 dalla CFTC che ha citato in giudizio davanti alla corte federale<sup>47</sup> la Gemini Trust Company LLC (Gemini) per presunte dichiarazioni infedeli rilasciate in occasione della presentazione, nel secondo semestre 2017, dell'istanza autorizzativa per la negoziazione del primo contratto derivato di tipo *future* sulla cripto-attività Bitcoin. La CFTC sostiene che l'istante era - ovvero avrebbe dovuto "ragionevolmente" essere - a conoscenza del fatto che il contratto *future* era "facilmente suscettibile di manipolazione". In particolare, la CFTC contesta che, contrariamente alle dichiarazioni rese dall'istante, non fosse vero che l'immissione di ordini sul sistema di scambi (*exchange*) di Gemini era subordinata alla presenza di una provvista (*pre-funded*). Infatti, la possibilità di inserire ordini anche in assenza di fondi (ordini che pertanto non potevano essere eseguiti, ma venivano cancellati subito dopo la loro immissione) consente il moltiplicarsi delle proposte di negoziazione e in tal modo di 'manipolare' il processo di formazione dei prezzi di mercato. Inoltre, soggetti connessi a Gemini, secondo la ricostruzione della CFTC, concedevano in prestito 'attività digitali', a tassi di interesse al di sotto di quelli di mercato e senza pretendere garanzie, a terze parti a patto che queste ultime si

---

[tokens-nfts-and-the-silence-of-the-eu-legislator?nav=FRbANEucS95NMLRN47z%2BeeOgEFct8EGQcV7IzHUHOGQ%3D&key=BcJlhLtdCv6%2FJTDZxvL23TQa3JHL2AIGr93BnQjo2SkGJpG9xDX7S2thDpAQsCconWHAwe6cJTn%2Fzwe4%2FkPc93OjGmtaEjr&uid=hPcSjBln1IBvCdRThlyn8hhiNTQ5OWZd&utm\\_medium=email&utm\\_source=daily](https://www.eurobarometer.europa.eu/legislator?nav=FRbANEucS95NMLRN47z%2BeeOgEFct8EGQcV7IzHUHOGQ%3D&key=BcJlhLtdCv6%2FJTDZxvL23TQa3JHL2AIGr93BnQjo2SkGJpG9xDX7S2thDpAQsCconWHAwe6cJTn%2Fzwe4%2FkPc93OjGmtaEjr&uid=hPcSjBln1IBvCdRThlyn8hhiNTQ5OWZd&utm_medium=email&utm_source=daily)

<sup>44</sup> Cfr. Report on the proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets and amending Directive (EU) 2019/1937 del 17-03-2022 [https://www.europarl.europa.eu/doceo/document/A-9-2022-0052\\_EN.html](https://www.europarl.europa.eu/doceo/document/A-9-2022-0052_EN.html)

<sup>45</sup> Sezione 1a(9) dello U.S. Code of law.

<sup>46</sup> La Commissione è un'agenzia del governo federale competente per la regolamentazione e vigilanza sui mercati dei prodotti derivanti aventi come sottostante le *commodity*.

<sup>47</sup> La citazione in giudizio è finalizzata a ottenere una condanna a carico del convenuto con applicazione di una sanzione pecuniaria e l'interdizione dallo svolgimento di certe connesse al mercato degli strumenti finanziari derivati <https://www.cftc.gov/media/7316/enfgeminicomplaint060222/download>

impegnassero a generare un certo volume minimo di negoziazioni sull'*exchange* di Gemini. Per esempio, Gemini concesse a fine 2016 un prestito di 400.000 dollari a un'impresa – attiva quale *market maker*<sup>48</sup> sul suo *exchange* – per consentirle di partecipare all'asta per la fissazione del prezzo di Bitcoin da prendere a riferimento per la liquidazione del contratto *future* in scadenza. Similmente Gemini aveva concesso in prestito 750 Bitcoin<sup>49</sup> ad un altro *market maker* nel luglio 2017 affinché quest'ultimo generasse "maggiori volumi negoziali" sull'*exchange*. La CFTC ha contestato a Gemini anche l'omessa istituzione di efficaci meccanismi di controllo atti a prevenire che gli ordini di segno opposto (acquisto e vendita) immessi da uno stesso operatore possano essere incrociati e quindi eseguiti (c.d. *self-crossing*)<sup>50</sup>.

