

SP

SISTEMA
PENALE

FASCICOLO

4/2021

COMITATO EDITORIALE Giuseppe Amarelli, Roberto Bartoli, Hervè Belluta, Michele Caianiello, Massimo Ceresagastaldo, Adolfo Ceretti, Cristiano Cupelli, Francesco D'Alessandro, Angela Della Bella, Gian Paolo Demuro, Emilio Dolcini, Novella Galantini, Mitja Gialuz, Glauco Giostra, Antonio Gullo, Stefano Manacorda, Vittorio Manes, Luca Masera, Anna Maria Maugeri, Melissa Miedico, Vincenzo Mongillo, Francesco Mucciarelli, Claudia Pecorella, Marco Pelissero, Lucia Riscato, Marco Scoletta, Carlo Sotis, Costantino Visconti

COMITATO SCIENTIFICO (REVISORI) Alberto Alessandri, Silvia Allegrezza, Ennio Amodio, Gastone Andreatza, Ercole Aprile, Giuliano Balbi, Marta Bargis, Fabio Basile, Alessandra Bassi, Teresa Bene, Carlo Benussi, Alessandro Bernardi, Marta Bertolino, Rocco Blaiotta, Manfredi Bontempelli, Renato Bricchetti, David Brunelli, Carlo Brusco, Silvia Buzzelli, Alberto Cadoppi, Lucio Camaldo, Stefano Canestrari, Giovanni Canzio, Francesco Caprioli, Matteo Caputo, Fabio Salvatore Cassibba, Donato Castronuovo, Elena Maria Catalano, Mauro Catenacci, Antonio Cavaliere, Francesco Centonze, Federico Consulich, Stefano Corbetta, Roberto Cornelli, Fabrizio D'Arcangelo, Marcello Daniele, Gaetano De Amicis, Cristina De Maglie, Alberto De Vita, Ombretta Di Giovine, Gabriella Di Paolo, Giandomenico Dodaro, Massimo Donini, Salvatore Dovere, Tomaso Emilio Epidendio, Luciano Eusebi, Riccardo Ferrante, Giovanni Fiandaca, Giorgio Fidelbo, Carlo Fiorio, Roberto Flor, Luigi Foffani, Désirée Fondaroli, Gabriele Fornasari, Gabrio Forti, Piero Gaeta, Marco Gambardella, Alberto Gargani, Loredana Garlati, Giovanni Grasso, Giulio Illuminati, Gaetano Insolera, Roberto E. Kostoris, Sergio Lorusso, Ernesto Lupo, Raffaello Magi, Vincenzo Maiello, Grazia Mannozi, Marco Mantovani, Marco Mantovani, Luca Marafioti, Enrico Marzaduri, Maria Novella Masullo, Oliviero Mazza, Claudia Mazzucato, Alessandro Melchionda, Chantal Meloni, Vincenzo Militello, Andrea Montagni, Gaetana Morgante, Lorenzo Natali, Renzo Orlandi, Luigi Orsi, Francesco Palazzo, Carlo Enrico Paliero, Lucia Parlato, Annamaria Peccioli, Chiara Perini, Carlo Piergallini, Paolo Pisa, Luca Pistorelli, Daniele Piva, Oreste Pollicino, Domenico Pulitanò, Serena Quattrococo, Tommaso Rafaraci, Paolo Renon, Maurizio Romanelli, Gioacchino Romeo, Alessandra Rossi, Carlo Ruga Riva, Francesca Ruggieri, Elisa Scaroina, Laura Scomparin, Nicola Selvaggi, Sergio Seminara, Paola Severino, Rosaria Sicurella, Piero Silvestri, Fabrizio Siracusano, Andrea Francesco Tripodi, Giulio Ubertis, Antonio Vallini, Gianluca Varraso, Vito Velluzzi, Paolo Veneziani, Francesco Viganò, Daniela Vighè, Francesco Zacchè, Stefano Zirulia

REDAZIONE Francesco Lazzeri (coordinatore), Enrico Andolfatto, Enrico Basile, Silvia Bernardi, Carlo Bray, Pietro Chiaraviglio, Stefano Finocchiaro, Beatrice Fragasso, Alessandra Galluccio, Cecilia Pagella, Tommaso Trinchera, Maria Chiara Ubiali

Sistema penale (SP) è una rivista *online*, aggiornata quotidianamente e fascicolata mensilmente, ad accesso libero, pubblicata dal 18 novembre 2019.

La *Rivista*, realizzata con la collaborazione scientifica dell'Università degli Studi di Milano e dell'Università Bocconi di Milano, è edita da Progetto giustizia penale, associazione senza fine di lucro con sede presso il Dipartimento di Scienze Giuridiche "C. Beccaria" dell'Università degli Studi di Milano, dove pure hanno sede la direzione e la redazione centrale. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.

La *Rivista* si uniforma agli standard internazionali definiti dal *Committee on Publication Ethics (COPE)* e fa proprie le relative linee guida.

I materiali pubblicati su *Sistema Penale* sono oggetto di licenza CC BY-NC-ND 4.00 International. Il lettore può riprodurli e condividerli, in tutto o in parte, con ogni mezzo di comunicazione e segnalazione anche tramite collegamento ipertestuale, con qualsiasi mezzo, supporto e formato, per qualsiasi scopo lecito e non commerciale, conservando l'indicazione del nome dell'autore, del titolo del contributo, della fonte, del logo e del formato grafico originale (salve le modifiche tecnicamente indispensabili).

Il testo completo della licenza è consultabile su <https://creativecommons.org/licenses/by-nc-nd/4.0/>.

Peer review I contributi che la direzione ritiene di destinare alla sezione "Articoli" del fascicolo mensile sono inviati a un revisore, individuato secondo criteri di rotazione tra i membri del Comitato scientifico, composto da esperti esterni alla direzione e al comitato editoriale. La scelta del revisore è effettuata garantendo l'assenza di conflitti di interesse. I contributi sono inviati ai revisori in forma anonima. La direzione, tramite la redazione, comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se la valutazione è positiva, il contributo è pubblicato. Se il revisore raccomanda modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se il revisore esprime parere negativo alla pubblicazione. La direzione si riserva la facoltà di pubblicare nella sezione "Altri contributi" una selezione di contributi diversi dagli articoli, non previamente sottoposti alla procedura di *peer review*. Di ciò è data notizia nella prima pagina della relativa sezione.

Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione Per la citazione dei contributi presenti nei fascicoli di *Sistema penale*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Sist. pen. (o SP)*, 1/2020, p. 5 ss.

**CYBERLAUNDERING E VALUTE VIRTUALI.
LA LOTTA AL RICICLAGGIO
NELL'ERA DELLA DISTRIBUTED ECONOMY^(*)**

di Mariachiara Croce

SOMMARIO: 1. Introduzione. – 2. Valute virtuali e riciclaggio: inquadramento del fenomeno. – 3. La disciplina preventiva del riciclaggio: dal D. Lgs. 90/2017 al D. Lgs. 125/2019. – 4. La disciplina sanzionatoria del riciclaggio. – 4.1 Il *cyberlaundering* – 5. L'autoriciclaggio – 5.1 Il *cyber self-laundering* – 5.2. La responsabilità per riciclaggio di *exchangers, wallet providers, mixers* e *miners*. – 6. Normativa antiriciclaggio e valute virtuali. Esperienze regolatorie a confronto. – 7. Considerazioni conclusive.

1. Introduzione.

Il *cyberlaundering* è una manifestazione parziale dell'ampio fenomeno del *cybercrime*, al quale è riconducibile ogni forma di sfruttamento delle *new technologies* a fini delittuosi¹. Mutuando la classica distinzione dottrinale² tra delitti informatici in senso stretto e delitti informatici in senso lato³, è possibile ricondurre il *cyberlaundering* a questa seconda categoria: quale ipotesi di riciclaggio comune commesso avvalendosi di un *computer* come mezzo, e non come oggetto materiale del reato, esso è suscettibile di assumere soltanto eventualmente le vesti di un reato informatico.

^(*) Il contributo è destinato alla pubblicazione in A. Nuzzo (a cura di), *Fintech, Smart technologies e Governance dei mercati*, Luiss University Press.

¹ Per *cyberlaundering* si intende una particolare forma di utilizzo della rete internet a scopo criminoso. Come si evince dal termine, esso costituisce, infatti, una trasposizione in chiave moderna e digitale dei "classici" delitti di cui agli artt. 648-bis c.p. e 648-ter.1 c.p. Per un inquadramento del tema v. V. PLANTAMURA, *Il cybericiclaggio*, in A. Cadoppi – S. Canestrari – A. Manna – M. Papa (a cura di), *Cybercrime*, Milano, 2019, 859 ss.

² L. PICOTTI, *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. ec.*, 2011, 4, 827 ss.; R. FLOR, *Cyber-criminality: Finding a Balance between Freedom and Security*, nella raccolta di scritti del convegno *Cybercrime: Global Phenomenon and its Challenges*, *International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme (ISPAC)*, 13 ss. Per alcuni interessanti spunti di riflessione inerenti alla prima reazione legislativa a fronte dell'affermarsi della criminalità informatica, R. BLAIOTTA – F. BERGHELLA, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 1995, 9, 2329 ss.

³ Nella prima categoria di reati informatici rientrano tutte le condotte criminoso che abbiano come *target* il computer, come, ad esempio, le attività di *cyberspying* o la commissione di estorsioni via internet. La seconda tipologia di reati informatici, invece, è comprensiva di ogni condotta criminosa perpetrata sfruttando le caratteristiche della rete.

Se le prime manifestazioni criminose rivolte allo sfruttamento delle nuove tecnologie a fini di riciclaggio si registravano già da tempo⁴, mediante ricorso a *smart cards* e monete elettroniche⁵, è stato solo con l'avvento delle valute virtuali che il fenomeno ha avuto una crescita esponenziale, in quanto le relative operazioni permettono il consolidamento dei proventi delittuosi senza alcun previo passaggio per la dimensione reale dell'economia: nella *distributed economy* il riciclaggio diviene un fenomeno di regola totalmente digitale.

Per comprendere la serietà dei rischi associati alla diffusione di questi valori, è sufficiente richiamare le più recenti statistiche sulla capitalizzazione del mercato delle *criptocurrencies*⁶, che evidenziano come il volume di transazioni stia crescendo in modo rapido e costante e con esso, inevitabilmente, anche il numero di operazioni sospette⁷.

Nel presente contributo saranno esaminate le questioni più significative connesse proprio all'utilizzo delle valute virtuali per fini di riciclaggio, concentrando l'attenzione non solo sui profili repressivi, ma anche sulla disciplina preventiva di recente introduzione.

2. Valute virtuali e riciclaggio: inquadramento del fenomeno.

L'art. 1, comma 2, lett. qq) del D. Lgs. 231/2007⁸ definisce la valuta virtuale come una «rappresentazione digitale di valore, non emessa né garantita da una banca centrale o un'autorità pubblica, non necessariamente collegata ad 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»⁹.

⁴ Il *cyberlaundering* trae origine dalla progressiva dematerializzazione del denaro e dall'avvento della c.d. moneta elettronica. In argomento, D.A. LESLIE, *Legal Principles for Combatting Cyberlaundering*, *Law, Governance and Technology Series*, Basilea, 2014, 55.

⁵ L. PICOTTI, *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. trim. dir. pen. econ.*, 2018, 3-4, 594-598.

⁶ Il mercato delle valute virtuali, sebbene sia sorto solo nel 2009 dalle rovine della crisi economico-finanziaria dell'anno precedente, può contare oggi su di un giro d'affari multimiliardario: se, solo a maggio 2017 il mercato aveva una capitalizzazione di 91 miliardi di dollari, all'inizio del 2018 il volume globale di ha superato i 150 miliardi di dollari, facendo registrare una media di transazioni giornaliere in criptomoneta pari a 3,5 miliardi di euro. Cfr. il sito [Coin Market Cap](#).

⁷ «Quaderni dell'antiriciclaggio dell'Unità di Informazione Finanziaria», sul sito della UIF, Semestre I, 2018, 59.

⁸ La disposizione è stata introdotta dall'art. 1, comma 1 del D. Lgs. 25 maggio 2017 n. 90 («Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo»). Per un primo commento alla riforma, L. D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptomoneta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D.Lgs. 90/2017*, in *Dir. banc.*, 2018, 1, 4 ss. Le parole «né garantita» e «o per finalità di investimento» sono state introdotte dall'art. 1, comma 1, lett. h) del D. Lgs. 125/2019.

⁹ A seconda del grado di convertibilità in moneta reale, si 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

Nella prassi, gli utenti entrano in possesso delle valute virtuali cambiando *fiat money*, offrendo merci o servizi dietro corrispettivo (previamente pattuito) in criptovalute ovvero ricevendole in regalo o a titolo di ricompensa per l'attività prestata all'infrastruttura¹⁰.

A rendere particolarmente attraente la valuta virtuale agli occhi degli investitori è la perfetta fusione dei vantaggi della moneta reale e di quelli della moneta elettronica in essa riscontrabile. Come la moneta fisica, essa è accessibile a chiunque, ha carattere anonimo¹¹ ed è agevolmente trasferibile; come la moneta elettronica, consente di effettuare agevolmente pagamenti a distanza e garantisce transazioni rapide e a basso costo¹².

