SISTEMA PENALE

FASCICOLO 5/2020

ISSN 2704-8098

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 *Committe on Publication Ethics* (COPE) e fa proprie le relative linee guida.

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 sezo "*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.

5/2020

CYBERSECURITY E CRIPTOVALUTE. PROFILI DI RILEVANZA PENALE DOPO LA QUINTA DIRETTIVA

di Giovanni Paolo Accinni

1. Premessa.

La diffusione dello strumento criptovalutario rappresenta uno dei fenomeni più distintivi dell'epoca in corso. Secondo uno studio promosso tra il 2017 ed il 2019 riferito solo alla criptovaluta più rappresentativa, il BitCoin, quasi il novanta per cento dei cittadini americani ha contezza dell'esistenza delle *criptocurrencies*, mentre oltre il sessanta per cento dei più giovani (fascia d'età tra i diciotto ed i trentaquattro anni) dichiara di avere familiarità con il *trading* di moneta virtuale[1]. Tra i cittadini europei, oltre il dodici per cento dei polacchi ed il dieci per cento degli spagnoli dichiara di possedere criptovalute; ed anche in Italia la "febbre del BitCoin" parrebbe riguardare l'otto per cento della popolazione, ovvero quasi cinque milioni di persone[2]. La criptovaluta ha modificato ogni aspetto della vita quotidiana: se nel 2010 la prima transazione basata sulla *blockchain* era servita a pagare una pizza[3], nel corso degli anni il Bitcoin (ed i suoi fratelli) sono stati accettati come mezzo di pagamento per le tasse universitarie, per i servizi pubblici, sono stati equiparati alla moneta legale in alcuni Paesi del mondo[4] e rappresentano, grazie all'enorme capitalizzazione di cui godono, una rilevantissima fonte di risparmio.

Nondimeno, la nascita di tali strumenti, in assenza di una solida base regolamentare, ha attirato l'attenzione della criminalità organizzata, alla ricerca di metodologie innovative per sfuggire ai controlli antiriciclaggio e poter così reinvestire i

[1] In *medium.com*, 30 aprile 2019, a questo *link*. Lo studio è stato promosso da una società privata, la Blockchain Capital, a mezzo di un *survey* distribuito ad un campione di cittadini americani.
[2] In *statista.com*, a questo *link*. Lo studio è a cura della multinazionale ING.
[3] In *wired.it*, 3 gennaio 2019, a questo *link*.
[4] Cfr. questo *link*, in *www.ilsole24ore.com*, quanto all'emblematico caso del Giappone.

proventi delle proprie attività illecite. Allo stesso tempo, il sorgere del terrorismo internazionale di matrice islamica ha acceso i riflettori sul rischio di un asservimento del sistema criptovalutario al finanziamento di tali gruppi, con particolare attenzione alle donazioni provenienti da micro-sostenitori localizzati nei paesi occidentali.

Il presente lavoro percorre due direttrici: per un verso, cerca di mettere in luce le connessioni, invero crescenti, tra mondo delle criptovalute e *cybercrime*, con particolare attenzione ai più rilevanti casi di cronaca ed alle principali tipologie di reati commessi mediante l'uso delle *cryptocurrencies*; per altro verso, esso mira a dare una rappresentazione della normativa europea, con specifico riferimento alla Quarta ed alla Quinta Direttiva Anti-Riciclaggio, nonché dell'attuazione dei principi comunitari in ambito nazionale. Da ultimo, si procederà con una sintetica disamina degli strumenti di diritto penale interno, per valutarne l'efficacia rispetto alle nuove manifestazioni della criminalità organizzata sul mercato delle monete virtuali.

2. Cenni sul funzionamento del sistema criptovalutario.

2.1. La moneta elettronica nel sistema tradizionale[5].

In via preliminare, è opportuno chiarire come il termine "criptovaluta" non sia, in alcun modo, un sinonimo di "moneta elettronica". Quest'ultima, infatti, costituisce una nozione ben più ampia, con una portata semantica differente a seconda che si faccia riferimento al sistema tradizionale o a quello criptovalutario.

Nel sistema monetario classico la moneta elettronica non è altro che una disponibilità di potere d'acquisto registrata su un conto corrente acceso presso una Banca. Le disposizioni patrimoniali attive e passive sul suddetto conto vengono pertanto effettuate mediante la semplice "scrittura" del valore della transazione, senza la necessità di un trasferimento "fisico" di denaro. In altri termini, la moneta elettronica è uno strumento standard nella vita di ogni risparmiatore e uno dei capisaldi dell'apparato creditizio: la "dematerializzazione" del capitale favorisce sia la rapidità sia la sicurezza delle operazioni economiche.

Siffatto schema si regge sul ruolo – invero centrale e, prima della nascita delle criptovalute, ritenuto imprescindibile – di una Banca, che è chiamata a svolgere, in maniera centralizzata ed affidabile, le seguenti operazioni:

- Verificare la disponibilità economica sul conto del soggetto acquirente;
- Eseguire l'ordine di pagamento, perfezionando l'addebito della somma;
- Eseguire l'accredito sul conto del ricevente/venditore.

La Banca, in quanto ente terzo rispetto alla transazione, garantisce che all'operazione economica effettuata in moneta elettronica corrisponda una situazione reale sottostante: in particolare, ella deve certificare, mediante i dati custoditi nei propri

[5] Ci si permette di rinviare a ACCINNI G., *Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017)*, in *Archivio Penale*, fasc. 1/2018, pp. 2 ss.

server protetti, l'identità dei soggetti coinvolti e la presenza di adeguate provviste sul conto dell'acquirente. Solo attraverso l'intervento di una Banca il sistema tradizionale è in grado di rispettare la corretta corrispondenza tra valori numerici (moneta elettronica) e valori economici nelle operazioni effettuate.

2.2. La natura decentralizzata delle criptovalute.

Il tratto distintivo del sistema criptovalutario risiede nell'aver elaborato un meccanismo di superamento della gestione centralizzata delle transazioni. In altri termini, monete come il BitCoin, Ethereum o Ripple non richiedono l'intervento di una Banca (o di altro ente regolatore) per garantire la rappresentazione del valore economico: la tenuta del dei conti, infatti, è affidata in maniera "decentralizzata" a ciascun utente, in un procedimento che prende il nome di "*blockchain*".

Ma si proceda con ordine.

La *blockchain* è un insieme di "blocchi" di dati, ciascuno dei quali contiene, per ogni transazione, l'identità del pagante, del beneficiario e l'importo trasferito, nonché la data e l'ora dell'operazione economica e un riferimento al blocco precedente, che ne costituisce, in senso atecnico, il "dante causa". Ciascun blocco non costituisce pertanto una realtà isolata, bensì acquista significato nella misura in cui è concatenato a quello immediatamente precedente, e così via fino al vertice della catena, rappresentato dal c.d. "blocco genesi". Il primo esemplare di tale blocco, che costituisce la matrice di tutta la catena, è il primo elemento della *blockchain* del BitCoin, la più famosa criptovaluta mondiale, creato dal misterioso sviluppatore Satoshi Nakamoto il 3 gennaio 2009[6].

Una volta inserito nella catena, il blocco non è più modificabile. Invero, i dati in esso contenuti non sono solo espressione della singola operazione economica, bensì costituiscono anche l'origine delle transazioni a valle, che ricevono credito solo in quanto inserite nella medesima *blockchain*.

Occorre altresì chiarire[7] come operi il meccanismo di validazione delle operazioni effettuate in criptovaluta. Nel momento in cui un soggetto effettua un'operazione in BitCoin, egli deve comunicare al sistema il proprio conto di addebito, l'importo della transazione e il conto di accredito. Tuttavia, la "fattibilità" dell'operazione non viene certificata da un ente terzo (ad es. una Banca), bensì dagli altri utenti della *blockchain*. Il sistema prevede infatti che chi effettua l'operazione debba trasmettere una chiave di accesso in forma "criptata": gli altri utenti saranno in conseguenza chiamati a decriptare siffatta chiave d'accesso attraverso la risoluzione di un complicato problema matematico

[6] L'identità di Nakamoto, nonostante le numerose congetture, è ancora ignota. Lo sviluppatore, che è ritenuto il principale possessore di BitCoin al mondo, con un patrimonio stimato in circa 1 milione BTC, è scomparso dal mercato nel 2011: nondimeno, l'intera *blockchain* si è diramata dal primo blocco da egli estratto e continua a svilupparsi come progressiva sedimentazione sul blocco genesi.

[7] Seppur sommariamente, non potendosi in tale sede affrontare nel dettaglio il meccanismo di validazione della *blockchain*, il cui sviluppo è connotato da un alto livello di tecnicismo ed è, in ultima analisi, estraneo agli scopi della presente trattazione.

e il sistema prevede quale "stimolo premiale" che il primo soggetto che riesca a decriptare il codice ed a verificare la fattibilita` dell'operazione venga ricompensato con un determinato ammontare di Bitcoin. In particolare, i soggetti 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. Le operazioni validate si innestano dunque sulla *blockchain* esistente, la quale trova la propria legittimazione nell'insieme consequenziale dei blocchi, singolarmente e progressivamente oggetto di controllo.

