L'INAFFERABILE FISIONOMIA DEL *CYBERLAUNDERING*

Costanza Bernasconi *

17.1.2024

SOMMARIO 1. Il *Cyberlaundering* nel contesto digitale. – 2. Dalle prime forme di sfruttamento delle nuove tecnologie a fini di riciclaggio all'avvento delle valute virtuali. – 3. Le criptomonete: una nuova possibile declinazione dell'oggetto materiale del riciclaggio? – 4. I punti di forza (nella prospettiva dell'autore del reato) della dimensione digitale del riciclaggio. – 5. I punti di debolezza (nella prospettiva di prevenzione e repressione delle condotte illecite) della dimensione digitale del riciclaggio. – 6. L'evoluzione della disciplina di contrasto nei confronti del *Cyberlaundering*. I primi passi normativi per prevenire i rischi di riciclaggio nel mondo delle criptovalute. – 7. Considerazioni conclusive.

1. Il *Cyberlaundering* nel contesto digitale

Il *Cyberlaundering* (o riciclaggio digitale) costituisce la manifestazione più recente ed evoluta del delitto di riciclaggio. Essa ha tratto origine dalla progressiva dematerializzazione del denaro, oltre che dallo sfruttamento degli enormi vantaggi e delle potenzialità (anche criminogene) di Internet[1]. Al concetto di *Cyberlaundering* viene, infatti, ricondotto l'insieme delle attività illecite volte a ripulire denaro, beni, valori e altre utilità di provenienza illecita mediante l'utilizzo delle nuove tecnologie (le c.d. ITC: *Information and Communication Technologies*)[2].

Proprio per questa sua stretta sinergia con lo sviluppo tecnologico, il fenomeno riciclatorio, come è facile intuire, ha profondamente cambiato pelle negli ultimi decenni. In particolare, la rivoluzione offerta dal *Web* nel campo dei sistemi di pagamento, con l'introduzione della moneta elettronica (*e-money*), prima, e della valuta virtuale (*e-cash* o *cyber-cash*)[3], poi, ha reso possibile l'eliminazione di uno dei più

* Professore associato di diritto penale nell'Università degli Studi di Ferrara

[1] M. TAYLOR, *Criminogenic qualities of the Internet, in Dynamics of Asymmetric Conflict*, vol. 8, 12 settembre 2015, consultabile al link: http://dx.doi.org/10.1080/17467586.2015.1065082; G.P. ACCINNI, *L'utilizzo criminogeno della blockchain: gli smart contract,* in *www.sistemapenale.it,* 15 giugno 2022.

[2] L. PICOTTI, *Profili penali del Cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. trim. dir. pen. econ.*, 2018, p. 591.

[3] Esistono differenze sostanziali tra moneta elettronica e moneta virtuale. Innanzitutto il valore della prima è perfettamente ancorato al valore di una valuta avente corso legale (euro, dollaro, ecc.): la moneta elettronica, infatti, è supportata da una valuta c.d. *fiat*, cioè non vincolata al prezzo di una materia prima come l'oro o l'argento, e rappresenta, dunque, semplice dematerializzazione della valuta di cui costituisce la memorizzazione. Inoltre, la circolazione della moneta elettronica comporta sempre

grandi problemi del riciclaggio, ovvero la movimentazione fisica dei flussi di denaro[4].

Ne consegue che la ripulitura del denaro *online* offre ai criminali numerosi vantaggi, tra i quali, segnatamente: la *dematerializzazione* delle operazioni, con la conseguente possibilità di agire in qualsiasi momento, per lo più in modo anonimo (o pseudoanonimo), senza che sia necessario interfacciarsi *face to face* con persone fisiche; la *dispersione* delle responsabilità, legata all'opportunità di coinvolgere direttamente sul *Web* una pluralità di soggetti fiduciari per il compimento di operazioni intermedie, con la connessa crescente difficoltà di identificare l'autore o gli autori dei comportamenti illeciti; la *delocalizzazione* delle condotte, che porta con sé enormi questioni relative all'individuazione del *locus commissi delicti* e, conseguentemente, della giurisdizione allorché l'attività illecita coinvolga diversi Paesi.

A questo si aggiunga che oltre al c.d. *Surface Web,* vale a dire la rete accessibile da parte di chiunque, esiste il c.d. *Deep Web,* la "rete nascosta", ossia quella rete raggiungibile solo attraverso *software* specifici e accessi criptati, dove lo scambio dei dati tra utenti è (ulteriormente) protetto proprio dalla complessità delle tecniche utilizzate[5].

Tanto premesso, si comprende la ragione in forza della quale, già nel dicembre del 2013, l'Autorità Bancaria Europea (ABE) avesse adottato una nota volta a informare i consumatori dei rischi derivanti dall'uso dei nuovi strumenti di pagamento digitali, nonché a favorire un utilizzo più cauto delle sempre più diffuse valute virtuali[6], denunciando, altresì, i rischi connessi ad attività di "riciclaggio di denaro sporco" insiti nell'uso di detti strumenti di pagamento[7].

2. Dalle prime forme di sfruttamento delle nuove tecnologie a fini di riciclaggio all'avvento delle valute virtuali

Invero, le prime fenomenologie criminose volte allo sfruttamento delle nuove

l'esercizio dell'attività di controllo da parte di una Banca. Diversamente, la moneta virtuale non si pone in rapporto con alcuna valuta avente corso legale e non è soggetta ad alcuna autorità centrale che la emetta o la gestisca controllandone la domanda e l'offerta.

[4] E. SIMONCINI, *Il Cyberlaundering: la nuova frontiera del riciclaggio,* in *Riv. trim dir. pen. econ.,* 2015, p. 899.