Le transazioni in valuta virtuale sono un formidabile veicolo di *business*, poiché consentono agli operatori economici di entrare in contatto con le più svariate realtà internazionali e di interagire con le stesse a costi ridotti e con possibilità di perfezionare in modo istantaneo trasferimenti di ingenti somme di denaro¹³. Per queste stesse ragioni, la criptomoneta ha attirato su di sé l'attenzione dei criminali informatici, specialmente nel periodo immediatamente successivo alla sua creazione¹⁴.

virtuale di riferimento e, pertanto, rappresentano la forma di *e-cash* tipica delle piattaforme di giochi virtuali; 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, infine, sono liberamente convertibili e riconvertibili e possono pertanto essere acquistate mediante *fiat money* e vendute in cambio dello stesso (a tale ultima categoria appartiene il Bitcoin, la più nota e diffusa *virtual currency*). Pur essendo valute di carattere privato, le valute virtuali si distinguono, inoltre, in valute virtuali centralizzate, create da un emittente privato, e valute virtuali decentralizzate, generate dagli utenti della rete avvalendosi di specifici *software* basati su meccanismi di crittografia. Sul punto si veda la «Avvertenza sull'utilizzo delle cosiddette 'valute virtuali'», 30 gennaio 2015, pubblicato dalla Banca D'Italia sul [sito istituzionale](#), 2 ss.

¹⁰ A quest'ultima ipotesi è riconducibile la ricompensa in *virtual currency* riconosciuta dal sistema Bitcoin ai *miners* che risolvano la *proof of work* prevista dal protocollo base. Di recente, G.P. ACCINNI, *Profili di rilevanza penale delle criptovalute (nella riforma della disciplina antiriciclaggio del 2017)*, in *Archivio Penale*, 2018, 1, 4.

¹¹ L'anonimato (*rectius*, lo pseudo-anonimato) garantito agli *users* di valute virtuali è il principale elemento che induce la criminalità a sfruttare la *piazza finanziaria digitale* per polverizzare le ingenti liquidità di origine illecita.

¹² Queste caratteristiche rendono le valute virtuali uno strumento utile al consolidamento della ricchezza proveniente da reato. La rapidità degli scambi rappresenta un serio ostacolo all'identificazione della provenienza delittuosa, mentre l'accettazione su larga scala assicura l'*integration* del profitto nelle mani del reo attraverso semplici operazioni di acquisto di beni o servizi o scambio in altri valori virtuali. Cfr. N. PASSARELLI, *Bitcoin e antiriciclaggio*, sul [sito del Sistema di Informazione per la Sicurezza della Repubblica](#), 15 novembre 2016; L. STURZO, *Bitcoin e riciclaggio 2.0*, in *Dir. pen. cont.*, 5/2018, 20.

¹³ Inoltre, concretizzando il sogno di democratizzazione finanziaria, i valori virtuali agevolano il coinvolgimento dei soggetti più deboli nelle attività commerciali e finanziarie. La pseudoanonimizzazione delle transazioni e la garanzia dell'anonimato assicurano ai cittadini di Paesi retti da governi dispotici che vietino l'utilizzo del circolante virtuale di tutelare le proprie legittime esigenze di tutela della riservatezza. Cfr. G. GASPARRI, *Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*, in *Dir. inf.*, 2015, 3, 415.

¹⁴ Sulle possibili forme di sfruttamento ai fini criminosi delle valute virtuali si veda P. SEVERINO, *Sicurezza informatica e prevenzione del cybercrime*, in *LuissOpen*, 8 settembre 2017, 10.

Le innegabili potenzialità criminogene delle valute virtuali non debbono, tuttavia, condurre a conclusioni affrettate circa la natura del circolante virtuale e la legittimità del suo utilizzo.

A ben vedere, una transazione in valuta virtuale – quale che sia l’infrastruttura o la base monetaria utilizzata – è di per sé neutra: l’illiceità dell’operazione potrebbe eventualmente dipendere dalla causa della transazione o dall’oggetto di essa. A tal proposito, in dottrina è stato correttamente osservato che il *pactum fiduciae* tra utenti si basa sulla stabilità e sulla legittimità del protocollo informatico che governa la catena dei blocchi. La fiducia sarebbe minata alle fondamenta se l’infrastruttura fosse utilizzata prevalentemente o esclusivamente per scopi criminosi¹⁵. Risulta quindi chiaro che l’impiego delle valute virtuali a fini di riciclaggio rappresenta una patologia del sistema, una cifra nera che rischia di disgregare la fiducia che l’utente medio ripone nella tecnologia a registro diffuso e nei relativi valori¹⁶.

Come avviene per ogni innovazione tecnologica, anche nella nuova dimensione virtuale dell’economia è presente un rischio intrinseco¹⁷. È noto che nel 2014 la *European Banking Authority*¹⁸ ha individuato ben settanta distinti rischi del sistema delle criptovalute, distinguendoli a seconda che riguardino gli utenti, i professionisti, le imprese ovvero la stabilità del mercato. Nella medesima direzione, l’*European Cybercrime Center* ha evidenziato un rapporto di diretta proporzionalità tra l’aumento di capitalizzazione del mercato delle criptovalute e lo sviluppo del *cybercrime*, con speciale riferimento al *cyberlaundering* e al dilagare dei mercati neri nel *dark web*¹⁹. Per quel che qui interessa, il riciclaggio mediante valori virtuali dovrebbe condurre ad una riflessione criminologica certamente più ampia sull’asservimento della *distributed economy* ai propositi della criminalità organizzata²⁰.

¹⁵ Cfr. L. D’AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell’emanazione del D.Lgs. 90/2017*, cit., 5.

¹⁶ Le stesse caratteristiche delle *virtual currencies* che hanno portato all’affermazione ed alla rapida capitalizzazione del mercato valutario virtuale rischiano di condurlo verso l’autodistruzione. Infatti, pur non dubitando del fatto che le peculiarità del mercato delle criptovalute (anonimato, la rapidità delle transazioni, agevolazione delle operazioni transnazionali, abbattimento dei costi ed assenza di banche ed intermediari) le rendano meritevoli di essere paragonate, quanto a portata rivoluzionaria, all’affissione sulla porta della chiesa di Wittenberg nel 1517 delle famose novantacinque tesi di Martin Lutero non si possono trascurare le derive criminose del sistema riscontrabili nella prassi. Cfr. R. GUTTMAN, *The Bitcoin Bible gold edition. All you need to know about bitcoins and more*, Norderstedt, 2013, 368; G. GASPARRI, *Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*, cit., 431.

¹⁷ L’espressione è di N. PASSARELLI, *Bitcoin e antiriciclaggio*, cit., 1.

¹⁸ European Banking Authority (EBA), *Opinion on virtual currencies*, 4 luglio 2014, disponibile sul [sito dell’EBA](#), 21 ss.

¹⁹ «Internet Organised Crime Threat Assessment 2017», pubblicato dall’*Internet Cybercrime Centre* (EC3) costituito presso Europol, sul [sito di Europol](#), 47 ss.

²⁰ Secondo E. SIMONCINI, *Il cyberlaundering: la «nuova frontiera» del riciclaggio*, in *Riv. trim. dir. pen. econ.*, 4, 2015, 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». In effetti, la forza attrattiva esercitata dal mercato delle valute virtuali è particolarmente preoccupante laddove si consideri l’uso che ne potrebbe fare la criminalità

Le infrastrutture basate sulla tecnologia *blockchain*²¹, sebbene permettano a chiunque di visionare le transazioni effettuate dagli altri nodi della rete, verificandone l'importo e individuando gli indirizzi dell'ordinante e del beneficiario, non consentono, tuttavia, di risalire all'identità dei singoli *users*²². Sul pubblico registro le transazioni sono infatti catalogate in stringhe numeriche esadecimali corrispondenti agli indirizzi di invio/recezione della valuta (*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.

Una forte spinta criminogena è data poi dall'assenza di Autorità centrali nel sistema valutario virtuale. Com'è noto, le normative antiriciclaggio presuppongono la presenza di un sistema di intermediazione bancaria e finanziaria quale canale maestro per la segnalazione di operazioni sospette, a compendio degli obblighi di identificazione della clientela e di informativa sui controlli attribuiti all'Unità di Informazione Finanziaria²³. In un ecosistema *peer to peer*, l'assenza di intermediari sottrarrebbe alle autorità di vigilanza ed alla magistratura inquirente un fondamentale interlocutore istituzionale²⁴ per la prevenzione e il contrasto del riciclaggio. Tuttavia, nel mercato delle valute virtuali operano anche molti operatori professionali che, offrendo agli utenti servizi di portafoglio o di scambio (*wallet providers* ed *exchangers*), consentono di recuperare l'intermediazione perduta, figurando di fatto come intermediari nel compimento di operazioni in criptovaluta.

3. La disciplina preventiva del riciclaggio: dal D. Lgs. 90/2017 al D.Lgs. 125/2019.

Con l'emanazione del D. Lgs. 27 maggio 2017, n. 90 il Legislatore ha segnato un importante passo in avanti per l'adeguamento della disciplina antiriciclaggio ai nuovi

organizzata, soprattutto se di stampo mafioso. Quest'ultima, essendo impegnata nella costante ricerca di tecniche sempre più sofisticate per delinquere, sembra aver sviluppato una raffinata elasticità nell'impiegare a fini criminosi i nuovi ritrovati tecnologici.

²¹ E. FERRARI, *Bitcoin e criptovalute: la moneta virtuale tra fisco ed antiriciclaggio*, in *Il Fisco*, 2018, 9, 861 ss.

²² Esistono in verità delle euristiche di *blockchain intelligence* che consentono di aggregare indirizzi per poi confrontarli con i risultati delle indagini *open source*. Si tratta comunque di tecniche dal valore soltanto indiziario, che non sono in grado di superare da sé la barriera dell'anonimato.

²³ Il decreto legislativo 21 novembre 2007, n. 231 prevede che i soggetti destinatari della disciplina siano gravati da obblighi di adeguata verifica della clientela, di registrazione e conservazione della documentazione e di segnalazione delle operazioni sospette.

²⁴ Si veda l'informativa «Utilizzo anomalo di valute virtuali», sul [sito della UIF](#), con cui la Unità di Informazione Finanziaria (UIF), prima dell'emanazione del D. Lgs. 90/2017, esprimeva la propria preoccupazione per l'assenza di obblighi antiriciclaggio in capo agli operatori professionali nel settore delle valute virtuali, rilevando nello specifico che «i prestatori di attività funzionali all'utilizzo, allo scambio e alla conservazione di valute virtuali e alla loro conversione da/in valute aventi corso legale non sono, in quanto tali, destinatari della normativa antiriciclaggio e quindi non sono tenuti all'osservanza degli obblighi di adeguata verifica della clientela, registrazione dei dati e segnalazione delle operazioni sospette. Tale circostanza può rendere appetibile lo strumento virtuale per coloro che intendono porre in essere condotte criminali e non agevola le attività di prevenzione e contrasto».

rischi derivanti dalla dimensione virtuale dell'economia²⁵, giocando addirittura d'anticipo rispetto alle Istituzioni dell'Unione Europea²⁶.

Oltre ad aver introdotto una definizione di valuta virtuale²⁷, l'intervento riformatore ha toccato numerose disposizioni del Decreto Legislativo 21 novembre 2007, n. 231, includendo i prestatori di servizi relativi all'utilizzo di valuta virtuale²⁸ tra i destinatari degli obblighi antiriciclaggio²⁹. Tali soggetti vengono inseriti nel novero degli operatori non finanziari di cui all'art. 3, comma 5 del Decreto³⁰, destinatari degli obblighi di adeguata verifica della clientela, di registrazione e conservazione della documentazione, nonché di segnalazione delle operazioni sospette. In particolare, optando per l'assoggettamento alla normativa antiriciclaggio della sola attività di cambio di valuta virtuale in reale (e viceversa) svolta dagli *exchangers*, il Legislatore delegato mirava a delimitare l'espansione della normativa antiriciclaggio alle sole «aree di diretta interferenza delle valute virtuali con le monete correnti e l'economia reale»³¹.

Il Decreto delegato del 2017 è intervenuto anche su alcune disposizioni del D. Lgs. 13 agosto 2010, n. 141, imponendo agli *exchangers* l'iscrizione in una sezione speciale del registro dei cambiavalute tenuto dall'Organismo degli agenti e dei mediatori creditizi³².

²⁵ Il Decreto, intitolato «Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006», è stato adottato in base alla delega conferita con legge 12 agosto 2016, n. 170 (art. 15).

²⁶ L. D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D.Lgs. 90/2017*, cit., 6 ss.

²⁷ *Supra* § 2.

²⁸ L'art. 1, comma 2, del D. Lgs. 21 novembre 2007 n. 231 definisce prestatore di servizi relativi all'utilizzo di valuta virtuale "ogni persona fisica o giuridica che fornisce a terzi, a titolo professionale, servizi funzionali all'utilizzo, allo scambio, alla conservazione di valuta virtuale e alla loro conversione da ovvero in valute aventi corso legale" (lett. ff).

²⁹ M.R. DE RITIS, *Bitcoin: una moneta senza frontiere e senza padrone? Il recente intervento del legislatore italiano*, in *giustiziacivile.com*, 2018, 3, 9; M. MICCOLI, *"Bitcoin" fra bolla speculativa e controllo antiriciclaggio*, in *Notariato*, 2018, 2, 151 ss.

³⁰ «Rientrano nella categoria di altri operatori non finanziari: [...] 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» (lett. i). Per approfondimenti sulla natura finanziaria/valutaria delle valute virtuali si rinvia a G. LEMME – E. S. PELUSO, *Criptomoneta e distacco dalla moneta legale: il caso Bitcoin*, in *Riv. dir. banc.*, 2016, 11, 22 ss.

³¹ In questi termini, F. DI VIZIO, [Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti](#), in *Dir. pen. cont.*, 10/2018, 87. La dottrina ha utilizzato l'efficace metafora della cinta daziaria in riferimento alla necessità di regolare i rapporti dal la dimensione reale e quella virtuale dell'economia: "una "cinta daziaria" dotata di alcune "porte" per individuare chi e che cosa passa dal mondo reale a quello virtuale e viceversa. Solo alle transazioni *compliant* sarà garantito l'accesso al mondo reale, mentre le altre saranno destinate ad essere isolate in quello virtuale" (D. MAJORANA, *Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web*, in *Corr. trib.*, 2018, 8, 630).