2.3. I soggetti.

La complessità del sistema *blockchain* evidenzia – pur nella teorica parità dei ruoli – una differenziazione soggettiva tra i vari utenti della rete. Nell'intento di identificare alcune figure tipiche, si possono agevolmente distinguere:

- *Miners*

Sono utenti della rete, in possesso di sistemi di calcolo ad alte prestazioni, che si dedicano al controllo della crittografia e alla validazione della rete. In linea teorica, qualsiasi utente della rete può svolgere la funzione di "minatore"; in pratica, solo un gruppo di utenti in possesso dell'adeguata strumentazione può dedicarsi all'attività di validazione. La ricompensa per i *miners* è l'erogazione, da parte del sistema, di BitCoin in loro favore: dal punto di vista concettuale, dunque, l'attività di *mining* frutta una percentuale del tutto assimilabile ad una commissione.

Il funzionamento del sistema scoraggia l'eventuale proliferare di *miners* fraudolenti. La validazione di un blocco falso, infatti, comporterebbe un enorme dispendio di energie, nonché l'utilizzo di calcolatori infinitamente più potenti di quelli necessari per l'ordinario sviluppo della catena: il "minatore" dovrebbe infatti riuscire ad innestare il proprio blocco falso sulla *blockchain* esistente e, pertanto, alterare quantomeno l'insieme di dati immediatamente precedente al proprio. La scoperta di un'operazione illegale, infine, farebbe crollare la fiducia nel BitCoin e il valore della moneta, azzerando la spendibilità del vantaggio economico illecitamente ottenuto.

- *Users*

Gli *users* sono persone fisiche o giuridiche 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.

Le dimensioni di ciascun portafoglio di BitCoin sono estremamente variabili: esistono investitori occasionali, detentori di pochi BitCoin o addirittura di frazioni di moneta, e grandi investitori, conosciuti nel gergo come "balene", che secondo la stima di *Bloomberg*, nel corso del 2017 detenevano oltre il 40% della criptovaluta in

circolazione[8]. La presenza di grandi concentrazioni di moneta virtuale rende il mercato estremamente sensibile alle scelte di investimento (o disinvestimento) di tali soggetti.

- *Virtual currency exchangers* e *wallet providers*

Sono soggetti professionali, che forniscono agli *users* una serie di servizi imprescindibili per entrare nel mercato delle criptovalute. Gli *exchangers* sono essenzialmente dei cambiavalute, che consentono la conversione della moneta virtuale in moneta legale (e viceversa) dietro il pagamento di una commissione. L'attività di tali soggetti, in origine libera, è stata progressivamente oggetto di regolamentazione da parte degli ordinamenti sovranazionali e nazionali.

I *wallet providers* sono societa` che forniscono agli *users* i portafogli elettronici, cioè dei meccanismi per detenere, immagazzinare e trasferire i BitCoin o le altre criptovalute. Nello specifico, oltre a fornire l'*e-wallet*, il *wallet provider* conserva le chiavi private del conto, agevola le operazioni degli *users* e degli *exchanger*s e si comporta, in ultima analisi, come un intermediario.

- Fornitori di servizi collaterali

Sussistono poi una serie di soggetti diversi da quelli tipizzati, che forniscono numerosi servizi accessori rispetto al *trading* di criptovalute. In tale categoria possono ricomprendersi i servizi di consulenza, assicurativi e di gestione del portafoglio. La diffusione di tali soggetti è condizionata dal livello di regolamentazione delle criptovalute nei singoli ordinamenti nazionali.

2.4. L'anonimato nella blockchain.

Uno dei principali vantaggi della *blockchain* è la capacità di coniugare la trasparenza della rete – e, dunque, l'identificabilità di ogni operazione compiuta lungo la catena – con l'anonimato garantito ai singoli operatori. In altri termini, benché ogni utente della rete possa visionare in qualunque momento tutte le operazioni in Bitcoin intervenute in un determinato arco temporale, la tracciabilita` delle singole operazioni non giunge sino al punto di consentire di risalire alla reale identita` degli investitori. Infatti, allorquando si effettui un pagamento, la *blockchain* tiene nota della chiave pubblica del pagante e l'importo dell'operazione, mentre la chiave privata (la password) non viene pubblicata sulla *blockchain*, ma rimane nella esclusiva disponibilita` del titolare del portafoglio.

Con riferimento a tale sistema, alcuni commentatori hanno sostenuto che esso non garantisca un anonimato completo ma piuttosto uno "pseudo-anonimato"[9]: in caso di operazioni sospette, l'utilizzo di appositi software potrebbe infatti consentire alle Autorità di ricollegare il numero di chiave all'identità anagrafica dell'investitore. Nondimeno, la generazione di plurime chiavi pubbliche (i.e. visibili) collegate alle chiavi

---

[8] *The Bitcoin Whales: 1,000 People Who Own 40 Percent of the Market*, in *bloomberg.com*, 8 dicembre 2017.

[9] 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 perfect knowledge of all transactions*».

private (i.e. segrete) renderebbe tale accertamento molto più complesso. A ciò si aggiunga la nascita di un nuovo settore, quello del c.d. *mixing*: 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 destinazione di ogni singolo pagamento[10].

La volontà di garantire la *privacy* degli investitori e l'esigenza di perseguire la trasparenza del sistema finanziario costituisce (come si avrà modo di vedere) uno dei punti maggiormente controversi della regolamentazione delle criptovalute.

2.5. AltCoin *e criptovalute statali.*

Oltre al BitCoin, che rappresenta tutt'oggi lo strumento criptovalutario di maggior diffusione sul mercato, l'evoluzione delle tecnologie ha portato alla nascita di ulteriori monete virtuali, ciascuna basata su una propria *blockchain*. L'insieme di queste criptovalute è altresì noto come *AltCoin* (ovvero "*alternative coin*", monete alternative rispetto al BitCoin).

Tra le più note, si annoverano *Litecoin* (2011), *Ethereum* (2015), *Ripple* (2012), *Dash* (2014) e *Monero* (2014). Molte di esse sono apprezzate dagli investitori per l'alto grado di *privacy*, la maggiore rapidità delle transazioni, la versatilità delle operazioni: in particolare, *Ethereum* supporta non solo il *trading* meramente finanziario ma anche la sottoscrizione di *smart contracts* a mezzo della criptovaluta.

Negli ultimi anni la crescente attenzione delle Autorità Pubbliche verso il mondo delle criptovalute ha prodotto alcuni tentativi di *cryptocurrencies* statali. Rispetto al modello tradizionale, decentralizzato, tali esperimenti vedono l'intervento, totale o parziale, di un'Autorità di regolamentazione e presentano, pertanto, numerose difformità dalla struttura di base di una moneta virtuale. Significativo, inoltre, che siffatte sperimentazioni siano avvenute in paesi in forte difficoltà economica o soggetti a sanzioni.

Un primo, significativo caso è rappresentato dal *Petro*, moneta nata in Venezuela sotto il regime del presidente Maduro. Il *Petro* ha la funzione di gestire le transazioni finanziarie verso l'estero ed è dunque "vincolato" *ab origine* quanto agli scopi per i quali può essere utilizzato.

Rispetto alle criptovalute "classiche", il *Petro* non risulta garantito dalla sola *blockchain*, bensì anche da beni fisici di proprietà dello Stato: riserve aurifere, petrolifere, di gas e diamanti, che costituiscono il "controvalore" della moneta. Per un verso, siffatta scelta tutela l'economia nazionale da eccessive oscillazioni e speculazioni; per altro verso, viene meno uno dei cardini del sistema criptovalutario, rendendo il *Petro* molto più affine ad una moneta dematerializzata che ad una *cryptocurrency*.

---

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

Negli ultimi anni, a più riprese, l'Iran ha annunciato la volontà di dotarsi di una propria moneta virtuale per aggirare le sanzioni imposte dagli Stati Uniti. A dicembre 2019 il presidente Rouhani, intervenuto alla Conferenza dei paesi islamici in Malesia, ha dichiarato che "*il mondo musulmano dovrebbe avanzare delle misure per tutelarsi dal dominio del dollaro statunitense e dal regime finanziario americano*"[11].

Analoghe misure – a metà strada tra moneta virtuale e dematerializzazione del conio statale – sono in fase di studio in vari paesi: tra i primi a muoversi vi è l'Uruguay, la cui banca centrale ha avviato un progetto sperimentale fin dal 2017.

3. I problemi di sicurezza: alcuni casi rappresentativi.

Il proliferare delle criptovalute ha attirato l'attenzione della criminalità organizzata, il cui sviluppo verso il *cybercrime* è oggetto di crescenti preoccupazioni a livello sovranazionale. In effetti, lo pseudoanonimato delle *cryptocurrencies*, la possibilità di usufruire di servizi di *mixing* e di effettuare transazioni rapide ed irreversibili a livello transnazionale costituiscono elementi di primario interesse non solo per gli investitori "legali", ma anche e soprattutto per chi abbia interesse a celare l'origine illecita dei proventi e riciclare denaro riducendo il rischio di essere tracciato.

