22.07.2020

Alessandra Rea

Criptovalute: a che punto siamo?

Funzionamento, trasparenza e rischi di riciclaggio

#danno #economia #Europa #normativa #processo_penale #rischio #tecnologia #società

Fascicolo 7-8/2020

Abstract. *Le recenti modifiche legislative in tema di* cyberlaundering *e criptovalute: un'introduzione all'interlocuzione tra gli operatori del mercato digitale.*

SOMMARIO: 1. Premessa e chiarimenti terminologici. – 2. Prevenzione e repressione del *cyberlaundering*: dalla IV Direttiva Europea antiriciclaggio al D.lgs. 231/2007. – 3.1. Criptovalute, *blockchain* e anonimato. – 3.2. Il ruolo del *wallet provider* nella circolazione di valuta elettronica: la V Direttiva Europea antiriciclaggio e il D.lgs. 125/2019. – 4. Ostacoli all'emersione dei capitali illeciti. – 5. Conclusioni e prospettive *de lege ferenda*.

***

1. Premessa e chiarimenti terminologici.

Al fine di garantire una migliore intellegibilità dell'analisi che segue, si rende opportuna una sintetica descrizione del sistema di scambio di criptovaluta.

La criptovaluta (*rectius*, "valuta virtuale"), è «la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente»[1].

Dalla definizione normativa si deducono alcuni elementi di carattere generale sulle modalità di circolazione delle *cryptocurrencies*:

1. l'inesistenza di un "sistema di controllo centralizzato", posto che la "moneta" non è «emessa né garantita da una banca centrale o da un'autorità pubblica»;
2. il meccanismo di archiviazione e negoziazione si sviluppa esclusivamente su piattaforma elettronica.

Lo scambio di valuta virtuale avverrà per il tramite di piattaforme di *trading*, a cui l'utente (*user*) potrà accedere attraverso una "chiave pubblica" e una "chiave privata" (*rectius*, uno *username* ed una *password*), custodite dal c.d. *wallet provider*[2].

Per volontà del controverso ideatore del sistema di scambio di criptovalute, le transazioni saranno presidiate da una forma di c.d. pseudo-anonimato: l'identità dell'utente sarà "garantita" da un sistema di crittografia, quindi la sua identità sarà ignota ad altri *users*.

> Per volontà del controverso ideatore del sistema di scambio di criptovalute, le transazioni saranno presidiate da una forma di c.d. pseudo-anonimato: l'identità dell'utente sarà "garantita" da un sistema di crittografia, quindi la sua identità sarà ignota ad altri users

Le esigenze di tracciabilità di flussi saranno assicurate (pur con le opportune riserve, che si esporranno *infra*) da un sistema di controllo *peer-to-peer*.

In altre parole, non esistendo un sistema di controllo centralizzato (come, ad esempio, quello cui sono preposti gli Istituti di credito), la "verifica" degli scambi sarà affidata ad altri utenti del *network*, i c.d. *miners* (invero, *users* con approfondita conoscenza della *blockchain*)[3], in una rete di controllo "diffusa".

2. Prevenzione e repressione del cyberlaundering: dalla IV Direttiva Europea antiriciclaggio al D.lgs. 231/2007.

Nonostante «il crollo più estremo e repentino dal 2013»[4] del 12-13 marzo 2020, ad oggi il valore di capitalizzazione di *Bitcoin*, *major* tra le criptovalute, si aggira a quasi 90 miliardi di dollari (nei primi giorni di marzo era di 137,8 miliardi).

Secondo l'Agenda Digitale dell'Unione Europea, sebbene poco più dell'1% delle transazioni in criptovaluta avvenga per scopi illeciti[5], tra il 2018 e il 2019 si è registrato un aumento esponenziale delle transazioni illegali in valuta virtuale.

> Nonostante «il crollo più estremo e repentino dal 2013» del 12-13 marzo 2020, ad oggi il valore di capitalizzazione di Bitcoin, major tra le criptovalute, si aggira a quasi 90 miliardi di dollari

La "cultura" del *trading* di "*Bitcoin*" è in espansione anche in Italia, dove ormai un terzo della popolazione esaminata da *Statista*, nel 2019, ha manifestato una – seppure parziale – conoscenza delle criptovalute (in particolare di *Bitcoin*), associandole al fenomeno della *blockchain*. Tuttavia, soltanto il 10% del campione analizzato ha "sentito parlare" di *cyber security* e sistemi di crittografia[6].