³² L'art. 8 del decreto delegato, nel modificare l'art. 17-bis del D. Lgs. 141/2010, ha introdotto un nuovo comma 8-bis «le previsioni di cui al presente articolo si applicano, altresì, ai prestatori di servizi relativi all'utilizzo di valuta virtuale, come definiti nell'articolo 1, comma 2, lettera ff), del decreto legislativo 21 novembre 2007, n. 231, e successive modificazioni tenuti, in forza della presente disposizione, all'iscrizione

L'esempio italiano è stato seguito dal Legislatore eurounitario³³ che, con l'emanazione della Direttiva 2018/843/UE, è intervenuto sul quadro normativo includendo però tutti gli operatori professionali del mercato delle valute virtuali tra i destinatari della normativa antiriciclaggio³⁴.

Nello specifico, oltre a dettare una nozione di valuta virtuale³⁵ analoga a quella contenuta nell'art. 1, comma 2, lett. qq) del D. Lgs. 231/2007, la Direttiva delinea la categoria dei prestatori di servizi di portafoglio digitale (i cosiddetti *wallet providers*)³⁶, includendoli tra i soggetti destinatari degli obblighi antiriciclaggio, accanto agli *exchange providers*³⁷, imponendo, pertanto, ad entrambe le categorie di operatori di verificare

in una sezione speciale del registro di cui al comma 1». L'art. 8 disciplina l'esercizio professionale, nei confronti del pubblico, dell'attività di cambiavalute e le prerogative pubbliche di controllo sul relativo esercizio. «Il legislatore ha in sostanza equiparato le attività svolte dai professionisti del mercato delle criptovalute a quella dei cambiavalute, senza effettuare alcuna distinzione tra attività di trading (diretto e indiretto), *mining* e *mixing*. Ne consegue che tutti i prestatori di servizi relativi all'utilizzo di valuta virtuale saranno sottoposti alla medesima disciplina, senza distinzioni in base al tipo di attività in concreto svolta» (in questi termini, L. D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D.Lgs. 90/2017*, cit., 18).

³³ La disciplina antiriciclaggio ha conosciuto, a livello europeo, una progressiva evoluzione. Prima della Direttiva 2018/843/UE, la Direttiva 1991/308/CE poneva le basi per il contrasto al riciclaggio, entro ambiti oggettivi e soggettivi piuttosto ristretti. La seconda Direttiva 2001/97/CE, oltre ad estendere l'ambito applicativo della precedente, imponeva agli stati Membri di dotarsi di validi sistemi di identificazione e controllo del *paper trail*. La terza Direttiva 2005/60/UE espandeva l'ambito soggettivo dei destinatari degli obblighi previsti dalla precedente normativa. La quarta Direttiva (2015/849/UE) faceva proprie le raccomandazioni adottate nel 2012 dal FATF (*International standards on combating money laundering and the financing of terrorism and proliferation*), estendendo notevolmente l'ambito oggettivo di operatività della normativa antiriciclaggio. Sull'evoluzione della normativa europea, V. MITSILEGAS – N. VAVOULA, *The evolving EU anti-money laundering regime*, in *Maastricht Journal of European and Comparative Law*, 2016, 23, 2, 261 ss.

³⁴ Con la presentazione della proposta di Direttiva 2016/0208 (COD) la Commissione aveva posto in evidenza la improrogabile necessità di inserire i prestatori di servizi connessi alle valute virtuale tra i destinatari della quarta Direttiva antiriciclaggio. «È di fondamentale importanza ampliare il campo di applicazione della direttiva (UE) 2015/849 in modo da includere le piattaforme di cambio di valute virtuali e i prestatori di servizi di portafoglio digitale. È necessario che le autorità competenti possano monitorare l'uso delle valute virtuali. Ciò consentirebbe un approccio equilibrato e proporzionale, salvaguardando i progressi tecnici e l'elevato livello di trasparenza raggiunto in materia di finanziamenti alternativi e imprenditorialità sociale» (considerando n. 6 della Proposta, oggi considerando n. 8 della Direttiva).

³⁵ L'art. 3, punto 18, della Direttiva 2015/849/UE, definisce la valuta virtuale come «una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è necessariamente legata a una valuta legalmente istituita, non possiede lo status giuridico di valuta o moneta, ma è accettata da persone fisiche e giuridiche come mezzo di scambio e può essere trasferita, memorizzata e scambiata elettronicamente».

³⁶ L'art. 3, punto 19, della Direttiva 2015/849/UE, nel testo modificato dall'art. 1, par. 2, lett. d) della Direttiva 2018/843/UE, definisce il *wallet provider* come il «soggetto che fornisce servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali».

³⁷ Definiti come i soggetti «la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso forzoso». Cfr. Art. 2, paragrafo 1, punto 3, lett. g) della Direttiva 2015/849/UE, come modificato dall'art. 1, par. 1, lett. c) della Direttiva 2018/843/UE.

costantemente l'adeguatezza della clientela, nonché di effettuare, laddove ne ricorrano i presupposti, segnalazioni di operazioni sospette alle Autorità nazionali competenti³⁸.

Con il D. Lgs. 4 ottobre 2019, n. 125 il Legislatore italiano ha recepito la Direttiva 2018/843/UE³⁹, portando a compimento quel delicato percorso di adeguamento della normativa antiriciclaggio, e delle disposizioni di carattere general-preventivo ivi previste, alla dimensione virtuale della criminalità economica, di fatto intrapreso con l'emanazione del già citato D. Lgs. 90/2017.

In primo luogo, mentre il D. Lgs. 90/2017 ravvisava nella valuta virtuale solo un mezzo di scambio per l'acquisto di beni e servizi, il D. Lgs. 125/2019 ha riconosciuto espressamente alla valuta virtuale anche la fondamentale funzione di strumento di investimento⁴⁰, così ampliando l'ambito di applicabilità del D. Lgs. 231/2007.

In secondo luogo, se con il D. Lgs. 90/2017, ben prima dell'emanazione della Direttiva 2018/843/UE, solo gli *exchangers* e non anche i *wallet providers* erano stati introdotti tra i soggetti obbligati di cui al D. Lgs. 231/2007, l'art. 1, lettera u), del D. Lgs. 125/2019, recependo l'art. 1 della quinta Direttiva, ha colmato tale lacuna, assoggettando agli obblighi antiriciclaggio anche i prestatori di servizi di portafoglio digitale (art. 3, comma quinto, lett. i-bis), D. Lgs. 231 del 2007).

L'analisi degli interventi di riforma più recenti, con particolare riguardo all'introduzione di *exchangers* e *wallet providers* tra i soggetti sottoposti agli obblighi antiriciclaggio di cui al D. Lgs. 231/2007, ci restituisce un quadro normativo certamente più idoneo che in passato a confrontarsi con fenomeni di riciclaggio digitale, ma non in grado di neutralizzare pienamente il rischio del loro verificarsi, alla luce del fatto che, potendo gli utenti «effettuare operazioni anche senza ricorrere a tali prestatori, gran parte dell'ambiente delle valute virtuali rimarrà caratterizzato dall'anonimato» (considerando n. 9 della quinta Direttiva).

4. La disciplina sanzionatoria del riciclaggio.

Sebbene il riciclaggio⁴¹ sia stato introdotto nel Titolo XIII del Libro II del codice penale, dedicato ai delitti contro il patrimonio, la dottrina più autorevole ritiene che il

³⁸ G. P. ACCINNI, *Profili di rilevanza penale delle criptovalute (nella riforma della disciplina antiriciclaggio del 2017)*, cit., 20; L. STURZO, *Bitcoin e riciclaggio 2.0*, cit., 30.

³⁹ Cfr. S. D. FLAMMINEIS, [Distrazione e riciclaggio di fondi europei. I progetti riciclatori tra emergenza economica e tutela penale degli interessi finanziari dell'UE](#), in questa *Rivista*, 2021, 2, 45.

⁴⁰ Sulle funzioni del circolante virtuale, anche con riferimento alle ricadute penalistiche, si veda F. DI VIZIO, *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti*, cit., 117.

⁴¹ L'art. 648-bis c.p., introdotto dall'art. 3 del D.L. 21.03.1978, n. 59 e da ultimo modificato dall'art. 3, comma 1, L. 15.12.2014, n. 186, punisce con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000 chi «fuori dei casi di concorso nel reato [...] sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo; ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa [...]». Si prevede un aggravamento di pena quando il fatto è commesso nell'esercizio di un'attività professionale; una diminuzione se il denaro, i beni o le altre utilità provengono da delitto per il quale è stabilita la pena della reclusione inferiore nel massimo a cinque anni. In dottrina, *ex multis*, M. ZANCHETTI, *Art. 648-bis c. p.*, in A. Crespi – G. Forti – G. Zuccalà (a cura

reato abbia natura plurioffensiva, essendo lesivo anche (del buon andamento del sistema economico e) dell'amministrazione della giustizia⁴².

Mentre in origine soltanto alcuni delitti di particolare gravità, tassativamente previsti dalla norma incriminatrice, potevano assurgere a *predicate crimes* del riciclaggio, l'attuale formulazione codicistica delimita la categoria dei reati presupposto mediante un generico richiamo a delitti non colposi⁴³.

Il Legislatore ha strutturato la norma incriminatrice del riciclaggio come fattispecie a forma libera: all'indicazione delle condotte di sostituzione e trasferimento – esordio all'apparenza tassativo – fa, infatti, seguito la locuzione «ovvero compie [...] altre operazioni», che estende l'ambito operativo della disposizione a una molteplicità di condotte⁴⁴.

La struttura della fattispecie come reato di pericolo concreto permette di sanzionare qualsiasi condotta che abbia carattere dissimulatorio, quale che ne sia la forma o il contenuto, purché idonea a ostacolare l'identificazione dell'origine di «denaro, beni o altre utilità provenienti da delitto non colposo».

Il riciclaggio, pur consistendo in un unico processo, si snoda in tre diverse fasi: *placement-stage*, *layering-stage* e *integration-stage*.

Il *placement*, caratterizzato dal collocamento del denaro (dei beni o delle altre utilità) di provenienza delittuosa nel circuito dell'economia legale, rappresenta per l'agente lo stadio più pericoloso della filiera criminosa. Il più delle volte sarà infatti necessario trasferire il denaro sporco presso istituti o intermediari bancari o creditizi, operanti nel sistema finanziario legale. Tale operazione presuppone che il riciclatore possa contare su diversi contatti di fiducia che gli permettano non solo di agire per interposta persona, ma anche di eludere i controlli imposti dalla disciplina preventiva del riciclaggio⁴⁵.

di), *Commentario breve al codice penale*, Padova, 2008, 1939 ss.; P. MAGRI, *I delitti contro il patrimonio mediante frode*, vol. VII, Padova, 2007, 419 ss.; G. COLOMBO, *Il riciclaggio*, Milano, 1990; G. M. FLICK, *La repressione del riciclaggio ed il controllo della intermediazione finanziaria. Problemi attuali e prospettive*, in *Riv. it. dir. proc. pen.* 1990, 3, 1264 ss.; L. MAGISTRO, *Riciclaggio dei capitali illeciti, rilevanza del fenomeno e strategie di contrasti in materia fiscale*, Milano, 1991; A. MANGIONE, *Mercati finanziari e criminalità organizzata: spunti problematici sui recenti interventi normativi di contrasto al riciclaggio*, in *Riv. it. dir. proc. pen.*, 2000, 3, 1138 ss.; P. COSTANZO, *Il riciclaggio di disponibilità di provenienza illecita. La disciplina penale italiana alla luce delle regole internazionali e comunitarie*, in A. Di Amato (a cura di), *Trattato di diritto penale dell'impresa*, Padova, 2007, 339 ss.; V. MANES, *Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale*, in *Riv. trim. dir. pen. econ.*, 2004, 1-2, 39 ss.

⁴² Cfr. F. ANTOLISEI, *Manuale di diritto penale. Parte speciale*, Milano, 2016, 463; G. FIANDACA – E. MUSCO, *Diritto penale. Parte speciale. I delitti contro il patrimonio*, Bologna, 2015, 247.

⁴³ Non si richiede peraltro che vi sia una sentenza passata in giudicato sulla commissione del delitto presupposto, essendo una questione incidentale che il giudice sarà chiamato a decidere sulla base delle prospettazioni e delle prove presentate dalle parti.

⁴⁴ A. ZACCHIA, *La natura del reato di riciclaggio. Nota a Cass. sez. II pen. 13 luglio 2016, n. 29611*, in *Cass. pen.*, 2017, 7, 2824 ss.

⁴⁵ Tuttavia, il riciclatore non può dirsi mai del tutto al riparo dal rischio di emersione e conseguente segnalazione delle operazioni poste in essere: infatti, qualsiasi forma di piazzamento od investimento di ingenti somme di denaro, la cui origine sia avvolta da una certa opacità, è suscettibile di attirare l'attenzione dei soggetti preposti ai controlli antiriciclaggio ex D. Lgs. 231/2007, oggetto di trattazione in precedenza.

Il *layering* è il *core* del processo riciclatorio. Esso consiste in una serie di operazioni volte ad impedire o rendere grandemente difficoltosa la ricostruzione della traccia documentale (*paper trail*) che collega il capitale ripulito all'origine delittuosa dei beni che lo compongono⁴⁶.

Il processo culmina con l'*integration*, la fase in cui il denaro di provenienza illecita – ripulito attraverso una complessa serie di operazioni, previo trattenimento (di regola) da parte del riciclatore di una percentuale a titolo di compenso per l'attività prestata – torna nella disponibilità dell'autore del reato presupposto, in modo da poter essere reimpiegato nell'economia legale nei modi più disparati.