#### **4. La giurisprudenza di legittimità italiana – note a sentenze di Cassazione n. 2868 del 7 ottobre 2021 e n. 45397 del 9 dicembre 2021.**

Già con la sentenza n. 26807 del 17 settembre 2020, la Cassazione penale si era per la prima volta occupata di un sequestro preventivo di fondi e altri beni emesso dal giudice per le indagini preliminari a carico di un indagato chiamato a rispondere dei reati riciclaggio (art. 648 bis) e abusivismo (art. 166 comma 1, lett. c) del Testo Unico della Finanza), in un procedimento di primo grado che vedeva come reato presupposto una serie di truffe *on-line* i cui proventi, dopo numerosi giri, veniva infine investito in *Bitcoin*. In quell'occasione la Cassazione aveva concentrato la sua attenzione sull'elemento soggettivo del reato di riciclaggio e sulla qualificazione da attribuire ad un'attività di pubblicizzazione sul sito Facebook della vendita di *Bitcoin*, secondo gli Ermellini reclamizzata come una proposta di investimento e come tale soggetta agli adempimenti in materia di comunicazione ed autorizzazione della CONSOB<sup>51</sup>. Si versa, pertanto, in

---

<sup>48</sup> Il *market maker* è un intermediario che si assume il compito di garantire, in via continuativa, la negoziabilità di determinati titoli. Il *market maker* in sostanza si impegna a immettere sul mercato proposte sia di acquisto che di vendita di certi titoli. A seconda del tipo di mercato l'impegno assunto dal *market maker* varia, ma in generale si può affermare che l'impegno contrattuale che assume è di garantire sufficiente liquidità agli scambi di certi strumenti finanziari.

<sup>49</sup> In base alle quotazioni dell'epoca il prestito aveva un controvalore di circa due milioni di dollari.

<sup>50</sup> Il *self-crossing* determina l'inflazione dei volumi negoziali, ma essi non rappresentano transazioni aventi un valido e lecito movente economico.

<sup>51</sup> La sentenza è stata commentata in questa rivista nello studio di N. Mainieri, *La Cassazione penale esamina le valute virtuali sotto il profilo del Testo Unico della Finanza – le precedenti qualificazioni e i richiami della Direttiva penale sulla lotta al riciclaggio mediante l'uso del penale* (n. 2018/1673 UE), *Giurisprudenza Penale Web*, 2020, 10, cui si rimanda

tema di 'abusivismo sollecitatorio' che la legge<sup>52</sup> riferisce ai prodotti e strumenti finanziari, servizi o attività di investimento, laddove l'ordinanza impugnata, oggetto della sentenza di Cassazione, parla esplicitamente di 'prodotti finanziari'.

Con sentenza n. 2868 del 7 ottobre 2021<sup>53</sup>, i giudici di legittimità sono tornati ad occuparsi di transazioni operate con acquisto di *Bitcoin*, questa volta per una questione loro sottoposta di autoriciclaggio ex art. 648 ter1 c.p.<sup>54</sup>, così formulato a fronte di un reato presupposto di favoreggiamento e sfruttamento della prostituzione.

In precedenza, il Tribunale di La Spezia, accogliendo l'appello del Pubblico Ministero, aveva disposto sequestro preventivo, anche per equivalente ex art. 648 quater c.p., del profitto del reato presupposto sopra menzionato, dal momento che l'indagato aveva poi operato il trasferimento dei relativi profitti a società estere operanti nella compravendita di cripto-valute, tramite bonifici di somme di denaro effettuati da carte prepagate intestati a prestanome o all'indagato stesso. L'imputato ricorreva in Cassazione senza contestare la sussistenza dei reati presupposto ma quella del reato di autoriciclaggio, sostenendo così che le transazioni in cripto non potessero ritenersi anonime, ma anzi di dominio pubblico e accessibile costantemente da chiunque, tramite il registro contabile digitale – quale appunto la *blockchain*, il che farebbe venir meno la mancanza di un concreto ostacolo all'identificazione della provenienza del bene, come nella condotta richiesta dall'autoriciclaggio.