La sostanziale noncuranza del fenomeno potrebbe essere dovuta al ritardo con cui si è mossa l'Italia nella lotta ai *cybercrimes*, dapprima, e poi ai *crypto crimes*[7]. Dopo risposte legislative occasionali, risale al 1993 il primo adeguamento organico del sistema all'evoluzione della criminalità informatica, ed è solo con il D.lgs. n. 90/2017, attuativo della IV Direttiva Europea in tema di antiriciclaggio, che il Legislatore ha introdotto nel D.lgs. n. 231/2007 una vera e propria definizione di "valuta virtuale", oggi intesta come una «rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente»[8].

> La "cultura" del trading di "Bitcoin" è in espansione anche in Italia, dove ormai un terzo della popolazione esaminata da Statista, nel 2019, ha manifestato una – seppure parziale – conoscenza delle criptovalute (in particolare di Bitcoin), associandole al fenomeno della blockchain

D'altro canto, già alla IV Direttiva Antiriciclaggio (2015) il Legislatore *lento pede pervenit*, recependola solo due anni dopo la sua emanazione (2017). E dalla V Direttiva finalmente mutua lo scopo di prevenire e contrastare il riciclaggio virtuale attraverso lo "studio" degli attori e delle modalità operative delle transazioni in *cryptocurrencies*, condividendo l'assunto secondo il quale proprio l'anonimato del sistema *peer-to-peer* «ne consente il potenziale uso improprio per scopi criminali». Tuttavia, «l'inclusione dei prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra valute virtuali e valute reali e dei prestatori di servizi di portafoglio digitale non risolve completamente il problema dell'anonimato delle operazioni in valuta virtuale: infatti, poiché gli utenti possono effettuare operazioni anche senza ricorrere a tali prestatori, gran parte dell'ambiente delle valute virtuali rimarrà caratterizzato dall'anonimato»[9].

Non sorprende come l'attenzione alle *cryptocurrencies* sia stata attualizzata attraverso la normativa antiriciclaggio, essendo il tema del *cyberlaundering* comune denominatore tra tutte le forme di *crypto crimes*, atteso che ogni profitto conseguito necessiterà di essere "ripulito" già solo per essere convertito in moneta reale.

> Non sorprende come l'attenzione alle cryptocurrencies sia stata attualizzata attraverso la normativa antiriciclaggio, essendo il tema del cyberlaundering comune denominatore tra tutte le forme di crypto crimes, atteso che ogni profitto conseguito necessiterà di essere "ripulito" già solo per essere convertito in moneta reale

3.1. Criptovalute, blockchain e anonimato.

Le forme di "pseudo-anonimato" che presidiano le transazioni in valuta virtuale rendono la *blockchain* ambiente fertile per il parassitismo criminale, specie in tema di riciclaggio: «il *cyberlaundering* si realizza per lo più bypassando l'intervento di intermediari bancari e finanziari, grazie ai moderni sistemi digitalizzati di pagamento e di trasferimento fondi *online*, carte elettroniche, catene *peer-to-peer*, *blockchain*, con cui circolano e si accreditano fra il pubblico le "criptovalute", soprattutto nel *dark web*»[10].

Bitcoin, la più diffusa delle *cryptocurrencies* tra le *species* di *altcoins*, «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»[11]. Neppure è moneta elettronica, atteso che «nello schema tradizionale la moneta elettronica non è altro che una disponibilità di potere d'acquisto registrata su un conto corrente acceso presso una Banca»[12], mentre la peculiarità delle criptovalute consiste in un sistema che sembra aver superato il *network* di *check-up* centralizzato: le transazioni saranno verificate attraverso una *blockchain*, una "catena di controllo" formata da diversi *miners* che operano mediante un sistema *peer-to-peer*.