4.1. Il cyberlaundering.

Il *cyberlaundering* rappresenta la nuova frontiera del riciclaggio. Esso consiste nell'utilizzo delle nuove tecnologie, *rectius* delle tecnologie informatiche e telematiche, per la ripulitura dei proventi delittuosi. Le origini del *cyberlaundering* sono riconducibili alla progressiva dematerializzazione e informatizzazione dei flussi di denaro che ha consentito agli attori economici di compiere operazioni in valuta senza il previo passaggio per la dimensione tangibile dell'economia. La interconnessione globale tra sistemi informatici, da una parte, e la diffusione di piattaforme di *home banking*, dall'altra, rendono la rete un luogo ideale per il compimento di attività riciclatorie⁴⁷.

Alcuni autori distinguono due diverse forme di *cyberlaundering*: il riciclaggio digitale strumentale e il riciclaggio digitale integrale⁴⁸.

Il primo può essere definito come un *cyberlaundering* "parziale", in quanto il denaro oggetto della condotta di piazzamento non è *ex ante* dematerializzato. La fase di *placement* dei capitali illeciti presenta quindi difficoltà analoghe a quelle riscontrabili nel riciclaggio non digitale, richiedendo una forma di movimentazione fisica del contante al fine di trasformarlo in *e-cash*. Al contrario, nel riciclaggio totalmente digitale⁴⁹ le somme,

⁴⁶ In un'operazione di riciclaggio in valuta reale, le transazioni finanziarie compiute nella fase di *layering* si articolano in due fasi successive: dapprima, il riciclatore movimenta la liquidità in conti accesi in diversi Stati esteri; in seguito, investe tali fondi in strumenti finanziari ovvero in società aventi sede in paesi *off-shore*. Secondo E. SIMONCINI, *Il cyberlaundering: la «nuova frontiera» del riciclaggio*, cit., 901, il *layering* è lo stadio del riciclaggio maggiormente facilitato dal *web*.

⁴⁷ S. MULINARI, *Cyberlaundering*, Milano, 2003, 62.

⁴⁸ E. SIMONCINI, *Il cyberlaundering: la «nuova frontiera» del riciclaggio*, cit., 900.

⁴⁹ A differenza del riciclaggio digitale strumentale, quello integrale presuppone che il denaro sporco, oggetto della condotta riciclatoria, abbia forma digitale. Non è quindi necessario alcun contatto materiale tra riciclatore e contante. La differente natura del denaro oggetto del *cyberlaundering* integrale rispetto a quello suscettibile di lavaggio mediante il *cyberlaundering* strumentale comporta anche una distinzione strutturale tra i due processi criminosi. Secondo alcuni, mentre il riciclaggio digitale strumentale è costituito da tre fasi (*placement*, *layering*, *integration*) che si manifestano in modo ben distinto tra loro, il processo del *cyberlaundering* integrale, in quanto caratterizzato dal compimento di transazioni economico-finanziarie condotte integralmente *online*, inizia e finisce con il *placement-stage*, il quale assorbe le due fasi successive. R. GUTTMAN, *Cybercash: the coming Era of electronic money*, Londra, 2003, 28 ss.; S. MULINARI, *Cyberlaundering*, cit., 41.

già disponibili in forma dematerializzata, possono essere ripulite senza passare per la realtà materiale.

La ripulitura del denaro *online* presenta per i criminali numerosi vantaggi, tra cui: la possibilità di agire in qualsiasi momento e in modo anonimo, senza che sia necessario interfacciarsi *de visu* con persone fisiche; l'opportunità di assoldare direttamente sul *web* terzi fiduciari per il compimento delle operazioni intermedie (*money mules*); le difficoltà nell'individuazione del *locus commissi delicti* e dell'identità dei soggetti coinvolti nella filiera del *laundering*.

L'utilizzo delle valute virtuali massimizza i predetti vantaggi, rendendo assai più agevole la movimentazione dei capitali. A differenza dell'infrastruttura bancaria tradizionale, un ecosistema decentralizzato riduce drasticamente i tempi di transazione e permette uno scambio *peer to peer*, senza passare per soggetti terzi gravati dagli obblighi antiriciclaggio⁵⁰. Vieppiù, la criptomoneta consente di inviare e ricevere denaro con garanzie di anonimità come nessun altro sistema al mondo. Difatti, anche gli Stati storicamente più legati al segreto bancario ammettono oggi ampie deroghe e riserve in forza degli accordi internazionali di mutua collaborazione in materia penale e/o tributaria⁵¹.

Date queste premesse, veniamo ora ad esaminare le questioni più rilevanti in merito all'utilizzo delle valute virtuali a scopo di riciclaggio.

Una prima questione riguarda la riconducibilità del *cyberlaundering* alla fattispecie di cui all'art. 648-*bis* c.p., con particolare riguardo alle modalità esecutive della condotta e all'oggetto materiale del reato. Poiché il Legislatore ha costruito il riciclaggio come un reato a forma libera, la rilevanza penale dell'operazione posta in essere dipende dalle concrete modalità del fatto, *melius* dalla sua idoneità a ostacolare l'identificazione della provenienza illecita del denaro, dei beni o delle altre utilità. Pertanto, non sovviene alcun dubbio sulla configurabilità del delitto *de quo* in caso di transazioni in valori virtuali che, per loro natura, rendono estremamente difficoltosa la ricostruzione del *digital trail*⁵².

Risulta, invece, più complessa la corretta individuazione dell'oggetto materiale del riciclaggio, non essendo affatto chiara la natura giuridica da attribuire alle valute virtuali. In base all'opinione attualmente prevalente, la criptomoneta non potrebbe essere considerata una valuta in senso proprio poiché, diversamente dalle valute *fiat*,

⁵⁰ A parere di chi scrive, la criptomoneta è la valuta della rete per eccellenza, condividendo con essa la *ratio* e alcune caratteristiche di fondo. Infatti, come la rete Internet è il risultato del movimento di democratizzazione informativa, le valute virtuali sono il prodotto dell'esigenza di democratizzazione finanziaria.

⁵¹ Del resto, anche se il lavaggio del denaro si realizzasse in paesi che garantiscono appieno il segreto bancario o in Stati che non prevedono presidi antiriciclaggio, i criminali dovrebbero comunque trovare un espediente per rientrare in possesso dei capitali ripuliti senza compiere operazioni sospette. L'utilizzo del circolante virtuale risolve a monte il problema, poiché, quale che sia lo Stato di residenza del destinatario finale delle somme, non esistono segnali "spia" della illiceità della transazione.

⁵² Cfr. L. D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D.Lgs. 90/2017*, cit., 4.

quelle virtuali non hanno corso forzoso né corso legale⁵³, né sarebbero in grado di assicurare *in toto* le funzioni di riserva di valore, unità di conto e mezzo di scambio⁵⁴.

Pertanto, senza entrare nel merito della questione, che esulerebbe dall'economia del presente lavoro, possiamo limitarci ad affermare che, nella prospettiva penalistica, l'assimilazione della valuta virtuale al denaro contravverrebbe al divieto di analogia *in malam partem*.

Esclusa la riconducibilità della moneta virtuale al denaro, si ritiene che essa non possa neppure essere inquadrata nella categoria dei beni. La più consolidata corrente di pensiero⁵⁵ – solo di recente messa in discussione da una pronuncia di legittimità⁵⁶ – abbraccia un'interpretazione restrittiva, secondo la quale sono beni le sole *res* tangibili, suscettibili di essere oggetto di diritti.

Le valute virtuali possono, invece, essere pacificamente ricondotte alla categoria residuale delle altre utilità⁵⁷, trattandosi di una formula tanto ampia da ricomprendere qualsiasi entità economicamente apprezzabile.

Il circolante virtuale viene in considerazione sia nel riciclaggio digitale strumentale sia in quello digitale integrale.

Nel caso in cui il provento del reato non sia disponibile in forma dematerializzata⁵⁸, la fase di *placement* avrà ad oggetto un'operazione di cambio del circolante per moneta elettronica o direttamente per criptomoneta. Nella prima ipotesi sarà sufficiente depositare il denaro su conti correnti o carte prepagate ed utilizzare questi ultimi per l'acquisto di valuta virtuale; più complessa è la seconda ipotesi, possibile unicamente avvalendosi di appositi ATM che accettino rimesse in contante e forniscano in cambio le chiavi crittografiche del *tantundem* in Bitcoin.

⁵³ G. GASPARRI, *Timidi tentativi giuridici di messa a fuoco del Bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*, cit., 417. In tema, G. LEMME – E. S. PELUSO, *Criptomoneta e distacco dalla moneta legale: il caso Bitcoin*, cit., 24; N. VARDI, *“Criptovalute” e dintorni: alcune considerazioni sulla natura giuridica dei Bitcoin*, in *Dir. inf.*, 2015, 1, 450.

⁵⁴ Sul punto, D. YERMAK, *Is Bitcoin a real currency? An economic appraisal*, NBER Working Paper No. 19747, 2013, 2 ss.

⁵⁵ In questo senso, per tutti, G. FIANDACA – E. MUSCO, *Diritto penale. Parte speciale*, cit., 23 secondo cui “è definibile cosa, nel senso del diritto penale, ogni oggetto corporale o fisico: in altri termini, ogni entità fisica del mondo esterno che presenti i caratteri della definitezza spaziale e della esistenza autonoma”. Dal punto di vista ontologico le valute virtuali non sono altri che dati informatici, che sarebbe impossibile ricondurre al concetto penalistico di cosa o di bene, senza violare il principio di tassatività e il divieto di analogia.

⁵⁶ Secondo Cass. Pen., Sez. II, 13 aprile 2020, n. 11959, inerente alla sottrazione di dati informatici salvati su di un *personal computer* aziendale del quale il soggetto attivo aveva la disponibilità per ragioni di lavoro, i dati informatici dovrebbero essere considerati beni mobili.

⁵⁷ Cfr. S. CAPACCIOLI, *Criptovalute e bitcoin: un'analisi giuridica*, Milano, 2015, 252; L. STURZO, *Bitcoin e riciclaggio 2.0*, cit., 24.

⁵⁸ Non sia cioè moneta elettronica, secondo la definizione fornita dall'art. 1, comma 1, lett. h-ter) TUB «il valore monetario memorizzato elettronicamente, ivi inclusa la memorizzazione magnetica, rappresentato da un credito nei confronti dell'emittente che sia emesso per effettuare operazioni di pagamento come definite all'articolo 1, comma 1, lettera c), del decreto legislativo 27 gennaio 2010, n. 11, e che sia accettato da persone fisiche e giuridiche diverse dall'emittente».

Qualora, invece, la provvista sia costituita da moneta elettronica, l'interessato potrà convertirla in valuta virtuale tramite una piattaforma di scambio, effettuando un semplice bonifico bancario con indicazione delle coordinate dell'*account* del beneficiario.

Tanto nel primo quanto nel secondo caso, la prima fase del *cyberlaundering* (*placement stage*) si rivela particolarmente delicata, poiché i potenziali riciclatori debbono entrare in contatto con gli intermediari professionisti al fine di ottenere la conversione del provento delittuoso in circolante virtuale. Essendo questa la fase nella quale più facilmente si avvertono i segnali di allarme di possibili operazioni sospette, la scelta del Legislatore di imporre presidi antiriciclaggio in capo agli *exchange providers* appare sicuramente razionale.

La fase di *placement* non è però necessaria ogniqualvolta il provento del reato sia già disponibile in valuta virtuale, come nel caso in cui oggetto della ripulitura sia il prezzo pagato da terzi per l'acquisto di beni intrinsecamente illeciti sul *dark web* oppure il corrispettivo versato per liberare un sistema informatico da un *ransomware*. Si potrà configurare in questi casi un riciclaggio (totalmente) virtuale, caratterizzato dalla mancanza del *placement stage*. L'assenza di intermediari nella conversione pone un serio ostacolo all'emersione dei capitali illeciti e all'individuazione dei responsabili, rendendo questa forma di riciclaggio la più difficile da contrastare.

La fase di (*cyber-*) *layering* consiste nella movimentazione di valuta virtuale tra più indirizzi appartenenti allo stesso soggetto o a prestanome virtuali (*money mules*). Le transazioni in criptomoneta sono annotate sulla *blockchain* e associate all'indirizzo di portafoglio degli utenti. Pertanto, le movimentazioni in valuta virtuale, anche se anonime, sono in linea di principio perfettamente tracciabili.

Le operazioni che compongono la fase di *layering* possono inoltre contare sull'opera dei *mixers*, un tempo aventi un ruolo chiave nell'ecosistema delle valute virtuali e oggi soggetti, invece, alla concorrenza delle altre modalità di realizzazione della fase di *layering*⁵⁹. L'attività svolta da questi soggetti ha lo scopo di sofisticare il *digital trail*, in modo da rendere estremamente difficoltosa la ricostruzione delle tracce dei trasferimenti di valuta virtuale⁶⁰. Il funzionamento di un servizio di *mixing*, o *mixnet*, può essere descritto nei termini seguenti: un utente deposita un determinato ammontare di criptovaluta su uno o più conti di ingresso, per poi ritirare il denaro virtuale su conti di uscita preesistenti o appositamente creati.

Compito del *mixer* è evitare che l'ammontare di denaro depositato possa essere direttamente associato all'ammontare ritirato alla fine. Per l'assolvimento di tale compito, il *mixer* trattiene – quale corrispettivo della propria attività – una percentuale sul valore della transazione⁶¹.

⁵⁹ Tra i più noti servizi di *mixing* rinvenibili in rete meritano di essere menzionati *Bitlaunder*, *Easycoin*, *Sharedcoin* e *Bitcoin Laundry*.

⁶⁰ Per non lasciare tracce di attività "sospette", ed evitare quindi un passaggio di "denaro" diretto tra due portafogli digitali, si dovrebbe spezzare la concatenazione di trascrizioni sul "libro mastro" pubblico.