[5] Sullo stretto legame tra riciclaggio attraverso criptovalute e *Dark Web*, cfr. G.P. ACCINNI, Cybersecurity *e criptovalute. Profili di rilevanza penale dopo la Quinta Direttiva*, in *www.sistemapenale.it,* 15 maggio 2020, in particolare p. 220.

[6] Autorità Bancaria Europea, *Avvertenze per i consumatori sulle monete virtuali*, ABE/WRG/2013/01, del 12 dicembre 2013.

[7] Autorità Bancaria Europea, *Avvertenze per i consumatori sulle monete virtuali*, cit., p. 3.

tecnologie a fini di riciclaggio si sono manifestate, già da tempo, soprattutto mediante ricorso a *smart cards* elettroniche ricaricate con proventi illeciti, successivamente reimmessi nel mercato legale attraverso l'acquisto di beni o servizi, a seguito dell'apparente "ripulitura" dei citati proventi tramite detto mezzo di pagamento comune[8]. Peraltro, proprio in considerazione dell'elevato pericolo di attività illecita che può celarsi dietro tali mezzi di pagamento, molti paesi prevedono limitazioni all'ammontare di denaro che può essere caricato su tali carte. Tuttavia, vi sono anche sistemi ove tali limitazioni non sono previste[9].

Pure il gioco d'azzardo *online* è un'attività che – già da tempo – ben si presta per ripulire denaro, posto che essa risulta accessibile da ogni luogo e a basso costo. Ovviamente, il gioco legale digitale ("*e-gaming*"), organizzato e controllato da specifici operatori preposti alla vigilanza della normativa nazionale di settore, deve essere distinto dal gioco virtuale illegale, gestito invece dalla criminalità organizzata[10]. Quest'ultimo, però, semplifica notevolmente l'eventuale processo di riciclaggio del denaro, in quanto tutte le diverse fasi dello stesso possono essere realizzate direttamente attraverso il sistema informatico, divenendo più complesso per le autorità riuscire a rintracciare i flussi delle giocate.

Più di recente si è, inoltre, sviluppato in modo significativo l'utilizzo indebito di account *PayPal*, mediante l'accredito di somme di provenienza illecita a favore di soggetti compiacenti, apparentemente giustificato – ancora una volta – dall'acquisto di beni o servizi, con conseguente restituzione in tutto o in parte degli importi in tal modo accreditati[11]. In effetti, un account *PayPal* è facilmente attivabile via Internet, senza alcun contatto fisico o personale con il fornitore del servizio, avvalendosi semplicemente di un indirizzo *e-mail* e di un numero di cellulare. Detto account consente, poi, di effettuare movimentazioni di denaro che vengono direttamente ed immediatamente eseguite *online* dall'utente, superando od almeno posticipando le singole registrazioni e verifiche, operate invece dagli intermediari bancari tradizionali[12].

Ma indubbiamente il fenomeno del *Cyberlaundering* ha conosciuto una crescita

[8] Così e *amplius* L. PICOTTI, *Profili penali del Cyberlaundering: le nuove tecniche di riciclaggio*, cit., p. 594 ss.

[9] E. SIMONCINI, *Il cyberlaundering: la «nuova frontiera» del riciclaggio,* cit., 2015, p. 904.

[10] E. SIMONCINI, *Il cyberlaundering: la «nuova frontiera» del riciclaggio*, cit., p. 910.

[11] In argomento C. PARODI, S. LOMBARDO, L. GHIRARDI, *Il riciclaggio e l'aggiotaggio telematico,* in *Diritto penale dell'informatica. Reati della rete e sulla rete,* a cura di C. PARODI, V. SELLAROLI, Milano, 2020, 450.

[12] Così L. PICOTTI, *Profili penali del* Cyberlaundering*: le nuove tecniche di riciclaggio*, cit., p. 598.

esponenziale con l'avvento delle valute virtuali[13], in quanto in molti casi le relative operazioni permettono il consolidamento dei proventi delittuosi senza alcun previo passaggio per la dimensione reale dell'economia[14].

Come è stato efficacemente sintetizzato[15], i nuovi sistemi "deregolamentati" di pagamento che si sviluppano nel *Cyberspace* sono sorti spontaneamente ad opera di programmatori, produttori e utenti, bypassando il ruolo essenziale di regolazione e controllo sulla moneta ad opera di autorità centrali (BCE, Banca d'Italia, ecc.) nella fase sia dell'emissione che della circolazione, nonché – più in generale – ad opera dei soggetti (banche ed altri intermediari finanziari) sui quali si concentrano da tempo i formali obblighi antiriciclaggio, in specie d'identificazione ed adeguata verifica della clientela, oltre che di registrazione e segnalazione di operazioni sospette. Per la *criptocurrency*, dunque, non interviene alcun soggetto emittente, che assuma il potere e la responsabilità giuridicamente riconosciuti della loro produzione, raccolta, accumulo e circolazione, essendo i valori utilizzati quali mezzi di pagamento o di scambio soltanto convenzionali, in quanto accettati come tali dagli utenti nel *Web*. Si tratta, in altre parole, di un sistema *open source*, che opera, in assenza di banche o altri organismi centrali.

Siffatte peculiari caratteristiche delle criptovalute hanno, però, sollevato un ampio novero di problematiche coinvolgenti diversi aspetti, che vanno dalle modalità di tassazione delle operazioni aventi ad oggetto le stesse[16], fino – per quanto qui

[13] Secondo E. SIMONCINI (*Il cyberlaundering: la «nuova frontiera» del riciclaggio*, cit., 2015, p. 907) l'economia virtuale è un «*cyber-heaven* non solo per il crimine organizzato, ma anche per tutte quelle società che intendano sfruttare un luogo ideale e "sicuro" per realizzare operazioni di *cyberlaundering* e conseguire illecite ricchezze».

