QUESITI

GIOVANNI PAOLO ACCINNI

Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017)

Con D.lgs. 25 maggio 2017 n. 90 l'Italia ha dato attuazione alla IV Direttiva Europea in tema di antiriciclaggio (Direttiva UE n. 849/2015) riformando integralmente le disposizioni di cui al D.lgs. n. 231/2007. Il nostro Paese non si è tuttavia limitato a recepire le disposizioni europee, ma, precorrendo i tempi, ha anticipato alcune previsioni in tema di "criptovalute" che dovrebbero costituire oggetto di una futura V Direttiva Europea ancora in fase di discussione. L'importanza di siffatto intervento normativo e la rapidissima ascesa delle valute virtuali suggeriscono l'opportunità di un primo esame dei possibili rischi di carattere penale connessi alle c.d. *virtual currencies*, con più specifico approfondimento dedicato al problema del riciclaggio di denaro sporco ed alle recenti misure adottate a livello nazionale.

On May 25th 2017 Italy implemented the IV European anti money laundering Directive (Directive UE n. 849/2015), by doing so reforming the Legislative Decree n. 231/2007. Nonetheless, our Country has not only transposed the european disposition, but it has also anticipated some provisions on cryptocurrencies which are supposed to be issued with a future V European anti money laundering directive still under discussion. The importance of such reformation and the rapid raise of cryptocurrencies demand a first exam of the possible risks of criminal relevance connected to virtual currencies as well as an in depth analysis concerning the problem of money laundering and the recent Italian AML legislation.

1. Premessa.

Il divampare della febbre da Bitcoin (novella forma di corsa all'oro del Klondike) ha dato avvio a numerose discussioni relative al nesso intercorrente tra criptovalute convertibili in moneta legale e mondo del crimine, nel non infondato sospetto che siffatto strumento di pagamento si presti ad essere sfruttato dalla criminalità e dai finanziatori del terrorismo internazionale al fine di poter movimentare, nascondere e "ripulire" i proventi dell'attività illecita in assenza di controlli da parte delle Autorità. Il problema affonda le sue radici nel fatto che, per via dell'algoritmo che ne regola il funzionamento, il Bitcoin

unisce in sé i vantaggi della moneta elettronica e quelli del contante: «come una banconota, è anonimo: non richiede che siano rese note le identità delle controparti né la causale di pagamento; ma, essendo digitale, ossia un puro numero, divisibile e moltiplicabile a piacere, consente trasferimenti per qualunque importo, dai micropagamenti di pochi centesimi al regolamento di traffici commerciali internazionali»[1].

Istituzioni e Governi di tutto il mondo sono perciò chiamati ad un pressante sforzo di regolamentazione che, per quanto concerne la prospettiva penalistica, pare aver trovato la propria prima "feritoia" nella normativa antiriciclaggio e di contrasto al terrorismo internazionale. Nella propria riforma della disciplina antiriciclaggio, attuata con il recente D.lgs. 90/2017, il nostro Paese ha infatti introdotto (primo in Europa) una definizione giuridica di valuta virtuale e di cambiavalute virtuale, sottoponendo alcuni operatori del settore ai presidi AML (*anti money laundering*). La presente trattazione si propone quindi di affrontare, nei limiti del tecnicismo informatico accessibile ad un giurista, il tema del Bitcoin (ma, in termini più generali, dell'intero mondo delle c.d. criptovalute convertibili) per chiarire in che modo alcune delle sue caratteristiche possano costituire un volano per la commissione di reati ed un forte ostacolo alla prevenzione del riciclaggio internazionale.

2. *Cenni sul funzionamento del sistema "criptovalutario".*

Nel sistema monetario tradizionale la moneta elettronica non è altro che una disponibilità di potere d'acquisto registrata su un conto corrente acceso presso una Banca. Allorquando si effettua un acquisto od un bonifico a favore di un beneficiario non si verifica alcun trasferimento fisico di denaro, ma, semplicemente, la riduzione del saldo dell'acquirente ed il contestuale aumento del saldo del venditore per un importo corrispondente. Il trasferimento si compie pertanto a mezzo di una semplice scrittura. Nondimeno, uno schema siffatto esige la partecipazione di una Banca, chiamata a verificare l'effettiva disponibilità di fondi sul conto dell'acquirente, ad eseguire l'ordine di pagamento, ad addebitare il conto dell'acquirente e ad (infine)
accreditare il conto del venditore. La moneta elettronica tradizionale richiede perciò che la tenuta dei conti sia "centralizzata", risultando indispensabile l'intervenuto di un ente terzo (una Banca) che, grazie ai dati custoditi nei propri *server* centralizzati e protetti, verifichi e confermi l'identità dell'ordinante, la disponibilità dei fondi, la correttezza dei codici di sicurezza; esegua l'operazione e la trascriva sui propri libri contabili.

[1] AMATO – FANTACCI, *Per un pugno di Bitcoin*, Milano, 2016, 3.

Ebbene, l'innovazione fondamentale portata dal Bitcoin (e dalle altre criptovalute convertibili in circolazione) consiste proprio nell'aver superato siffatta esigenza di gestione centralizzata delle transazioni. Il sistema è stato invero pensato e sviluppato in modo che la tenuta dei conti non sia affidata ad un unico gestore, ma distribuita tra tutti gli utenti. Il "libro contabile" su cui sono registrate tutte le operazioni non è cioè più appannaggio di una singola Banca o del sistema bancario nel suo complesso, ma è tenuto da ciascuno degli utenti nella memoria del proprio personal computer. In tal modo, il registro non è semplicemente decentrato, ma distribuito in una rete in cui nessun "nodo" è centrale. Questo libro contabile distribuito (*distributed ledger*) è quello che prende il nome di *blockchain.* In particolare, secondo una mirabile definizione, «la *blockchain* si compone di una serie concatenata di blocchi (da cui il nome), i quali registrano, per ogni transazione, l'identità del pagante, l'importo trasferito e l'identità del beneficiario. Ciascun blocco contiene quindi le informazioni relative a tutte le transazioni che si sono svolte consecutivamente nell'arco di dieci minuti, nonché un riferimento al blocco precedente. Pertanto, la serie concatenata di blocchi che costituisce la *blockchain* fornisce in ogni istante una rappresentazione completa e aggiornata di tutte le transazioni che si sono svolte dall'avvio del sistema sino a quel momento»[2]. La fine (insomma) del monopolio della documentazione a cura di un unico soggetto. In siffatto sistema decentrato e distribuito sono invero tutti gli utenti (e non più un solo soggetto) a dover verificare la fattibilità e quindi autorizzare ogni singola transazione. Ciò che fanno attraverso un sofisticato meccanismo di decriptazione di codici. Più in specifico, allorquando un soggetto effettui un ordine di trasferimento di Bitcoin (così come accade nelle normali operazioni bancarie) dovrà comunicare al sistema il proprio conto di addebito, l'importo dell'operazione ed il conto di accredito. Nondimeno, non essendo previsto l'intervento di un soggetto terzo (come un Istituto di Credito) a cui poter comunicare in via riservata le proprie chiavi di accesso al conto e che possa quindi verificare la disponibilità dei fondi, il sistema prevede che chi effettua l'operazione trasmetta agli altri utenti (i.e. al sistema) una chiave di accesso al conto in forma "criptata". Per poter autorizzare l'operazione gli altri utenti saranno in conseguenza chiamati a decriptare siffatta chiave d'accesso attraverso la risoluzione di un complicato problema matematico e il sistema prevede quale "stimolo premiale" che il primo soggetto che riesca a decriptare il codice ed a verificare la fattibilità dell'operazione venga ricompensato con un determinato ammontare di Bitcoin. In particolare, i soggetti

[2] AMATO – FANTACCI, *Per un pugno di Bitcoin*, cit., 16.

dediti a siffatte operazioni di verifica (potenzialmente ciascun utente) sono denominati *miners* (o minatori) ed operano attraverso *hardware* dotati di un'elevata potenza di calcolo[3]. Allorquando il codice sia stato decriptato e l'operazione validata, la stessa verrà inserita nel *block* contenente un determinato numero di operazioni, che, sommandosi ai *block* precedenti, darà vita appunto alla *blockchain*[4].

2.1. La natura decentralizzata del sistema.

Come detto il Bitcoin (così come la gran parte delle altre criptovalute convertibili) è una moneta virtuale decentralizzata (c.d. *non centralised virtual currency*). Ciò significa che il sistema non dipende da un amministratore che assuma un ruolo preminente rispetto agli altri[5], ma dall'interazione di soggetti indipendenti che svolgono funzioni parimenti necessarie al funzionamento ed allo sviluppo dell'intero *network*. Tra questi soggetti rientrano ovviamente gli *users*, persone o società che acquistano od ottengono la valuta virtuale per acquistare beni o servizi materiali o virtuali, per poi trasferirla ad altri soggetti a fini personali o per detenerla a titolo di investimento. In particolare, gli *users* possono entrare in possesso di valuta virtuale acquistandola con moneta avente corso legale, offrendo merci e servizi che contemplino il pagamento in criptovaluta, ovvero ricevendola a titolo di regalo o ricompensa. Vi sono poi i *miners*, che, come chiarito, sono i soggetti che confermano le operazioni realizzate dagli utenti e che vengono ripagati con un certo numero di Bitcoin.
Un ruolo di primaria importanza è quindi quello degli *exchanger* (o *virtual currency exchanger*), ovverosia i soggetti (persone fisiche o giuridiche) che offrono agli *users* servizi di cambio di moneta virtuale con moneta legale o

[3] Sul punto MANCINI, *Bitcoin: rischi e difficoltà normative*, in *Banca impresa soc.*, 2016, 1, 126 ss., osserva come l'operazione di *mining* venga «eseguita attraverso una serie di algoritmi il cui calcolo può essere eseguito da qualunque *hardware*. Nei primi anni di funzionamento del Bitcoin chiunque scaricava il programma di *mining* aveva la possibilità di effettuare tale controllo, giacché anche il singolo utente dotato di un modesto elaboratore era in grado di svolgere il *mining*. La progressiva diffusione del Bitcoin ha richiesto sempre più potenza di calcolo ed ha costretto i *miners* a costituire gruppi di collaborazione: tramite appositi programmi, i *pool* di *miners* uniscono la potenza dei propri computer per effettuare più verifiche possibili».