Già nel corso del 2014 il FAFT ha segnalato come "*il protocollo Bitcoin non richiede e non provvede all'identificazione e alla verifica dei partecipanti e non genera un registro cronologico delle transazioni che abbia corrispondenza con la loro identità nel mondo reale*. *Non c'è un organismo centrale di vigilanza e manca un software antiriciclaggio per monitorare ed identificare sospetti schemi fraudolenti*"[12]. E ancora, nel proprio rapporto annuale sul crimine cibernetico 2017, l'Europol ha sottolineato che "*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 [...]"[13].

Bene, per opportunità di classificazione, è utile distinguere tra le condotte di *cybercrime* nelle quali le criptovalute costituiscono un mero elemento accidentale della fattispecie e condotte nelle quali, al contrario, il fatto di reato è posto in essere mediante un attacco diretto alla *blockchain* o ai portafogli virtuali. Infatti, mentre il primo gruppo rappresenta la trasposizione "*online*" di illeciti comuni, la seconda tipologia ha richiesto un intenso sforzo di adeguamento sia a livello di sicurezza delle transazioni sia sul versante della regolamentazione del mercato delle criptovalute.

---

[11] In *cointelegraph.com*, 20 dicembre 2019 (consultabile qui).

[12] FAFT Report "*Virtual Currencies Key Definitions and Potential AML/CFT Risks*", in *faft-gafi.org*, giugno 2014, p. 9 (traduzione a cura dell'autore).

[13] Cfr. *Internet organised crime threat assessment* (IOCTA) 2017, in *www.europol.europa.eu*.

3.1. Criptovalute come elemento accidentale della fattispecie.

Siffatto gruppo ricomprende reati a natura comune, quali truffe, scommesse illegali, pedopornografia, compravendita di merci o servizi illegali, estorsione, la cui diffusione sul *web* è stata agevolata dalla comparsa delle criptovalute. Nello specifico, le *criptocurrencies* rappresentano (negli schemi più semplici) il metodo di pagamento più richiesto dai criminali quale contropartita della propria attività illecita.

La cronaca degli ultimi anni fornisce numerosi esempi in tal senso. A maggio 2017 il c.d. attacco *WannaCry* ha dato vita ad un'epidemia informatica sui computer dotati del sistema operativo Microsoft Windows. Il virus era capace di criptare i file presenti sui computer e di chiedere un riscatto in Bitcoin per decriptarli: in altri termini, esso rendeva inservibile il *pc* ed esigeva un pagamento in moneta virtuale per liberarlo dal blocco virale. L'attacco *WannaCry* ha colpito numerose istituzioni a livello globale, quali FedEx, Telefónica, Renault e il Ministero dell'interno russo. Il settore degli attacchi *ransomware* è in continua crescita: nel corso del 2016 essi sono aumentati di più del 50% rispetto al 2015 e 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[14]. Ancor più di recente, l'azienda canadese *LifeLabs*, che ogni anno effettua oltre 112 milioni di test di laboratorio, ha dovuto corrispondere un'ingente somma, il cui esatto importo è rimasto ignoto, per ottenere la restituzione dei dati sanitari di oltre 15 milioni di pazienti[15].

Le conseguenze di un attacco *ransomware* divengono esponenzialmente più grandi al crescere della dimensione dell'Ente colpito. Al di là del danno economico rappresentato dal prezzo del riscatto, le società devono altresì affrontare il delicato tema del risarcimento alle persone fisiche i cui dati sono stati aggrediti dall'attacco hacker, nonché fronteggiare il crollo reputazionale. La necessità di un approccio preventivo rispetto ai fenomeni *ransomware* ha indotto sempre più *big companies* ad implementare i servizi di sicurezza informatica e ad accelerare l'adeguamento alle sempre più stringenti normative in materia di privacy.

Su un altro versante, le notizie di cronaca riportano sempre più vicende di rapimenti nei quali i sequestratori, nel chiedere il riscatto, hanno voluto essere pagati in BitCoin o in altra moneta virtuale. Tra i casi più noti, si segnalano:

– Ucraina, 2017. Il Sig. Pavel Lerner, cittadino russo e dirigente di una società attiva nel settore delle criptovalute, viene rapito in Ucraina da una banda di uomini armati, che richiede un milione di euro in Bitcoin per la sua liberazione. A pagamento avvenuto, il Sig. Lerner è stato rilasciato senza aver subito lesioni, ma i malviventi hanno fatto perdere le loro tracce e la polizia ucraina non è mai riuscita a risalire all'impiego della somma[16];

---

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

[15] In *startmag.it* (a questo *link*) e in *accademiaitalianaprivacy.it* (a questo *link*).

[16] In *businessinsider.com*, a questo *link*.

– Thailandia, 2018. Un turista russo, le cui generalità sono rimaste ignote, è stato sequestrato e sottoposto a sevizie fino a quando non ha acconsentito a trasferire oltre 100.000 euro in BitCoin al suo rapitore: una somma apparentemente contenuta ma in realtà estremamente elevata per gli standard thailandesi. Il rapitore è stato rintracciato poche ore dopo, poiché aveva con sé il computer della vittima, la cui scia digitale era stata seguita dagli investigatori, oltre ad altri beni sottratti al turista[17];

– Norvegia, 2019. La moglie di Tom Hagen, magnate nel settore dell'energia, con un patrimonio stimato in 1,7 miliardi di corone (174 milioni di euro), viene rapita nella casa di famiglia, a 20 km da Oslo: i malviventi hanno chiesto come riscatto la corresponsione di 9 milioni di euro nella criptovaluta "Monero"[18]. Si tratta del primo caso nel paese nordico, nel quale il tasso di criminalità è tra i più bassi del mondo.

Il vantaggio di percepire un riscatto in criptovaluta risiede nella possibilità di un agevole sparizione del denaro, nonché nella garanzia di (pseudo)anonimato. Inoltre, gli strumenti tradizionali, quali il congelamento dei conti correnti dei familiari dei rapiti, si rivelano molto meno efficaci, poiché la mappatura degli *e-wallet* è un'operazione estremamente complessa, soprattutto in presenza di patrimoni articolati e di grandi dimensioni.

Da ultimo, un sensibile incremento dell'utilizzo di valute virtuali è stato altresì registrato nell'ambito della compravendita di servizi pedopornografici online, di carte di credito clonate e in tutti i c.d. *darknet markets*, siti internet presenti nel c.d. *dark web* ed in cui viene venduta la più ampia tipologia di merci e di servizi illeciti, tra cui armi, droga e servizi di *hacking*[19].

3.2. Criptovalute come "elemento costitutivo"[20] del reato.

A questo secondo gruppo afferiscono tutte quelle condotte illecite nelle quali la criptovaluta non costituisce una semplice modalità alternativa di ottenimento del provento, bensì rappresentano l'oggetto materiale del reato. In esso possono essere distinte tre macroaree: il furto di criptovalute, il riciclaggio di denaro e il finanziamento del terrorismo internazionale.

La prima area ingloba i fenomeni di sottrazione di criptovalute sia dagli *e-wallet* degli utenti sia dalle piattaforme di investimento. Secondo le stime del portale *CipherTrace*, nel corso del 2019 il totale delle perdite connesse al furto ed alle frodi sulle criptovalute ha raggiunto l'impressionante cifra di 4.4 miliardi di dollari: un quantitativo di denaro enorme, che rappresenta solo una parte dei proventi illeciti connessi al mondo

---

[17] Cfr. questo *link* in *quotidiano.net*.

[18] L'indagine è ancora in corso, stando al sito *www.iol.co.za*.

[19] Un'ampia casistica è presente nel report IOCTA 2019, a cura di Europol.

[20] Si precisa fin da subito che il termine "elemento costitutivo" non è da intendersi in senso tecnico, quale nozione di diritto penale. Con tale locuzione si fa infatti riferimento a tutti quei casi in cui la criptovaluta non è un semplice mezzo alternativo alla moneta tradizionale nel compimento del reato, bensì costituisce un tratto caratterizzante ed insostituibile della concreta manifestazione criminosa.

delle *cryptocurrencies*[21]. I meccanismi di furto variano dalla diffusione di virus che infettano i terminali degli investitori, rivelando agli *hacker* le chiavi crittografiche, a veri e propri attacchi "di massa" sui server delle piattaforme, in modo tale da avere accesso a tutti i portafogli attivi e portare a termine la sottrazione di grandi somme con una sola operazione. Non è peraltro escluso l'utilizzo di siti di larga diffusione per la perpetrazione dei suddetti reati: nel corso del 2020, ad esempio, sono stati registrati molti casi di sottrazione dei canali *Youtube* ai legittimi proprietari. I ladri, dopo aver cancellato il materiale presente, sono soliti ricondividere un video nel quale promettono la distribuzione gratuita di criptovalute in cambio delle chiavi di accesso[22]. L'effetto dirompente che una simile condotta può ingenerare su investitori poco esperti, nonché sul vasto pubblico di *Youtube*, ha spinto numerose piattaforme a richiedere una *policy* più stringente sulla titolarità degli account video[23].