[14] Così M. CROCE, Cyberlaundering *e valute virtuali. La lotta al riciclaggio nell'era della* distributed economy, in *www.sistemapenale.it*, n. 4 del 2021, p. 128.

[15] L. PICOTTI, *Profili penali del* Cyberlaundering*: le nuove tecniche di riciclaggio*, cit., p. 599. In argomento, *amplius,* M. CROCE, Cyberlaundering *e valute virtuali. La lotta al riciclaggio nell'era della* distributed economy, cit., p. 130 ss.

[16] Su tale specifico profilo cfr. la Risoluzione n. 72 del 2 settembre 2016, assunta dall'Agenzia delle entrate a seguito di Interpello ai sensi dell'art. 11, legge 27 luglio 2000, n. 212 ("Trattamento fiscale applicabile alle società che svolgono attività di servizi relativi a monete virtuali"). Ad avviso dell'Agenzia delle entrate «il bitcoin è una tipologia di moneta "virtuale", o meglio "criptovaluta", utilizzata come "moneta" alternativa a quella tradizionale avente corso legale emessa da una Autorità monetaria. La circolazione dei bitcoin, quale mezzo di pagamento si fonda sull'accettazione volontaria da parte degli operatori del mercato che, sulla base della fiducia, la ricevono come corrispettivo nello scambio di beni e servizi, riconoscendone, quindi, il valore di scambio indipendentemente da un obbligo di legge. Si tratta, pertanto, di sistema di pagamento decentralizzato, che utilizza una rete di soggetti paritari (*peer to peer*) non soggetto ad alcuna disciplina regolamentare specifica né ad una Autorità centrale che ne governa la stabilità nella circolazione. Le criptovalute, inoltre, hanno due ulteriori fondamentali caratteristiche. In primo luogo, non hanno natura fisica, bensì digitale, essendo create, memorizzate e

maggiormente interessa – alla possibile riconducibilità di esse all'oggetto materiale di operazioni di riciclaggio, così come definite dall'art. 648 *bis* c.p.

3. Le criptomonete: una nuova possibile declinazione dell'oggetto materiale del riciclaggio?

Come anticipato, quella delle criptovalute è senz'altro la nuova frontiera del *Cyberlaundering*, posto che esso si realizza sempre più spesso mediante l'impiego della valuta virtuale quale mezzo elusivo della tracciabilità dei flussi di denaro. Del resto, come è stato anche di recente osservato[17], «la spinta criminogena che le monete virtuali veicolano è indubbia». In tale prospettiva appare, dunque, evidente l'importanza di comprendere se le criptovalute siano sussumibili in una delle diverse declinazioni dell'oggetto materiale del reato di riciclaggio ai sensi dell'art. 648 *bis* c.p.

Invero, il quesito non parrebbe essere di immediata soluzione, alla luce della controversa natura giuridica delle criptovalute[18]. Queste ultime «sono entità inafferrabili da ogni punto di vista, sicché non fa eccezione quello della loro qualificazione giuridica»[19].

Il nostro ordinamento ha introdotto per la prima volta una definizione di

utilizzate non su supporto fisico bensì su dispositivi elettronici (ad esempio *smartphone*), nei quali vengono conservate in "portafogli elettronici" (c.d. *wallet*) e sono pertanto liberamente accessibili e trasferibili dal titolare, in possesso delle necessarie credenziali, in qualsiasi momento, senza bisogno dell'intervento di terzi. In secondo luogo, i bitcoin vengono emessi e funzionano grazie a dei codici crittografici e a dei complessi calcoli algoritmici. In sostanza, i bitcoin vengono generati grazie alla creazione di algoritmi matematici, tramite un processo di *mining* (letteralmente "estrazione") e i soggetti che creano e sviluppano tali algoritmi sono detti *miner*. Lo scambio dei predetti codici criptati tra gli utenti (*user*), operatori sia economici che privati, avviene per mezzo di una applicazione software. Per utilizzare i bitcoin, gli utenti devono entrarne in possesso: - acquistandoli da altri soggetti in cambio di valuta legale; - accettandoli come corrispettivo per la vendita di beni o servizi. (…)». Tanto premesso, si conclude che, in ossequio a quanto affermato dai giudici europei (Corte di Giustizia dell'Unione europea nella sentenza 22 ottobre 2015, causa C-264/14), «l'attività di intermediazione di valute tradizionali con bitcoin, svolta in modo professionale ed abituale, costituisce una attività rilevante oltre agli effetti dell'Iva anche dell'Ires e dell'Irap» (p. 4 della citata Risoluzione).

[17] F. CONSULICH, *Nella wunderkammer del legislatore penale contemporaneo: monete virtuali che causano danni reali*, in *Diritto penale e processo* 2022, p. 154.

[18] In argomento, E. CORAGGIO, *Virtual currency fra difficoltà esegetiche e tentativi di inquadramento dogmatico in seguito al recepimento della Quinta Direttiva UE anti-money laundering,* in *www.innovazionediritto.it,* dicembre 2019; G. GASPARRI, *Riflessioni sulla natura giuridica del bitcoin tra aspetti strutturali e profili funzionali,* in *www.dirittobancario.it,* 2 dicembre 2021.

[19] F. CONSULICH, *Nella wunderkammer del legislatore penale contemporaneo: monete virtuali che causano danni reali*, cit., p 154.

cripovaluta solo con il d. lgs. n. 90 del 2017, che ha inserito nel d.lgs, n. 231 del 2007 la nozione di cui all'art. 1, comma 2, lett. *qq*)**,** in forza della quale detta criptovaluta si identifica con «*la rappresentazione digitale di valore, non emessa 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[20] *e trasferita, archiviata e negoziata elettronicamente*»[21].