[4] In merito alle modalità di funzionamento del sistema criptovalutario, cfr. *ex multis*: NAKAMOTO, *Bitcoin: a peer to peer electronic cash system*, in http://bitcoin.org/bitcoin.pdf, ultimo accesso 8 gennaio 2018; DE STASIO, *Ordine di pagamento non autorizzato e restituzione della moneta*, Milano, 2016, 58 ess; MANCINI, *Bitcoin: rischi e difficoltà normative*, cit., 126 ss; CALAPRICE, *Gli acquisti online*, Milano, 2014, 59 ss.; GREENFIELD, *Tecnologie radicali*, Torino, 2017, 121 ss.

[5] Ad esempio un garante che emetta moneta, stabilisca delle regole per il suo utilizzo, mantenga un sistema di pagamento centralizzato, abbia l'autorità per ritirare la valuta o per decidere il tasso di cambio con la moneta avente corso legale.

metalli preziosi (e vice versa), in cambio di una commissione[6]. Imprescindibili sono infine anche i *wallet provider*, società che forniscono agli *users* i *virtual currency wallet* (i c.d. *e.wallet*, o portafogli elettronici) attraverso la creazione di specifici programmi ed applicazioni che consentano agli *users* di detenere, immagazzinare e trasferire i Bitcoin o le altre criptovalute. In specifico, oltre a fornire l'*e.wallet*, il *wallet provider* conserva le chiavi private del conto, agevola le operazioni degli *users* e degli *exchanger*, i rapporti tra *users* e venditori virtuali e può (altresì) interagire con tutti gli altri *wallet providers.*
Da ultimo, a fianco di siffatti soggetti "istituzionali" si rinvengono numerose entità terze che possono prendere anch'esse parte al sistema in maniera non predeterminabile. Si tratta di specifici sviluppatori di *software* od applicazioni che offrono una varia tipologia di servizi collaterali e che possono essere affiliati ad *exchanger* e *wallet providers*, ovvero agire in maniera del tutto indipendente.

3. Anonimato e pseudonimato.

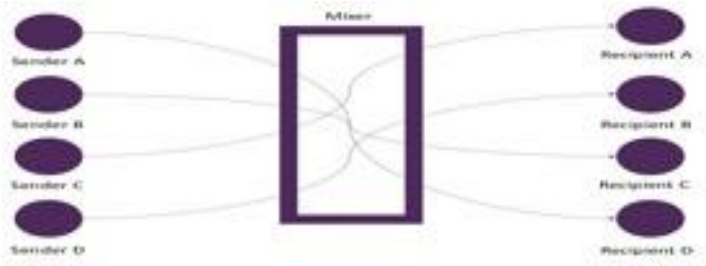
Riassunti i tratti fondamentali del sistema va chiarito che, con riferimento alle possibili implicazioni criminali delle *virtual currencies*, un ruolo determinante è certamente quello giocato dal loro essere valute anonime o (meglio) pseudanonime. Per espresso volere dei suoi ideatori[7], la *blockchain* è infatti pubblica e trasparente, tanto che ogni utente della rete può visionare in qualunque momento tutte le operazioni in Bitcoin intervenute in un determinato arco temporale, il relativo importo ed i soggetti ordinante e ricevente[8]. Nondimeno, la tracciabilità delle singole operazioni non giunge sino al punto di consentire di risalire alla reale identità dei singoli operatori. Vero infatti che in ogni operazione ciascun *user* è identificato da una chiave pubblica ed una privata[9]. Allorquando si effettui un pagamento, la *blockchain* registra quindi la chiave pubblica del pagante e l'importo dell'operazione, mentre la chiave privata (la *password*) non viene pubblicata sulla *blockchain*, ma rimane nella esclusiva disponibilità del titolare dell'*e.wallet*. Quanto risulterà visibile sulla *blockchain* non sarà quindi mai il reale nominativo di chi effettui un'operazione, ma un mero numero identificativo corrispondente alla chiave

[6] In particolare, tra i mezzi di pagamento generalmente accettati dagli *exchanger* rientrano il denaro contante, bonifici bancari, carte di credito o valute virtuali diverse.
[7] Cfr. NAKAMOTO, *Bitcoin: a peer to peer electronic cash system*, in http://bitcoin.org/bitcoin.pdf, ultimo accesso 8 gennaio 2018.
[8] Il sito www.blockexplorer.com consente così di visionare in tempo reale tutte le informazioni relative alle operazioni in Bitcoin realizzate dagli utenti.
[9] Si pensi allo *username* ed alla *password* che si utilizzano per accedere alla posta elettronica.

pubblica dei soggetti coinvolti. In tal senso si è appunto soliti parlare di *pseudonimato* del sistema Bitcoin, intendendosi che, pur essendo pubblico il registro delle operazioni, gli operatori non sono identificabili tramite il proprio nome e cognome, ma solo a mezzo di numeri rappresentativi della loro chiave pubblica di accesso al sistema.
Alcuni commentatori hanno osservato come un sistema così strutturato non sarebbe in realtà idoneo a garantire l'anonimato degli operatori in valuta virtuale. A fronte di un'incertezza rispetto alla generalità dell'utente, la pubblicità della *blockchain* fornisce invero una completa conoscenza rispetto a tutte le operazioni generate da un determinato *account*, i rispettivi importi e l'*account* di destinazione[10]. Nel caso in cui sulla *blockchain* vengano individuate operazioni sospette (si pensi ad un soggetto che ponga in essere numero elevato numero di operazioni tutte dirette ad una medesima controparte in un ristretto arco temporale o ad un soggetto che ponga in essere una singola operazione di importo estremamente rilevante) le Autorità interessate potrebbero risalire al reale titolare del conto (*e.wallet*) attraverso l'utilizzo di appositi *software*. Una delle principali caratteristiche del Bitcoin è, pur tuttavia, quella di offrire ad ogni utente la possibilità di generare un numero pressoché illimitato di chiavi pubbliche associate ad altrettante chiavi private, potendo così decidere di utilizzare un identificativo differente per ogni singola operazione realizzata. Manifesto allora che, nel caso di sostituzione frequente delle chiavi crittografiche, diverrà assai complicato poter rinvenire elementi di sospetto nell'operatività degli *users* a partire dalla *blockchain* e dare quindi avvio ad eventuali accertamenti sulle loro reali identità. Si soggiunga pure che, come ormai posto in evidenza da numerosi organismi nazionali ed internazionali di prevenzione e contrasto al riciclaggio[11], l'industria di settore sta sviluppando sistemi *software* sempre più complessi ed efficienti che vengono offerti agli utenti interessati e la cui finalità è proprio quella di aumentare la *privacy* bypassando la natura pubblica della *blockchain*. Il più noto è costituito dal c.d. *mixing service* (conosciuto anche come *tumbler*), un servizio che consente agli utenti di oscurare la cronologia delle proprie transazioni aggregando un certo numero di trasferimenti e quindi "mischiando" l'origine e la destinazio-

[10] Come invero acutamente osservato da MÖSER, BÖHME, BREUKER, *An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem*, in *Ecrime Researchers Summit*, 2013, 1 – 2: «*AML in Bitcoin has to deal with imperfect knowledge of identifies, but may exploit perfecte knowledge of all transactions*».
[11] Cfr: Royal United Services Institute for Defence and Security Study, *Occasional paper, virtual currencies and financial crime: challenges and opportunities*, in *www.*rusi.org.
.pdf, ultimo accesso 19 dicembre 2017, 9; Financial Action Task Force, *Virtual currencies: key definition and potential aml/cft risks*, in *www.fatf-gafi.org*.

ne di ogni singolo pagamento[12]. Per mezzo del *mixing*, il pagamento da A ad A verrà perciò dirottato su B, e quello da B a B (di importo corrispondente al primo) verrà dirottato su A, in modo che risultino confusi i nominativi degli ordinanti ed i rapporti in dare e avere tra questi e i riceventi[13].



Occorre ancora tener poi presente anche che il mercato delle criptovalute convertibili in denaro non si compone del solo Bitcoin, ma (come pure noto) è composto di un numero estremamente elevato e crescente di monete a maggiore o minore diffusione e complessivamente definite Altcoins[14]. Ebbene, pur ispirandosi allo schema di funzionamento del Bitcoin, alcune tipologie di Altcoins prevedono un algoritmo di funzionamento in grado di garantire un livello di *privacy* assai più elevato di quello offerto dal loro parente più noto. Nel 2014 è stata ad esempio lanciata sul mercato la valuta Monero, il cui protocollo di funzionamento (denominato CryptoNote[15]) prevede la creazione automatica di nuove coppie di chiavi per ogni operazione e rende visi-

[12] Tra i più noti servizi di *mixing* rinvenibili in rete si annoverano Bitlaunder, Easycoin, Sharedcoin e Bitcoin Laundry.

[13] Per un esame analitico del funzionamento del *mixing service* ci si permette rinviare a MÖSER, BÖHME, BREUKER, *An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem*, cit., 2. Gli autori osservano in particolare che «*the primary motivation for providing these services is making profit. Hence, they send back to their users only what has been payed in minus a fee. The fee varies between the services and may consist of a fixable and a variable part*». Quanto perciò alla diffusione del fenomeno vi è che, secondo stime operate da esperti del settore, il 10% delle operazioni giornaliere realizzate in Bitcoin nel corso del 2016 avrebbe contemplato l'utilizzo di sistemi di *mixing*; cfr: Coinfirm Blog, *What are bitcoin mixers/tumblers and how often are they being used*, in https://medium.com/@Coinfirm/what-are-bitcoin-mixers-tumblers-and-how-often-are-they-being-used-1924b0965853, ultimo accesso 19 dicembre 2017.

[14] Tra le più note è così possibile citare (ad esempio) gli Ethereum, i Ripple, i Litecoin, gli Etherium Classic, i Dash. In particolare, come posto in evidenza dal Royal United Services Institute for Defence and Security Study, *Occasional paper, virtual currencies and financial crime: challenges and Opportunities*, cit., 2, alla data di marzo 2017 «*the total present market capitalisation of cryptocurrencies [...] is an estimated $24 billion, with approximately 70% of that comprised of Bitcoin*», mentre il 30% è riconducibile appunto a valute alternative.