Gli *users* (utenti), «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»[13], sono garantiti da un anonimato "controllato", detto *pseudo-anonimato*: all'interno del *network*, saranno titolari di una "chiave pubblica" e di una "chiave privata", attraverso le quali potranno prendere visione in qualsiasi momento delle transazioni effettuate tramite valuta virtuale.

Il c.d. pseudo-anonimato del sistema di scambio di *cryptocurrencies* consiste proprio nella possibilità di avere una piena visione di tutte le attività compiute, il cui *paper trail* sarà facilmente dissimulabile tramite la creazione di più *account* riconducibili allo stesso utente.

Al medesimo scopo sono orientate diverse piattaforme che si stanno diffondendo tra i *trader*, i c.d. *mixers*, ossia *software* offerti agli utenti interessati, la cui finalità è quella di aumentare la *privacy*, dirottando la transazione su un *server* diverso da quello dell'agente.

> Il c.d. pseudo-anonimato del sistema di scambio di cryptocurrencies consiste [...] nella possibilità di avere una piena visione di tutte le attività compiute, il cui paper trail sarà facilmente dissimulabile tramite la creazione di più account riconducibili allo stesso utente

Le piattaforme di *trading* diventano mercato nell'accezione classica del termine, dove l'*exchanger*, tramite piattaforme gestite dal *wallet provider*, cura l'incontro tra domanda e offerta, quale intermediario nel deposito o conversione di *cryptocurrencies*.

3.2. Il ruolo dei wallet provider nella circolazione di valuta elettronica: la V Direttiva Europea antiriciclaggio e il D.lgs. 125/2019.

Con il D.lgs. n. 125 del 04 ottobre 2019, entrato in vigore il successivo 10 novembre, l'Italia ha dato attuazione alla V Direttiva Europea in tema di antiriciclaggio (n. 2018/843 UE): il legislatore, compulsato dall'Unione Europea, continua a seguire il percorso di definizione normativa degli operatori del mercato digitale già tracciato con il D.lgs. n. 90/2017, intensificando l'azione di prevenzione al riciclaggio e mostrandosi particolarmente sensibile alle implicazioni del regime di 'pseudo-anonimato' che caratterizza la *blockchain*.

D'altronde, la Direttiva (UE) 2018/843 fa palese il timore per attacchi terroristici finanziati per il tramite di «servizi basati sulle moderne tecnologie» che stanno diventando «sempre più popolari come sistemi finanziari alternativi, considerando che restano al di fuori dell'ambito di applicazione del diritto dell'Unione o che beneficiano di deroghe all'applicazione di obblighi giuridici che potrebbero essere non più giustificate». Lo scopo prefisso è quello di «adottare ulteriori misure volte a garantire la maggiore trasparenza delle operazioni finanziarie» atte a «migliorare l'attuale quadro di prevenzione e di contrastare più efficacemente il finanziamento del terrorismo»[14], da realizzare anche attraverso un accrescimento della «trasparenza generale del contesto economico e finanziario