Come noto, il legislatore – introducendo nell'ordinamento penalistico l'autoriciclaggio<sup>55</sup> - ha operato una sorta di sintesi terminologica tra le condotte già in precedenza criminalizzate nei reati di riciclaggio (art. 648 bis) e di impiego (art. 648 ter), ed ha altresì inserito ulteriori specifiche tendenti in qualche modo a limitare la condotta punibile delle fattispecie "autoriciclatorie".

---

<sup>52</sup> Art. 166, comma 1, lettera c del Testo Unico della Finanza.

<sup>53</sup> Cassazione penale, sez. II, n. 2868 del 7 ottobre 2021 (dep. 25 gennaio 2022).

<sup>54</sup> Art. 648 ter1 c.p. comma 1: "*Si applica la pena della reclusione da due a otto anni e della multa da euro 5.000 a euro 25.000 a chiunque, avendo commesso o concorso a commettere un delitto impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o le altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa*"

<sup>55</sup> Tramite l'art. 3 comma 3 della legge 186/2014 "Disposizioni in materia di emersione e rientro di capitali detenuti all'estero nonché per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di autoriciclaggio"

Il primo comma 648 ter1 prevede, infatti, che l'impiego, la sostituzione, il trasferimento di quanto proveniente dalla commissione di un delitto non colposo debba avvenire in "attività economiche, finanziarie, imprenditoriali o speculative", termini del tutto assenti dalla condotta del riciclaggio ed altresì aggiungendo "imprenditoriali o speculative" alle "attività economiche o finanziarie" invece presenti nella condotta del reato di impiego. Inoltre, il citato primo comma dell'autoriciclaggio, nello specificare l'idoneità della condotta di ostacolo alla provenienza delittuosa dei beni, riproduce in parte la terminologia del 648 bis ma vi aggiunge l'avverbio "concretamente", lasciando anche qui alla giurisprudenza il compito di definirne poi il contenuto <sup>56</sup>.

Nella sentenza in esame, la Cassazione – dopo aver richiamato la definizione di valuta virtuale fornita dal legislatore amministrativo antiriciclaggio <sup>57</sup> - sottolinea, anzitutto, le modalità operative delle operazioni contestate al ricorrente, consistenti appunto non in acquisto diretto di *bitcoin* ma di un trasferimento tramite bonifici di valuta *fiat* (euro nel caso in questione) a società estere, successivamente incaricate di cambiare l'euro in valuta virtuale, il tutto per il tramite poi di altre società estere. Da ciò la Corte deduce che detti trasferimenti di valuta verso società estere che si sono interposte nell'acquisto delle cripto - anche a mezzo di prestanomi - costituiscano il "*serio ostacolo all'identificazione del ricorrente come beneficiario finale delle transazioni ed effettivo titolare di bitcoin acquistati non da lui ma dalle società estere che fungevano da exchange provider*". Ciò integra, secondo gli Ermellini, il reato di cui autoriciclaggio che richiede "non un assoluto impedimento" all'identificazione della provenienza delittuosa di denaro, beni o altre utilità tramite una condotta di impiego, sostituzione o trasferimento di questi, ritenendosi – al contrario – sufficiente una "*qualunque attività concretamente idonea ad ostacolare gli accertamenti sulla loro provenienza*". La Cassazione aggiunge infatti che "*l'intervenuta tracciabilità, per effetto delle indagini poste in essere dopo la consumazione del reato, delle operazioni di trasferimento delle utilità provenienti dal delitto presupposto, non esclude l'idoneità ex ante della condotta ad ostacolare concretamente l'identificazione della loro provenienza delittuosa*".

---

<sup>56</sup> Cfr. in proposito N. Mainieri – G. M. Tovini, *I primi quattro anni dell'autoriciclaggio nell'interpretazione della Cassazione* in *Giurisprudenza Penale web*, 2019, 3.