[15] Redatto nel corso del 2012 da tale Nicolas van Saberhagen.

bili le informazioni relative alla transazione (ad esempio il suo importo) al solo ricevente ovvero ad un terzo dotato di un'apposita *viewkey* fornitagli dall'ordinante. Il sistema Monero prevede anche un sistema di *mixing* automatico e garantito indistintamente a tutti gli utenti, con la logica conseguenza che tutte le operazioni risulteranno oscurate e difficilmente ricostruibili nel loro concreto dipanarsi[16]. Caratteristiche simili a Monero presenta anche ZCash, una valuta virtuale immessa sul mercato nel corso del 2016 e che consente agli utenti di decidere se rendere o meno pubblici i dati delle proprie transazioni[17]. Con riferimento quindi al crescente numero di *tools* deputati ad aumentare il livello di *privacy* offerto dal "classico" sistema Bitcoin nel corso della conferenza dal titolo *Blockchain money conference*, tenutasi a Londra nel corso di novembre 2016, l'Amministratore Delegato di Elliptic, *startup* creata per coadiuvare le Autorità nell'individuazione di operazioni sospette sulla *blockchain*, ha evocativamente osservato che «se è *naïve* pensare che muoveremo verso un mondo in cui tutte le transazioni siano opache [...] è però realistico pensare che muoveremo verso un mondo di trasparenza *selettiva*»[18].

4. Le principali possibili connessioni tra virtual currencies e mondo del crimine

Com'è facilmente intuibile, il genetico anonimato (o psedonimato) delle *cryptocurrencies*, unito al diffondersi di servizi di *mixing* e alla possibilità di effettuare transazioni rapide ed irreversibili a livello transnazionale, dà adito a più di una fondata preoccupazione in chiave di prevenzione e repressione criminale. Il rischio più serio ed immediato è in particolare rappresentato dal loro utilizzo da parte dei *cybercriminals*, ossia da coloro che commettono reati attraverso l'utilizzo di sistemi informatici. Si tratta di soggetti che operano in gruppi organizzati e secondo una specifica ripartizione di competenze, distinguendosi (ad esempio) il ruolo dei *programmatori*, ovverosia i soggetti che elaborano i programmi utilizzati dalle organizzazioni dei *cybercriminals*, quello dei *distributori*, che distribuiscono o vendono i dati o merci illecitamente acquisite o, ancora, quello dei c.d. *money mule*, e cioè i soggetti che si occu-

[16] In argomento si rinvia in particolare a PEARSON, *Meet Monero, the currency dark net dealers hope is more anonymous than Bitcoin*, in *www.motherboard.vice.com*.

[17] Ha caratteristiche simili a Monero anche ZCash, che ha iniziato a venire immesso sul mercato nel corso del 2016 e che consente agli utenti di decidere se rendere o meno pubblici i dati delle proprie transazioniPer una sommaria panoramica del sistema ZCash ci si permette fare rinvio all'articolo *What is ZCash*, in https://news.bitcoin.com/snowden-zcash-bitcoin-risks/, ultimo accesso 2 gennaio 2018.

[18] SMITH, relazione alla conferenza *Blockchain money conference*, in https://www.ccn.com/bitcoin-is-too-transparent/.

pano di acquisire e "ripulire" i proventi dell'attività illecita[19]. L'esperienza maturata negli ultimi anni ha dimostrato come siffatti soggetti agiscano secondo due direttrici principali: possono prendere a bersaglio computer di privati od istituzioni (pubbliche o private) per diffondere virus, ovvero per rubare od alterare dati sensibili od identità (da un lato); utilizzare i sistemi informatici per porre in essere reati di natura comune come frodi, scommesse illegali, reati pedopornografici, compravendita di beni o servizi illeciti[20] (dall'altro lato).

In un siffatto contesto l'avvento delle criptovalute ha dunque consentito di consolidare meccanismi di perpetrazione dei *cybercrime* già esistenti, rendendoli addirittura più efficaci grazie alla sicurezza garantita dal regime di anonimato in cui è possibile scambiare le valute virtuali[21]. Più in specifico, come posto in evidenza dall'Euoropol nel proprio rapporto annuale sul crimine cibernetico 2017, «le criptovalute continuano ad essere sfruttate da cybercriminals ed il Bitcoin è la valuta maggiormente utilizzata per operare nei mercati di prodotti illeciti e per ricevere pagamenti frutto di *cyber*-estorsioni [...]»[22]. Un utilizzo crescente delle valute virtuali avviene in particolare nell'ambito dei c.d. *ransomware attacks*, ovvero attacchi informatici consistenti nella diffusione di virus che criptano i dati presenti in sistemi informatici altrui e per la cui decriptazione viene richiesta una somma di denaro. Grande notorietà ha avuto ad esempio il c.d. attacco *WannaCry*, responsabile di un'epidemia su larga scala avvenuta nel maggio 2017 su computer dotati di sistema operativo Microsoft Windows. Il virus diffuso dagli *hackers* era capace di criptare i *file* presenti sui computer e di chiedere un riscatto in Bitcoin per decriptarli. Il 12 maggio 2017 il *malware* ha così infettato i sistemi informatici di numerose aziende ed organizzazioni in tutto il mondo, tra le quali

[19] Per un approfondimento sul mondo dei *cybercriminals* e sugli specifici ruoli rivestiti dai membri di siffatte organizzazioni criminali v. *What is cybercriminal*, in https://www.technopedia.com/definition/27435/cybercriminal, ultimo accesso 2 gennaio 2018.

[20] All'interno della macrocategoria dei crimini informatici si è perciò soliti individuare due sottocategorie: quella dei "*computer crimes*" e quella dei "*computer faciltated crimes*". Nella prima i computer rappresentano gli obiettivi della condotta illecita; nella seconda questi (ed in generale la rete informatica) costituiscono gli strumenti attraverso cui realizzare il reato.

[21] Sul punto di rimanda a BRYANS, *Bitcoin and money laundering: mining for an effective solution*, in *Indiana law journal*, 2014, 89, 441 ss., ove si legge che «*new virtual currencies, such as Bitcoin, add yet another layer of anonymity by allowing users to transfer value without the collection of any personally identificable information. Regulations often fail to affect such virtual currencies due to lack of foresight by the regulation writers, creating a legal grey area. Thus, criminals can continue to capitalize on technological innovation to bolster their illegal activities*»

[22] Cfr. *Internet organised crime threat assessment (IOCTA)* 2017, in *www.europol.europa.eu* (la traduzione è nostra).

Portugal Telecom, Deutsche Bahn, FedEx, Telefónica, Tuenti, Renault, il National Health Service, il Ministero dell'interno russo, l'Università degli Studi di Milano-Bicocca etc. Il 28 maggio 2017 sono stati poi colpiti oltre duecentotrentamila computer in 150 paesi, rendendo WannaCry uno dei maggiori contagi informatici mai avvenuti[23]. Non stupisce allora che l'avvento e lo sviluppo delle valute virtuali, in grado di rendere assai più complessa l'identificazione dei beneficiari delle *cyber*-estorsioni, possa costituire un volano alla commissione di siffatta tipologia di reati, tanto che nel corso del 2016 gli attacchi c.d. *ransomware* sono aumentati di più del 50% rispetto al 2015 e che nello stesso anno le società bersaglio hanno corrisposto a titolo di riscatto importi equivalenti ad 850 milioni di dollari, a fronte dei 25 milioni corrisposti del 2015[24].

Un crescente utilizzo di *cryptocurrencies* (tra cui Bitcoin, Monero e ZCash) avviene quindi anche in sede di attacchi c.d. DDoS (acronimo della locuzione *Distributed Denial of Service*), la cui peculiarità è quella di far esaurire deliberatamente le risorse di un sistema informatico che fornisce un servizio ai *client*, ad esempio un sito web, fino a renderlo non più in grado di erogare il servizio al soggetto richiedente[25]. Un vorticoso incremento dell'utilizzo di valute virtuali (e del Bitcoin in particolare) è stato altresì registrato nell'ambito della compravendita di servizi pedopornografici *online*[26], di carte di credito clonate[27] e, in termini più generali, in tutti i c.d. *dark-net markets*, siti internet presenti nel c.d. *dark web*[28] ed in cui viene venduta la più ampia tipologia di merci e di servizi illeciti, tra cui armi, droga e servizi di *hacking*[29].

Significativo porre ancora in evidenza che, seppure possa apparire paradossale, non è neppure infrequente che i *cybercriminals* facciano oggetto delle proprie condotte criminose gli stessi detentori di valute virtuali, portando attacchi informatici agli *exchanger* od ai *wallet providers* al fine di carpire le

---

[23] Cfr. *Attacco hacker mondiale: virus Wannacry chiede il riscatto, ospedali britannici in tilt*, in *www.repubblica.it*.

[24] Cfr. *Carbon Black, Threat report. Non-Malware attacks and ransomware. Take center stage 2016*, in *www.carbonblack.com*.

[25] Cfr. *Internet organised crime threat assessment (IOCTA)* 2017, cit., 27.

[26] Cfr. *Internet organised crime threat assessment (IOCTA)* 2017, cit., 39.

[27] Cfr. *Internet organised crime threat assessment (IOCTA)* 2017, cit., 44.

[28] Con la locuzione *dark web* (in italiano: *web oscuro* o *rete* oscura) si intendono i contenuti del world wide web contenuti nelle c.d. dark-net (reti oscure), reti telematiche non raggiungibili attraverso gli usuali motori di ricerca, ma solo tramite specifici *software*, configurazioni ed accessi autorizzativi. Cfr. ANDY GREENBERG, *Hacker Lexicon: What Is the dark web?*, in *www.wired.com*.

[29] Cfr. *Internet organised crime threat assessment (IOCTA)* 2017, cit., 49. Come posto in evidenza dalla UK National crime agency (NCA), *National strategic assessment of serious and organised crime*, 9 settembre 2016, 29, «*Bitcoins remains the virtual currency of choice for dark web trading*».

chiavi private di accesso ai conti e derubare i loro possessori. A mero titolo di esempio è così possibile citare il c.d. caso Bitfinex, un *virtual currecies exchanger* con sede ad Honk Kong che in data 2 agosto 2016 ha subito il furto di monete virtuali per un controvalore complessivo pari a 72 milioni di dollari[30]. Ancora più eclatante il caso dell'*exchanger* Mt-Gox, sino al 2014 uno dei maggiori *exchanger* a livello planetario, a cui gli degli *hacker* avrebbero sottratto n. 744.408 Bitcoin, equivalenti a 350 milioni di dollari statunitensi[31]. Non meno emblematico anche l'attacco perpetrato ai danni del progetto di raccolta fondi "*The Dao*", nel corso del quale sono stati sottratti dagli *hacker* più di 152 milioni di dollari. Il furto è stato perpetrato nel corso di una *Ico (Initial coin offering)*, ossia quell'operazione attraverso cui un'azienda creatrice di una nuova valuta virtuale la offre in vendita al pubblico per la prima volta[32].