⁶¹ In argomento, L. D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D.Lgs. 90/2017*, cit., 11, secondo cui «il mixing è avvolto da un'aura tale di sospetto sull'impiego a fini criminosi (in particolare al fine di ostacolare l'identificazione della provenienza dei flussi di valuta virtuale), da poterla considerare in sé

I prestatori di servizi di *mixing* utilizzano generalmente quattro distinti conti: di ingresso, *bounce*, *pool*, di uscita⁶². Dapprima, l'utente deposita il denaro di provenienza delittuosa su conti di entrata, dove viene prelevato dal *mixer*. Quest'ultimo può frammentare il denaro di provenienza illecita e indirizzarlo verso diversi conti di rimbalzo (di qui la definizione *bounce*) ovvero destinare il denaro di più utenti a un unico conto (detto *pool*). Infine, il denaro, oggetto di molteplici transazioni intermedie, confluisce in un conto di uscita controllato dal fruitore del servizio⁶³.

Il ciclo si chiude con il rientro dei capitali ripuliti nel circuito dell'economia legale, nelle stesse forme tipiche del riciclaggio analogico ovvero senza abbandonare la dimensione dell'economia virtuale.

Il beneficiario delle transazioni potrà nuovamente convertire la valuta virtuale in moneta *fiat* tramite una piattaforma di scambio, inviare il denaro verso conti accesi in Paesi *off-shore* che garantiscano la massima segretezza bancaria o adottare procedure di *remote banking* al fine di trasferire su nuovi conti il denaro sporco; infine, il denaro sporco potrebbe essere impiegato anche per l'acquisto o la ricarica di *smart cards* prepagate⁶⁴.

Preme, infine, rilevare che alcune tecniche riciclatorie si distinguono per una peculiare artificiosità. Tra esse rientra il cosiddetto *loan back*. Trattasi di una particolare operazione con cui il riciclatore, con il pretesto di voler avviare un'attività produttiva o commerciale ovvero per rilevare un'azienda, contrae un prestito offrendo in garanzia i fondi virtuali di provenienza delittuosa. Dopo aver ottenuto il finanziamento, il riciclatore non adempie, tuttavia, le proprie obbligazioni nei confronti della banca, la quale procede, dunque, ad escutere la garanzia. In tal modo è lo stesso istituto creditizio a perfezionare, inconsapevolmente, la ripulitura del denaro di provenienza illecita⁶⁵.

Infine, poiché la maggior parte delle valute virtuali sono accettate come mezzo di pagamento da un crescente numero di operatori economici, il rientro nel circuito dell'economia lecita potrà realizzarsi anche senza la previa conversione in moneta avente corso legale, semplicemente acquistando beni o servizi.

Sarebbe, dunque, opportuno procedere all'imposizione e all'attivazione dei presidi antiriciclaggio in capo a tutti quei professionisti che, pur non svolgendo attività di cambiavalute virtuali, accettino a qualsiasi titolo pagamenti in valuta virtuale. È difatti lecito attendersi che, nel prossimo futuro, all'aumento del numero di utenti disposti ad

intrinsecamente illecita».

⁶² Così, O. CALZONE, *Servizi di mixing e Monero*, in *Gnosis*, 28 luglio 2017, 5.

⁶³ Tra le valute più utilizzate per il *mixing* si segnala *Monero*, che, garantendo ai suoi *users* un solido anonimato e la non tracciabilità delle operazioni, rappresenta l'infrastruttura migliore per l'erogazione di questo tipo di servizi.

⁶⁴ L'utilizzo di *smart cards* risulta particolarmente insidioso, in quanto il denaro può esservi immesso istantaneamente in molteplici modi: tramite operazioni telefoniche, da *e-wallets*, presso ATM, dall'*hard drive* di un computer ovvero mediante trasferimenti di denaro via *home banking*. Di recente, D.A. LESLIE, *Legal Principles for Combatting Cyberlaundering, Law, Governance and Technology Series*, cit., 71.

⁶⁵ E. SIMONCINI, *Il cyberlaundering: la «nuova frontiera» del riciclaggio*, cit., 903. Deve comunque rilevarsi come nel nostro ordinamento tale tecnica non potrebbe funzionare se non quando ricorrano ipotesi di patto marciano o di previo passaggio per la vendita coatta dei valori virtuali. L'acquisizione diretta della garanzia *sic et simpliciter* contravviene, infatti, al generale divieto di patto commissorio di cui all'art. 2744 c.c.

accettare pagamenti in contante virtuale corrisponderà una riduzione della quantità di criptomoneta da riconvertire in moneta reale. Ciò farebbe cadere nel vuoto la disciplina preventiva disegnata dal Legislatore, rivolta ad oggi ai soli *exchangers* e *wallet providers*.

5. L'autoriciclaggio.

L'art. 3 della L. 15 dicembre 2014 n. 186 ha introdotto nel codice penale, all'art. 648-ter.1 c.p., il delitto di autoriciclaggio⁶⁶, facendo venir meno il c.d. "privilegio di autoriciclaggio"⁶⁷. Prima della riforma, i fatti di riciclaggio realizzati dallo stesso autore del reato presupposto integravano un mero *post factum* non punibile, figurando come uno sviluppo logicamente naturale e prevedibile della prima azione delittuosa, se non addirittura come una peculiare manifestazione di esercizio del diritto di difesa da parte del reo⁶⁸. La modifica legislativa ha inoltre inciso sulla disciplina di cui al D.Lgs. 231/2001, introducendo il delitto di autoriciclaggio nel *numerus clausus* dei reati presupposto della responsabilità degli enti⁶⁹.

L'autoriciclaggio consiste nell'immissione nel circuito dell'economia legale da parte dell'autore (o del concorrente) di un delitto non colposo dei proventi derivanti dalla propria precedente condotta criminosa, in modo da ostacolarne concretamente la tracciabilità⁷⁰.

Oltre al patrimonio e all'amministrazione della giustizia, la norma è posta a presidio della libera concorrenza nel mercato, la quale rischia di essere falsata

⁶⁶ «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 non colposo, 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 [...]».

⁶⁷ P. CORSO, *Il declino di un "privilegio": l'autoriciclaggio (anche da reato tributario) ha rilievo penale autonomo*, in *Corr. trib.*, 2015, 3, 159 ss.; S. SEMINARA, *Spunti interpretativi sul delitto di autoriciclaggio*, in *Dir. pen. proc.*, 2016, 12, 1631 ss.

⁶⁸ *Ex multis*, A. R. CASTALDO – M. NADDEO, *Il denaro sporco. Prevenzione e repressione nella lotta al riciclaggio*, Padova, 2010, 92 ss.; S. SEMINARA, *I soggetti attivi del reato di riciclaggio tra diritto vigente e prospettive di riforma*, in *Dir. pen. proc.*, 2005, 2, 236; V. MANES, *Il riciclaggio dei proventi illeciti: teoria e prassi dell'intervento penale*, in *Riv. trim. dir. pen. econ.*, 2004, 1-2, 75 ss.; R. BRICCHETTI, *Riciclaggio e autoriciclaggio*, in *Riv. it. dir. proc. pen.*, 2014, 2, 684 ss.

⁶⁹ La Legge n. 186/2014 ha modificato l'art. 25-octies del D.Lgs. 231/2001. Il nuovo testo recita: «In relazione ai reati di cui agli articoli 648, 648-bis, 648-ter e 648-ter.1 del codice penale, si applica all'ente la sanzione pecuniaria da 200 a 800 quote. Nel caso in cui il denaro, i beni o le altre utilità provengano da delitto per il quale è stabilita la pena della reclusione superiore nel massimo a cinque anni si applica la sanzione pecuniaria da 400 a 1000 quote». In argomento, G. GAREGNANI – G. GALLI – L. TROYER, *Brevi note sull'introduzione del nuovo delitto di autoriciclaggio nel novero dei reati presupposto della responsabilità amministrativa da reato di cui al D. Lgs. 231/01*, in *Riv. dottori comm.*, 2015, 3, 467 ss.; G. STILE, *Profili problematici della responsabilità dell'ente da riciclaggio*, in *Resp. amm. soc. enti*, 2009, 3, 105 ss.; A. ROSSI, *Autoriciclaggio e responsabilità degli enti da reato*, in *Nuovo notiziario giuridico*, 2017, 2, 492 ss.

⁷⁰ E. BASILE, *L'autoriciclaggio nel sistema penalistico di contrasto al "money laundering" e il nodo gordiano del concorso di persone*, in *Cass. pen.*, 2017, 3, 1277 ss.

dall'impiego di capitali di provenienza illecita da parte di alcuni attori economici. Sebbene la norma esordisca con il termine "chiunque", l'autoriciclaggio è un reato proprio, in quanto il soggetto attivo deve essere individuato *per relationem* rispetto alla previa commissione di un delitto presupposto non colposo⁷¹.

Per quel che riguarda le condotte esecutive, la *littera legis* sembra essere il risultato della fusione della fattispecie di riciclaggio di cui all'art. 648-bis c.p. con quella di impiego di denaro, beni o utilità di provenienza illecita, *ex art.* 648-ter c.p.⁷²

A caratterizzare la condotta autoriciclatoria, secondo l'attenta analisi effettuata in dottrina⁷³, sono le tre fasi già individuate in sede di trattazione del riciclaggio: *placement, layering e integration*. L'ultima fase della condotta autoriciclatoria deve, però, assumere la forma di destinazione del provento illecito ad «attività economiche, finanziarie, imprenditoriali o speculative»⁷⁴ e deve essere non astrattamente, bensì concretamente idonea ad ostacolare l'identificazione della provenienza delittuosa dell'oggetto materiale.

Prima di entrare nel merito della questione relativa all'utilizzo delle valute virtuali come strumento di *self-laundering*, è opportuno premettere brevi cenni su uno dei profili più problematici della materia: il concorso di persone nel reato⁷⁵.

Subito dopo l'entrata in vigore della riforma del 2014, la dottrina si è interrogata sulla possibilità di ravvisare nel fatto dell'*extraneus* che fornisca un contributo concorsuale alla condotta autoriciclatoria dell'autore del delitto presupposto un concorso in autoriciclaggio ovvero la più grave fattispecie di riciclaggio.

La questione è stata infine oggetto di una sentenza⁷⁶ della Seconda sezione Penale della Corte di Cassazione nella quale i giudici di legittimità, chiamati a definire l'ambito applicativo delle fattispecie di riciclaggio e autoriciclaggio, muovendo dalla *ratio* sottesa

⁷¹ A. GULLO, [Realizzazione plurisoggettiva dell'autoriciclaggio: la Cassazione opta per la differenziazione dei titoli di reato](#), in *Dir. pen. cont.*, 6/2018, 262 ss.; V. CITRARO, *Il delitto di autoriciclaggio, art. 648-ter. 1 c.p.*, in *De Iure Criminalibus*, 8 marzo 2016.

⁷² M. LANZI, *La difficile individuazione di limiti applicativi all'autoriciclaggio: il bene giuridico, il tempo e l'oggetto*, in *L'Indice penale*, 2017, 2, 506 ss.

⁷³ A. GULLO, [Autoriciclaggio. Voce per "Il libro dell'anno del diritto Treccani 2016"](#), in *Dir. pen. cont.*, 21 dicembre 2015; A. D'AVIRRO – M. GIGLIOLI, *Autoriciclaggio e reati tributari*, in *Dir. pen. proc.*, 2015, 2, 135 ss.; S. CAVALLINI – L. TROYER, [Apocalittici o integrati? Il nuovo reato di autoriciclaggio: ragionevoli sentieri ermeneutici all'ombra del vicino ingombrante](#), in *Dir. pen. cont. – Riv. trim.*, 1/2015, 95 ss.; L. VITALE, *Autoriciclaggio e reati tributari*, in *Bollettino tributario d'informazioni*, 2018, 1, 13 ss.

⁷⁴ Le attività economiche e imprenditoriali, come si ricava dagli artt. 2082 c.c. (Imprenditore), 2135 c.c. (Imprenditore agricolo), 2195 c.c. (Imprenditori soggetti a registrazione), ricomprendono non soltanto le attività produttive in senso stretto, dirette alla produzione di beni o servizi, ma anche quelle di scambio e distribuzione dei beni nel mercato del consumo, nonché ogni altra attività che possa rientrare in una di quelle previste dalle summenzionate norme civilistiche. Cfr. A. GULLO, *Autoriciclaggio*, cit.; Id, *Il delitto di autoriciclaggio al banco di prova della prassi: i primi (rassicuranti) chiarimenti della Cassazione. Nota a Cass. sez. II pen. 28 luglio 2016, n. 33074*, in *Dir. pen. proc.*, 2017, 4, 483 ss. Di recente anche A. M. DELL'OSSO, *Riciclaggio di proventi illeciti e sistema penale*, Torino, 2017, 180.

⁷⁵ Sul tema, *ex multis*, D. BRUNELLI, *Autoriciclaggio: profili del concorso di persone*, in E. Mezzetti – D. Piva (a cura di), *Punire l'autoriciclaggio: come, quando e perché*, Torino, 2016, 19 ss.

⁷⁶ Cass. Pen., Sez. II, 17 gennaio 2018, n. 17235 con nota di A. GULLO, [Realizzazione plurisoggettiva dell'autoriciclaggio: la Cassazione opta per la differenziazione dei titoli di reato](#), cit.

all'introduzione dell'art. 648-ter. 1 c.p. nell'ordinamento giuridico italiano e richiamando alcune preesistenti ipotesi codicistiche di diversificazione del titolo di reato rispetto a condotte concorrenti (tra cui, ad esempio, il delitto di evasione e quello di procurata evasione, di cui agli artt. 385 e 386 c.p.), hanno escluso che nel fatto dell'*extraneus* che ponga in essere la condotta tipica di autoriciclaggio ovvero contribuisca alla realizzazione della stessa da parte dell'*intraneus* sia ravvisabile un concorso nel reato di autoriciclaggio. In tale ipotesi, dunque, mentre l'*intraneus* risponderà di autoriciclaggio, la condotta dell'*extraneus* non potrà che essere ricondotta alla più grave fattispecie riciclatoria prevista e punita dall'art. 648-bis c.p.