<sup>57</sup> "*valuta virtuale: rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente*", così art. 1 comma 2, lett. ff) d.lgs. 231/2007

Da ultimo, la sentenza ricorda che all'attività di cambio della valuta deve essere attribuito quel "*carattere finanziario*" richiesto dalla norma dell'autoriciclaggio, tanto che "*in Italia è regolamentata dalla legge e il soggetto che la esercita deve essere iscritto in appositi registri*": su detto ultimo punto ci soffermeremo nel successivo paragrafo.

Si aggiunge che in tema di "concretezza" dell'ostacolo nel reato di autoriciclaggio, la Suprema Corte si era già espressa, affermando che la condotta richiesta dal legislatore resta caratterizzata da una particolare capacità dissimulativa, in grado di dimostrare che l'autore del delitto presupposto abbia effettivamente voluto effettuare un impiego finalizzato ad occultare l'origine illecita del denaro o dei beni oggetto del profitto, e non semplicemente godere del profitto. Proprio sul tema della condotta dissimulativa con riferimento all'identificazione della provenienza illecita del bene di cui al reato presupposto dell'autoriciclaggio, si evidenzia che più di recente - con sentenza n. 45397 del 9 dicembre 2021 - la Suprema Corte ha considerato come tale anche il reinvestimento del profitto illecito in attività economiche, finanziarie o speculative attuato tramite intestazione ad un terzo, persona fisica o società, in quanto ciò "*muta la titolarità giuridica del profitto illecito*"; in tali casi, conclude la Corte "*la sua apprensione non è più immediata e richiede la ricerca ed individuazione del successivo trasferimento*"<sup>58</sup>.

Queste ultime considerazioni confermano come il reato di autoriciclaggio (nonché anche quelli di riciclaggio ed impiego) siano soltanto nominalmente collocati nella sezione del codice penale relativa ai reati contro il patrimonio, per una scelta legislativa un tempo giustificata dal fatto che riciclaggio e impiego erano nati come reati speciali rispetto alla norma della ricettazione (art. 648) che ne costituiva norma generale, ma che oramai la giurisprudenza li considera appartenere sostanzialmente ai reati contro l'amministrazione della giustizia, in quanto finalizzati ad impedire la ricostruzione della "traccia" dei fondi e il conseguente recupero degli stessi da parte degli organi giurisdizionali.

## **5. Le novità regolamentari italiane: il decreto M.E.F. del 13 gennaio 2022**

L'Italia è stato il primo Paese europeo ad applicare la legislazione antiriciclaggio ai prestatori di servizi in valute virtuali, dapprima intesi come piattaforme di scambio, *exchange*, che consentono il passaggio dalla valuta legale *fiat* alla cripto: ciò è stato realizzato in sede di recepimento della quarta direttiva antiriciclaggio (UE) n. 2015/849, tramite il d.lgs. 90/2017 e la sua riscrittura del precedente D.lgs. 231/2007 (che aveva recepito la terza

---

<sup>58</sup> In senso conforme, già Cass. Pen., sez. 2, n. 16059 del 18 dicembre 2019

direttiva), così anticipando i contenuti della quinta direttiva, allora in bozza. Con il successivo recepimento di quest'ultima, gli obblighi sono stati estesi anche ai portafogli digitali, *e-wallet*, che forniscono "servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare o trasferire valute virtuali"<sup>59</sup>.

Se da una parte detti prestatori di servizi sono stati fatti rientrare tra i soggetti obbligati al rispetto delle norme AML/CFT - assoggettandoli quindi agli obblighi preventivi in tema di adeguata verifica del cliente, registrazione e conservazione dei dati, invio delle segnalazioni di operazioni sospette - dall'altra si è previsto l'obbligo della loro registrazione - considerandoli nell'innovativa figura dei "cambiavalute virtuali" - in una sezione speciale del registro dei cambiavalute, dal 2015 tenuto dall'Organismo per la gestione degli elenchi degli Agenti in attività finanziaria e dei Mediatori creditizi - OAM, persona giuridica di diritto privato nella forma di Fondazione<sup>60</sup>.