Accanto poi all'accertato crescente utilizzo da parte dei *cybercriminals* vi è l'utilizzo di *virtual currencies* per l'acquisto di beni e servizi suscettibile di un non trascurabile rischio di frode in danno degli utenti. Una delle peculiarità delle transazioni in Bitcoin è invero quella di essere irretrattabili e non modificabili, sicché una volta che sia stato effettuata un'operazione, la stessa non potrà più essere annullata. Manifesto perciò come siffatta caratteristica, in uno con l'anonimia (pseudonimia) delle *cryptocurrencies*, esponga gli acquirenti ad un alto rischio di rimanere truffati. Nel caso infatti di mancata ricezione di quanto acquistato ovvero di ricezione di merce contraffatta o danneggiata, non sarà possibile annullare il pagamento né si riuscirà ad identificare compiutamente il venditore truffaldino[33]. Ulteriori rischi sono quindi connessi a possibili frodi in danno di chi intenda partecipare al sistema criptovalutario a soli fini speculativi. Esistono infatti numerosi esempi di operatori finanziari che agivano (ad agiscono) secondo il c.d. "schema Ponzi", adescando i potenziali investitori su *blog* specializzati attraverso la prospettiva di lauti guadagni che non vengono tuttavia alimentati da una legittima attività di *trading,* ma (al contrario) dalle sole immissioni di liquidità conferita dai nuovi ignari investitori in Bitcoin[34]. Da ultimo, neppure infrequenti i casi di siti internet operanti come Bitcoin *exchanger* che, da un giorno all'altro, sono semplicemente

[30] Cfr. BALDWIN, *Grumpy Hold-Outs could sink Bitfinex recovery plan after bitcoin theft*, in *www.reuters.com*.
[31] Per un approfondimento sul caso Mt-Gox cfr: *ww.wired.it*.
[32] Sul punto v. Vigna, *Criptovalute, i segreti delle Ico,* in Milano Finanza, 3 ottobre 2017, 4.
[33] Royal United Services Institute for Defence and Security Study, *Occasional paper, virtual currencies and financial crime: challenges and opportunities*, cit., 19.
[34] Cfr. U.S. Security and exchange commission, *Investor Alert. Ponzi schemes using virtual currencies*, in *www.sec.gov*.

"spariti dalla rete", venendo cancellati dai rispettivi gestori nel frattempo appropriatisi dell'integralità dei depositi in Bitcoin dei propri clienti[35].

5. I rischi di riciclaggio connessi alla struttura del sistema Bitcoin e delle altre criptovalute convertibili.

Accanto ai non trascurabili aspetti criminogeni a cui si è fatto cenno vi è che (come ormai posto in sempre maggiore evidenza da numerosi organismi internazionali) le criptovalute convertibili in moneta legale, quale il Bitcoin, presentano elevatissimi profili di rischio in punto di riciclaggio e di finanziamento al terrorismo internazionale[36]. Il principale di questi discende in particolare dal fatto che il sistema criptovalutario è in grado di essere finanziato in via totalmente anonima. Molti detentori di valuta virtuale pongono infatti in vendita Bitcoin ed altre *cryptocurrencies* privatamente, attraverso semplici annunci postati *online*, su *blog*, ovvero su siti specializzati, senza perciò l'intermediazione di un *exchanger* o di altro soggetto astrattamente controllabile dall'Autorità[37]. I metodi di pagamento generalmente accettati da siffatti venditori sono molteplici, rientrandovi (a titolo di esempio) le ricariche di carte postepay, di carte di debito, ovvero di carte di servizio. La natura immediata della transazione in criptovaluta fa poi si che l'acquisto di Bitcoin possa ben avvenire in contanti e "faccia a faccia", essendo sufficiente che l'aspirante acquirente si doti di un portafoglio digitale, contatti il potenziale venditore, lo incontri in un luogo pubblico, gli consegni il denaro contante ed attenda che questi esegua l'operazione di trasferimento utilizzando (ad esempio) l'apposita applicazione installata sul telefono cellulare[38]. Manifesto insomma che un soggetto dotato di ingente liquidità frutto di attività illecita (si pensi – ad esempio – a proventi rinvenienti da reati di evasione fiscale) potrebbe agevolmente contattare un privato cittadino intenzionato a cedere la propria valuta virtuale ed acquistarla sulla "pubblica piazza", senza che di siffatto acquisto

---

[35] SHUBBER, *Dollar 4,1 million goes missing as chinese bitcoin trading platform GBL vanishes*, in *www.geek.com*.

[36] Cfr. Financial Action Task Force, *Virtual currencies: key definition and potential aml/cft risks*, cit., 9-10; EBA, *Eba opinion on virtual currencies*, 4 luglio 2014, in www.eba.europa.eu, ultimo accesso 2 gennaio 2018, 25 ss.; BCE, *Virtual currencies schemes. A further analysis*, febbraio 2015, in www.ecb.europa.eu, ultimo accesso 10 gennaio 2018, 25 ss. In argomento v. anche SIMONCINI, *Il cyberlaundering: la "nuova frontiera" del riciclaggio*, in *Riv. trim. dir. pen. econ.*, 2015, 4, 903.

[37] Tra i principali siti di intermediazione tra venditori ed acquirenti di Bitcoin è possibile citare www.bitboat.net. Fornisce invece un servizio di incontro tra domanda ed offerta di Bitcoin il sito www.localbitcoins.com.

[38] Per una breve panoramica sulle potenziali modalità di acquisito di Bitcoin in contanti ci si permette fare rinvio a: *I migliori sistemi per comprare Bitcoin in contanti*, in https://coinlist.me/it/bitcoin/comprare-bitcoin/contanti, ultimo accesso 3 gennaio 2018, 3 ss.

rimanga traccia alcuna.
A siffatta manifesta capacità di *funding* anonimo si affianca poi la circostanza che, come pure già chiarito, le *cryptocurrencies* garantiscono un livello di anonimato assai maggiore rispetto alle ordinarie transazioni bancarie, non solo poiché il loro protocollo di funzionamento non richiede l'identificazione o la verifica della reale identità dei detentori dei portafogli elettronici, ma perché (come si è pure visto) esistono numerosi *tools* che consentono di massimizzare la *privacy* degli utenti (ad es. i servizi di *mixing*) e delle valute virtuali (ad es. Monero o ZCash) che sono completamente anonime. Il titolare di un *e.wallet* alimentato con proventi di attività illecita potrebbe quindi ben disporne in maniera riservata, impiegando la provvista per acquisti di beni e servizi senza lasciare traccia della proprie effettive generalità. Si è poi avuto già modo di rappresentare anche che il sistema delle valute virtuali ha ormai raggiunto scala globale, sicché il Bitcoin e le altre *cryptocurrencie*s sono agevolmente utilizzabili per effettuare trasferimenti a livello sovrannazionale, permettendo agli interessati di trasferire capitali ingenti in molti paesi del mondo spesso privi di alcun presidio antiriciclaggio. Tornando all'esempio tipico dell'evasore fiscale vi è che, una volta entrato in possesso, in modo anonimo, della valuta virtuale, questi potrebbe trasferirla liberamente ed anonimamente in paesi privi di qualunque regolamentazione antiriciclaggio, per convertirla nuovamente in valuta avente corso legale da reimmettere nel sistema. In ultima analisi mette conto soggiungersi che, in termini generali, l'assenza di intermediari centralizzati che effettuino le operazioni per conto dei clienti costituisce un ostacolo assai rilevante all'implementazione dei presidi antiriciclaggio tradizionalmente intesi. Come noto, gli interventi di contrasto alle transazioni illecite si sviluppano in via ordinaria con indagini di polizia giudiziaria[39] e (soprattutto) con l'approfondimento delle segnalazioni di operazioni sospette provenienti da Banche od altri intermediari finanziari. La mancanza di un gestore centralizzato nell'ambito del mondo criptovalutario sottrae pertanto alle Autorità preposte un interlocutore affidabile, rendendone assai più difficile l'operato. In tal senso, non può neppure sottacersi che, la natura decentrata e frammentata del sistema, fa si che i trasferimenti di valute virtuali coinvolgano entità distinte e spesso operanti in nazioni diverse, sicché (da un lato) risulta complicato determinare la competenza territoriale delle singole Autorità antiriciclaggio e (dall'altro) rimane preclusa la possibilità di individuare i sog-

[39] Cfr. Guardia di Finanza, *L'attività della guardia di finanza nella lotta al finanziamento del terrorismo*, in *www.gdf.gov.it*.

getti a cui inoltrare eventuali richieste di natura investigativa o cautelare[40].

6. La concretizzazione del rischio: i più noti casi di riciclaggio noti connessi all'utilizzo di valute virtuali.

Le Autorità giudiziarie internazionali hanno avuto modo di confrontarsi con rilevanti casi di riciclaggio posti in essere attraverso l'utilizzo indebito di criptovalute, giungendo così alla conclusione che siffatta *bad practice* si sviluppi secondo due direttrice fondamentali. La prima, secondo cui un criminale "comune" converte il provento di reati in *cryptocurrencies* e dà avvio ad una serie di transazioni, trasferimenti in favore di altri portafogli virtuali, ovvero acquisti di merce, al fine oscurare l'origine illecita dei fondi. La seconda, secondo cui un criminale informatico vende merce di natura illecita a fronte del pagamento di valuta virtuale, converte siffatta valuta in moneta avente corso legale e pone poi in essere transazioni, trasferimenti di denaro, prelevamenti, acquisti, etc., allo scopo di nascondere l'origine delittuosa del denaro[41].

Un eclatante esempio di riciclaggio appartenente al primo dei *genus* descritti è costituito dal c.d. caso *Liberty Reserve*, ancora oggi il maggiore caso di riciclaggio *online* mai verificatosi. Nel corso del maggio 2013 il Dipartimento di Giustizia degli Stati Uniti d'America ha accusato la società Liberty Reserve, ente di intermediazione mobiliare con sede in Costa Rica, di aver concorso nel riciclaggio di 6 miliardi di dollari di profitti illeciti. In particolare, le indagini avevano fatto emergere come siffatta società fosse stata costituita al solo fine di fornire supporto ad associazioni criminali interessate a riciclare i proventi rinvenienti dalla clonazione di carte di credito, furti di identità, reati informatici, narcotraffico e pornografia minorile, consentendogli di porre in essere transazioni anonime e non tracciabili. Liberty Reserve vantava addirittura un milione di clienti sparsi in tutto il mondo (200.000 nei soli Stati Uniti d'America) e risulta aver gestito non meno di 55 milioni di transazioni illegali. Più in dettaglio, per conseguire il proprio "oggetto sociale" la società usava emettere una propria moneta virtuale, il Liberty Dollar[42], che periodicamente veniva quotato in dollari statunitensi. Al fine di utilizzare il Liberty Dollar gli utenti dovevano aprire un *account* (i.e. un portafoglio virtuale) utilizzando il

---

[40] Su questo aspetto ci si permette in particolare rinviare a Financial Action Task Force, *Virtual currencies: key definition and potential aml/cft risks*, cit., 9-10.