Tanto premesso, in base all'opinione attualmente prevalente, la criptomoneta non potrebbe essere considerata una valuta in senso proprio poiché, diversamente dalle valute *fiat,* quelle virtuali non hanno corso forzoso né corso legale, non sarebbero in grado di assicurare le funzioni di riserva di valore, unità di conto e mezzo di scambio[22].

Esclusa la riconducibilità della moneta virtuale al denaro, si ritiene tuttavia che essa non possa neppure essere inquadrata nella categoria dei beni[23], stante l'impossibilità di un pacifico inserimento della stessa «sia tra i "beni materiali" (giacché, difatti, non esistono nella realtà, se non come sequenza numerica su di un computer), sia tra i "beni immateriali" (tenuto conto che questi ultimi sono tipici: il diritto sul bene immateriale esiste se esiste una norma che lo riconosce)»[24].

[20] Invero, la "finalità di investimento" è stata ricompresa tra le finalità di utilizzo della moneta virtuale dal successivo d.lgs. n. 125 del 2019, in attuazione della Quinta Direttiva antiriciclaggio.

[21] Come è noto, a seconda del grado di convertibilità in moneta reale, è poi possibile distingue tra valute virtuali non convertibili (o a schema chiuso), valute virtuali a convertibilità limitata (o unidirezionale), valute virtuali a convertibilità piena (o bidirezionale). Le valute virtuali a schema chiuso possono essere utilizzate solo nell'ambito della comunità virtuale di riferimento; le valute virtuali a flusso unidirezionale, acquistabili mediante moneta reale, si caratterizzano per essere non riconvertibili in *fiat money;* le valute virtuali a flusso bidirezionale, invece, sono liberamente convertibili e riconvertibili, sicché possono essere acquistate mediante *fiat money* e vendute in cambio dello stesso.

[22] In argomento, per tutti N. VARDI, *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei bitcoin*, in *Diritto dell'Informazione e dell'Informatica*, 2015, p. 443 ss.; P. IEMMA, N. CUPPINI, *La qualificazione giuridica delle criptovalute: affermazioni sicure e caute diffidenze*, in *www.dirittobancario.it,* 8 marzo 2018; F. DI VIZIO, *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti*, in *www.penalecontemporaneo.it,* 2 ottobre 2018, p. 40 ss.

[23] In argomento, F. DI VIZIO, *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti*, cit., p. 44 ss. Nella giurisprudenza, il Tribunale di Brescia – e successivamente anche la Corte d'Appello di Brescia – si è pronunciato sulla natura delle criptovalute, negando che possano essere assimilate a beni in natura. In tale prospettiva, il Tribunale ha rilevato come costituiscano requisiti fondamentali di qualunque bene oggetto di conferimento: l'idoneità ad essere oggetto di valutazione; l'esistenza di un mercato del bene; l'idoneità ad essere oggetto di forme di esecuzione forzata. Sulla base di tali premesse, il Tribunale ha ritenuto che la criptovaluta considerata non presentasse i requisiti minimi per poter essere assimilata ad un bene suscettibile in concreto di una valutazione economica attendibile, essendo il suo sviluppo e la sua diffusione ancora «in fase sostanzialmente embrionale» (così Trib. di Brescia, 18 luglio 2018, n.7556; conforme, Corte d'Appello di Brescia, sez. I, 30 ottobre 2018).

[24] P. IEMMA, N. CUPPINI, *La qualificazione giuridica delle criptovalute: affermazioni sicure e caute*

Le valute virtuali parrebbero, invece, riconducibili alla categoria residuale delle altre utilità, trattandosi di una formula tanto ampia da ricomprendere qualsiasi entità economicamente apprezzabile. Costituisce, del resto, «circostanza ormai nota che molti investitori hanno deciso di acquistare bitcoin non già al fine di utilizzarli come mezzo di pagamento nelle transazioni, bensì in vista della possibilità di lucrare ingenti profitti dalle fluttuazioni del tasso di cambio rispetto alla moneta legale»[25].

Il contributo giurisprudenziale sull'argomento risulta, tuttavia, ad oggi ancora molto limitato. Una delle rare pronunce circa la natura giuridica della criptomoneta, e sulla conseguente disciplina civilistica ad essa applicabile, è stata resa dal Tribunale di Verona[26], il quale parrebbe aver condiviso la tesi della riconducibilità dei bitcoin alla categoria dello «strumento finanziario utilizzato per compiere una serie di particolari forme di transazioni *online*» costituito da «una moneta che può essere coniata da qualunque utente ed è sfruttabile per compiere transazioni, possibili grazie ad un software *open source* e ad una rete *peer to peer*».

Siffatta impostazione è stata successivamente confermata anche dalla Cassazione[27], la quale ha affermato che «allo stato, può ritenersi il bitcoin un prodotto finanziario qualora acquistato con finalità d'investimento: la valuta virtuale, quando assume la funzione, e cioè la causa concreta, di strumento d'investimento e, quindi, di prodotto finanziario, va disciplinata con le norme in tema di intermediazione finanziaria (art. 94 ss. t.u.f.), le quali garantiscono attraverso una disciplina unitaria di diritto speciale la tutela dell'investimento».

4. I punti di forza (nella prospettiva dell'autore del reato) della dimensione digitale del riciclaggio

È ormai pacifico che il *Cyberspace* possa costituire un terreno particolarmente fertile per la realizzazione di attività illecite[28], tra le quali le operazioni di riciclaggio

diffidenze, cit.. Nello stesso senso A. CASTELLANETA, V. GUARRIELLO, *Bitcoin e riciclaggio: un'analisi interdisciplinare,* in *www.salvisjuribus,* 12 agosto 2021, par. 5.