Tra i principali casi di furto di criptovalute in anni recenti[24] si annoverano:

- *Binance*: un buco da 41 milioni di dollari[25]

In data 8 maggio 2019 la piattaforma *Binance*, uno dei principali siti di *exchange* al mondo, è stata oggetto di un attacco *hacker*, che ha sottratto oltre 7000 BitCoin per un controvalore stimato di 41 milioni di dollari. I *cyber*-criminali hanno utilizzato varie tecniche, tra le quali il c.d. *phishing* (invio di false comunicazioni a mezzo *e-mail*) e l'introduzione di virus nella piattaforma. L'attacco a *Binance* ha messo in luce una delle principali debolezze del sistema *blockchain*: una volta inserito nella catena, il blocco di operazioni, anche se contenente furti e frodi, non è revocabile, se non pregiudicando l'intero meccanismo fin dal c.d. blocco genesi.

Il CEO di *Binance*, Changpeng Zao, ha dichiarato di aver provato a convincere i *miners* a forzare il blocco ma di essersi dovuto arrendere di fronte ai limiti intrinseci del sistema *blockchain*. La piattaforma ha dovuto ripianare le perdite subite dagli utenti con le proprie riserve personali, nonché sospendere le operazioni per alcuni giorni. Benché la chiave pubblica dell'indirizzo sul quale i BitCoin rubati sono stati accreditati sia stata identificata, non è stato possibile risalire alle persone fisiche beneficiarie dell'attività illecita.

- La piattaforma italiana: il caso Nano

La piattaforma italiana *BitGrail* era uno dei principali "cambiavalute" sul *web*: essa consentiva di scambiare le monete virtuali in una nuova valuta, chiamata "Nano", ritenuta particolarmente conveniente dagli investitori. Fin dall'autunno 2017 venivano registrati episodi di malfunzionamento sulla piattaforma, con casi di considerevoli ritardi nei prelievi e negli accrediti delle somme. Tali disservizi aumentavano in concomitanza con il picco del valore dei Nano (circa 30 euro per ogni unità) a gennaio 2018, quando numerosi utenti registravano un'errata contabilizzazione "al ribasso" dei

---

[21] Uno studio di *Bloomberg* stima che dal 2017 quasi 10 miliardi di dollari in criptovalute sia stato oggetto di furto.

[22] In *innovazione.tiscali.it* (consultabile qui).

[23] Si veda, ad esempio, l'appello della piattaforma Binance (su *cryptonomist.ch*, 21 febbraio 2020).

[24] Ormai datate risultano essere le vicende di Liberty Dollar, BTC-e, nonché il celebre caso di Silk Road.

[25] Cfr. *www.ilsole24ore.com* dell'8 maggio 2019.

fondi visibili sui conti, chiedendo conseguentemente al gestore di correggere l'errore. Per tutta risposta, in data 12 gennaio 2018 il titolare della piattaforma bloccava ogni operazione verso i conti esterni, bloccando di fatto le somme sulla piattaforma e asserendo di dover procedere alle operazioni di verifica della clientela imposte dalla normativa antiriciclaggio prima di poter riattivare la possibilità di prelievo. Infine, il 9 febbraio 2018 il gestore annunciava la sparizione di oltre 17 milioni di Nano, pari a circa 120 milioni di euro, dai portafogli degli utenti di *BitGrail*: i fondi asseritamente scomparsi, pari a circa l'80% dei Nano sulla piattaforma, sarebbero stati oggetto di un non meglio identificato attacco *hacker*. A seguito dei dubbi sollevati dalla stampa specializzata, gli utenti proseguivano nel chiedere spiegazioni alla piattaforma: tuttavia, la scarsa trasparenza di *BitGrail* proseguiva. Nei mesi successivi il gestore proponeva degli accordi transattivi estremamente sconvenienti per gli investitori, improntati sulla rinuncia alla maggior parte dei crediti e sulla conversione del residuo in una nuova criptovaluta.

A seguito dell'istanza di alcuni investitori, il Tribunale di Firenze[26] ha dichiarato il fallimento di *BitGrail*, riconoscendo le gravi responsabilità del gestore nel non aver predisposto adeguate misure di sicurezza contro l'ammanco dei Nano e nell'essersi, al contrario, astenuto dal salvaguardare i conti degli utenti, provvedendo invece a trasferire parte dei propri fondi personali su piattaforme terze. In particolare, è stato ricostruito che fin da luglio 2017 il gestore aveva registrato numerosi episodi di "doppi prelievi", ovvero situazioni nelle quali, a fronte di un unico ordine di ritiro delle somme, il c.d. nodo Nano di riferimento rilasciava plurime volte la cifra richiesta. Pur essendo a conoscenza del malfunzionamento mesi prima del comunicato ufficiale, il gestore non aveva apportato le opportune modifiche al sistema. La sua inazione aveva dunque determinato l'aggravamento del problema, dal quale egli aveva cercato (invero maldestramente) di disimpegnarsi in via transattiva.

Con riferimento ai reati di riciclaggio, è opportuno sottolineare che il reimpiego di capitali illeciti nel settore criptovalutario rappresenta uno dei principali canali del *cybercrime*. Esso, infatti, costituisce una modalità di investimento dei proventi da reato che garantisce alle consorterie criminali maggiore anonimato e minori rischi rispetto agli schemi tradizionali, consentendo inoltre lo spostamento di grandi somme di denaro verso giurisdizioni più compiacenti o meno attrezzate nella lotta al riciclaggio[27].

Quanto agli scopi della presente trattazione, i reati in esame possono essere distinti in due macroaeree: il riciclaggio operato su piattaforme legali, inconsapevoli del meccanismo fraudolento in atto; il riciclaggio operato mediante piattaforme asservite alla criminalità, che schermano la propria attività illecita dietro una parvenza di legalità.

---

[26] Tribunale di Firenze, sez. fallimentare, sentenza del 21 gennaio 2019, n. 18. La suddetta sentenza ripercorre anche le fasi salienti della vicenda ed è la fonte principale per la ricostruzione dei fatti.

[27] Si veda HOUBEN R.– SNYERS A., *Cryptocurrencies and blockchain - Legal context and implications for financial crime, money laundering and tax evasion*, in *European Parliament – Study Requested by the TAX3 committee*, Bruxelles 2018, p. 13.

Secondo uno studio di *Chainanalysis*[28] nell'anno 2019 le entità criminali avrebbero spostato un totale di 2,8 miliardi di dollari in Bitcoin negli *exchange* di criptovalute. I siti maggiormente utilizzati sarebbero stati Binance e Huobi, due delle più grandi piattaforme di *trading* al mondo, sui cui *server* sarebbero transitati oltre 1,5 miliardi di capitale illecito. Lo studio ha consentito di porre in luce alcune interessanti caratteristiche di siffatto riciclaggio: infatti, mentre gli account attivi nell'inviare denaro sospetto sono stati oltre 300 mila, i destinatari finali di tali fondi sono stimati in soli 810 account. Un numero ridotto di investitori, dunque, che manifesta l'esistenza di un meccanismo accentrato di gestione dei proventi criminali. Il medesimo studio ha identificato una lista di broker, denominata "*Rogue 100*", particolarmente attivi nel riciclaggio di denaro. Nondimeno, la lista rappresenterebbe solo una piccola parte dei broker coinvolti in attività criminali; allo stesso modo, i soggetti identificati potrebbero operare su altre piattaforme sotto pseudonimo, sfuggendo così alle indagini internazionali in corso.

Tra le piattaforme illegali, merita particolare attenzione il caso di *Helix*, uno dei principali servizi di *cyberlaundering* disponibili nel *dark web*. Il sito in esame forniva, dietro il pagamento di una commissione del 2,5% dell'importo, un servizio di *mixing* volto ad occultare l'origine delle criptovalute e a favorirne un reimpiego sul mercato, come se fossero "monete nuove". *Helix*, attiva dal 2014 al 2017, garantiva la totale pulitura delle criptovalute in meno di un'ora, profilandosi come strumento estremamente appetibile per la criminalità organizzata, che attraverso il passaggio sulla piattaforma era in grado di schermare l'origine del denaro[29]. A febbraio 2020 un cittadino statunitense, ritenuto il gestore di *Helix*, è stato arrestato dall'FBI con l'accusa di riciclaggio di denaro e di esercizio abusivo della professione di intermediario finanziario. Secondo le stime degli investigatori, egli avrebbe contribuito a ripulire oltre 300 milioni di dollari, collaborando con siti criminosi come il *dark market Alpha Bay*"[30].