[41] Royal United Services Institute for Defence and Security Study, *Occasional paper, virtual currencies and financial crime: challenges and Opportunities*, cit., 14.

[42] Bene quindi sottolineare che, a differenza delle monete virtuali decentralizzate (come il Bitcoin) il Liberty Dollar era quindi una valuta centralizzata, postulando l'esistenza di un amministratore centrale (Liberty Reserve) che ne gestiva le emissioni ed i rapporti di cambio con le monete aventi corso legale.

sito internet della società. Questa non provvedeva tuttavia ad una reale verifica delle genuinità dei dati immessi dagli utenti, accontentandosi anzi di intestazioni manifestamente false quali *Russia Hachers*, *Hacher Account*, *Russia Bugs* e di indirizzi quali *123 Fake Main Street* o *Completely Made Up City.* Liberty Reserve chiedeva dunque ai propri clienti di effettuare i depositi ed i prelevamenti di denaro servendosi di *exchanger* terzi e fidati, generalmente degli intermediari mobiliari non registrati con sede in Russia o in numerosi paesi sprovvisti di qualunque presidio antiriciclaggio o di contrasto al terrorismo internazionale (ad es. Malasya, Nigeria e Vietnam). Una volta creato il proprio conto ogni utente poteva quindi effettuare ogni tipo di transazione, tra cui trasferire i propri Liberty Dollar ad altri utenti del sistema residenti in Paesi diversi, ovvero effettuare acquisti *online* servendosi di *online markets* compiacenti che accettavano i Liberty Dollar come mezzo di pagamento. All'atto dell'inchiesta Liberty Reserve risultava perciò pienamente operativa in paesi quali l'Australia, Cipro, la Cina, Hong Kong, il Marocco, la Russia e la Spagna, tanto che le indagini che hanno condotto infine allo *shut down* del sistema hanno richiesto la collaborazione di ben 18 giurisdizioni sparse in tutto il mondo.

Un esempio del secondo tipo di riciclaggio è poi rappresentato dal noto caso Silk Road. Nel corso del settembre 2013 il Dipartimento di Giustizia degli Stati Uniti ha reso pubblica un'indagine afferente un sito internet, denominato appunto Silk Road, che operava nel *dark web* e consentiva ai propri utenti di acquistare e vendere droga, armi, dati personali trafugati ed altre merci di carattere illecito in concorso con organizzazioni di narcotrafficanti, di *hackers* e di soggetti dediti al riciclaggio. Silk Road vantava circa 100.000 clienti sparsi in tutto il mondo e generava ricavi complessivi pari a circa 1,2 miliardi di dollari l'anno, corrispondenti ad 80 milioni di dollari di ricavi annuali per il sito internet. Più in specifico, il sito perseguiva l'anonimato dei propri clienti operando nel *dark web* ed accettando in pagamento solo Bitcoin. Il suo meccanismo di funzionamento prevedeva che ogni utente dovesse collegare il proprio portafoglio virtuale di Bitcoin ad uno o più portafogli virtuali gestiti dalla stessa Silk Road. Quando l'utente effettuava un acquisto i Bitcoin venivano dunque trasferiti dal primo al secondo portafoglio elettronico dove venivano mantenuti fino a quando non si aveva avuta conferma del perfezionamento della compravendita. Solo in questo momento i Bitcoin trasferiti sull'*account* Silk Road venivano infine immessi nel portafoglio virtuale in Bitcoin appartenente al venditore. Bene peraltro soggiungere che Silk Road forniva ai propri utenti degli appositi servizi di *mixing* per ogni transazione, rendendo così praticamente impossibile identificare acquirente e venditore intervenuti che avevano

posto in essere la singola transazione. Manifesto allora come il sistema descritto abbia permesso agli *users* di lucrare ingenti profitti illeciti in via completamente anonima, potendo poi convertire i Bitcoin così guadagnati nei propri paesi d'origine con moneta avente corso legale[43].

Degni di nota sono infine anche il caso Western Express International[44] e (da ultimo) quello di Alexander Vinnik, un cittadino russo arrestato a luglio 2017 con l'accusa di aver riciclato 4 miliardi di dollari provenienti da narcotraffico, hackeraggio ed evasione fiscale tramite la piattaforma BTC-e, una delle più grandi borse di valute digitali esistenti al mondo. Nel comunicato stampa rilasciato dall'organismo statunitense Financial Crimes Enforcement Network (FinCen) in data 26 luglio 2017 si legge in particolare che «BTC-e è un intermediario mobiliare estero che cambia valute e criptovalute quali Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum e Dash. E' uno dei maggiori convertitori di valute al mondo ed ha agevolato transazioni di denaro provenienti da attacchi *ransomware*, hackeraggio informatico, furti di identità, evasione fiscale, corruzione e spaccio di droga. [...] Tra le altre violazioni, BTC-e ha omesso di richiedere agli utenti informazioni ulteriori rispetto a username, password ed indirizzo email. Invece di agire per scongiurare rischi di riciclaggio, BTC-e ed i suoi amministratori hanno abbracciato gli evidenti intenti criminosi dei propri utenti. Gli utenti discutevano apertamente ed esplicitamente la natura e le finalità della propria attività criminosa sulla *chat* di BTC-e. Il servizio clienti di BTC-e offriva consigli su come processare ed avere libero acceso a proventi di attività illecita quale la vendita di droga sui *dark-net markets* quali Silk Road, Hansa Market ed Alphabay»[45].

Nel panorama italiano non constano essersi registrati episodi di gravità pari a quelli qui descritti. Nondimeno, nei Quaderni dell'antiriciclaggio pubblicati da Banca d'Italia e UIF in data 7 dicembre 2016 si dà conto di un tentativo di riciclaggio operato da una cooperativa nazionale per il tramite di investimenti in *cryptocurrencies*. Dalla lettura di siffatto documento è dato di comprendere come il caso abbia tratto origine dalla segnalazione di un'operazione sospetta pervenuta da una Banca e relativa all'accredito sul conto corrente di una cooperativa di fondi provenienti da altri conti correnti intrattenuti dalla

---

[43] Per una ricostruzione analitica della vicenda v. Financial Action Task Force, *Virtual currencies: key definition and potential aml/cft risks*, cit., 10-11.

[44] Cfr. Financial Action Task Force, *Virtual currencies: key definition and potential aml/cft risks*, cit., 12.

[45] Financial Crimes Enforcement Network (FinCen), *FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales*, in https://www.fincen.gov/sites/default/files/2017-07/BTC-e%20July%2026%20Press%20Release%20FINAL1.pdf, ultimo accesso 3 gennaio 2016 (la traduzione è nostra).

medesima cooperativa presso altri Istituti di Credito. I fondi così ricevuti venivano quindi impiegati per disporre bonifici esteri in favore di piattaforme di investimento e cambio di valute virtuali – in particolare Bitcoin – con rapporti incardinati in diversi stati esteri, alcuni *off shore*. Ebbene, l'analisi finanziaria eseguita con riguardo all'origine della provvista utilizzata per i trasferimenti all'estero evidenziava che i girofondi iniziali disposti dalla cooperativa a valere sui rapporti intrattenuti presso gli altri intermediari derivassero da bonifici disposti da un ente pubblico territoriale e fossero riferiti a finanziamenti pubblici di scopo[46].

7. La normativa antiriciclaggio «Europea»: le proposte di modifica alla Direttiva n. 849/2015.

Le descritte problematiche hanno indotto la Commissione Europea ad avviare una repentina riflessione intesa, tra l'altro, ad estendere ad alcuni operatori del settore delle *virtual currencies* gli obblighi previsti dalla normativa antiriciclaggio. Con la Direttiva n. 849/2015 del Parlamento Europeo e del Consiglio in data 20 maggio 2015 (la c.d. IV Direttiva Europea antiriciclaggio) l'Unione ha infatti provveduto a riformare integralmente la propria disciplina in materia. Gli operatori del settore criptovalutario sono nondimeno rimasti all'epoca esclusi dal novero dei soggetti obbligati. Siffatta ed altre mancanze hanno dunque poi condotto in tempi brevi alla formulazione della nuova Proposta di Direttiva n. 0208/2016, che è stata trasmessa dalla Commissione al Consiglio Europeo in data 6 luglio 2016 e con cui si intenderebbe colmare un vuoto normativo che, alla luce di quanto sopra rappresentato, si fatica sempre più a comprendere. Come infatti riconosce la stessa Proposta di modifica, nonostante recenti analisi abbiano «evidenziato [...] rischi, in particolare per quanto riguarda i prestatori di servizi di cambio tra valute virtuali e valute legali», che siffatte valute «beneficiano di un maggior grado di anonimato rispetto ai classici trasferimenti di fondi» e che possono venire utilmente utilizzate dalle «organizzazioni terroristiche [...] per nascondere trasferimenti finanziari», «attualmente i trasferimenti di valute virtuali non sono oggetto di alcun tipo di monitoraggio nell'Unione Europea da parte delle autorità pubbliche perché non sono state fissate norme vincolanti per stabilire le condizioni di questo monitoraggio né a livello dell'Unione né dei singoli stati membri». Si riconosce perciò l'esigenza improcrastinabile di definire «un quadro normativo per il funzionamento dei cambiavalute e dei prestatori di servizi di portafoglio di-

[46] Cfr. *Quaderni dell'antiriciclaggio. Analisi e studi. Casistiche di riciclaggio e di finanziamento del terrorismo*, dicembre 2016, n. 7, 16-17.

gitale che operano controllando l'accesso del pubblico ai diversi sistemi di valute virtuali» stabilendosi altresì la necessità di una loro inclusione tra i soggetti sottoposti alle disposizioni antiriciclaggio previste nella Direttiva n. 849/2015[47].