[25] P. IEMMA, N. CUPPINI, *La qualificazione giuridica delle criptovalute: affermazioni sicure e caute diffidenze*, cit.

[26] Tribunale di Verona, sent. n. 195 del 24 gennaio 2017.

[27] Cass. pen., sez. II, 10 ottobre 2021, n. 44337.

[28] In argomento, G.P. ACCINNI, Cybersecurity *e criptovalute. Profili di rilevanza penale dopo la Quinta Direttiva*, cit., in particolare p. 215 ss.

assumono senz'altro un ruolo di primo piano per diversi fattori che operano in sinergia tra loro[29].

Innanzitutto, occorre tenere presente che (anche nella sua dimensione *offline*) la fase del "lavaggio" (*layering*) del denaro sporco molto spesso si concretizza nel compimento di una serie di operazioni volte a polverizzare ingenti quantità di contante da riciclare in piccole somme, facendo in tal modo perdere le tracce della loro originaria provenienza illecita. Si comprende, dunque, come dette operazioni risultino agevolate dalla possibilità di realizzare transazioni economico-finanziarie integralmente *online* in forma anonima (o pseudoanonima), senza la necessità di alcun contatto materiale tra il riciclatore ed il contante medesimo. In tal modo, infatti, si elimina *tout court* la movimentazione fisica del denaro, venendo meno uno dei rischi potenzialmente più alti del riciclaggio, ossia lo spostamento materiale dei capitali.

In siffatto contesto digitale possono assumere un ruolo importante i c.d. *mixers*, i quali hanno il compito di rendere più complessa la ricostruzione del c.d. *digital trial*, ossia la successione dei trasferimenti di valuta virtuale. L'attività di *mixing* può, dunque, costituire un tratto particolarmente caratterizzante del *Cyberlaundering*[30]. Tale servizio permette, infatti, all'utente di depositare un determinato ammontare in criptovaluta su uno o più conti di ingresso per poi ritirare il denaro (virtuale) "mixato", ovvero "frammentato", su conti di uscita appositamente creati o già esistenti. In altre parole, l'obiettivo principale per il *mixer* deve essere quello di far sì che la somma di denaro depositata *ab initio* sia diversa da quella ritirata alla fine del procedimento[31]. E siffatto esito è agevolato dalla circostanza che le *cryptocurrencies* garantiscono un livello di anonimato assai maggiore rispetto alle ordinarie transazioni bancarie. Infatti, per quanto il registro contabile delle operazioni sia pubblico, gli *users* non sono identificabili tramite il proprio nome e cognome, ma solo a mezzo di numeri rappresentativi della loro chiave di accesso al sistema[32]. Sicché, nel caso di sostituzione frequente

[29] Sul rapporto tra uso delle valute virtuali e riciclaggio, *amplius,* G. J. SICIGNANO, *L'acquisto di bitcoin con denaro di provenienza illecita,* in *Archivio Penale* 2020, n. 2, p. 1 ss.

[30] In argomento v, tra gli altri, F. DI VIZIO, *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti*, cit., p. 38.

[31] Esistono alcune piattaforme, come ad esempio Monero, che includono "al proprio interno il concetto di *mixing* in maniera nativa"; così e *amplius* O. CALZONE, *Servizi di mixting e Monero,* in https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/07/mixing-monero-Calzone.pdf, pubblicato il 28 luglio 2017, p. 10.

[32] Come, infatti, è stato ricordato (M. CROCE, Cyberlaundering *e valute virtuali. La lotta al riciclaggio nell'era della* distributed economy, cit., p. 131), sul pubblico registro le transazioni sono catalogate in stringhe numeriche esadecimali corrispondenti agli indirizzi di invio/recezione della valuta

delle chiavi crittografiche, diverrà assai complicato poter rinvenire elementi di sospetto nell'operatività degli utenti nel sistema della *blockchain*[33] e dare quindi avvio ad eventuali accertamenti sulle loro reali identità[34].

Una forte spinta criminogena è rappresentata inoltre – come già anticipato – dall'assenza di Autorità centrali nel sistema valutario virtuale. Le normative antiriciclaggio, infatti, presuppongono la presenza di un sistema di intermediazione bancaria e finanziaria quale canale privilegiato per la segnalazione di operazioni sospette, a compendio degli obblighi di identificazione della clientela[35]. E, in effetti, gli interventi di contrasto alle transazioni illecite si sviluppano per lo più proprio con l'approfondimento delle segnalazioni di operazioni sospette provenienti da Banche od altri intermediari finanziari. In un sistema *peer to peer*, invece, l'assenza di intermediari finisce con il sottrarre alle autorità di vigilanza ed alla magistratura un fondamentale interlocutore istituzionale affidabile per la prevenzione e il contrasto del riciclaggio[36]. Si comprende, dunque, la ragione in forza della quale, le descritte problematiche abbiano ben presto indotto anche la Commissione europea ad avviare una riflessione intesa, tra l'altro, ad estendere ad alcuni operatori del settore delle *virtual currencies* gli obblighi previsti dalla normativa antiriciclaggio[37].

Infine, non si trascuri la circostanza che il sistema delle valute virtuali ha ormai raggiunto scala globale, sicché le *cryptocurrencies* sono agevolmente utilizzabili per effettuare trasferimenti a livello sovrannazionale, permettendo agli interessati di trasferire capitali ingenti in diversi paesi del mondo, spesso privi di presidi antiriciclaggio. In molti casi si tratta di aree ove, peraltro, il segreto bancario viene garantito con un grado così elevato da risultare sostanzialmente impermeabile alle Autorità.

(*transaction address*). Peraltro, gran parte dei protocolli di gestione delle transazioni consente agli *users* di formare identificativi (chiave pubblica privata e indirizzo) differenti per ogni singola transazione, rendendo difficoltosa, se non impossibile, l'identificazione dei titolari degli *accounts* coinvolti.