Infine, negli ultimi anni le preoccupazioni della comunità internazionale si sono focalizzate sul possibile utilizzo del mercato criptovalutario per il finanziamento del terrorismo internazionale. Rispetto ai fenomeni criminosi già analizzati, il finanziamento del terrorismo a mezzo delle *cryptocurrencies* non sembra averne ancora raggiunto né la dimensione economica né la diffusione capillare, affidandosi in primo luogo a micro-donazioni da parte di singole persone fisiche. Nondimeno, la pericolosità di tale *modus operandi* è evidente: intercettare migliaia di piccoli donatori, che versano somme ridotte, può infatti risultare molto più difficile di interrompere i grandi flussi di denaro che caratterizzano altre branche del *cybercrime*.

La prima organizzazione ad aver compreso le potenzialità delle criptovalute è stata *Al Sadaqah*. Il gruppo raccoglieva i combattenti attivi nel nord della Siria contro il

---

[28] *Think tank* indipendente che fornisce supporto a Governi ed Organizzazioni Internazionali nella comprensione del fenomeno criptovalutario e nell'elaborazione di strategie di contrasto al *cybercrime*: *www.chainalysis.com*.

[29] Un approfondimento sul funzionamento di *Helix* e di altre piattaforme analoghe è presente in FLORINDI E., *Criptovalute: manuale di sopravvivenza*, Reggio Emilia 2018.

[30] In *www.justice.gov* (consultabile qui).

regime di Assad, ed era noto per le connessioni con realtà più grandi, quali *Al Qaeda* e *Isis*. La campagna è stata indirizzata ai finanziatori occidentali utilizzando i più comuni canali social (Whatsapp, Telegram) ed è circolata per svariati mesi su account ritenuti vicini al terrorismo islamico.

A seguire, la stessa *Al Qaeda*, entrata in crisi di liquidità dopo la morte del *leader* Osama Bin Laden, ha lanciato un appello sul suo *web magazine al-Haqiqa* (la Verità), invitando i lettori ad usare i BitCoin per finanziare l'organizzazione. Un analogo sollecito è stato rivolto dall'ISIS, attraverso un banner pubblicitario su uno dei suoi siti d'informazione, a gennaio 2018[31].

Tra i casi di cronaca più rilevanti, ci si permette menzionare la vicenda della cittadina statunitense Zoobia Shabaz, assistente di laboratorio di Long Island, radicalizzatasi nel corso di un viaggio in Siria nel 2015 ed arrestata a New York nel 2017. Secondo l'ipotesi accusatoria la ragazza avrebbe dapprima sottratto un quantitativo di Bitcoin pari a circa 75.000 dollari, per poi tentare di trasferirlo a degli esponenti dell'ISIS sia via *web* sia attraverso il trasporto di valigette di contanti all'estero[32]. Più di recente, gli attacchi terroristici di Pasqua 2019 in Sri Lanka, con oltre 250 vittime e rivendicati dall'ISIS, parrebbero essere stati finanziati attraverso il *trading* di BitCoin su una piattaforma canadese[33].

Al di là di simili vicende, il finanziamento del terrorismo a mezzo di criptovalute costituisce un fenomeno ancora marginale. I canali principali rimangono pertanto il *money transfer* e, principalmente, l'*hawala*, il tradizionale meccanismo di trasferimento di denaro vigente da tempo immemore nel mondo islamico e basato sulla fiducia reciproca. Il "vantaggio" dell'*hawala* risiede nella circostanza che esso non richiede il passaggio fisico della somma, essendo sufficiente un ordine di pagamento (ad es. in un paese europeo) ed un soggetto pronto ad eseguirlo con fondi propri nello stato di destinazione. I conti tra l'ordinante e l'intermediario verranno poi compensati o saldati in un momento diverso rispetto a quello dell'effettiva consegna del denaro (o dei beni) al destinatario finale.

4. La normativa europea e la Quinta Direttiva.

L'opportunità di regolamentare le criptovalute era stata posta all'attenzione del legislatore europeo da numerosi organismi internazionali. Invero, già nel 2012 la BCE aveva definito le criptovalute come "*una tipologia di moneta digitale non regolamentata, che è gestita e controllata dai suoi sviluppatori ed usata ed accettata dai membri di una specifica comunità digitale*"[34]; la stessa Istituzione, nel corso di un approfondimento di febbraio 2015 aveva ulteriormente alzato il tiro, focalizzandosi sulla necessità di "*osservare più da*

[31] Una cronistoria delle vicende è effettuata da BARONE D.M., *Criptovalute e Jihad*, nel Periodico del Ministero della Difesa, fasc. 1/2019.
[32] In *www.repubblica.it*, 15 dicembre 2017.
[33] In *www.ccn.com*, 2 maggio 2019 (consultabile qui).
[34] European Central Bank, *Virtual Currency Schemes*, Francoforte 2012, p. 6.

vicino i BitCoin e la loro diffusione, così come le implicazioni positive e negative di tale fenomeno e l'eventuale distorsione del mercato cui esso può dar luogo"[35].

Allo stesso modo, il FAFT-GAFI – le cui indicazioni costituiscono, di regola, la base concettuale per l'emanazione delle Direttive AML – aveva auspicato l'inizio di una serie di progetti a breve termine con l'obbiettivo di "*sviluppare una matrice di rischio per le criptovalute* […] *e stimolare una discussione sull'implementazione di una regolamentazione AML risk based del settore*"[36].

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 tuttavia disatteso le aspettative. Nell'ambito di una riforma complessiva della propria disciplina antiriciclaggio, infatti, essa ha omesso di assoggettare gli operatori del settore criptovalutario ai relativi obblighi (tra i quali, su tutti, la registrazione e l'adeguata verifica della clientela). Siffatta mancanza, prontamente segnalata dagli operatori legali[37], ha prontamente condotto il legislatore comunitario alla formulazione della Proposta di modifica n. 0208/2016 ed infine, dopo solo due anni dalla precedente riforma, all'adozione della Quinta Direttiva Antiriciclaggio. Il ritardo accumulato in sede europea non ha comunque impedito ad alcuni Stati membri di anticipare la regolamentazione comunitaria già in sede di adattamento alla Quarta Direttiva: su tutti, l'Italia, con il d.lgs. n. 90/2017, ha adottato degli standard estremamente elevati in materia di criptovalute, come si vedrà in dettaglio nel successivo §5.

La Direttiva n. 843/2018 (c.d. Quinta Direttiva) sottolinea fin dai *Considerando* che "*i recenti attentati terroristici hanno evidenziato l'emergere di nuove tendenze, in particolare per quanto riguarda le modalità con cui i gruppi terroristici finanziano e svolgono le proprie operazioni. Taluni servizi basati sulle moderne tecnologie stanno diventando sempre più popolari come sistemi finanziari alternativi, considerando che restano al di fuori dell'ambito di applicazione del diritto dell'Unione*[38] […]".

Con riguardo alle criptovalute, l'Unione riconosce che "*i prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute aventi corso legale* […] *e i prestatori di servizi di portafoglio digitale non sono soggetti all'obbligo dell'Unione di individuare le attività sospette. Pertanto, i gruppi terroristici possono essere in grado di trasferire denaro* […] *dissimulando i trasferimenti o beneficiando di un certo livello di anonimato su queste piattaforme. È pertanto di fondamentale importanza* […] *includere i prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute legali e i prestatori di servizi di portafoglio digitale*"[39].

Ciò premesso, per quanto d'interesse in questa sede le novità della Direttiva possono essere compendiate in tre categorie principali: la definizione di alcuni concetti

---

[35] European Central Bank, *Virtual Currency Schemes – A further analysis*, Francoforte 2012, p. 29.

[36] FAFT Report "*Virtual Currencies Key Definitions and Potential AML/CFT Risks*", in *faft-gafi.org*, giugno 2014, p. 93 (traduzione a cura dell'autore).

[37] Si veda, a titolo esemplificativo, HOLMAN D.– STETTNER B., *Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches*, in A&L LLP, ICLG TO: Anti-Money Laundering 2018, NY 2018.

[38] Considerando n. 2 alla Quinta Direttiva AML.

[39] Considerando n. 8 alla Quinta Direttiva AML.

fondamentali, quali moneta virtuale e *wallet provider*; l'ampliamento dei soggetti tenuti all'adeguata verifica della clientela; il potere della Commissione di identificare "Paesi terzi" ritenuti ad alto rischio di riciclaggio e di finanziamento del terrorismo.

4.1. Le definizioni ed i nuovi soggetti obbligati: in particolare, i wallet providers.

In base alla Direttiva, con la locuzione valuta virtuale deve intendersi "*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*".

La normativa recepisce quasi testualmente l'enunciazione proposta dalla BCE e fatta propria dall'ordinamento italiano con il d.lgs. n. 90/2017. Meritevole di attenzione è l'assenza di un riferimento al meccanismo *blockchain*: in astratto, la Quinta Direttiva mira a regolare anche (future) criptovalute fondate su diversi sistemi di garanzia, purché non emesse da un'Autorità Centrale ed accettate come mezzo di scambio dalla collettività.