L'obbligo di registrazione, di fondamentale importanza per prevenire forme di abusivismo purtroppo diffuse nel settore ed assoggettare i "cambiavalute virtuali" a una forma di vigilanza, cartolare ed ispettiva<sup>61</sup> - era subordinato dal d.lgs. 90/2017 come poi ribadito dal successivo d.lgs. 125/2019 - all'emanazione di un decreto del Ministro dell'economia e delle finanze in tema di comunicazione della loro operatività sul territorio nazionale, comunicazione considerata "condizione essenziale per l'esercizio legale dell'attività da parte dei suddetti prestatori". Detto decreto veniva richiesto anche stabilire "forme di cooperazione tra il Ministero dell'economia e delle finanze e le forze di polizia, idonee ad interdire l'erogazione dei servizi relativi all'utilizzo di valuta virtuale da parte dei prestatori che non ottemperino all'obbligo di comunicazione"<sup>62</sup>.

---

<sup>59</sup> Secondo la definizione che ne fornisce la direttiva (UE) 2018/843, quinta direttiva, recepita con il dlgs125/2019

<sup>60</sup> L'OAM è stato istituito dall'art. 128-undecies del TUB e dal 1° luglio 2011 quando, in adempimento alla riforma di settore introdotta dal D.lgs. n. 141/2010, sono cessate le iscrizioni nell'elenco degli agenti in attività finanziaria e nell'albo dei mediatori creditizi prima tenuti dalla Banca d'Italia

<sup>61</sup> "L'Ufficio Vigilanza dell'OAM provvede all'accertamento dei requisiti richiesti dall'ordinamento di settore per il mantenimento dell'iscrizione degli Agenti in attività finanziaria e dei Mediatori creditizi nonché alla verifica dello svolgimento della relativa attività in linea con le norme legislative o amministrative che la regolano" cfr. sito OAM <https://www.organismo-am.it/vigilanza>

<sup>62</sup> Cfr. d.lgs. 90/2017 art.8 comma 1 per quanto riguardava i prestatori di servizi di cambio, con obbligo poi esteso dal d.lgs. 125/2019 art. 5 ai prestatori di servizi di portafoglio digitale

Il previsto decreto non ha avuto per lungo tempo molta fortuna; dopo un'iniziale pubblica consultazione del primo schema nel febbraio 2018, il testo definitivo è stato emanato poco meno di quattro anni dopo, a gennaio 2022 <sup>63</sup>, dopo aver ricevuto i pareri favorevoli prima dell'O.A.M. e poi del Garante per la protezione dei dati personali.

Il decreto prevede in sintesi che:

- L'esercizio sul territorio italiano dei servizi in valute virtuali (*exchange* ed *e-wallet*) è riservato ai soggetti iscritti nella sezione speciale del registro informatizzato dei cambiavalute tenuto da O.A.M.<sup>64</sup>, salvo si tratti di attività di emissione in proprio di valute virtuali senza che tale attività venga svolta a titolo professionale e per conto della clientela
- L'iscrizione nel registro è subordinata al possesso dei requisiti già previsti per i cambiavalute, ossia: per le persone fisiche cittadinanza italiana o di uno Stato dell'Unione europea, per i soggetti diversi dalle persone fisiche sede legale e amministrativa o, per i soggetti comunitari, stabile organizzazione nel territorio della Repubblica. Ne consegue che i prestatori di servizi in valute virtuali, se diversi dalle persone fisiche e con sede al di fuori del nostro Paese, per svolgere l'attività in Italia devono costituirvi una sede legale o amministrativa (nel caso di operatori extra-UE) o una stabile organizzazione, es. una succursale, se operatori UE <sup>65</sup>
- Ai fini dell'iscrizione i soggetti che intendono svolgere la propria attività, anche on-line, devono comunicare in via telematica i dati previsti <sup>66</sup> all'O.A.M. e tale comunicazione "costituisce condizione essenziale per l'esercizio legale dell'attività sul territorio della repubblica"; i prestatori di tali servizi, che alla data di avvio della sezione speciale del registro "già svolgono l'attività, anche on-line", effettuano la comunicazione entro sessanta giorni dall'avvio della sezione speciale: in caso di mancata comunicazione "l'eventuale