La proporzionalità e la necessità di evitare di costituire un freno all'innovazione tecnologica costituita dalle *criptocurrencies* ha tuttavia indotto la Commissione Europea a limitare l'estensione degli obblighi di identificazione e di segnalazione delle operazioni sospette ai soli *exchanger* e *wallet provider*. In particolare, l'articolo 1, n. 1, della Proposta di modifica prevede che all'articolo 2, paragrafo 1, punto 3) della Direttiva n. 849/2015 (ove si elencano i soggetti obbligati agli adempimenti antiriciclaggio) siano aggiunte le lettere g) ed h), ovverosia:

- g) i «prestatori di servizi la cui attività principale e professionale consiste nella fornitura di servizi di cambio tra valute virtuali e valute legali» e;
- h) i «prestatori di servizi di custodia delle credenziali necessarie per accedere alle valute virtuali»[48].

Ancora, l'articolo 1, n. 3, lettera c) della Proposta prevede che tra le definizioni di moneta contenute all'articolo 3 della Direttiva n. 849/2015 venga introdotto un punto 18) relativo alle monete virtuali, da intendersi quale «rappresentazione di valore digitale che non è emessa da una banca centrale o da un ente pubblico ne è necessariamente legata a una valuta legale, ma è accettata da persone fisiche e giuridiche come mezzo di pagamento e può essere trasferita, memorizzata o scambiata elettronicamente». Non pare inutile infine

---

[47] Commissione Europea, *Proposta di Direttiva del Parlamento Europeo e del Consiglio 2016/0208*, *5* luglio 2016, p. 14, in http://eur-lex.europa.eu/procedure/IT/2016_208, ultimo accesso 3 gennaio 2018.

[48] In particolare, per una definizione più esaustiva di *exchanger* e di *wallet providers* cfr. Banca Centrale Europea, *Virtual currencies schemes. A further analysis*, cit., 8, secondo cui:

«*Exchanges: offer trading services to users by quoting the exchange rates by which the exchange will buy/sell virtual currency against the main currencies (US dollar, renminbi, yen, euro) or against other virtual currencies. These actors, most of them non-financial companies, can be either issuer-affiliated or a third party. They generally accept a wide range of payment options, including cash, credit transfers and payments with other virtual currencies. Moreover, some exchanges also provide statistics (e.g. volumes traded and volatility), act as wallet providers and offer (immediate) conversion services for merchants who accept VCS as an alternative payment method*».

«*Wallet providers: offer a digital wallet to users for storing their virtual currency cryptographic keys and transaction authentication codes, initiating transactions and providing an overview of their transaction history. There are basically two types of wallet, which differ as regards their immediate usability versus their safety from cyber crime: online wallets (hot storage) and offline wallets (cold storage). From a functional perspective, these services are offered for desktop PCs, mobile devices and as cloud-based applications. Nevertheless, users can also set up and maintain a wallet themselves without making use of a wallet provider*».

dar conto che, al settimo considerando della Proposta di modifica, si evidenzia comunque come l'inclusione degli *exchanger* e dei *wallet provider* nel novero dei soggetti obbligati ad attuare i presidi antiriciclaggio «non risolve [comunque] completamente il problema dell'anonimato delle operazioni in valuta virtuale: infatti poiché gli utenti possono effettuare operazioni anche senza ricorrere a piattaforme di cambio o prestazioni di servizi di portafoglio digitale, gran parte dell'ambiente delle valute virtuali rimarrà caratterizzato dall'anonimato».

8. La normativa antiriciclaggio italiana alla luce del D.lgs. n. 90 in data 25 maggio 2017.

La Proposta di modifica alla Direttiva n. 849/2015 non è stata ancora approvata in sede Europea e la prima lettura in discussione plenaria si è tenuta ad ottobre 2017. Con la pubblicazione del Decreto di recepimento della (ormai superata) Direttiva n. 849/2015 il nostro Paese ne ha tuttavia già anticipato alcuni contenuti, ponendosi così quale vero e proprio *front runner* a livello continentale. Il D.lgs. 90/2017 contiene invero una definizione di valuta virtuale sovrapponibile a quella di cui alla Proposta di modifica citata, stabilendo cioè che con siffatta locuzione debba intendersi una «rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente»[49]. Il Decreto precisa quindi cosa siano – e quali attività svolgano – i prestatori di servizi relativi all'utilizzo di valuta virtuale, che vengono segnatamente identificati in «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»[50]. Seppur più ampia e non sovrapponibile alla definizione prevista nella Proposta di modifica della Direttiva n. 849/2015, è quindi indubbio che in siffatta definizione rientrino gli *exchanger*, ovverosia coloro che conservano e convertono valute virtuali in valute aventi corso legale. Il D.lgs. 90/2017 si sofferma dunque sull'attività di siffatti soggetti (i c.d. cambiavalute virtuali) facendone rientrare l'esercizio sotto vigilanza delle Autorità competenti di settore, ossia obbligando il prestatore a conformarsi alla disciplina an-

[49] Cfr. articolo 1, comma 2 lettera qq) del D.lgs. 21 novembre 2007, n. 231, come modificato dal D.lgs. 25 maggio 2017, n. 90.
[50] Cfr. articolo 1, comma 2 lettera ff) del D.lgs. 21 novembre 2007, n. 231, come modificato dal D.lgs. 25 maggio 2017, n. 90.

tiriciclaggio: si dice insomma che l'*exchanger* dovrà essere – anch'esso – un soggetto obbligato. In particolare, per i soggetti che svolgono l'attività di *exchanger* o cambia-valute virtuali, il D.lgs. 25 maggio 2017, n. 90 (intervenendo sulla normativa prevista dal D.lgs. 13 agosto 2010, n. 141, articolo 17-bis[51]) introduce l'obbligo di iscrizione in una sezione speciale del registro dei cambiavalute tenuto dall'Organismo degli Agenti e dei Mediatori ai sensi dell'art. 128 *undecies* del Testo Unico Bancario, parificandoli così ai tradizionali cambiavalute e sottoponendoli pertanto alle disposizioni antiriciclaggio. Per contro, la normativa italiana di recente introduzione non ha sottoposto alle disposizioni *anti money laundering* i prestatori di servizi di portafoglio digitale – ovverosia i *wallet provider* – che offrono servizi di custodia delle credenziali necessarie per accedere alle valute virtuali e che, come si è avuto modo di chiarire, vengono invece espressamente menzionati dalla Proposta di modifica della Direttiva n. 849/2015 quali futuri destinatari degli obblighi antiriciclaggio.

9. Gli obblighi di identificazione e verifica gravanti sull'*exchanger*.

In quanto soggetto obbligato l'*exchanger*, allorquando contragga un rapporto con il cliente, sarà peciò tenuto ad identificarlo secondo le procedure di adeguata verifica della clientela (c.d. *customer due diligence*) segnatamente previste dagli artt. 17 e ss. del D.lgs. 231/2007 come modificato dal D.lgs. 90/2017. Con la locuzione identificazione e verifica del cliente si intende in particolare un processo che deve avvenire mediante l'acquisizione dei dati identificativi forniti dall'interessato (o tratti da un documento d'identità non scaduto) e con la verifica dei medesimi, che deve avvenire attraverso il confronto di questi con quelli desumibili da una fonte affidabile e indipendente di cui va acquisita

[51] In particolare, l'articolo 8, comma 1, del D.lgs. 25 maggio 2017, n. 90 prevede che:
«1. Al decreto legislativo 13 agosto 2010, n. 141, come modificato dal decreto legislativo 14 dicembre 2010, n. 218, e dal decreto legislativo 19 settembre 2012, n. 169, all'articolo 17-*bis*, dopo il comma 8, sono aggiunti i seguenti:
«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 in una sezione speciale del registro di cui al comma 1.
8-*ter*. Ai fini dell'efficiente popolamento della sezione speciale di cui al comma 8-*bis*, con decreto del Ministro dell'economia e delle finanze sono stabilite le modalità e la tempistica con cui i prestatori di servizi relativi all'utilizzo di valuta virtuale sono tenuti a comunicare al Ministero dell'economia e delle finanze la propria operatività sul territorio nazionale. La comunicazione costituisce condizione essenziale per l'esercizio legale dell'attività da parte dei suddetti prestatori. Con il decreto di cui al presente comma sono stabilite forme di cooperazione tra il Ministero dell'economia e delle finanze e le forze di polizia, idonee ad interdire l'erogazione dei servizi relativi all'utilizzo di valuta virtuale da parte dei prestatori che non ottemperino all'obbligo di comunicazione».

e conservata copia in formato cartaceo o elettronico. In sostanza, è possibile affermare che, mediante un procedimento di identificazione, si acquisisce un'asserzione ("questo sono io"), che deve però poter essere stata verificata da un terzo che abbia realmente riscontrato chi io dico di essere, assegnandomi qualcosa che mi permetta di essere riconosciuto da altri.
Ai sensi della normativa di nuova introduzione l'*exchanger* dovrà quindi provvedere alla identificazione e verifica del cliente nei termini predetti tanto in occasione dell'instaurazione di un rapporto continuativo che in occorrenza dell'esecuzione di un'operazione occasionale di importo pari (o superiore) a 15.000 euro, indipendentemente dal fatto che la stessa sia effettuata in unica soluzione, ovvero con più operazioni che appaiano collegate per realizzare una transazione frazionata. Dovrà poi (in ogni caso) provvedere all'adeguata verifica (anche a prescindere dalle predette condizioni) quando vi sia il sospetto di riciclaggio o di finanziamento del terrorismo, ovvero quando vi siano dubbi sulla veridicità o adeguatezza dei dati ottenuti dal cliente. Ancora, qualora questi sia una persona giuridica, un *trust* od un soggetto giuridico affine, l'*exchanger* dovrà altresì identificare e verificare l'identità del suo titolare effettivo, adottando misure che consentano di ricostruire, con ragionevole attendibilità, il suo assetto proprietario e di controllo.
In caso di instaurazione di un rapporto continuativo le norme dettate dal Decreto prevedono inoltre che l'obbligato debba acquisire informazioni anche sullo scopo e sulla natura del rapporto continuativo, verificando la compatibilità delle stesse con le informazioni acquisite autonomamente dall'obbligato. Un siffatto controllo andrà quindi operato anche in caso di prestazioni occasionali, allorché ci si trovi di fronte ad «un elevato rischio di riciclaggio». In tali casi è dunque stabilito che l'obbligato operi un controllo costante nel corso della durata di tutto il rapporto continuativo attraverso un'analisi delle operazioni effettuate e delle attività svolte dal cliente durante tutta la durata del rapporto, in modo da verificare che le stesse siano coerenti con la conoscenza che il soggetto obbligato ha del cliente[52]. Bene peraltro precisare che, ai sensi del comma 2 dell'art. 19 D.lgs. 90/2017, l'estensione delle verifiche, delle valutazioni e dei controlli predetti dovrà essere sempre commisurata «al livello di rischio rilevato» e che il Decreto prevede a tal fine due specifiche classificazioni di obblighi di identificazione e verifica: gli obblighi semplificati di adeguata verifica – o *simiplified due diligence* – regolati dall'art. 23 del D.lgs. 231/2007, e gli obblighi rafforzati di adeguata verifica – o *enanched due dili-*