Con riferimento ai prestatori di servizi di portafoglio digitale, essi sono definiti come soggetti che forniscono "*servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*". Il ruolo di siffatti intermediari è centrale nella gestione del rischio-riciclaggio: la casistica, infatti, testimonia che raramente gli utenti pongono in essere condotte illecite in proprio, bensì tendono ad affidarsi alla "professionalità" di broker specializzati. Siffatti operatori possono infatti distribuire le somme da occultare su molteplici portafogli, schermandone l'origine comune; essi dispongono altresì delle conoscenze tecniche necessarie per accedere alle piattaforme di *mixing*, le quali, come già analizzato, costituiscono nella maggior parte dei casi un ostacolo definitivo alle attività d'indagine.

In considerazione di tali fattori di rischio, la Quinta Direttiva obbliga i *wallet providers*, così come i gestori delle piattaforme di *exchange*, a presidiare il rapporto con la clientela attraverso l'acquisizione di informazioni rilevanti, aventi ad oggetto:

- i dati identificativi del cliente, sia esso una persona fisica o giuridica;
- nel caso di instaurazione di un rapporto continuativo, lo scopo e la natura degli affari. La ricezione di tali dati dovrà poi essere corredata con un opportuno "incrocio" con altri eventualmente già detenuti dal soggetto obbligato.

In ogni caso, l'adeguata verifica dovrà essere particolarmente accorta qualora vi sia il fondato sospetto di riciclaggio di denaro o di finanziamento del terrorismo. Il soggetto obbligato dovrà inoltre segnalare le operazioni dubbie all'Autorità competente nello Stato membro, a pena di sanzioni sia amministrative sia penali dotate di un alto grado di dissuasività[40]. Da ultimo, il soggetto obbligato deve garantire alle Autorità di settore ed alle UIF un rapido accesso alle informazioni raccolte: ciò comporta la capacità

[40] In considerazione della pressoché totale sovrapponibilità tra le disposizioni sanzionatorie europee e quelle di diritto interno a seguito dei d.lgs. n. 90/2017 e n. 125/2019, l'analisi delle fattispecie incriminatrici è pertanto demandata al successivo §6.

dell'intermediario di provvedere alla conservazione dei dati con modalità che garantiscano sia il rispetto della privacy dei clienti, prioritaria in base alle norme c.d. "GDPR", sia la pronta risposta agli organi investigativi nel caso di operazioni sospette.

4.2. L'individuazione dei Paesi a rischio.

L'art. 9, par. 2, della Direttiva (UE) 2015/849, così come modificato dalla Quinta Direttiva, consente alla Commissione di redigere un catalogo dei Paesi terzi il cui quadro giuridico antiriciclaggio evidenzia delle carenze strutturali. L'individuazione delle suddette giurisdizioni, che è fondata sulle indicazioni di "*organizzazioni ed enti di normazione internazionali con competenze nel campo della prevenzione del riciclaggio e del contrasto al finanziamento del terrorismo*", è effettuata tenendo conto dei seguenti criteri:

- il quadro giuridico e istituzionale del Paese terzo, relativamente alla perseguibilità delle suddette condotte criminose, alle misure di adeguata verifica (ivi compresa la conservazione dei documenti e la segnalazione delle operazioni sospette);
- l'esistenza di Autorità nazionali autonome e competenti, dotate di adeguati poteri ed in grado di interagire con le UIF degli Stati Membri;
- l'efficacia del sistema di prevenzione del Paese terzo di fronte al rischio di riciclaggio e finanziamento del terrorismo.

Le operazioni con i Paesi inseriti nella lista soffrono di una "presunzione di pericolosità". Graverà dunque sul soggetto obbligato l'onere di monitorare le transazioni da e per i suddetti Paesi, nonché di segnalare all'Autorità competente ogni fondato sospetto. La valutazione preventiva di pericolosità effettuata dalla Commissione vincola pertanto l'intermediario ad adottare il più alto standard possibile nella verifica delle transazioni poste in essere per suo tramite.

In base alla lista vigente, aggiornata al 13 febbraio 2019, le giurisdizioni a rischio sono le seguenti ventitrè: Le 23 giurisdizioni sono: Afghanistan, Samoa americane, Bahamas, Botswana, Repubblica popolare democratica di Corea, Etiopia, Ghana, Guam, Iran, Iraq, Libia, Nigeria, Pakistan, Panama, Portorico, Samoa, Arabia Saudita, Sri Lanka, Siria, Trinidad e Tobago, Tunisia, Isole Vergini americane e Yemen[41].

5. Il recepimento delle Direttiva in Italia: una panoramica.

5.1. L'ordinamento interno come frontrunner *europeo: il d.lgs. n. 90/2017.*

Il d.lgs. n. 90 del 25 marzo 2017, con il quale l'Italia ha assolto agli obblighi di adeguamento agli standard della Quarta Direttiva, ha rappresentato un nodo fondamentale nel processo di regolamentazione delle criptovalute. In esso, infatti, il

[41] Cfr. https://ec.europa.eu/commission/presscorner/detail/it/IP_19_781.

legislatore nazionale non si è limitato a recepire le norme europee, bensì ha anticipato sotto plurimi profili le disposizioni della Quinta Direttiva in materia di criptovalute.

In primo luogo, il d.lgs. n. 90/2017 fornisce una definizione di valuta virtuale, così identificando "*la rappresentazione digitale di valore, non emessa da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi e trasferita, archiviata e negoziata elettronicamente*"[42]. Si tratta di una definizione che mette in luce i tratti caratterizzanti delle criptovalute, così come delineati dal GAFI già nel corso del 2014[43]. Il Decreto precisa inoltre quali soggetti debbano essere qualificati come prestatori di servizi relativi all'utilizzo di valuta virtuale: in tale nozione ricade "*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*"[44]. In siffatta definizione rientrano dunque gli *exchanger*, ovverosia coloro che conservano e convertono valute virtuali in valute aventi corso legale.

L'attività dell'*exchanger è* individuata dal legislatore nazionale come il fulcro del *trading* di moneta virtuale. Per siffatto motivo, il d.lgs. n. 90/2017 dispone l'estensione degli obblighi di registrazione e di adeguata verifica della clientela anche a tali operatori economici, la cui attività viene sottoposta alla vigilanza delle Autorità di Settore. In altri termini, a seguito della riforma gli *exchangers* di moneta virtuale sono tenuti all'iscrizione in una sezione speciale del registro tenuto dall'Organismo degli Agenti e dei Mediatori (ai sensi dell'art. 128-*undecies* del Testo Unico Bancario), risultando così parificati ai tradizionali cambiavalute e parimenti soggetti pertanto alle disposizioni antiriciclaggio.

Il principale corollario dell'obbligo di registrazione risiede nella circostanza che all'*exchanger*, in quanto soggetto obbligato, sono estesi i doveri di adeguata verifica. In particolare, tali obblighi si declinano:

- nell'acquisizione dei dati identificativi del cliente, sia esso una persona fisica o giuridica, nel caso di operazione occasionale di importo pari (o superiore) a 15.000 euro, anche se effettuata con più disposizioni collegate;
- nel caso di instaurazione di un rapporto continuativo, nell'acquisizione dei dati anagrafici e nella richiesta di informazioni sullo scopo e la natura degli affari. I dati raccolti vanno altresì comparati con quelli di cui l'*exchanger* eventualmente già disponga, al fine di verificarne la verosimiglianza;
- in ogni caso, l'adeguata verifica dovrà essere particolarmente accorta qualora vi sia il fondato sospetto di riciclaggio di denaro o di finanziamento del terrorismo.

Inoltre, il controllo dell'*exchanger* non può limitarsi alla fase genetica del rapporto, bensì deve prolungarsi per tutta la permanenza del cliente nella sfera operativa del cambiavalute[45]. Ciò comporta non solo l'esigenza di provvedere ad un

---

[42] Art. 1, c. 2, lett qq) del d.lgs. n. 231 del 21 novembre 2007, così come modificato dall'art. 1 del d.lgs. n. 90 del 25 marzo 2017.

[43] FAFT-GAFI, *Virtual Currencies Key Definitions and Potential AML/CFT Risks*, giugno 2014, p. 4.

[44] Art 1, comma 2 lettera ff) del d.lgs. 21 novembre 2007, n. 231, come modificato dal d.lgs. 25 maggio 2017, n. 90.

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

periodico aggiornamento delle informazioni raccolte presso la clientela, bensì obbliga il cambiavalute a predisporre un adeguato sistema di conservazione dei documenti acquisiti. La conseguenza di una simile disposizione è la naturale selezione del mercato degli *exchangers*: i soggetti più attrezzati dal punto di vista organizzativo (e che, nell'ottica del decreto, offrono maggiori garanzie alla clientela) vantano un rapido adattamento alle nuove norme; di converso, gli operatori più piccoli o più predisposti a tollerare (se non addirittura a favorire) operazioni poco trasparenti, sono destinati ad essere espulsi dal mercato, poiché privi delle strutture necessarie per adeguarsi ai nuovi, stringenti, obblighi di legge.