[33] La *blockchain* si compone di una serie concatenata di blocchi (da cui il nome), i quali registrano, per ogni transazione, l'identità del pagante, l'importo trasferito e l'identità del beneficiario. Ciascun blocco contiene quindi le informazioni relative a tutte le transazioni che si sono svolte consecutivamente in unncerto arco temporale.

[34] G.P. ACCINNI, *Profili di rilevanza penale delle criptovalute (nella riforma della disciplina antiriciclaggio del 2017*), in *Archivio Penale*, 2018, 1, p. 4.

[35] M. CROCE, *Cyberlaundering e valute virtuali. La lotta al riciclaggio nell'era della distributed economy,* cit., p. 131.

[36] G.P. ACCINNI, *Profili di rilevanza penale delle criptovalute (nella riforma della disciplina antiriciclaggio del 2017*), cit., p. 13.

[37] Sul punto v. *amplius infra* par. 6.

5. I punti di debolezza (nella prospettiva di prevenzione e repressione delle condotte illecite) della dimensione digitale del riciclaggio

Tanto premesso, e come è facile intuire, nella prospettiva della prevenzione e repressione delle condotte illecite, tutti quelli che per l'autore delle stesse appaiono come punti di forza[38], si rivelano viceversa come altrettante rilevanti criticità.

A quanto già considerato nel paragrafo precedente con peculiare riguardo alle caratteristiche tecniche del *Cyberlaundering*, sia qui consentito aggiungere solo alcune rapsodiche considerazioni che – almeno in parte – coinvolgono peraltro anche altre fenomenologie criminose realizzate nel *Cyberspace*.

Solo nel corso del tempo, infatti, ci si è resi conto di come il reato informatico possa presentare rilevanti fronti di rottura rispetto alle tradizionali categorie tradizionali del diritto penale – segnatamente quelle impiegate per determinare la collocazione spaziale e temporale del fatto – in virtù della natura virtuale (e comunque non fisica) della dimensione cibernetica, con la conseguente creazione di uno stato di forte disorientamento nell'operatore del diritto. Quandanche, infatti, ci si trovi effettivamente dinanzi a forme di aggressione nei confronti di beni giuridici "tradizionali", già tutelati dall'ordinamento, nell'architettura digitale le fenomenologie criminose risultano caratterizzate da una rapidissima velocità di esecuzione, nonché dalla portata tendenzialmente globale del fatto, non più connotato da precisi vincoli di natura territoriale.

In tale prospettiva, basti pensare che la rete Bitcoin integra un sistema di transazioni distribuito al quale si può accedere da qualunque luogo in cui vi sia una connessione Internet. Sicché, come è stato osservato, «affermare di usare la rete per trasferire del denaro all'estero è in un certo senso fuorviante. Per la rete non esiste il concetto di estero: sono gli scambi commerciali di beni acquistati con il bitcoin che possono avvenire in una nazione o nell'altra, ma la valuta virtuale spedita e ricevuta si troverà sempre e solo sulla rete, registrata simultaneamente su tutti i nodi»[39].

Siffatte caratteristiche, come è intuitivo, sollevano rilevanti problematiche in merito all'individuazione del *tempus* e del *locus commissi delicti* nelle ipotesi, appunto, di attività illecite. Nel *Cyberspace,* infatti, i criteri tradizionali per collocare le condotte umane nel tempo e nello spazio entrano completamente in crisi[40]. È addirittura la condotta, commessa in un ambiente informatico, ad assumere specifiche

[38] V. *supra* par. 4.

[39] O. CALZONE, *Servizi di mixting e Monero,* cit., p. 3.

[40] Così anche Cass. pen., SS.UU., 26 marzo 2015, n. 17325, Rv. 263020, punto n. 3 del Considerato in diritto.

peculiarità, posto che la componente umana costituisce solo un segmento che si salda con un impulso elettronico[41], il quale potrebbe anche rendere possibile la detemporalizzazione di determinate attività, pianificate dall'utente ma poi svolte attraverso operazioni automatizzate, senza che sia necessaria la presenza fisica della persona umana davanti allo schermo di un computer[42].

Da qui derivano, dunque, alcune grandi questioni per il diritto penale, che si possono in questa sede solo abbozzare. Occorre, infatti, chiedersi; innanzitutto attraverso quali criteri sia possibile individuare la condotta da imputare al soggetto agente, là dove detta condotta assuma natura ibrida (vale a dire, umana ed elettronica); in secondo luogo, fino a che punto sia possibile imputare all'agente l'eventuale autonomia delle scelte operative dei sistemi informatici; infine, in quale momento e in quale luogo si possa ritenere perfezionato il reato e radicata la giurisdizione.

Si tratta di interrogativi di non poco momento che, oltre a rendere sempre più evanescente ed inafferrabile la fisionomia di alcuni reati cibernetici – il riciclaggio *in primis* – condizionano pesantemente la costruzione di efficaci presidi preventivi e sanzionatori.

6. L'evoluzione della disciplina di contrasto nei confronti del *Cyberlaundering*. I primi passi normativi per prevenire i rischi di riciclaggio nel mondo delle criptovalute

La disciplina generale antiriciclaggio, a livello europeo, si è articolata, ad oggi, nell'adozione di sei diverse direttive (la Direttiva 1991/308/CE; la Direttiva 2001/97/CE; la Direttiva 2005/60/UE; la Direttiva 2015/849/UE; la Direttiva 2018/843/UE, la Direttiva 2018/1673/UE), tutte recepite dal legislatore nazionale.