---

<sup>63</sup> Ministero dell'economia e delle finanze, Decreto 13 gennaio 2022 "Modalità e tempistiche con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale e i prestatori di servizi di portafoglio digitale sono tenuti a comunicare la propria operatività sul territorio nazionale nonché forme di cooperazione tra il Ministero dell'economia e delle finanze e le forze di polizia", in G.U. n. 40 del 17 febbraio 2022.

<sup>64</sup> Disciplinato dall'art. 17-bis, comma 8-bis del d.lgs. 141/2010 e successive modifiche

<sup>65</sup> Vedi sul punto anche A. Di Giorgi - A. Lucchini "*Prime considerazioni sul decreto sui prestatori di servizi di valuta virtuale e portafoglio digitale*" in *Diritto Bancario web*, 18 febbraio 2022

<sup>66</sup> Ex art. 3 comma 4 del Decreto del MEF

esercizio dell'attività da parte dei predetti prestatori è considerato abusivo<sup>67</sup>

- L'avvio della gestione da parte di O.A.M. della sezione speciale del registro è stato fissato in 90 giorni dall'entrata in vigore del Decreto; il 16 maggio l'O.A.M. ha comunicato l'avvio operativo di detta sezione speciale, con conseguente inizio del termine di 60 giorni per la comunicazione prevista a carico dei soggetti già operativi; l'Organismo ha poi 15 giorni per verificare la regolarità sulla completezza della comunicazione e disporre o negare l'iscrizione
- I prestatori di servizi relativi all'utilizzo delle cripto e di portafoglio digitale trasmettono ad OAM per via telematica i dati relativi alle operazioni effettuate sul territorio nazionale, con cadenza trimestrale; tra essi sono previsti anche dati sintetici dell'operatività complessiva per singolo cliente<sup>68</sup>
- Qualora gli organi investigativi rilevino l'esercizio abusivo dei servizi in valuta virtuale, accertano e contestano la violazione con le modalità e i termini di cui alla legge 14 novembre 1981, n. 689; per via del rimando operato dalla legge antiriciclaggio<sup>69</sup>, la sanzione amministrativa per l'esercizio abusivo dell'attività va da 2.065 euro a 10.329 euro ed è emanata dal M.E.F.<sup>70</sup>
- O.A.M collabora con le Autorità antiriciclaggio di cui art. 21 comma 2, lett. a) del d.lgs.231/07<sup>71</sup> e la Direzione Nazionale Antimafia, per agevolare l'esercizio dei rispettivi compiti istituzionali e fornisce informazioni e documentazione sul registro, compresi i dati che le sono stati trasmessi ai sensi dell'art. 5 del decreto del MEF.

<sup>67</sup> Ex art. 3, commi 2 e 3 del Decreto

<sup>68</sup> Come dall'allegato n. 1 del Decreto

<sup>69</sup> D.lgs. 231/2007 art. 1, comma 2, lett. ff) e ff-bis)

<sup>70</sup> Secondo l'interpretazione funzionale della normativa, si dovranno anche applicare le altre norme della legge 689/81 anche in tema di accertamento (art. 13), sequestro (art. 19) e sanzioni accessorie (art. 20), secondo cui è previsto il sequestro cautelare, da parte degli organi di controllo, delle cose che possono formare oggetto di conoscenza amministrativa, nei modi e con i limiti in cui il Codice di procedura penale consente il sequestro alla P.G. Nel caso di siti *internet* le modalità operative del sequestro prevedono l'oscuramento del sito stesso mediante inibizione all'accesso attraverso notifica agli *internet service provider*; cfr. sul punto anche V. Vallefucio "Criptovalute, DM in Gazzetta: sanzioni a doppia via per gli operatori cripto", Sole24Ore, 7 febbraio 2022

<sup>71</sup> Individuate nel Ministero dell'economia e delle finanze, le Autorità di vigilanza di settore, l'Unità di informazione Finanziaria per l'Italia, la Direzione investigativa antimafia, la Guardia di finanza che opera nei casi previsti dal d.lgs. 231/07 attraverso il Nucleo Speciale Polizia Valutaria

L'Organismo dispone dei poteri di sospensione e cancellazione dalla sezione speciale del registro nei casi di violazione, perdita dei requisiti etc., di cui all'art. 17-bis, comma 4 del d.lgs. 141/2010.