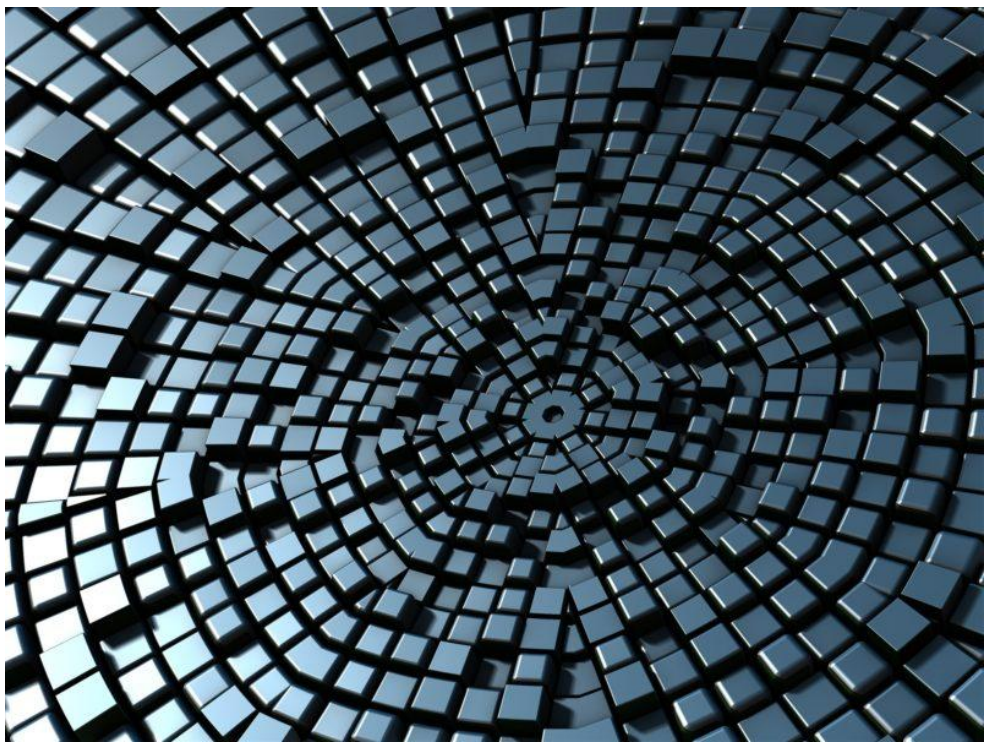
dell'Unione», posto che «la prevenzione del riciclaggio di denaro e del finanziamento del terrorismo può essere efficace solo se l'ambiente circostante è ostile ai criminali che cercano di proteggere le loro attività finanziarie attraverso strutture non trasparenti»[15].

> La Direttiva (UE) 2018/843 fa palese il timore per attacchi terroristici finanziati per il tramite di «servizi basati sulle moderne tecnologie» che stanno diventando «sempre più popolari come sistemi finanziari alternativi [...]»

In altre parole, il traguardo posto dalla V Direttiva Antiriciclaggio è quello di pervenire alla trasparenza dei flussi, da sfruttare quale deterrente alla sovvenzione delle attività terroristiche.

In questa ricostruzione, «le autorità competenti dovrebbero essere in grado di monitorare, attraverso i soggetti obbligati, l'uso delle valute virtuali»[16], assodato che «l'anonimato delle valute virtuali ne consente il potenziale uso improprio per scopi criminali»[17].

Tra le varie novità, quindi, l'introduzione tra i destinatari degli obblighi antiriciclaggio dei c.d. *custodian wallet providers*, «prestatori di servizio di portafoglio digitale», *alias* persone fisiche o giuridiche che forniscono «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 le valute virtuali»[18]. Brevemente, il *wallet provider* è il "custode" delle chiavi "pubblica" e "privata" che consentono all'utente di accedere al *network* per verificare le movimentazioni effettuate ed eseguire nuove transazioni in criptovalute.



Credits to Pixabay.com

4. Ostacoli all'emersione dei capitali illeciti.

Come detto, l'introduzione dei vari operatori dell'economia digitale nel novero dei sottoposti agli obblighi antiriciclaggio è soltanto tappa intermedia del fine ulteriore della salvaguardia dal rischio di finanziamento al terrorismo, nonostante l'accostamento riciclaggio-terrorismo sia in parte antinomico: se con le condotte di *laundering* vi sarà un *input* di denaro sporco e un *outpout* di denaro "pulito", operazione inversa avverrà in caso di finanziamento di attività illecite[19].

> L'introduzione dei vari operatori dell'economia digitale nel novero dei sottoposti agli obblighi antiriciclaggio è soltanto tappa intermedia del fine ulteriore della salvaguardia dal rischio di finanziamento al terrorismo

Tuttavia, se è vero che *pecunia non olet*, la ricostruzione del *paper trail* delle transazioni è utile ad identificare provenienza e destinazione della "liquidità": *a bad penny always turns up*, o almeno questo è l'obiettivo.

Vi saranno, però, due ostacoli per il raggiungimento dello scopo.

Da un lato, il profilo normativo dovrà scontrarsi con la realtà fenomenologica: nonostante i presìdi adottati, la verifica dell'utente che ha posto in essere la transazione sarà circostanza improbabile (in alcuni casi impossibile), posto il necessario "scollamento" tra identità reale e identità digitale.