È soprattutto con la trasposizione della Quarta e della Quinta direttiva che il nostro ordinamento ha reagito in termini più efficaci nei confronti del *Cyberlaundering*, nella consapevolezza che – come si legge nel Considerando n. 6 della Direttiva (UE) 2018/1673 – «l'uso delle valute virtuali presenta nuovi rischi e sfide nella

[41] Non è un caso che una parte della dottrina già evidenzi come, in pochi anni, moltissimi reati potranno essere spiegati solo sulla base della somma di azioni e omissioni con mezzi fisici e virtuali, poiché le interazioni umane saranno completamente ibride. Così J. R. AGUSTINA, *Nuevos retos dogmáticos ante la cibercriminalidad ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma?,* in *Estudios penales y criminológicos*, 2021, vol. 41, p. 743.

[42] R. FLOR, *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di internet*, in *www.penalecontemporaneo.it*, 2010, p. 2.

prospettiva della lotta al riciclaggio. Gli Stati membri dovrebbero garantire che tali rischi siano affrontati in modo adeguato».

Più nei dettagli, l'intervento riformatore attuato con d.lgs. n. 90 del 2017 (il quale ha recepito nell'ordinamento interno la Direttiva UE 2015/849, c.d. Quarta Direttiva), oltre ad avere introdotto una definizione di moneta virtuale[43], ha toccato numerose disposizioni del d. lgs. n. 231 del 2007, in particolare includendo i prestatori di servizi relativi all'utilizzo di detta valuta virtuale tra i destinatari degli obblighi antiriciclaggio[44].

In tal modo, il legislatore ha cercato di affrontare la più evidente dimensione rischiosa del fenomeno, vale a dire l'anonimia o pseudo-anonimia delle transazioni che le rende, astrattamente, un perfetto strumento di riciclaggio[45]. Ne è derivata l'estensione degli obblighi di registrazione e di adeguata verifica della clientela anche in capo ai prestatori di servizi relativi all'utilizzo di valuta virtuale, la cui attività viene, altresì, ora sottoposta alla vigilanza delle autorità di settore.

Il ruolo di siffatti intermediari è, infatti, centrale nella gestione del rischio-riciclaggio, posto che, come la prassi testimonia, raramente gli utenti pongono in essere condotte illecite in proprio, cioè senza affidarsi alla "professionalità" di broker specializzati, che dispongono delle conoscenze tecniche necessarie per accedere alle piattaforme di *mixing*, le quali – come anticipato – costituiscono nella maggior parte dei casi un ostacolo definitivo alle attività d'indagine[46]. Talché, si è ritenuto opportuno prevedere meccanismi di registrazione del denaro in uscita dal mondo reale o «attenderlo al guado, al momento dell'uscita dal mondo virtuale»[47]. In tale prospettiva, sono stati, dunque, introdotti l'obbligo di adeguata verifica della clientela e quello di segnalazione di operazioni sospette a carico degli scambiatori (*exchangers*)[48], i quali «svolgono

[43] Sul punto v. *supra,* par. 3.

[44] L'art. 3, comma 5, lett. *i*), d.lgs. n. 231 del 2007, così come modificato ai sensi del d.lgs. n. 90 del 2017, annovera, infatti, «i prestatori di servizi relativi all'utilizzo di valuta virtuale, limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso» tra gli operatori non finanziari.

[45] F. CONSULICH, *Nella wunderkammer del legislatore penale contemporaneo: monete virtuali che causano danni reali*, cit., p. 155.

[46] G.P. ACCINNI, Cybersecurity *e criptovalute. Profili di rilevanza penale dopo la Quinta Direttiva*, cit., in particolare p. 223.

[47] Così D. MAJORANA, *Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web*, in *Corriere tributario*, n. 8 del 2018, p. 634. In argomento v., altresì, L. STURZO, *Bitcoin e riciclaggio 2.0,* in *www.penalecontemporaneo.it,* n. 5 del 2018, p. 29.

[48] V. art. 3, comma 5, lett. *i*), d.lgs. n. 231 del 2007. Con il termine *exchanger* (o *virtual currency exchanger*), si fa riferimento alla persona fisica o giuridica che fornisce a terzi, a titolo professionale,

una funzione assimilabile alle porte poste lungo le antiche cinte daziarie: infatti gli *exchangers* sono gli unici operatori che, cambiando le criptovalute in moneta reale e viceversa, sono in grado di identificare le persone che danno luogo a tali transazioni»[49].

Successivamente a tale intervento normativo, il Legislatore ha poi recepito la c.d. Quinta Direttiva (Direttiva (UE) 2018/1673) con il d. lgs. 4 ottobre 2019, n. 125[50], il quale ha ampliato la definizione di valuta virtuale, includendo in essa anche la finalità di finanziamento, oltre che di scambio. Inoltre, la nuova disciplina ha esteso gli obblighi inerenti alla prevenzione del riciclaggio anche ai "prestatori di servizi di portafoglio digitale" (c.d. *wallet providers*)[51], e cioè ad «ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche *online*, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali»[52].

Tali previsioni hanno, conseguentemente, aperto la strada alla possibilità di applicare anche agli *exchangers* e ai *wallet providers* le sanzioni amministrative e penali previste dal d.lgs. n. 231 del 2007, nonché di considerarli potenzialmente esposti a contestazioni di concorso nei reati di riciclaggio e/o autoriciclaggio che vengano eventualmente realizzati dagli *users* mediante impiego di *virtual currencies*.

7. Considerazioni conclusive

È innegabile che tanto in sede europea, quanto nel nostro ordinamento interno si sia registrato negli ultimi anni un intenso sforzo di regolamentazione del mondo delle criptovalute – in origine libero da qualsiasi vincolo – anche in chiave di prevenzione del fenomeno riciclaggio.

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 (art. 1, comma 2, lett. *ff*, d.lgs. n. 231 del 2007).