Infine, sui cambiavalute virtuali grava altresì il dovere di segnalazione all'UIF di ogni operazione sospetta, così come di tutti i casi in cui si abbia fondato motivo di ritenere che la provenienza dei fondi possa essere illecita. L'art. 35 del d.lgs. n. 231/2007, così come riformato dal d.lgs. n. 90/2017, chiarisce 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*". All'evidenza, un simile controllo appare effettuabile solo in caso di relazione continuativa con la clientela, laddove il prolungarsi del rapporto tra piattaforma ed investitore può fornire alla prima una serie di elementi tali da far desumere un fondato sospetto di illiceità delle operazioni. Al contrario, in caso di transazione singola, la segnalazione alla UIF potrà avvenire solo in caso di evidente illiceità dell'operazione: l'effettuazione di una sola operazione, infatti, difficilmente potrà fornire all'*exchanger* elementi adeguati a fondare un legittimo sospetto.

Rinviando al successivo §6 per l'analisi dei profili sanzionatoria a carico degli *exchangers*, appare opportuno segnalare fin d'ora che il d.lgs. n. 90/2017 ha rappresentato un fondamentale passo in avanti per l'ordinamento nazionale nella regolamentazione delle criptovalute: sotto molteplici aspetti, infatti, esso non si è limitato a recepire la Quarta Direttiva, bensì ha sensibilmente anticipato gli standard normativi imposti dalla Quinta Direttiva. Invero, i successivi aggiornamenti (quantomeno con riferimento al mondo delle *cryptocurrencies*) hanno approntato integrazioni solo marginali, ora ampliando la platea dei soggetti obbligati, ora aumentando le forme di collaborazione tra le UIF a livello europeo.

5.2. Il d.lgs. n. 125/2019.

Il recente d.lgs. n. 125/2019, che ha recepito le indicazioni della Quinta Direttiva non ricomprese nel decreto del 2017, ha introdotto alcune rilevanti modifiche, delle quali si fornisce in questa sede una sintetica descrizione:

– quanto alla definizione di "*moneta virtuale*", la nuova disciplina ricomprende tra le finalità di utilizzo anche le "*finalità di investimento*"[46]. L'aggiunta di tale specificazione (che lascia sostanzialmente immutata la struttura definitoria del d.lgs. n. 90/2017) consente di includere tutti quegli strumenti criptovalutari utilizzati solo per finalità di *trading*, i quali necessitano di essere convertiti in altra moneta virtuale prima di poter essere impiegati per l'acquisto di beni e servizi o di essere tramutati in denaro avente corso legale;

– con riferimento ai soggetti obbligati, la nuova disciplina ricomprende in tale categoria anche i "*prestatori di servizi di portafoglio digitale*" (c.d. *wallet* providers), e cioè "*ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche online, servizi di salvaguardia di chiavi crittografiche private per conto dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*"[47]. L'estensione, che accoglie le istanze della dottrina di settore, mira a sottoporre alla normativa antiriciclaggio tutti i possibili operatori attraverso i quali i privati possono accedere al mercato criptovalutario: pertanto, con l'entrata in vigore del decreto l'obbligo di adeguata verifica non è limitato alle sole piattaforme di investimento (*exchangers*), bensì anche ai soggetti che, gestendo portafogli virtuali per conto terzi, svolgono il ruolo di "broker" sulle piattaforme stesse;

– ampliamento dei poteri di controllo del Nucleo Speciale di Polizia Valutaria della Guardia di Finanza. Quest'ultimo, infatti, su segnalazione della UIF, potrà acquisire informazioni sulle operazioni sospette direttamente presso i soggetti obbligati, anche laddove essi non fossero sottoposti alla sua vigilanza (ad es. gli intermediari finanziari, di competenza di Banca d'Italia). Allo stesso modo, la Direzione Nazionale Antimafia e Antiterrorismo può disporre del Nucleo di Polizia Valutaria nello svolgimento delle sue attività. La norma mira a creare una stretta connessione tra gli organismi d'indagine, accentrando i poteri d'indagine su un organismo ad elevato potenziale "tecnico", in grado di intercettare (unitamente alla UIF) i fenomeni di riciclaggio criptovalutario.

6. Il diritto penale nazionale.

6.1. Le fattispecie sanzionatorie applicabili al mondo delle criptovalute.

L'analisi delle condotte delittuose connesse all'esercizio di attività di intermediario nel settore criptovalutario presuppone la preventiva distinzione tra la violazione degli obblighi relativi all'adeguata verifica della clientela (fattispecie previste e punite dall'art. 55 del d.lgs. 231/07) e i casi di concorso dell'*exchanger* (o del *wallet provider*) nei reati di riciclaggio, autoriciclaggio, finanziamento del terrorismo e, in linea teorica, in tutte le figure di reato commesse a mezzo di criptovalute.

---

[46] Art. 1, c. 2, lett pp) del D.lgs. n. 231 del 21 novembre 2007, così come modificato dall'art. 1 del d.lgs. n. 125/2019.

[47] Art. 1, c. 2, lett. ff-*bis*) del d.lgs. n. 231/2007, così come modificato dal d.lgs. n. 125/2019.

L'art. 55 del d.lgs. 231/2007, così come da ultimo modificato con il d.lgs. 125/2019, prevede tre distinte 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 medesima 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*". La summenzionata norma si applica a condotte attive di falsificazione di dati, nonché a loro utilizzo in sede di comunicazione alle Autorità di settore. Perché si possa configurare il delitto in esame è sempre necessaria la consapevolezza, in capo al soggetto obbligato, della falsità delle informazioni utilizzate.

Ai sensi dell'art. 55, c. 2, "*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*". Rispetto al delitto di cui al primo comma, la suddetta condotta è caratterizzata dalla presenza del dolo specifico di compromissione della corretta tenuta dei dati della clientela. Tale specificazione restringe sensibilmente l'area del punibile: mentre la falsificazione di cui al c. 1 è perseguita anche a titolo di dolo generico, l'acquisizione di dati falsi (prodotti da terzi) è meritevole di sanzione solo laddove finalizzata ad una sistematica elusione degli obblighi di adeguata verifica.

Il c. 3 dell'art. 55 completa l'apparato sanzionatorio predisponendo un delitto a carico del cliente. Nello specifico, "*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*".

Infine, il soggetto obbligato che, rilevata un'operazione sospetta, ne dia notizia al cliente violando il disposto dell'art. 39, è punito "*salvo che il fatto costituisca più grave reato* […] *con l'arresto da sei mesi a un anno e con l'ammenda da 5000 euro a 30.000 euro*". La norma presidia con una previsione contravvenzionale uno dei capisaldi della normativa antiriciclaggio, ovvero il divieto per l'intermediario di comunicare al cliente la possibile indagine a suo carico. La fattispecie potrà essere integrata anche da una "fuga di notizie" meramente colposa.

Fuori dalle fattispecie incriminatrici di cui al riformato d.lgs. 231/07, la condotta dell'*exchanger*, del *wallet provider* o del prestatore di servizi criptovalutari potrebbe assumere rilevanza a titolo di concorso nei reati commessi dagli utenti della piattaforma,

tipicamente quelli *ex* artt. 648 ss. c.p.[48] La piena operatività delle norme sul concorso di persone nel reato si desume dallo stesso articolo 5 del d.lgs. 90/2017, che ribadisce espressamente l'operativita` dell'art. 648 quater c.p. (che disciplina la confisca per i reati di ricettazione, riciclaggio, impiego di denari di provenienza illecita ed autoriciclaggio), nonche´ quella dell'art. 25-*octies* D.lgs. del 231/2001 (che detta le norme per la responsabilita` amministrativa delle societa`e degli enti per le ipotesi delittuose di cui agli artt. 648, 648-*bis*, 648-*ter* e 648-*ter*.1).

Pertanto, il soggetto obbligato che abbia avuto consapevolezza, anche solo a titolo di dolo eventuale, dell'illecita provenienza dei fondi criptovalutari e abbia comunque predisposto l'operazione richiesta dal cliente, risponderà *ex* art. 110 c.p. del contributo illecito fornito. Nondimeno, la prova della consapevolezza dovrà essere fornita con particolare rigore, avuto riguardo alle concrete modalità delle transazioni illecite. 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.

*6.2. L'art. 270-*quinquies*.1 c.p.: una forte anticipazione della tutela penale.*

Progredendo nell'analisi, è inoltre utile volgere brevemente l'attenzione al reato di finanziamento di condotte con finalità di terrorismo, così come delineato dall'art. 270-*quinquies*.1 c.p.; le vicende relative a tale ipotesi di reato manifestano la volontà del legislatore di coprire quanto più possibile i comportamenti prodromici alla commissione di fatti di terrorismo, anche a costo di produrre norme con ridotto margine di applicazione.

L'art. 270-*quinquies*.1 è stata introdotto con la L. 18 luglio 2016, n.153, nella quale il legislatore ha dato esecuzione ad una serie di Accordi Internazionali, tra i quali la Convenzione del Consiglio d'Europa per la prevenzione del terrorismo e la Convenzione del Consiglio d'Europa sul riciclaggio, la ricerca, il sequestro e la confisca dei proventi di reato e sul finanziamento del terrorismo, ambedue stipulate a Varsavia il 16 maggio 2005. Con la stessa legge, l'Italia ha parimenti dato esecuzione alla Convenzione internazionale per la soppressione di atti di terrorismo nucleare (New York, 14 settembre 2005)[49].