[52] Cfr. artt. 17, 18 e 19 del D.lgs. 21 novembre 2007, n. 231, come modificato dal D.lgs. 25 maggio 2017, n. 90.

gence – regolati dall'art. 25 del medesimo Decreto. La prima delle richiamate disposizioni prevede in particolare che «in presenza di un basso rischio di riciclaggio o di finanziamento del terrorismo, i soggetti obbligati possono applicare misure di adeguata verifica della clientela semplificate sotto il profilo dell'estensione e della frequenza degli adempimenti previsti dall'art. 18». Per contro, il primo comma dell'art. 25 stabilisce che «i soggetti obbligati, in presenza di un elevato rischio di riciclaggio o di finanziamento del terrorismo, adottano misure rafforzate di adeguata verifica della clientela acquisendo informazioni aggiuntive sul cliente e sul titolare effettivo, approfondendo gli elementi posti a fondamento delle valutazioni sullo scopo e sulla natura del rapporto ed intensificando la frequenza dell'applicazione delle procedure finalizzate a garantire il controllo costante nel corso del rapporto continuativo o della prestazione professionale». Quanto quindi alla pregnanza dei controlli (semplificati ovvero rafforzati) demandati agli *exchanger*, è possibile osservare che, ai fini dell'applicazione delle misure semplificate di adeguata verifica (e fermo l'obbligo di commisurarne l'estensione al rischio rilevato in concreta effettività), l'articolo 23 del Decreto prevede che i soggetti obbligati debbano tener conto (tra l'altro) dei seguenti indici di basso rischio: a) indici di rischio relativi a tipologie di clienti, b) indici di rischio relativi a tipologie di prodotti, servizi, operazioni o canali di distribuzione, c) indici di rischio relativi ad aree geografiche. Il terzo comma della medesima disposizione soggiunge poi che le Autorità di vigilanza di settore e gli organismi di autoregolamentazione possano individuare ulteriori fattori di rischio da prendere in considerazione al fine di integrare o modificare l'elenco degli indici di rischio dinnanzi elencati. A tal riguardo è specificamente affermato che «nell'esercizio di queste stesse attribuzioni le autorità di vigilanza di settore individuano la tipologia delle misure di adeguata verifica semplificata che le banche e gli istituti di moneta elettronica sono autorizzati ad applicare in relazione a prodotti di moneta elettronica, ricorrendo, cumulativamente, le seguenti condizioni:

a) lo strumento di pagamento non è ricaricabile ovvero è previsto un limite mensile massimo di utilizzo di 250 euro che può essere speso solo nel territorio della Repubblica;

b) l'importo massimo memorizzato sul dispositivo non supera i 250 euro;

c) lo strumento di pagamento è utilizzato esclusivamente per l'acquisto di beni o servizi;

d) lo strumento di pagamento non è alimentato con moneta elettronica anonima;

e) l'emittente effettua un controllo sulle operazioni effettuate idoneo a

consentire la rilevazione di operazioni anomale o sospette;

f) qualora l'importo memorizzato sul dispositivo sia superiore a 100 euro, tale importo non sia rimborsato o ritirato in contanti».

Da quanto sopra riportato parrebbe dunque potersi evincere che le Autorità di vigilanza competenti (anche) per gli *istituti di moneta elettronica*, non siano autorizzati a prevedere procedure di identificazione e controllo semplificate nel caso in cui la *moneta elettronica* sia utilizzata anche per fini diversi dall'acquisto di beni e servizi, ad esempio per effettuare trasferimenti di somme da persona a persona (c.d. P2P *payment*). Ipotizzando perciò di assimilare (a questi soli fini) le diverse nozioni di valuta virtuale e moneta elettronica contenute nel Decreto, sembrerebbe potersi affermare (il condizionale è d'obbligo, in attesa delle necessarie norme attuative) che gli *exchanger* non potrebbero usufruire della procedura semplificata di identificazione e verifica di cui all'art. 23 del Decreto (atteso che le valute virtuali consentono, ovviamente, trasferimenti da persona a persona), dovendo invece attuare la procedura di verifica ordinaria ovvero (al più) la verifica rafforzata *ex* art. 25 del Decreto in caso di elevato rischio di riciclaggio.

10. Obblighi di segnalazione gravanti sull'*exchanger*: i motivi di sospetto e gli obblighi di riservatezza.

A norma del riformato articolo 35 del D.lgs. 231/2007«i soggetti obbligati, prima di compiere l'operazione, inviano senza ritardo all'UIF, una segnalazione di operazione sospetta quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa». La disposizione precisa in particolare che il sospetto debba essere desunto «dalle caratteristiche, dall'entità, dalla natura delle operazioni, dal loro collegamento o frazionamento o da qualsivoglia altra circostanza conosciuta, in ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, in base agli elementi acquisiti ai sensi del presente decreto». A tal proposito, si precisa che «il ricorso frequente o ingiustificato ad operazioni in contante [...] e, in particolare, il prelievo o il versamento in contante di importi non coerenti con il profilo di rischio del cliente costituisce elemento di sospetto», specificandosi poi che «le [...] comunicazioni non comportano responsabilità di alcun tipo anche nelle ipotesi in cui colui che le effettua non sia a conoscenza dell'attività criminosa sottostante e a prescindere dal fatto che l'attività illegale sia stata realizzata».

Da ultimo, non inutile segnalare che (come pure comprensibile) i soggetti

obbligati sono tenuti ad un obbligo di riservatezza tanto rispetto alle segnalazioni di operazioni sospette effettuate all'UIF che alle successive comunicazioni scambiate con l'Autorità di controllo. In specifico, ai sensi della disposizione di cui all'art. 39, comma 1 del Decreto «fuori dei casi previsti dal presente decreto, è fatto divieto ai soggetti tenuti alla segnalazione di un'operazione sospetta e a chiunque ne sia comunque a conoscenza, di dare comunicazione al cliente interessato o a terzi dell'avvenuta segnalazione, dell'invio di ulteriori informazioni richieste dalla UIF o dell'esistenza ovvero della probabilità di indagini o approfondimenti in materia di riciclaggio o di finanziamento del terrorismo». La disposizione di cui all'art. 41, comma 3 del Decreto prevede a sua volta che «il flusso di ritorno delle informazioni è sottoposto allo stesso divieto di comunicazione ai clienti o ai terzi previsto dall'articolo 39».

11. Le disposizioni sanzionatorie di carattere penale.

Il D.lgs. 90/2017 ha riformato profondamente il regime sanzionatorio già disciplinato dal D.lgs. 231/2007, limitando la possibilità di comminatoria penale alle sole condotte dotate di particolare gravità. La Legge delega n. 170/2016 (e, segnatamente, l'articolo 15, lett. h, n. 1 del provvedimento) stabiliva invero che il Governo dovesse ridurre l'area di rilevanza penalistica, anche (e soprattutto) in considerazione del principio del «*ne bis in idem* sostanziale» in relazione all'articolato apparato sanzionatorio amministrativo di nuova introduzione. Il Legislatore delegato aveva quindi il compito di «limitare la previsione di fattispecie incriminatrici alle sole condotte di grave violazione degli obblighi di adeguata verifica e di conservazione dei documenti perpetrate attraverso frode o falsificazione, e di violazione del divieto di comunicazione dell'avvenuta segnalazione, prevedendo sanzioni penali adeguate alla gravità della condotta e non eccedenti, nel massimo, tre anni di reclusione e 30.000 euro di multa». Siffatta linea di indirizzo ha quindi trovato attuazione nel novellato articolo 55 del D.lgs. 231/2007, che ai primi tre commi, ha introdotto tre nuove fattispecie delittuose intese a sanzionare gravi violazioni (i) degli obblighi di adeguata verifica; (ii) degli obblighi di conservazione delle informazioni raccolte e (iii) degli obblighi di fornire informazioni veritiere.

Ai sensi dell'art. 55, comma 1, D.lgs. 231/2007 è così previsto che «chiunque, essendo tenuto all'osservanza degli obblighi di adeguata verifica ai sensi del presente decreto, falsifica i dati e le informazioni relative al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale e all'operazione è punito con la reclusione da sei mesi a tre anni e con la multa da 10.000 euro a 30.000 euro. Alla mede-

sima pena soggiace chiunque essendo tenuto all'osservanza degli obblighi di adeguata verifica ai sensi del presente decreto, in occasione dell'adempimento dei predetti obblighi, utilizza dati e informazioni falsi relativi al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale e all'operazione». Siffatta fattispecie si applica perciò a condotte attive di falsificazione di dati ed informazioni relativi al cliente, al titolare effettivo, all'esecutore, allo scopo e alla natura del rapporto continuativo o della prestazione professionale, nonché all'utilizzo di dati e informazioni false, in occasione dell'adempimento degli obblighi di adeguata verifica. Bene precisare solo che, trattandosi di delitto, per l'integrazione della condotta di utilizzo di informazioni e dati falsi o non veritieri sarà ovviamente necessaria, in capo al soggetto obbligato, la conoscenza della falsità delle informazioni utilizzate.

Il secondo comma dell'articolo 55 prevede quindi che «chiunque, essendo tenuto all'osservanza degli obblighi di adeguata verifica ai sensi del presente decreto, acquisisce o conserva dati falsi o informazioni non veritiere sul cliente, sul titolare effettivo, sull'esecutore, sullo scopo e sulla natura del rapporto continuativo o della prestazione professionale e sull'operazione, ovvero si avvale di mezzi fraudolenti al fine di pregiudicare la corretta conservazione dei predetti dati e informazioni è punito con la reclusione da sei mesi a tre anni e con la multa da 10.000 euro a 30.000 euro». La fattispecie si applica dunque a colui che acquisisce o conserva dati falsi o non veritieri, ovvero a chi si avvalga di (non meglio descritti) mezzi fraudolenti al fine di pregiudicare la corretta conservazione dei dati e delle informazioni. Se in relazione alla prima delle condotte descritte è quindi necessaria (e sufficiente) la conoscenza – in capo all'agente – della natura falsa o non veritiera dei dati; per la seconda, costituita dal ricorso a mezzi fraudolenti, risulta particolarmente significativo l'elemento del dolo specifico del *fine di* pregiudicare la corretta conservazione dei dati.