[49] D. MAJORANA, *Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web*, cit., p. 634.

[50] In argomento, per tutti, R. M. VADALÀ, *Criptovalute e* cyberlaundering*: novità antiriciclaggio nell'attesa del recepimento della Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale*, in *www.sistemapenale.it,* 6 maggio 2020.

[51] Infatti, con il d. lgs. n. 90 del 2017, solo gli *exchangers* e non anche i *wallet providers* erano stati inseriti tra i soggetti obbligati di cui al d. lgs. n. 231 del 2007, sicché il d. lgs. n. 125 del 2019, recependo l'art. 1 della Quinta Direttiva, ha colmato tale lacuna, assoggettando agli obblighi antiriciclaggio anche i prestatori di servizi di portafoglio digitale (cfr. art. 3, comma 5, lett. *i-bis*, d. lgs. 231 del 2007).

[52] Art. 1, comma 2, lett. *ff-bis*, d.lgs. n. 231 del 2007.

I citati interventi di riforma tratteggiano, infatti, ad oggi un quadro normativo più adeguato, rispetto al passato, a confrontarsi con fenomeni di *Cyberlaundering*; nondimeno, essi non parrebbero ancora in grado di neutralizzare pienamente il rischio del loro verificarsi.

Permangono, infatti, perplessità e preoccupazioni condivise recentemente anche nella V Direttiva antiriciclaggio, del Parlamento e del Consiglio dell'Unione Europea, secondo cui «l'anonimato delle valute virtuali ne consente il potenziale uso improprio per scopi criminali. L'inclusione dei prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute reali e dei prestatori di servizi di portafoglio digitale non risolve completamente il problema dell'anonimato delle operazioni in valuta virtuale: infatti, poiché gli utenti possono effettuare operazioni anche senza ricorrere a tali prestatori, gran parte dell'ambiente delle valute virtuali rimarrà caratterizzato dall'anonimato. Per contrastare i rischi legati all'anonimato, le unità nazionali di informazione finanziaria (FIU) dovrebbero poter ottenere informazioni che consentano loro di associare gli indirizzi della valuta virtuale all'identità del proprietario di tale valuta. Occorre inoltre esaminare ulteriormente la possibilità di consentire agli utenti di presentare, su base volontaria, un'autodichiarazione alle autorità designate»[53].

Non si trascuri inoltre la circostanza che qualunque misura difficilmente potrà avere l'efficacia desiderata finché permarrà il fenomeno dello *Shadow Banking System,* cioè l'esistenza di "paradisi" in cui poter operare in spregio a qualsivoglia procedura di identificazione, con conseguente frustrazione di tutti gli sforzi normativi intrapresi da singoli Paesi virtuosi[54].

Sicché, per contrastare un fenomeno come quello delle valute virtuali, nell'ambito del quale i *players* risiedono nei punti più disparati del mondo, è necessario che almeno la maggior parte degli Stati adottino presidi legislativi adeguati, sviluppando una strategia che risulti il più possibile condivisa e uniforme.

Inoltre, come già anticipato, le caratteristiche dell'architettura digitale impongono un ripensamento complessivo dell'approccio giuridico alla nuova realtà. Il diritto penale tradizionale ed i relativi schemi di imputazione non sembrano "attrezzati" a governare un fenomeno informatico in continua e rapida evoluzione[55]. Sicché, la

[53] Direttiva (UE) 2018/843 del Parlamento Europeo e del Consiglio, del 30 maggio 2018.

[54] G.P. ACCINNI, *Profili di rilevanza penale delle criptovalute (nella riforma della disciplina antiriciclaggio del 2017*), cit., p. 29.

[55] G.P. ACCINNI, *L'utilizzo criminogeno della blockchain: gli smart contract,* cit., p. 16.

natura estremamente "fluida" della criptomoneta, unitamente all'opacità dei meccanismi di operatività della Rete, fanno del *Cyberlaundering* un esempio emblematico delle nuove sfide con le quali non è più rinviabile un serrato confronto.

ABSTRACT

Il contributo si propone l'obiettivo di tratteggiare la sfuggente fisionomia del delitto di riciclaggio digitale, la quale appare il risultato, da un lato, della più generale opacità dei meccanismi di operatività della Rete, e, dall'altro lato, della natura estremamente "fluida" e controversa della criptomoneta, invero sempre più frequentemente utilizzata per il compimento di attività illecite. Sennonché, detta fisionomia sfuggente si ripercuote inevitabilmente sull'individuazione di specifici ed efficaci strumenti di contrasto, oltre che sull'impiego delle tradizionali categorie del diritto penale, sollecitando una non rinviabile riflessione sulla necessità di ripensare schemi di imputazione in grado di governare fenomenologie criminose in continua evoluzione in quanto legate alle peculiari dinamiche dello sviluppo tecnologico.

PAROLE CHIAVE

Riciclaggio digitale – Reato cibernetico – Spazio digitale – Moneta virtuale

* * *

THE ELUSIVE APPEARANCE OF CYBERLAUNDERUNG

ABSTRACT

The article aims to outline the elusive physiognomy of the crime of digital money laundering, which appears to be the result, on the one hand, of the more general opacity of the operational mechanisms of the Internet, and, on the other hand , of the extremely "fluid" and controversial nature of cryptocurrency, which is indeed increasingly used to carry out illicit activities. However, this elusive physiognomy inevitably has repercussions on the identification of specific and effective instruments of contrast, as well as on the use of the traditional categories of criminal law, prompting a non-postponable reflection on the need to rethink attribution schemes capable of governing the constantly evolving criminal phenomenologies because linked to the peculiar dynamics of technological development.

KEYWORDS

Cyberlaundering – Cybercrime – Cyberspace – Virtual Currencies