> Il profilo normativo dovrà scontrarsi con la realtà fenomenologica: nonostante i presìdi adottati, la verifica dell'utente che ha posto in essere la transazione sarà circostanza improbabile (in alcuni casi impossibile), posto il necessario "scollamento" tra identità reale e identità digitale

Invero, l'utilizzatore della piattaforma vi accederà con uno *username* e una *password*, "custoditi" dal *wallet provider*, ma non necessariamente le informazioni che fornirà al prestatore di servizi di portafoglio digitale potranno corrispondere a verità, né quest'ultimo avrà a disposizione strumenti idonei per individuare chi si cela dietro l'*avatar*.

Unico "strumento" per verificare la provenienza dei dati forniti è il tracciamento dell'*Internet Protocol address*, meglio conosciuto come "indirizzo IP", una «sequenza numerica assegnata a *computer* collegati a *Internet* al fine di consentire la comunicazione tra i medesimi attraverso tale rete»[20].

Ma anche il "tracciamento" dell'IP non sarà operazione di per sé sufficiente ad individuare la persona fisica che si cela dietro l'identità digitale, posta l'esistenza di strumenti (quali, ad esempio, i *bouncer*) che inibiscono la "localizzazione" della connessione.

Dall'altro lato, anche il dato oggettivo, relativo al *quantum* del trasferimento effettuato, potrà essere facilmente aggirato utilizzando un c.d. "*Bilateral Payment Channel*".

È il caso di *Lightning Network*, una piattaforma che consente più trasferimenti tra due parti all'interno dello stesso *smart contract*. Può considerarsi l'esempio di Tizio e Caio che «vogliono iniziare ad interagire economicamente costantemente l'uno con l'altro»[21], come in un classico rapporto di lavoro. Grazie a *Lightning Network*, potranno aprire un canale bilaterale di pagamento (*Bilateral Paymant Channel*) che consentirà loro di trasferire *Bitcoin off-chain*. Quando sarà terminato il flusso di transazioni, potranno "chiudere" la storia delle transazioni, che andrà a formare un "blocco" da innestare sulla *blockchain*.

> Dall'altro lato, anche il dato oggettivo, relativo al quantum del trasferimento effettuato, potrà essere facilmente aggirato

Quello che gli altri utenti potranno "vedere" non sarà l'elenco delle singole transazioni (che non verranno registrate), ma la somma totale del valore delle operazioni.

Effetti: riduzione delle commissioni e velocizzazione delle transazioni, ma «le stesse sono realmente anonime, atteso che verranno registrate sulla *blockchain* solo le transazioni iniziali e quelle finali, ma non quelle intermedie»[22].

In sostanza, il "controllo" non solo sarà differito ad un momento successivo rispetto al versamento delle "liquidità" nelle mani del destinatario, ma sarà eseguito su una cifra differente rispetto a quella oggetto delle singole transazioni.

Non è mancato chi ha considerato *Lightning Network* un espediente virtuoso per la lotta al riciclaggio: la somma delle transazioni potrà "saltare all'occhio" più facilmente rispetto a singole operazioni di scambio, magari *nummo uno*[23].

I più, tuttavia, concordano sul probabile utilizzo di *Lightning Network* quale mezzo per attività di riciclaggio di denaro, anche utilizzando il popolare metodo "*playing-poker-badly*": potrebbe darsi il caso di Tizio, Caio e Sempronio che colludono per fingere che un pagamento legittimo (tra Tizio e Caio, parti apparenti della transazione) sia stato effettuato e perso a causa di un nodo intermedio "sconosciuto" (Sempronio), innestatosi nello *smart contract* durante il trasferimento. In questo caso, l'intenzione è destinare fondi a Sempronio, ma le parti creeranno il falso pretesto di una transazione apparentemente "lecita" (anche per consentire al mittente di ripetere i fondi che sono stati versati ma non ricevuti dal destinatario)[24].

5. Conclusioni e prospettive de lege ferenda.

Gli operatori del *trading* in criptovaluta, dopo le modifiche introdotte dal D.lgs. n. 125/2019, potrebbero rispondere di riciclaggio nel caso in cui, prestando la propria attività, contribuiscano dolosamente a mutare la natura del provento del delitto presupposto, pur sospettandone la provenienza illecita[25].