Al terzo comma della disposizione in commento si introduce poi una fattispecie delittuosa a carico del cliente, prevedendosi che «salvo che il fatto costituisca più grave reato, chiunque essendo obbligato, ai sensi del presente decreto, a fornire i dati e le informazioni necessarie ai fini dell'adeguata verifica della clientela, fornisce dati falsi o informazioni non veritiere, è punito con la reclusione da sei mesi a tre anni e con la multa da 10.000 euro a 30.000 euro». Siffatta previsione sanzionatoria, che si apre con una clausola di riserva che fa salva l'applicazione di reati più gravi, concerne i soggetti che devono comunicare le informazioni necessarie all'assolvimento dell'adeguata verifica e, in tale sede, forniscano dati o informazioni non veritiere.

Rispetto all'opera di integrale riformulazione delle richiamate fattispecie di reato previste per i soggetti obbligati e per i clienti, il D.lgs. 90/2017 ha invece mantenuto inalterata l'ipotesi di reato di violazione del divieto di comunicazione, già previsto dal D.lgs. 231/2007 nella sua precedente formulazione. In particolare, il quarto comma dell'art. 55 prevede ancora testualmente che «salvo che il fatto costituisca più grave reato, chiunque, essendovi tenuto, viola il divieto di comunicazione di cui agli articoli 39, comma 1, e 41, comma 3, è punito con l'arresto da sei mesi a un anno e con l'ammenda da 5000 euro a 30.000 euro». Si tratta pertanto di una fattispecie contravvenzionale che, come tale, potrà risultare integrata anche laddove la "fuga di notizie" assuma caratteri meramente colposi.
Invariate rispetto alla precedente formulazione sono rimaste anche le più gravi fattispecie delittuose relative all'uso indebito ed alla falsificazione di carte di pagamento e di possesso, cessione o acquisizione di tali documenti di provenienza illecita. In particolare, il comma 5 dell'art. 55 seguita a stabilire che «chiunque al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da 310 euro a 1550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi». Si tratta insomma di delitti che, pur avendo a che fare con la repressione della circolazione di denaro illecito, hanno scarsa attinenza con la disciplina antiriciclaggio di cui all'art. 55 D.lgs. 231/2007. Nondimeno, le fattispecie di cui trattasi sono anche le uniche, tra quelle già disciplinate, ad aver trovato una qualche applicazione, e solo per esse l'intervento di riforma ha previsto un'ipotesi di confisca obbligatoria (anche nella forma per equivalente). In specifico, ai sensi del comma 6, seconda parte, dell'art. 55, «in caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al comma 5 è ordinata la confisca delle cose che servirono o furono destinate a commettere il reato, nonché del profitto o del prodotto, salvo che appartengano a persona estranea al reato, ovvero quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un

valore corrispondente a tale profitto o prodotto»[53].

12. Profili di concorso dell'exchanger nei reati di ricettazione, riciclaggio, impiego di denaro di provenienza illecita ed autoriciclaggio.

L'articolo 5 del D.lgs. 90/2017 ha ribadito espressamente l'operatività dell'art. 648 *quater* c.p. che disciplina la confisca per i reati di ricettazione, riciclaggio, impiego di denari di provenienza illecita ed autoriciclaggio, nonché quella dell'art. 25-*octies* D.lgs. del 231/2001 a disciplina della responsabilità amministrativa delle società e degli enti per le ipotesi delittuose di cui agli artt. 648, 648*bis*, 648*ter* e 648*ter*1. Allorché si intendano porre in rassegna le possibili conseguenze di carattere penale gravanti sul *virtual currency exchanger* in relazione alla normativa di contrasto al riciclaggio, non può quindi non operarsi anche un (pur rapido) cenno all'astratta possibilità di un suo concorso nei reati di ricettazione, riciclaggio, impiego di denaro di provenienza illecita ed autoriciclaggio previsti dal codice penale. Secondo indiscussa affermazione giurisprudenziale, per potersi dire integrato il concorso in siffatte ipotesi di reato è invero sufficiente la sussistenza, in capo al terzo, del dolo eventuale, ovverosia la rappresentazione del rischio che i beni o le somme ricevute siano di provenienza illecita. E' stato così testualmente precisato che «la consapevolezza dell'agente in ordine alla provenienza dei beni da delitti può essere desunta da qualsiasi elemento e sussiste quando gli indizi in proposito siano così gravi e univoci da autorizzare la logica conclusione che i beni ricevuti per la sostituzione siano di derivazione delittuosa specifica, anche mediata; e ciò anche perché, nel riciclaggio, è sufficiente anche il dolo eventuale, che si configura quando l'agente si rappresenta la concreta possibilità, accettandone il rischio, della provenienza delittuosa dei beni ricevuti»[54].

Muovendo perciò da siffatte coordinate interpretative occorre ponderare il rischio che la natura intrinsecamente "opaca" ed "anonima" delle critptovalute presti il fianco a legittimi dubbi di consapevolezza, in capo all'*exchanger* (o al diverso soggetto che compia l'operazione di conversione di valuta avente corso legale in valuta virtuale), della provenienza illecita dei fondi utilizzati per l'acquisto della *virtual currency* di volta in volta considerara. In specifico, sif-

[53] Per un primo (pur breve) commento alle disposizioni penali previste dalla novellata disciplina antiriciclaggio cfr. GIACOMETTI – FORMENTI, *La nuova disciplina del riciclaggio e di finanziamento del terrorismo*, *Dir. pen. cont.*, 7-8, 2017. Per un commento alle previgenti disposizioni sanzionatorie cfr. BEVILACQUA, *Le previsioni sanzionatorie della normativa antiriciclaggio*, in Alessandri (a cura di), *Reati in materia economica*, Torino, 2017, 377.

[54] Cfr. *ex multis*: Cass. pen., sez. II, 5 giugno 2015, n. 27806, in *Guida al diritto*, 2015, 44, 78 ss.; Cass. pen., sez. II, 24 ottobre 2013, n. 47147, in *Guida al diritto*, 2014, 6, 102 ss.; Cass. pen., sez. II, 17 giugno 2011, n. 25960, in *Giuda al diritto*, 2011, 44, 76 ss.

fatto rischio potrà essere tanto maggiore quanto maggiore risulti il livello di anonimato garantito dalla valuta virtuale opzionata, riconfermandosi come assai significativo in caso di conversione di moneta avente corso legale in criptovalute completamente anonime, quali Monero e ZCasch. Bene perciò sottolineare che, il coinvolgimento in delitti quali quelli di cui agli artt. 648, 648*bis*, 648*ter* e 648*ter*1, comporterà per l'*exchanger* (o per il diverso operatore in criptovalute che venga attinto dalla contestazione) sanzioni penali con limiti edittali assai più elevati rispetto a quelli previsti dalle fattispecie di cui all'art. 55 D.lgs. 231/2007 a cui pure si affiancherà, ai sensi dell'art. 648-*quater* c.p. (e con la sola esclusione del delitto di ricettazione di cui all'art. 648 c.p.) la confisca obbligatoria – anche nella forma per equivalente – dei beni che ne costituiscono il prodotto o il profitto. Allo stesso modo, laddove l'*exchanger* (o il diverso operatore in criptovalute che venga attinto dalla contestazione) operi in forma societaria o sia comunque riconducibile ad uno degli enti sottoposti al D.lgs. 231/2001[55], all'ente risulteranno applicabili le sanzioni disciplinate dall'art. 25-*octies* del medesimo Decreto legislativo[56].

13. Brevi considerazioni conclusive.

Nelle pagine che precedono si è tentato di gettare una prima (timida) luce sui possibili rischi penali generati da un fenomeno la cui rapida espansione rende assai difficile la più compiuta comprensione. Se la diffusione su scala mondiale delle monete virtuali ha fatto emergere con grande prepotenza la necessità di una loro regolamentazione, non si riscontra infatti ancora alcuna unanimità sulle concrete modalità di intervento. Siffatto ritardo rischia nondimeno di trasformare il mondo delle *cryptocurrencies* in un "paradiso virtuale" in cui andare impuniti grazie all'anonimato garantito in egual misura al piccolo criminale come alla grande società. In un siffatto contesto, lo stesso intervento da ultimo adottato a livello nazionale per estendere le norme antiriciclaggio ad alcuni operatori del settore, per quanto meritorio, rischia di risolversi in

[55] In particolare, come noto, ai sensi dell'art. 1, comma 2, del D.lgs. 231/2001 le disposizioni in esso previste «si applicano agli enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica».

[56] In particolare, a tenore di siffatta disposizione sanzionatoria «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. Nei casi di condanna per uno dei delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'art. 9, comma 2, per una durata non superiore a due anni. In relazione agli illeciti di cui ai commi 1 e 2, il Ministero della giustizia, sentito il parere dell'UIF, formula le osservazioni di cui all'art. 6 del decreto legislativo 8 giugno 2001, n. 231».

una "goccia" nel mare dell'illiceità digitale. La diffusione globale raggiunta dalle criptovalute rende infatti quanto mai necessario un coordinamento legislativo a livello globale, giacché ad un disallineamento normativo consegue la nascita di nuovi "paradisi" in cui poter operare in spregio a qualsivoglia procedura di identificazione, con conseguente frustrazione di tutti gli sforzi normativi intrapresi dal singolo paese.

Le criptovalute sono allora da demonizzare in assoluto? La rete ed i suoi prodotti rappresentano il futuro e non è certo osteggiandoli che si potranno eliminare (o quanto meno attenuare) i rischi connessi. Le difficoltà sorgono dalla complessità delle realtà fattuali ancora non sufficientemente esplorate e comprese. Per quanto di difficile scioglimento, la "matassa" del fenomeno criptovalutario esige tuttavia una soluzione che inizi subito a poter operare per poi poter seguitare ad evolversi (specie nella sua componente di natura amministrativa), ad evitarsi il proliferare di un nuovo *far west* 2.0 in cui l'assenza di regolamentazione sia, essa stessa, motivo di incentivo per il proliferare dei nuovi "pistoleri digitali". Per contro, se regolamentate e "domate" le criptovalute, grazie alla tecnologia blockchain, potrebbero addirittura rappresentare un efficace alleato nella lotta all'evasione fiscale.