L'intera vicenda merita anzitutto due osservazioni. La prima concerne la scelta operata dal Ministero in merito alla riferibilità del provvedimento e dei suoi obblighi. Già la norma del legislatore antiriciclaggio italiano appare più ampia di quella adottata dalla vigente quinta direttiva europea che impone vincoli AML/CFT solo a chi fornisce servizi di cambio tra le valute *fiat* e le valute virtuali e servizi di portafoglio digitale: l'ampia dizione legislativa della 231/07<sup>72</sup> pone obblighi anche a carico di attività diverse dal cambio e dal portafoglio digitale, a queste solo indirettamente collegate. Se il legislatore nazionale ha inteso così coprire tutti i servizi connessi ai c.d. *token fungibili*, ci si è chiesto se avesse voluto estendere il perimetro anche ai c.d. *token non fungibili* o NFT. Mentre una cripto-valuta è fungibile poiché può essere sostituita con un'altra, gli NFT, invece, sono pezzi unici: non possono, cioè, essere replicati né sostituiti<sup>73</sup>. Con gli NFT è nata la *Crypto Art*, protagonista di un vero e proprio recente boom, con opere e oggetti digitali venduti all'asta.

Dal testo del decreto sembra proprio di no: una piattaforma di scambio di opere d'arte NFT appare essere esclusa dall'applicazione di questi obblighi. Il Ministero dell'Economia, rispondendo ad un'interrogazione parlamentare, nel settembre 2021 aveva infatti indicato di aver espunto dallo schema di decreto allora in pubblica consultazione "il riferimento anche agli operatori commerciali che accettano valuta virtuale quale corrispettivo di qualsivoglia prestazione avente ad oggetto beni, servizi o altre utilità"<sup>74</sup>.

---

<sup>72</sup> Il già citato art. 1 comma 2, lett. ff) del d.lgs. 231/07 definisce infatti prestatori di servizi relativi all'utilizzo di valuta virtuale "ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, anche online, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale o in rappresentazioni digitali di valore, ivi comprese quelle convertibili in altre valute virtuali nonché i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute"

<sup>73</sup> Grazie alla tecnologia *blockchain* NFT può essere qualsiasi oggetto digitale: un video, una foto, una GIF, un testo, un articolo, un audio. Quando un oggetto digitale è certificato con un NFT è come se sopra ci fosse la firma dell'autore, e nessuno può dire che non sia originale o che ce ne siano altre copie se non firmate con un NFT

<sup>74</sup> Interrogazione parlamentare n. 5.06521 dell'8 settembre 2021 davanti alla VI Commissione permanente – Finanze, reperibile <http://documenti.camera.it/leg18/resoconti/commissioni/bollettini/pdf/2021/09/08/leg.18.bol0652.data20210908.com06.pdf>

## 6. Conclusioni

È oramai evidente la rapidità con cui le innovazioni tecnologiche caratterizzate da evidenti riflessi in campo finanziario, quali appunto la *blockchain* e le cripto-attività, possono essere sfruttate a fini illeciti. Di contrasto, i tempi della loro disciplina, affidati al legislatore europeo o nazionale, risultano ovviamente ben più lunghi a motivo della necessità di analizzare compiutamente i fenomeni e regolamentarli sia in termini definitivi, che in termini prescrittivi, valutandone poi l'aspetto sanzionatorio. In ragione di ciò può comprendersi come le autorità di controllo in diversi Paesi stiano anche adottando sempre di più un approccio in termini di *'regulation by enforcement'* al fine di fronteggiare con maggiore tempestività le condotte – in senso ampio - antisociali realizzate a mezzo delle cripto-attività<sup>75</sup>. Un'attività, come si è visto, basata sull'adozione di una nuova interpretazione della regolamentazione esistente al fine di coprire condotte individuali e strumenti (tecnologici) ancora non 'censiti' dal diritto e su cui la dottrina esprime numerose perplessità.