---

[48] Cfr. STURZO L., *Bitcoin e riciclaggio 2.0*, in *Dir. pen. cont.*, fasc. 5/2018, p. 24 ss.

[49] Il frutto di questa Convenzione è il reato *ex* art. 280-*ter*: "*È punito con la reclusione non inferiore ad anni quindici chiunque, con le finalità di terrorismo di cui all'articolo 270-*sexies*: 1) procura a sé o ad altri materia radioattiva; 2) crea un ordigno nucleare o ne viene altrimenti in possesso. È punito con la reclusione non inferiore ad anni venti chiunque, con le finalità di terrorismo di cui all'articolo 270-*sexies*: 1) utilizza materia radioattiva o un ordigno nucleare; 2) utilizza o danneggia un impianto nucleare in modo tale da rilasciare o con il concreto pericolo che rilasci materia radioattiva.*

L'art. 270-*quinquies*.1 punisce con la reclusione da sette a quindici anni "*chiunque, al di fuori dei casi di cui agli articoli 270-*bis *e 270* quater *1, raccoglie, eroga o mette a disposizione beni o denaro, in qualunque modo realizzati, destinati a essere in tutto o in parte utilizzati per il compimento delle condotte con finalità di terrorismo di cui all'articolo 270-*sexies", e ciò a prescindere "*dall'effettivo utilizzo dei fondi per la commissione delle citate condotte*". Il secondo comma punisce con la reclusione da cinque a dieci anni "*chiunque deposita o custodisce i beni o il denaro indicati al primo comma*". In virtù della clausola di sussidiarietà espressa, l'art. 270-*quinquies*.1 c.p. si pone in stretta correlazione con l'art. 270-*bis* c.p., norma cardine del sistema antiterrorismo, che a seguito della modifica apportata dalla L. 15 dicembre 2001, n. 438, prevede tra le condotte incriminate anche il finanziamento di "*associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratico*".

Art. 270-*bis* c.p.	Art. 270-*quinquies*.1 c.p.
Chiunque promuove, costituisce, organizza, dirige o finanzia associazioni che si propongono il compimento di atti di violenza con finalità di terrorismo o di eversione dell'ordine democratico è punito con la reclusione da sette a quindici anni.	Chiunque, al di fuori dei casi di cui agli articoli 270-*bis* e 270-*quater*.1, raccoglie, eroga o mette a disposizione beni o denaro, in qualunque modo realizzati, destinati a essere in tutto o in parte utilizzati per il compimento delle condotte con finalità di terrorismo di cui all'articolo 270 sexies è punito con la reclusione da sette a quindici anni, indipendentemente dall'effettivo utilizzo dei fondi per la commissione delle citate condotte.

Al di là delle scelte lessicali, la sovrapponibilità delle due condotte materiali appare pressoché completa. Di conseguenza, il non semplice compito di rinvenire un'utilità applicativa alla norma sussidiaria è affidato all'interprete, il quale peraltro può contare su un numero esiguo di pronunce giurisprudenziali alle quali fare riferimento[50].

L'orientamento prevalente[51] argomenta che l'art. 270-*quinquies*.1 c.p. troverebbe spazio solo nei riguardi di quei finanziatori i quali, agendo *uti singuli*, presterebbero il loro apporto economico al terrorismo senza tuttavia prendere parte ad alcuna struttura organizzata. In altri termini, si tratterebbe di figure esterne non solo all'associazione *strictu sensu* intesa, bensì anche alla rete di contatti della stessa, tanto da non fornire alcun contributo materiale diverso dalla mera contribuzione economica. Sotto il profilo

Le pene di cui al primo e al secondo comma si applicano altresì quando la condotta ivi descritta abbia ad oggetto materiali o aggressivi chimici o batteriologici."

[50] In effetti, lo scrivente ha contezza di una sola pronuncia nella quale si è fatta applicazione dell'art. 270-*quinquies*.1: un'ordinanza del G.I.P. di Brescia del 18 aprile 2018.

[51] L. STURZO, *Bitcoin e riciclaggio 2.0*, cit.

soggettivo, è in ogni caso richiesta la consapevolezza dolosa della destinazione "terroristica" dei fondi. L'interpretazione in esame, in assenza di decisioni della Corte di Cassazione[52], è accolta dall'unica pronuncia di merito che abbia esplicitamente affrontato il confine tra le due norme: l'ordinanza del G.I.P. di Brescia del 18 aprile 2018. La vicenda sottoposta all'attenzione dell'A.G. riguardava un gruppo di cittadini mediorientali che, a vario titolo, avevano cercato di favorire l'operato dell'organizzazione "Al Nusra", gruppo armato attivo nella guerra civile siriana. Il G.I.P., prendendo le mosse dal presupposto che "*la destinazione è* […] *elemento costitutivo del reato* [art. 270-*quinquies*.1 c.p.]", specifica che "*l'intento dichiarato delle nuove fattispecie è quello di sanzionare in via autonoma comportamenti di "fiancheggiamento o sostegno del terrorismo internazionale*", pur riconoscendo che in precedenza "*la punibilità delle condotte di finanziamento al terrorismo era assicurata dal primo comma dell'art. 270 bis c.p. e dall'art. 270-quater.1 c.p. (che reprime la condotta di chi finanzia viaggi in territorio estero finalizzati al compimento delle condotte con finalità di terrorismo)*".

Le sintetiche vicende dell'art. 270-*quinquies*.1 c.p. consentono, in conclusione, di porre in luce la tendenza del legislatore a favorire il proliferare delle norme incriminatrici in settori, quali il terrorismo, in cui gli standard internazionali esigono una forte anticipazione della tutela penale. Siffatto *modus operandi* lascia tuttavia spazio a legittimi dubbi sull'opportunità di una simile tecnica legislativa, posta anche la ridottissima applicazione della fattispecie esaminata ad oltre quattro anni dalla sua entrata in vigore.

In ultima analisi, l'unico elemento di reale novità dell'art. 270-*quinquies*.1 risiede nell'inclusione (implicita) degli strumenti criptovalutari tra i metodi di finanziamento del terrorismo ("*beni o denaro, in qualunque modo realizzati*"): il che non appare, di per sé solo, giustificativo dell'introduzione del suddetto reato nell'ordinamento interno[53].

7. Conclusioni.

L'intenso sforzo di *regulation* in sede europea ha progressivamente avvicinato il mondo delle criptovalute – in origine libero da qualsiasi vincolo – a modelli legali già da tempo in uso. Ciò è avvenuto sia attraverso l'introduzione di nuove categorie concettuali (ad es. la valuta virtuale) sia mediante la predisposizione di considerevoli obblighi a carico degli intermediari criptovalutari, sottoposti alla penetrante sorveglianza delle UIF ed al controllo "interno" di utenti sempre più consapevoli dei loro diritti e doveri.

Ad ogni modo, la creazione di uno spazio comunitario sicuro e finanziariamente trasparente, perseguita attraverso il fermo contrasto ai fenomeni terroristici e di riciclaggio, pone nuove ed ambizione sfide per il futuro. In primo luogo, la comprensione dei meccanismi della *blockchain* obbliga le Autorità di settore ad un

[52] Si veda tuttavia lo studio (prettamente compilativo) a questo *link*, p. 16 ss.

[53] Al medesimo risultato, infatti, ben poteva pervenirsi in via interpretativa facendo applicazione dell'art. 270-*bis* c. 1 c.p., o, sotto un diverso profilo, sulla scia della crescente equiparazione tra valuta legale e valuta virtuale.

regolare aggiornamento, al fine di intercettare gli strumenti di recente emanazione e le criptovalute diffuse nel *deep* e nel *dark web*. In tale ottica, il BitCoin e le AltCoin più note rappresentano solo la "punta dell'*iceberg*" di un fenomeno in continuo sviluppo.

In secondo luogo, è altresì necessario migliorare i meccanismi di coordinamento tra le Autorità nazionali, in modo tale da evitare la creazione di "zone grigie" all'interno dell'area di libera circolazione. Allo stesso modo, la promozione di accordi con gli Stati esteri e il monitoraggio dei Paesi a rischio riveste carattere fondamentale sia per prevenire sia per perseguire le concrete manifestazioni criminose.

Infine, la regolamentazione degli istituti di nuova diffusione deve procedere, per quanto possibile, in maniera armonica, cogliendo le connessioni tra le varie sfaccettature del *cybercrime.* In tal senso, l'identificazione della titolarità effettiva, recentemente prevista anche per i *trust* e gli istituti giuridici ad essa affini, coglie nel segno, poiché consente, se correttamente attuata, di ricondurre l'operazione economica ad un destinatario anagraficamente determinato, a prescindere dalla natura e dalla complessità delle manovre finanziarie di "schermatura" della provenienza dei beni.