5.1. Il cyber self-laundering.

L'introduzione dell'art. 648-ter.1 nel codice penale stigmatizza anche quelle condotte di ripulitura del denaro commesse nel *cyberspazio*. Poiché il riciclaggio digitale, specie nella sua forma più evoluta – quella integralmente digitale – presenta dei vantaggi notevoli rispetto al riciclaggio analogico, è ragionevole ritenere che le reti telematiche costituiscano oggi il luogo preferito dai criminali per il lavaggio del denaro sporco⁷⁷.

A tal fine, non occorre che l'agente disponga di conoscenze tecnico-informatiche particolarmente raffinate né che sia in contatto con una rete criminale che si occupi dei passaggi intermedi del denaro. Infatti, nello scenario digitale, l'autore del delitto presupposto può agevolmente agire in totale autonomia, accendendo conti presso istituti di moneta elettronica, scommettendo *on-line*, convertendo il denaro in valuta virtuale, creando *fake accounts* su diverse piattaforme di scambio, generando plurimi indirizzi di transazione per rimbalzare il denaro e così via.

L'attività di terzi soggetti diviene così un fattore occasionale, certamente non necessario per la dispersione dei proventi illeciti nei meandri dello spazio virtuale. Prima dell'intervento del legislatore, la clausola di riserva contenuta in apertura delle disposizioni degli artt. 648-bis e 648-ter c.p. escludeva la rilevanza penale della condotta di chi, dopo aver commesso un delitto non colposo, avesse adottato in prima persona espedienti dissimulativi – anche di tipo informatico o telematico – per far perdere le tracce dei proventi del reato. La recente scelta legislativa di sanzionare tali condotte è senz'altro opportuna, considerando che lo spazio virtuale ha tutte le caratteristiche per diventare il principale terreno di applicazione del delitto di autoriciclaggio.

Occorre precisare che nella prassi, nel caso in cui oggetto materiale della condotta sia il denaro (*self-cyberlaundering* strumentale), l'autore del reato presupposto potrebbe

⁷⁷ L'enorme cifra nera che avvolge il fenomeno del riciclaggio non permette però di conoscere con certezza quale sia la reale dimensione della *underground economy*. In Italia non risulta edita alcuna statistica precisa; gli unici studi disponibili sono basati su approssimazioni e mere congetture secondo cui i capitali illeciti oggetto di riciclaggio raggiungerebbero addirittura il 12% del PIL. Cfr. A. M. TARANTOLA, *Dimensioni delle attività criminali, costi per l'economia, effetti della crisi economica*, audizione del 6 giugno 2012, 5, disponibile sul sito del Senato.

scambiare moneta *fiat* sul mercato virtuale ricevendo in cambio criptovalute⁷⁸. Qualora, invece, il provento criminoso sia già disponibile in *token* di valuta virtuale, le condotte riciclatorie sarebbero ancor più agevolate, non essendovi la necessità di passare per la conversione del denaro e, quindi, per i presidi antiriciclaggio posti in capo ai fornitori dei servizi di *exchange*.

Ebbene, posto che l'autoriciclaggio è destinato a divenire la regola e il riciclaggio l'eccezione, occorre chiedersi se le operazioni poste in essere tramite valute virtuali possano essere ricondotte alla definizione normativa di cui all'art. 648-ter.1 c.p., con particolare riguardo alla destinazione dei proventi delittuosi («attività economiche, finanziarie, imprenditoriali o speculative»).

Grazie all'elasticità della formulazione della fattispecie di cui all'art. 648-ter.1 c.p., è ben possibile ricondurre ad essa, *sub specie* di impiego di proventi delittuosi in attività economiche e finanziarie, le operazioni di pagamento, trasferimento o scambio che abbiano ad oggetto valute virtuali⁷⁹.

A conclusioni solo parzialmente dissimili pare doversi pervenire qualora l'autore di un delitto non colposo utilizzi le valute reali che ne siano il provento per acquistare *virtual currencies*. Anche tale condotta, infatti, sembra integrare il delitto di autoriciclaggio, ma a venire in rilievo in tal caso, quale destinazione tipica ex art. 648-ter.1 c.p., non sembrerebbe essere un'attività economica o finanziaria, bensì speculativa.

Tale assunto si basa su due diverse considerazioni.

In primo luogo, la recente modifica dell'art. 1, comma 2, lett. qq) del D. Lgs. 231/2007 da parte del D. Lgs. 125/2019 ha formalizzato la duplice natura delle valute virtuali, riconducendole non solo a mezzi di scambio per l'acquisto di beni o servizi, ma anche a strumenti di investimento.

In secondo luogo, una recente pronuncia della Corte di cassazione (inerente ad un caso di impiego, da parte dell'autore del *predicate crime*, del denaro di provenienza delittuosa nel settore dei giochi e delle scommesse) ha riconosciuto alla nozione di "attività speculativa" un'ampiezza tale da ricomprendere tutte quelle attività caratterizzate dalla "assunzione di posizioni in base ad aspettative sull'andamento futuro di una o più variabili aleatorie"⁸⁰.

Pertanto, premesso che l'acquisto di valute virtuali costituisce (anche) una forma di investimento e che esse sono caratterizzate da rilevante volatilità, ci sembra che l'utilizzo di *fiat money* di origine criminosa per l'ottenimento di valute virtuali sia astrattamente riconducibile a un'ipotesi di impiego di proventi delittuosi in attività speculative ex art. 648-ter.1 c.p.

Il terreno risulta comunque scivoloso, non potendosi negare il rischio di andare oltre il dettato normativo, cadendo in un'applicazione analogica *in malam partem* della norma⁸¹.

⁷⁸ F. DI VIZIO, *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti*, cit., 39.

⁷⁹ L. PICOTTI, *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, cit., 608-609.

⁸⁰ Cass. Pen., Sez. II, 7 marzo 2019, n. 13795.

⁸¹ Sulla necessità di un'interpretazione restrittiva del concetto di "attività speculativa" si veda Cass. Pen., Sez. II, 13 dicembre 2018, n. 9751.

La questione della tipicità degli impieghi è piuttosto spinosa. Si potrebbe, ad esempio, sostenere che la norma di cui all'art. 648-ter. 1 c.p. sia deputata a "schermare" il solo sistema finanziario reale da infiltrazioni criminose e che, pertanto, le condotte autoriciclatorie che rimangano confinate nella realtà virtuale non siano ricomprese nell'ambito operativo della disposizione. Tuttavia, tale interpretazione della norma si porrebbe in contrasto con la *voluntas legis* sottesa alla riforma del 2014, riconducibile al consolidamento di una generale tutela, oltre che del patrimonio, anche della concorrenza nel mercato (incluso quello dei valori mobiliari) e dell'amministrazione della giustizia.

5.2. La responsabilità per riciclaggio di exchangers, wallet providers, mixers e miners.

Appurato che le condotte dell'autore del *predicate crime* consistenti nell'acquisto, nella conversione e nel trasferimento di criptovaluta sono agevolmente riconducibili alla fattispecie tipica di cui all'art. 648-ter.1 c.p., occorre chiedersi di quale reato possano essere chiamati a rispondere quanti si trovino a concorrere con l'*intraneus*, agevolando le operazioni di conversione e conservazione (*exchangers* e *wallet providers*), convalidando le transazioni (*miners*) o facendo perdere le tracce delle stesse (*mixers*).

A tal fine, è necessario soffermarsi dapprima sull'attività svolta da tali soggetti.

Mentre i *wallet providers* consentono agli utenti di custodire in rete le chiavi crittografiche necessarie per effettuare transazioni in valute virtuali, gli *exchange providers*, operando come intermediari finanziari *sui generis*, forniscono agli *users* servizi di cambio tra valute virtuali e valute reali (e viceversa)⁸². La maggior parte delle piattaforme di *exchange* offre un servizio meramente prodromico al *trading* valutario vero e proprio (*trading indiretto*), limitandosi a mettere a disposizione degli utenti valute virtuali⁸³.

I *miners*, costituendo di fatto una rete di *computer* privati con elevata potenza di calcolo (*mining rigs*), contribuiscono, mediante la risoluzione di complessi calcoli matematici finalizzati alla convalida di diverse transazioni, alla creazione e all'emissione di nuovo circolante virtuale.

I prestatori di servizi di *mixing*, infine, consentono agli utenti del sistema *blockchain* che effettuino transazioni di nascondere le tracce, spezzando l'ordinato concatenarsi delle operazioni⁸⁴.

Sulla base dell'orientamento giurisprudenziale di legittimità precedentemente richiamato⁸⁵, data l'indubbia incidenza causale dell'attività prestata da *miners*, *mixers*, *exchangers* e *wallet providers* nella perpetrazione del reato di autoriciclaggio da parte

⁸² F. DI VIZIO, *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti*, cit., 37; L. D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D.Lgs. 90/2017*, cit., 10.

⁸³ Al fine di poter soddisfare la massiccia domanda di valute virtuali, gli *exchangers* operano sul mercato alla costante ricerca di vantaggiose occasioni di acquisto di valuta virtuale ovvero autoproducono tale valuta mediante l'attività di *mining*.

⁸⁴ F. DI VIZIO, *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti*, cit., 38.

⁸⁵ Cass. Pen., Sez. II, 17 gennaio 2018, n. 17235.

dell'autore del *predicate crime*, questi potrebbero essere chiamati a rispondere del delitto di riciclaggio, purché sia integrato l'elemento soggettivo richiesto dalla norma incriminatrice.

A tal riguardo, in dottrina è stata avanzata la tesi della sistematica configurabilità in capo a tali soggetti del dolo, quantomeno nella forma eventuale: l'opacità e l'anonimato del mercato delle valute virtuali sarebbero elementi sintomatici di una presunzione dell'origine delittuosa dei fondi e dell'accettazione, da parte dei soggetti in esame, del rischio di agevolare la condotta auto-riciclatoria dell'autore del *predicate crime*⁸⁶.

Tuttavia, la tesi del dolo eventuale "presunto" non ci convince pienamente. L'imputazione del fatto a titolo di dolo eventuale dovrebbe, infatti, rifuggire da automatismi di sorta e seguire le cadenze di accertamento delineate dalla giurisprudenza di legittimità a proposito del delitto di ricettazione⁸⁷. Pertanto, l'elemento volitivo del dolo eventuale dovrà resistere al sillogismo logico, secondo il quale l'operatore che ha prestato il servizio avrebbe convertito o trasferito valute virtuali, anche se avesse avuto la certezza della provenienza illecita della provvista.

Riteniamo che, in ragione della peculiare attività svolta dai *mixers*, nei confronti di tali soggetti sia tendenzialmente agevole raggiungere la prova del dolo, quantomeno nella forma eventuale. Infatti, poiché il *mixing* assolve la funzione di ostacolare la ricostruzione del reticolo di transazioni in valute virtuali, pur non potendosi escludere, in astratto, che gli utenti della rete ricorrano ai *mixers* perseguendo scopi leciti⁸⁸, ci sembra che, in concreto e di regola, il ricorso al servizio offerto da questi ultimi si inserisca nel contesto della realizzazione di piani criminosi, in particolare riciclatori.

A conclusioni ben differenti pare si debba, invece, pervenire rispetto all'attività svolta da *miners*, *wallet providers* ed *exchangers*.

Poiché i *miners* convalidano le transazioni in modo del tutto casuale attraverso la soluzione di complessi problemi matematici, sicché non potrebbero scegliere su quali transazioni intervenire (quand'anche un minatore stringa accordi per validare una o più transazioni illecite, sarebbe assai improbabile che quest'ultime gli vengano concretamente attribuite) né prevedere *ex ante* quali transazioni saranno processate dai loro computer⁸⁹, sembra che la prova del dolo (anche in forma eventuale) dei *miners* sia

⁸⁶ Sulla rilevanza penale delle condotte dei *virtual currency exchangers*, si veda G. P. ACCINNI, *Profili di rilevanza penale delle criptovalute (nella riforma della disciplina antiriciclaggio del 2017)*, cit., 27. Con specifico riguardo a *miners* e *mixers*, L. STURZO, *Bitcoin e riciclaggio 2.0*, cit., 24.

⁸⁷ Il riferimento è in particolare alla nota pronuncia delle Sezioni Unite sulla compatibilità del dolo eventuale con il delitto di ricettazione: Cass. Pen., Sez. Un., 26.11.2009, n. 12433, *Nocera*, in *Dir. pen. cont.*, 20 dicembre 2010, con nota di G. ABBADESSA, [Ricettazione e dolo eventuale](#).

⁸⁸ Si pensi al caso di un soggetto che, dopo aver reso pubblica la corrispondenza di un determinato indirizzo alla propria persona, intenda effettuare un'ingente donazione ad un terzo, volendosi però assicurare (per ragioni di privacy o semplicemente di opportunità o convenienza) che questa non possa essere a lui attribuita.

⁸⁹ In realtà esistono alcune infrastrutture che permettono un'indicizzazione delle transazioni da parte dei *miners* per predeterminare a quali sarà data la precedenza. Il sistema Ethereum utilizza, ad esempio, il *gas price* (costo di transazione massimo che l'utente è disposto a pagare) per stabilire la priorità delle operazioni da validare. Anche in questo caso però l'attribuzione ai vari nodi avviene in modo del tutto casuale.

alquanto ardua, se non, di fatto, impossibile. La responsabilità del *miner* per riciclaggio parrebbe, invero, configurabile solo nel (remoto) caso in cui un minatore controlli la totalità o un'ampia maggioranza dei nodi della rete e, nella consapevolezza della provenienza delittuosa della provvista virtuale che costituisca l'oggetto di una determinata transazione, decida di validarla.