La natura decentralizzata, la peculiarità tecnologica e le caratteristiche tipiche di strumenti *over the counter* rendono particolarmente difficoltosa per i *Regulators* la qualificazione giuridica del fenomeno cripto-attività. Tant'è che per le cripto si è parlato di rappresentazioni digitali di valore, ma anche di *commodity* o, in taluni casi, persino di valute – cosa che abbiamo visto non sono - sia pure in quest'ultima ipotesi a fini più propriamente strumentali.

Ciononostante, la giurisprudenza le considera ormai pacificamente assimilabili al denaro, ai beni e alle altre utilità tramite i quali risulta possibile riciclare i proventi di origine illecita, finanziare il terrorismo ovvero ancora aggirare i programmi sanzionatori. In quest'ottica risulta interessante osservare come le autorità americane, per quanto visto, stiano applicando in via analogica alle cripto-attività le disposizioni penali statunitensi in tema di strumenti finanziari. Si tratta, in sostanza, dello stesso principio che la prima sentenza penale della nostra Corte di Cassazione in tema di cripto-valute<sup>76</sup> ha anch'essa analogicamente applicato. In estrema sintesi può dirsi che la giurisprudenza, in più parti del mondo, si mostra incline ad estendere al fenomeno istituti giuridici già esistenti per altre attività finanziarie, già disciplinate ma ad esso sostanzialmente riconducibili.

Da ultimo, nonostante lo sforzo perseguito dal legislatore (nazionale ed europeo) per rafforzare i presidi antiriciclaggio si intravede il rischio che

---

<sup>75</sup> La Comunicazione della Commissione sulla Strategia UE per contrastare il crimine organizzato 2021-2025 prevede che "le autorità di contrasto e giudiziarie devono stare al passo con le tecnologie in rapido sviluppo utilizzate dai criminali e con le loro attività transfrontaliere".

<sup>76</sup> Cfr. cit. sent. Cass. Pen. 26807 del 17 settembre 2020.

l'esclusione degli NFT dal perimetro della MiCA, e quindi indirettamente la non assoggettabilità dei prestatori dei soli servizi in NFT al *Single rule book AML*, possa offrire opportunità di attività illecite e riciclaggio (come nel caso sopra esaminato dell'ex dirigente di una società statunitense attiva nella commercializzazione di NFT, a giudizio per frode perpetrata con strumenti di comunicazione - o *wire fraud* - e riciclaggio).

Su quest'ultimo aspetto va rilevato come, sinora, il commercio degli NFT – i cui volumi sono sempre più in costante crescita – avvenga prevalentemente su piattaforme online che non sono attualmente incluse tra i soggetti tenuti ad obblighi di registrazione o licenza. Resta da chiarire se il commercio di opere d'arte e dell'ingegno rappresentato dagli NFT possa ritenersi attratto negli obblighi amministrativi antiriciclaggio solo se esercitato tramite le case d'arte e le case d'asta che da tempo fanno parte dei soggetti obbligati o se invece sul tema dovrà nuovamente confrontarsi il legislatore, come nella recente proposta del Parlamento europeo. Il rapporto sul crimine a mezzo cripto-attività pubblicato da Chainalysis a febbraio 2022 indica che nel mercato degli NFT potrebbero realizzarsi condotte illecite – quali i citati *wash-trades* - e di riciclaggio. Infatti, l'assenza di una qualificazione giuridica per gli NFT li rende vulnerabili, in particolare, alle pratiche di abuso di mercato senza che, però, le sanzioni previste dalla disciplina per tali abusi possano applicarsi<sup>77</sup>.

---

<sup>77</sup> La disciplina recata dal 'Regolamento (UE) 596/2014 relativo agli abusi di mercato' si applica esclusivamente agli strumenti finanziari (vedi art. 2).