Si rammenta che gli obblighi di controllo possono essere differenziati in semplificati (art. 23 D.lgs. n. 231/2007) e rafforzati (art. 25 del medesimo Decreto) di adeguata verifica[26].

- in caso di «basso rischio di riciclaggio o di finanziamento del terrorismo» gli obblighi di verifica saranno semplificati, in ragione della minore estensione e frequenza degli adempimenti previsti dall'art. 18 del D.lgs. n. 231/2007;
- ai sensi dell'art. 25, «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».

> Gli operatori del trading in criptovaluta, dopo le modifiche introdotte dal D.lgs. n. 125/2019, potrebbero rispondere di riciclaggio nel caso in cui, prestando la propria attività, contribuiscano dolosamente a mutare la natura del provento del delitto presupposto, pur sospettandone la provenienza illecita

L'attuale diffusione delle criptovalute, come evidenziato dall'Unione Europea, impone l'attuazione di obblighi di controllo rafforzato, ma al banco di prova della prassi la norma rischia di configurare una forma di responsabilità oggettiva in capo alle figure di nuovo conio.

Sebbene diversa sia la "posizione" dei nuovi attori dell'economia digitale rispetto agli operatori del mercato finanziario nella loro accezione classica, e nonostante il *network* di controllo *peer-to-peer*, pur creando un sistema di controllo "diffuso", sia comunque limitato dalle forme di pseudo-anonimato che presidiano le transazioni in criptovaluta, appare ingiustificato estendere i medesimi obblighi antiriciclaggio riservati agli intermediari finanziari, posto che gli operatori del mercato digitale incontreranno plurimi ostacoli per l'individuazione del rischio (primo fra tutti: si solleva il dubbio sulla possibilità di effettuare il *profiling* di un utente la cui identità reale potrebbe essere facilmente celata).

Più in generale, il controllo dei *supervisors* è ben complesso nella realtà digitale, posto che, per fare un esempio, la velocità di *Bitcoin* è di 7 transazioni al secondo.

Oltre al fattore tempo, si pone anche il limite del sostanziale anonimato della parte della transazione (coperta dallo "schermo" di uno *username*), nonché «la presenza di un doppio canale di scambio che può prescindere dalla presenza di un intermediario finanziario»[27].

> L'attuale diffusione delle criptovalute, come evidenziato dall'Unione Europea, impone l'attuazione di obblighi di controllo rafforzato, ma al banco di prova della prassi la norma rischia di configurare una forma di responsabilità oggettiva in capo alle figure di nuovo conio

Ciò posto, è impensabile, ad esempio, equiparare la posizione di un cambiavalute a quella dell'*exchanger*, stante l'enorme divario di quantità e portata delle operazioni verificate.

In calce alla questione si pone altresì la diffusione di "nuovi" protocolli, paralleli alla *blockchain*, di perfezionamento dei trasferimenti in valuta virtuale. Si fa riferimento al *Lightning Network*, che consente il compimento di più transazioni bilaterali all'interno dello stesso "blocco" della *blockchain*, postulando un controllo solo successivo, da parte degli *users*, sulla somma totale dei trasferimenti intervenuti.

Le vicende che interessano il progresso tecnologico pongono nuovi quesiti al Legislatore, per il quale la modifica delle *policies* del mercato digitale può rappresentare un ostacolo e una difficile parametrazione del rapporto tra prevenzione e repressione.

I rimedi da adottare dovrebbero basarsi su una responsabilizzazione dell'utente, adattando i moderni sistemi digitali alla necessaria trasparenza che deve caratterizzare qualsiasi tipo di trasferimento di valuta.

Le vicende che interessano il progresso tecnologico pongono nuovi quesiti al Legislatore, per il quale la modifica delle policies del mercato digitale può rappresentare un ostacolo e una difficile parametrazione del rapporto tra prevenzione e repressione

Una soluzione potrebbe essere l'alterazione dell'attuale sistema di pseudo-anonimato. Gli utenti potrebbero essere "coperti" dal velo dell'anonimato, ma non all'atto dell'iscrizione: l'attribuzione di uno *username* dovrebbe essere subordinata alla verifica della reale identità del fruitore del servizio informatico, anche implementando l'attuale Sistema Pubblico di Identità Digitale (SPID).