Exchangers e *wallet providers* si trovano, infine, in una posizione intermedia: essendo indiscutibile che il servizio – di per sé certamente lecito – da essi offerto possa agevolare, di fatto, l'eventuale condotta autoriciclatoria dell'autore del *predicate crime*, occorre rilevare che, perché possano essere chiamati a rispondere *ex art. 648-bis c.p.*, è necessario che venga accertata processualmente, caso per caso (con una difficoltà certamente ridotta rispetto a quella che connota l'accertamento dell'elemento soggettivo in capo ai *miners*), la sussistenza del dolo tipico, quantomeno nella forma eventuale⁹⁰.

6. Normativa antiriciclaggio e valute virtuali. Esperienze regolatorie a confronto.

Come è stato prontamente rilevato dalla dottrina, le esperienze regolatorie d'oltreconfine dimostrano una progressiva presa di coscienza dei legislatori nazionali nell'affrontare la dilagante diffusione delle valute virtuali⁹¹.

Prendendo le mosse dalla realtà degli Stati Uniti⁹², occorre rilevare che nel 2012 il *Federal Bureau of Investigation* (FBI), manifestando per la prima volta interesse rispetto alla possibile deriva criminosa delle operazioni in criptovaluta, ha pubblicato un documento intitolato «*Bitcoin Virtual Currency: FBI Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity*», dove non solo vengono analizzati tutti i profili di rischio legati all'uso delle valute virtuali, ma sono anche evidenziate in modo chiaro le debolezze legate all'assenza di un'Autorità centrale di riferimento nel sistema Bitcoin⁹³ (il riferimento è, tra l'altro, all'impossibilità di identificare e localizzare con

⁹⁰ Secondo G. P. ACCINNI, [Cybersecurity e criptovalute. Profili di rilevanza penale dopo la Quinta Direttiva](#), in questa *Rivista*, 2020, 5, 229, «il pericolo di riciclaggio (o di altro reato) e la correlata conoscenza da parte dell'intermediario sarà tanto più elevato quanto maggiore risulti il livello di anonimato garantito dalla valuta virtuale utilizzata: in base ai principi del *risk based approach* (che permea altresì le Direttive AML), tale livello sarà più basso per gli strumenti più diffusi, quali *BitCoin* o *Ethereum*, mentre sarà massimo per valute a diffusione locale, presenti solo su alcune piattaforme e in mano a pochi investitori di dubbia identità».

In extremis, si rileva che il recente assoggettamento di *exchangers* e *wallet providers* agli obblighi di cui al D. Lgs. 231/2007 ha riaperto il dibattito inerente alla possibilità di considerare i soggetti sottoposti agli obblighi antiriciclaggio titolari di una posizione di garanzia, come tali potenzialmente esposti a contestazioni di concorso omissivo nei reati di riciclaggio che vengano eventualmente realizzati dagli *users* mediante impiego di *virtual currencies*. Per un'analisi di carattere generale della questione, R. ACQUAROLI, *Il riciclaggio*, in F. Palazzo – C. E. Paliero (diretto da), *Trattato teorico pratico di diritto penale*, vol. VII, Torino, 2011, 805 ss.

⁹¹ L. D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D.Lgs. 90/2017*, cit., 19.

⁹² Per un'analisi delle prime esperienze regolatorie del *cyberlaundering*, T. EHRlich, *To Regulate or Not? Managing the Risks of E-Money and Its Potential Application in Money Laundering Schemes*, in *Harvard Journal of Law & Technology*, 1998, 11, 833 ss.

⁹³ Dalla lettura del documento *de quo* si evince che, sebbene l'FBI ritenesse assai probabile che le criptovalute fossero impiegate a fini riciclatori, a preoccuparlo maggiormente era, tuttavia, il rischio di finanziamento

esattezza i nodi della rete, all'assenza di punti di riferimento certi che colleghino le transazioni in valuta virtuale al mondo reale e alla notevole difficoltà di risalire alla fonte di provenienza delle criptovalute che siano oggetto di scambio nella rete⁹⁴).

Sulla scia del crescente interesse delle Autorità nei confronti del sistema Bitcoin, nel 2013 il *Financial Crimes Enforcement Network (FinCEN)* ha pubblicato a sua volta delle linee guida concernenti l'uso delle valute virtuali. Nel documento citato il *FinCEN* prende posizione su due distinte questioni: in primo luogo, equipara le criptovalute a *fiat money* e, in secondo luogo, evidenzia la necessità di imporre anche a quanti operino nel mercato delle criptovalute l'obbligo di procedere con la segnalazione di operazioni sospette ogniqualvolta riscontrino segnali di allarme indicativi del rischio che l'*e-cash* venga utilizzato a fini riciclatori⁹⁵.

Contrariamente alle attese, però, la strada tracciata dal *FinCEN* non ha trovato pieno consenso tra le autorità statunitensi. Infatti, nel 2014 l'*Internal Revenue Service (IRS)* ha elaborato una *Virtual Currency Guidance*⁹⁶ nella quale le *cryptocurrencies* non solo non vengono espressamente equiparate a *fiat money*, ma sono ricondotte ad una forma di *property*, invece che ad una specie di valuta.

Una notevole incertezza sulla riconducibilità delle criptovalute alla categoria degli strumenti di pagamento ovvero delle forme di proprietà è riscontrabile anche in ambito giurisprudenziale. Basti considerare, a titolo esemplificativo, la pronuncia con cui la Corte distrettuale di New York ha ritenuto applicabili alle criptovalute gli obblighi di registrazione legati ai *money transmitting businesses* e la sentenza con cui la Corte distrettuale di Miami ha, invece, sostenuto che le criptovalute debbano essere ricondotte alla categoria di *property*⁹⁷.

La principale causa di indeterminatezza è ravvisabile nel fatto che il Governo federale degli Stati Uniti sino ad ora non ha esercitato la propria prerogativa costituzionale di regolamentare il mercato valutario virtuale, rimettendo alla piena discrezionalità degli Stati la disciplina del fenomeno.

Tra le varie esperienze nazionali statunitensi merita di essere menzionata in particolare quella dello Stato di New York. Approvando nel 2014 il cosiddetto *BitLicense Regulatory Framework*, è stato, infatti, il primo Stato a intervenire in modo diretto nel mercato *cyber*valutario, fissando *standard* minimi di sicurezza per operare nel settore

del terrorismo e di furto di fondi in *e-cash*.

⁹⁴ Le criticità qui evidenziate rappresentano le caratteristiche che rendono il sistema Bitcoin la soluzione migliore per l'autofinanziamento della propria attività da parte delle organizzazioni terroristiche. Per un'analisi del pericoloso rapporto tra terrorismo e criptovalute si rinvia a J. HUNT, *The new frontier of money laundering: how terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them*, in *Information & Communications Technology Law*, 20, 2011, 133 ss.

⁹⁵ Vd. [sito della FINCEF](#).

⁹⁶ Vd. [sito dell'IRS](#).

⁹⁷ Secondo Teresa Mary Pooler, giudice precedente nel caso *de quo*, «*The Florida Legislature may choose to adopt statutes regulating virtual currency in the future,*» she wrote (...) *At this time, however, attempting to fit the sale of bitcoin into a statutory scheme regulating money services businesses is like fitting square peg in a round hole (...) This court is not an expert in economics, however, it is very clear, even to someone with limited knowledge in the area, that bitcoin has a long way to go before it is the equivalent of money*».

delle criptovalute e introducendo, a fini antiriciclaggio, specifici obblighi di *disclosure* a carico delle società autorizzate ad operare in *virtual currencies*⁹⁸.

Non è un caso che i primi tasselli del *regulatory framework* statunitense siano stati posizionati tra il 2012 e il 2014: trattasi, infatti, dell'arco temporale di emersione di due dei più importanti casi di indebito utilizzo di criptovalute negli Stati Uniti. Il riferimento è, in particolare, ai procedimenti *Liberty Reserve* e *Silk Road* concernenti, rispettivamente, fatti di *cyberlaundering* parziale e integrale⁹⁹.

Il primo dei casi citati riguarda l'emersione, a seguito di una complessa indagine svolta dal Dipartimento di Giustizia statunitense a carico della società costaricana *Liberty Reserve*, di una consolidata prassi di sfruttamento illecito della piattaforma *online* da essa amministrata - e della valuta virtuale ivi scambiata (il cosiddetto "*Liberty Dollar*"¹⁰⁰) - da parte di associazioni criminali, al fine di riciclare proventi delittuosi. In particolare, ad avvalersi, con la complicità della società *Liberty Reserve*, dell'anonimato e della non tracciabilità delle transazioni sulla piattaforma erano *de facto* tanto criminali informatici quanto narcotrafficanti o autori di reati di pedopornografia¹⁰¹.

Il secondo caso menzionato (divenuto, per la significatività dei numeri che lo caratterizzano¹⁰², *leading case* in materia di *cyberlaundering* integrale) ha, invece, ad oggetto l'indagine condotta dal Dipartimento di Giustizia statunitense a carico del sito internet *Silk Road*, attivo nel *darkweb* e strutturato in modo da consentire agli *users* di creare e utilizzare *e-wallets* ove far confluire i Bitcoin necessari per sostenere transazioni *online* aventi ad oggetto armi, droga, materiale pedopornografico o dati personali illecitamente carpiri.

Mettendo a disposizione degli *users* servizi di *mixing*, *Silk Road* consentiva alle parti delle transazioni virtuali illecite di assicurarsi, grazie all'anonimato garantito dal

⁹⁸ Nell'ambito dell'esperienza statunitense in materia di circolazione delle valute virtuali un ruolo fondamentale è rivestito dal c.d. *BitLicense*, approvato dal Dipartimento dei servizi finanziari dello Stato di New York nel 2014. Sul punto si rinvia a L. D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D.Lgs. 90/2017*, cit., 20, secondo cui «il provvedimento detta disposizioni sulla protezione dell'utente/consumatore, reca misure contro il riciclaggio e fissa gli *standards* minimi di *cybersecurity* per la gestione di servizi connessi all'utilizzo di valuta virtuale. Per ottenere l'autorizzazione all'esercizio dell'attività è necessario che l'istante sia in possesso di requisiti patrimoniali minimi atti a garantirne la stabilità finanziaria. Tra i soggetti obbligati figurano i professionisti dell'intermediazione sul VCs market che svolgono attività di *financial brokering* o altre attività connesse; restano invece esclusi gli operatori professionali che "estraggono" valuta virtuale alimentando la potenza di calcolo della *blockchain* (attività di *mining*) e le persone fisiche che acquistano valuta virtuale ai fini meramente speculativi. Le società autorizzate sono tenute a precisi obblighi di disclosure nei confronti delle Autorità di vigilanza, nonché di informazione ai clienti sui rischi connessi all'utilizzo delle valute virtuali».

⁹⁹ *Supra* § 4.1.

¹⁰⁰ Trattandosi di moneta scambiata su una piattaforma digitale facente capo alla società *Liberty Reserve*, il *Liberty Dollar* era, al contrario di Bitcoin, una valuta centralizzata.

¹⁰¹ Il rilievo del caso *Liberty Reserve*, nonché la pericolosità del fenomeno criminoso ad esso sotteso, sono facilmente evincibili dal commento di Richard Weber, capo della divisione investigativa dell'Internal Revenue Service, sulla vicenda: "*If Al Capone were alive today, this is how he would be hiding his money*".

¹⁰² Le indagini dei Procuratori federali hanno rivelato che *Silk Road*, potendo contare su circa centomila *users*, aveva ricavi di oltre ottanta milioni di dollari di ricavi annuali.

sistema, ingenti profitti, agevolando di fatto la conversione dei Bitcoin di provenienza delittuosa in valuta avente corso reale¹⁰³.

A nord degli Stati Uniti, il sistema canadese si è mostrato immediatamente favorevole alla circolazione all'interno dei propri confini delle valute virtuali, pur non riconoscendole come monete aventi corso legale. A carico delle società che intendano operare nel mercato *cyber*valutario è previsto unicamente l'obbligo di conformarsi alla normativa antiriciclaggio del Paese.

Il Giappone è stato il primo Stato a disciplinare le valute virtuali come strumenti di pagamento, includendole nella relativa categoria in sede di riforma del *Payment Services Act*¹⁰⁴. La riforma della normativa *de qua* ha offerto alle valute virtuali una *chance* di sopravvivenza nel Paese, nonostante un'iniziale perdita di fiducia legata allo scandalo che aveva investito la società *MtGox* per un caso di frode e furto di quattrocentocinquanta milioni di dollari in *Bitcoin*¹⁰⁵.

Nella vicina Cina, dal 2017 il ricorso a valute virtuali è, in via generale, vietato¹⁰⁶. Di recente, tuttavia, è stato reso pubblico il programma governativo di creazione e sperimentazione di una versione digitale dello yuan che sarà emessa direttamente dalla Banca centrale e avrà corso legale¹⁰⁷. In molti temono che l'e-yuan, finora oggetto di un progetto-pilota sviluppato nelle città di Shenzhen e Chengdu, «possa diventare uno strumento di sorveglianza e controllo, dal momento che le autorità saranno in grado di tracciare e monitorare i flussi finanziari in tempo reale, accumulando dati sulle transazioni e quindi acquisendo opportunità di sorveglianza senza precedenti. Allo stesso tempo, lo yuan digitale potrebbe offrire alla Cina la possibilità di creare una rete di pagamenti internazionali alternativa a quella controllata dalle banche americane e europee. Paesi che sono sotto sanzioni americane e europee – per esempio la Russia – sono già entrati nell'orbita dello yuan e si teme che lo yuan digitale favorirebbe questa tendenza»¹⁰⁸.