_____

[1] Art. 1, comma 2, *lett. qq*), D.lgs. n. 231/2007.

[2] Come meglio si vedrà *infra*, il *wallet provider* («prestatore di servizio di portafoglio digitale») è colui 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 le valute virtuali» (art. 1, comma 2, lett. ff–*bis*), D.lgs. n. 231/2007).

[3] Vale a dire, «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» (M. Amato, L. Fantacci, *Per un pugno di* Bitcoin, Università Bocconi Editore, 2016, p. 16).

[4] E. Spagnuolo, *Il crollo del* bitcoin *è colpa solo del coronavirus?,* in *Wired*, 17 marzo 2020.

[5] M. Prisco, *Criptovalute: attività illecite in crescita, ma l'Italia è in prima linea nel contrasto*, in *agenda digitale,* 25 febbraio 2020.

[6] Statista Research Department, *Share of individuals who have heard about blockchain in Italy 2019, by context*, 5 febbraio 2020.

[7] G. Neri, *Criminologia e reati informatici. Profili di diritto penale dell'economia*, Jovene editore, 2014, p. 29.

[8] Art. 1, comma 2, *lett. qq*), D.lgs. n. 231/2007.

[9] Considerando n. 9 alla V Direttiva Antiriciclaggio (Direttiva UE 2018/843).

[10] L. Picotti, *Profili penali del* cyberlaudering*: le nuove tecniche di riciclaggio*, in *Riv. Trim. Dir. Pen. Econ.*, n. 3-4/2018, p. 615.

[11] L. Fantacci, M. Amato, *Per un pugno*, cit., p. 3.

[12] G.P. Accinni, *Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017)*, in *Archivio penale*, n. 1/2018, p. 2.

[13] *Idem*, p. 4.

[14] Considerando n. 2 alla V Direttiva Antiriciclaggio (Direttiva UE 2018/843).

[15] *Idem,* Considerando n. 4.

[16] *Idem,* Considerando n. 8.

[17] *Idem,* Considerando n. 9.

[18] Art. 1, comma 2, lett. ff–*bis*), D.lgs. n. 231/2007.

[19] A. R. Castaldo, *Money laundering and self-laundering: Italian legislation and leading cases*, intervento tenuto in *The Fight against Money Laundering at International, European and National Level*, *Web Lecture* rientrante tra le Attività del *Modulo Jean Monnet "EU-Western Balkans Cooperation on Justice and Home Affairs" (EUWEB)*, Università degli Studi di Salerno, 15 maggio 20.

[20] Corte di Giustizia dell'Unione Europea, *Breyer* vs. *Germania*, sentenza del 19 ottobre 2016 (C-582/14).

[21] J. Sensana, *Cos'è e come funziona* lightning network, 16 aprile 2018.

[22] G.J. Sicignano, Bitcoin *e riciclaggio*, Giappichelli, 2019, p. 56.

[23] M. Lefebvre , Y. Ibrahim, *The Lightning Network Deconstructed and Evaluated*, 8 gennaio 2020.

[24] G. Peterson, S. Shenoi, *Advances in Digital Forensic XIII, Revised Selected Papers of the 13th IFIP WG 11.9 International Conference (Orlando, FL, USA, January 30 – February 1, 2017)*, Springer, 2017, p. 144.

[25] L. Sturzo, Bitcoin *e riciclaggio 2.0*, in *Diritto penale contemporaneo*, n. 5/2018, pp. 27 ss.

[26] A.R. Castaldo, *Riciclaggio*, in D. Pulitanò (*a cura di*), *Diritto penale parte speciale, vol. II: tutela penale del patrimonio*, Giappichelli, 2013, p. 224.

[27] D. Marino, *Criptovalute e riciclaggio, ecco l'illegalità che affligge il cuore dei* bitcoin *(e affini)*, 29 gennaio 2019.