¹⁰³ Per un'analisi completa delle vicende giudiziarie legate alla *Liberty Reserve* e a *Silk Road*, G. P. ACCINNI, *Profili di rilevanza penale delle criptovalute (nella riforma della disciplina antiriciclaggio del 2017)*, cit., 14 ss.

¹⁰⁴ C. WILSON, *Cryptocurrencies: the future of Finance?*, in F.T. Yu – D. S. Kwan (a cura di), *Contemporary Issues in International Political Economy*, Singapore, 2019, 375; C. BROWN – T. DOLAN – K. BUTLER, *Cryptoassets and initial coin offerings*, in J. Madir (a cura di), *Fintech. Law and Regulation*, Cheltenham-Northampton, 2019, 98.

¹⁰⁵ L. D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D.Lgs. 90/2017*, cit., 20, secondo cui, dopo la riforma del *Payment Services Act* «il mercato ha reagito in modo molto positivo, segnando un aumento del coefficiente di capitalizzazione e del numero di transazioni in valuta virtuale da e verso il Giappone».

¹⁰⁶ M. P. DE LA CUESTA DE LOS MOZOS – E. SEDANO VARO, *On Regulatory Experimentalism in European Private Law: The Legal Laboratory of Food and Finance*, in L. De Almeida – M. Cantero Gamito – M. Durovic – K. P. Purnhagen (a cura di), *The Transformation of Economic Law. Essays in Honour of Hans-W. Micklitz*, Oxford, 2019, 243.

¹⁰⁷ Come evidente, tale *digital currency* risponde ad una logica opposta a quella perseguita da Satoshi Nakamoto, essendo emessa e, di fatto, controllata dalla Banca centrale cinese.

¹⁰⁸ P. SUBACCHI, *Perché lo yuan digitale non è una sfida alla supremazia del dollaro*, in *Il Sole 24 Ore*, 21 gennaio 2021.

In Europa, meritano di essere menzionate la disciplina tedesca e quella francese: mentre, in base alla prima, le criptovalute debbono essere considerate strumenti finanziari, la seconda le qualifica come mere *commodities*¹⁰⁹.

Infine, uno sguardo alla realtà mediorientale permette di rendersi conto del differente approccio adottato nei confronti delle valute virtuali da Iran, Iraq e Turchia, da un lato, Afghanistan, Pakistan ed Egitto, dall'altro. Mentre i primi Paesi si sono dotati di mercati legali di *Bitcoin*, i secondi hanno introdotto diversi ostacoli normativi al *trading* valutario in *e-cash*¹¹⁰.

L'Arabia Saudita ha optato per una politica intermedia, vietando le transazioni in criptovaluta, ma, allo stesso tempo, intraprendendo con gli Emirati Arabi Uniti un progetto finalizzato alla creazione di una criptovaluta interstatale destinata ad essere utilizzata per le transazioni internazionali¹¹¹.

7. Considerazioni conclusive.

Benché il rafforzamento delle misure antiriciclaggio a livello nazionale ed europeo costituisca una prima forma di cinta daziaria¹¹² volta a proteggere il sistema finanziario reale da qualsiasi tentativo di inquinamento, le misure di recente introduzione appaiono inidonee a scongiurare la strumentalizzazione, a fini criminosi, del mercato valutario virtuale.

Come rilevato, il legislatore italiano è intervenuto in materia di *cyberlaundering* dapprima con il D. Lgs. 90/2017 e, in seguito, con il D. Lgs. 125/2019, in parte anticipando e in parte recependo le previsioni di cui alla quarta e alla quinta Direttiva antiriciclaggio. All'esito degli interventi di riforma, il *corpus* normativo costituito dal D. Lgs. 231/2007 si è arricchito non solo di una espressa definizione di "valuta virtuale", ma anche di nuovi soggetti vincolati dagli obblighi antiriciclaggio, stante l'introduzione di *exchangers* e *wallet providers* nell'art. 3, comma 5, lett. i) e i-bis), D. Lgs. 231/2007.

L'insufficienza di tali presidi risulta evidente laddove si consideri il concreto funzionamento della tecnologia *blockchain*. L'attività prestata da *exchangers* e *wallet providers* è soltanto eventuale: chi intenda avvalersi delle potenzialità del sistema *cyber*valutario al fine di riciclare denaro non è, infatti, costretto a rivolgersi a fornitori di servizi di cambiavalute ovvero di portafoglio digitale, potendo sia acquistare valute

¹⁰⁹ Sul punto v. F. DI VIZIO, *Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti*, cit., 25; J. K. MATSUURA, *Digital Currency: An International Legal and Regulatory Compliance Guide*, Sharjah, 2018, 52; F. MOSLEIN – C. RENNIG, *Fintech regulation in Germany*, in M. Cian – C. Sandei (a cura di), *Diritto del Fintech*, Padova, 2020, 475.

¹¹⁰ Per un quadro generale della regolazione del settore FinTech in Medio Oriente v. N. ALAM – S.N. ALI, *Fintech, Digital Currency and the Future of Islamic Finance. Strategic, Regulatory and Adoption Issues in the Gulf Cooperation Council*, Cham, 2020.

¹¹¹ Non a caso il relativo progetto è stato soprannominato "Aber", termine arabo che richiama l'"attraversamento dei confini". S. CHAKRAVARTY – P. SARKAR, *An Introduction to Algorithmic Finance, Algorithmic Trading and Blockchain*, Bingley, 2020, 164.

¹¹² D. MAJORANA, *Disciplina giuridica e fiscale delle criptovalute: sfida al legislatore dal web*, cit., 23.

virtuali senza ricorrere a intermediari (ad esempio, accordandosi da remoto oppure incontrando fisicamente la controparte) sia optare per forme di conservazione delle chiavi crittografiche diverse dall'*e-wallet* (dotandosi, ad esempio, di un portafoglio personale o *cold wallet*).¹¹³

Alla luce delle precedenti considerazioni, sembra che l'inclusione di *exchangers* e *wallet providers* tra i destinatari degli obblighi antiriciclaggio abbia generato una crepa pressoché impercettibile nella cinta muraria che protegge l'anonimato di chi sfrutti l'infrastruttura *blockchain* per fini criminosi.

A tal proposito, non può che condividersi l'auspicio dell'implementazione di una politica di massimizzazione della trasparenza riportato nel Considerando n. 9 della Direttiva 2018/843/UE, secondo cui «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»¹¹⁴.

Ci pare che tali previsioni siano destinate a trovare cittadinanza nell'ordinamento europeo e nazionale in un futuro tutt'altro che remoto.

Premesso che la chiave d'arco che sostiene l'intera infrastruttura sulla quale vengono effettuate le transazioni in valuta virtuale è costituita dalla fiducia e che a venire in considerazione è tanto la fiducia reciproca tra utenti quanto, e soprattutto, quella riposta dagli stessi nel sistema, considerato nel suo complesso, l'implementazione di una normativa che miri a contrastare l'utilizzo dell'infrastruttura *blockchain* per fini criminosi, mediante ricorso all'arma bianca della trasparenza, non sembra destinata a incontrare ostacoli insormontabili.

Infatti, consentendo alle unità nazionali di informazione finanziaria di risalire all'identità reale degli utenti della rete, coperta dallo pseudo-anonimato (tuttora assicurato dal sistema *blockchain* agli *users* che non si avvalgano del servizio prestato da *exchangers* e *wallet providers*¹¹⁵), nonché incentivando gli utenti che pongano in essere transazioni in valuta virtuale a effettuare una *disclosure* delle relative caratteristiche, il legislatore risponderebbe non solo all'interesse delle autorità pubbliche, ravvisabile in un'efficace prevenzione e repressione di *cyber-riciclaggio* e *cyber-autoriciclaggio*, ma anche a quello dei creatori delle valute virtuali e di quanti di esse si avvalgano a fini di investimento ovvero di acquisto di beni o servizi. Infatti, un'infrastruttura *blockchain* che non sia in grado di far fronte in modo adeguato alle potenzialità criminogene delle valute virtuali, e che si riveli comunque gravemente permeabile al loro sfruttamento criminoso, è destinata a porre le basi di un atteggiamento collettivo di sostanziale diffidenza che travolgerebbe il mercato delle criptovalute: gli utenti sarebbero infatti

¹¹³ L. STURZO, *Bitcoin e riciclaggio 2.0*, cit., 30.

¹¹⁴ Richiamato di recente da S. GALMARINI, *Monete virtuali e antiriciclaggio: terreni dai confini incerti*, su *Dir. bancario*, 11 ottobre 2018.

¹¹⁵ Come già rilevato, tanto gli *exchangers* quanto i *wallet providers* sono soggetti, tra l'altro, all'obbligo di identificazione della clientela.

gradualmente, e irreversibilmente, indotti ad abbandonarlo, lasciandosi alle spalle le rovine di una fallita promessa di modernità.

Alla luce delle precedenti considerazioni, riteniamo che un'efficace prevenzione dello sfruttamento dell'infrastruttura *blockchain* e delle valute virtuali per fini riciclatori non possa che passare attraverso l'accoglimento da parte del legislatore dell'auspicio di cui al Considerando n. 9 della Direttiva 2018/843/UE.

Trasferendo l'attenzione dal piano preventivo a quello repressivo, l'obbligo gravante sul legislatore varia nel contenuto, ma non nella forma. Infatti, anche al fine di reprimere efficacemente il *cyberlaundering*, il legislatore è obbligato a guardare alla normativa sovranazionale e, tuttavia, in tal caso a venire in considerazione è la Direttiva 2018/1673/UE sulla lotta al riciclaggio mediante il diritto penale¹¹⁶.

In particolare, dall'art. 6, par. 1, lett. b) della Direttiva si evince l'obbligo per gli Stati membri di introdurre una circostanza aggravante applicabile nel caso in cui la condotta riciclatoria sia posta in essere da un soggetto obbligato ai sensi dell'articolo 2 della direttiva 2015/849/UE, nell'esercizio della propria attività professionale.

Considerando che tra i soggetti obbligati di cui all'art. 2 della direttiva 2015/849/UE¹¹⁷ rientrano anche *exchangers* e *wallet providers*, occorre chiedersi se il legislatore italiano debba riformare i delitti di riciclaggio e autoriciclaggio, previsti e puniti dagli artt. 648-*bis* e 648-*ter*. 1 del codice penale, introducendo una nuova circostanza aggravante o se le indicazioni sovranazionali debbano intendersi soddisfatte dalle circostanze aggravanti già previste dal secondo comma dell'art. 648-*bis* c.p. e dal quinto comma dell'art. 648-*ter*.1 c.p., le quali comportano un aumento della pena qualora il delitto sia commesso nell'esercizio di un'attività professionale.

Ebbene, la particolare insidiosità delle valute virtuali¹¹⁸ e la scelta del legislatore sovranazionale di subordinare l'applicabilità della circostanza aggravante di cui all'art. 6 della Direttiva 2018/1673/UE non solo alla commissione del reato nell'esercizio di attività professionale, ma anche (e soprattutto) all'assoggettamento dell'autore dello stesso agli obblighi antiriciclaggio di cui all'art. 2 della Direttiva 2015/849/UE, sembrerebbero imporre l'introduzione nel *corpus* degli artt. 648-*bis* e 648-*ter*.1 c.p. di una specifica circostanza aggravante speciale.

Inoltre, premesso che l'aumento di pena previsto per il caso in cui i delitti di riciclaggio o autoriciclaggio siano commessi nell'esercizio di attività professionale è pari,

¹¹⁶ Preme rilevare che il mancato recepimento di tale Direttiva ha portato all'avvio, nei confronti dell'Italia, della procedura di infrazione n. 2021/0055, attualmente in fase di messa in mora ex art. 258 TFUE.

¹¹⁷ Il riferimento è all'art. 2 della Direttiva UE/2015/849, come modificato dall'art. 1, par. 1, lett. c) della Direttiva UE/2018/843.

¹¹⁸ Secondo il Considerando n. 6 della Direttiva (UE) 2018/1673 «L'uso delle valute virtuali presenta nuovi rischi e sfide nella prospettiva della lotta al riciclaggio. Gli Stati membri dovrebbero garantire che tali rischi siano affrontati in modo adeguato». In tema pare condivisibile la tesi dottrina secondo la quale la previsione di una specifica circostanza aggravante, applicabile alle fattispecie di *cyber-riciclaggio* e *cyber-autoriciclaggio*, dovrebbe intendersi giustificata in virtù del contesto digitale delle operazioni di lavaggio ovvero del carattere tecnologico del relativo oggetto (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 questa *Rivista*, 6 maggio 2020).

al massimo, ad un terzo¹¹⁹, e considerando l'opportunità di riconoscere maggiore gravità all'ipotesi in cui non solo il fatto tipico sia commesso nell'esercizio di un'attività professionale, ma autore dello stesso sia anche un soggetto sottoposto agli obblighi antiriciclaggio, pare che la nuova circostanza dovrebbe avere natura di circostanza aggravante non già ad efficacia comune, bensì speciale. In alternativa, in sede di recepimento della Direttiva citata, in ragione dell'indiscutibile elevata pericolosità propria delle valute virtuali, un aumento della pena superiore a un terzo ovvero una cornice edittale diversa e maggiormente gravosa rispetto a quella ordinaria dovrebbe essere oggetto di specifica previsione quantomeno per il caso in cui a porre in essere il fatto tipico, nell'esercizio della propria attività professionale, sia non un qualsiasi soggetto sottoposto agli obblighi antiriciclaggio, bensì il prestatore di un servizio di portafoglio digitale o di cambiavalute.

¹¹⁹ Le circostanze aggravanti di cui al secondo comma dell'art. 648-*bis* c.p. e al quinto comma dell'art. 648-*ter*.1 c.p. sono, infatti circostanze aggravanti a efficacia comune.